



1.0 TREND MICRO™ Deep Discovery™ Director Administrator's Guide

Breakthrough Protection Against APTs and Targeted Attacks



Endpoint Security



Network Security



Protected Cloud



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

<http://docs.trendmicro.com/en-us/enterprise/deep-discovery-director.aspx>

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

Copyright © 2016. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM17452/160713

Release Date: December 2016

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Chapter 1: Preface

Documentation	1-2
Document Conventions	1-2
About Trend Micro	1-3

Chapter 2: Deep Discovery Director

Chapter 3: Deployment and Installation

System Requirements	3-2
Deployment Types	3-3
Installing Deep Discovery Director	3-5
Configuring Network Addresses on the Preconfiguration Console	3-6
Logging on to the Management Console	3-7

Chapter 4: Directory

Directory Tasks	4-2
Other Directory Tasks	4-3

Chapter 5: Appliance Updates

Plans	5-2
Plan Tasks	5-3
Appliance Statuses	5-4
Other Plan Tasks	5-5
Repository	5-7
Uploading Files	5-7
Connection Settings	5-8
Registering to the Deep Discovery Director Server	5-8

Connecting to the Central Repository Server	5-8
Managing Connections to Local Repository Servers	5-9

Chapter 6: Administration

Updates	6-2
Installing a Hotfix / Patch	6-2
Rolling Back a Hotfix / Patch	6-3
Microsoft Active Directory Integration	6-4
Configuring Microsoft Active Directory Integration	6-4
System Settings	6-5
Network	6-6
Proxy	6-7
Time	6-8
Certificate	6-9
Session Timeout	6-10
Accounts	6-10
Adding a Local User Account	6-11
Adding an Active Directory User Account	6-12
Other Accounts Tasks	6-13
System Logs	6-14
Power Off / Restart	6-14

Index

Index	IN-1
-------------	------

Chapter 1

Preface

Documentation

The documentation set for Deep Discovery Director includes the following:

TABLE 1-1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Director, and explanations on Deep Discovery Director concepts and features.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	Web-based documentation that is accessible from the Deep Discovery Director management console. The Online Help contains explanations of Deep Discovery Director components and features, as well as procedures needed to configure Deep Discovery Director.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com





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

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

Document Conventions

The documentation uses the following conventions:

TABLE 1-2. Document Conventions

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

About Trend Micro

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

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

<http://www.trendmicro.com>

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

Chapter 2

Deep Discovery Director


Trend Micro Deep Discovery Director 1.0 is an on-premises update management solution that enables centralized deployment of product updates and upgrades to Deep Discovery products. To accommodate different organizational and infrastructural requirements, Deep Discovery Director provides flexible deployment options such as distributed mode and consolidated mode. Deep Discovery Director also supports out-of-the-box integration with Deep Discovery Analyzer, Deep Discovery Email Inspector, and Deep Discovery Inspector.

Chapter 3

Deployment and Installation

System Requirements

TABLE 3-1. System Requirements

REQUIREMENT	MINIMUM SPECIFICATIONS
Hardware	<ul style="list-style-type: none"> • CPU: 1.8GHz (at least 2 cores) • Memory: <ul style="list-style-type: none"> • Distributed mode: 24GB • Consolidated mode: 8GB • Network interface card: 1 with E1000 or VMXNET 3 adapter <hr/> <div>  Important <ul style="list-style-type: none"> • Deep Discovery Director does not support the VMXNET 2 (Enhanced) adapter type. • For port binding, specify the same adapter type to use for all network interface cards. </div> <hr/> <ul style="list-style-type: none"> • SCSI Controller: LSI Logic Parallel • Hard disk: <ul style="list-style-type: none"> • Distributed mode: <ul style="list-style-type: none"> • Management server: 150GB (thin provisioned) • Central Repository server: 400GB (thin provisioned) • Local Repository server: 400GB (thin provisioned) • Consolidated mode: 400GB (thin provisioned)
Software	<ul style="list-style-type: none"> • Hypervisor: VMware vSphere ESXi 5.5/6.0 • Guest operating system: CentOS Linux 6/7 (64-bit) or Red Hat Enterprise Linux 7 (64-bit)
Ports	<ul style="list-style-type: none"> • TCP 443 (Deep Discovery Director Server connection) • UDP 123 (default NTP server connection)

REQUIREMENT	MINIMUM SPECIFICATIONS
Certificate	<ul style="list-style-type: none"> • Self-signed • PEM format • Certificate and private key in the same file • No certificate chain <p>Encryption methods:</p> <ul style="list-style-type: none"> • Private key: RSA algorithm only • Certificate: Digest size of 256 (SHA-256) or higher <p>Generation command example (CentOS):</p> <pre># 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</pre>

Deployment Types

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

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

TABLE 3-2. Components

SERVER	ROLE
Management server	<ul style="list-style-type: none"> • Hosts the main management console that you can use to: <ul style="list-style-type: none"> • Create plans • View appliance, plan, and repository information • Manage user accounts • Configure system and update settings • Displays the list of update files available on the Central Repository server • Receives registration information and status reports from appliances • Sends plan information to appliances
Central Repository	<ul style="list-style-type: none"> • Enables you to upload packages and configure system settings through a limited version of the management console • Sends a list of available update files to the Deep Discovery Director server • Sends update files to Local Repository servers
Local Repository	<ul style="list-style-type: none"> • Enables you to configure system settings through a limited version of the management console • Downloads update files from the Central Repository server • Sends update files to appliances

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

Installing Deep Discovery Director

Procedure

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



Important

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

-
- SCSI Controller: LSI Logic Parallel
 - Hard disk: 400GB (thin provisioned)
 2. Open the virtual machine console, and then power on the virtual machine.
 3. Connect the CD/DVD device of the virtual machine to the Deep Discovery Director ISO image file, and then boot the virtual machine from the CD/DVD drive.

The Deep Discovery Director Installation screen appears.

4. Select **Install software**.

The Deep Discovery Director Components screen appears.

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

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



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 **Repartition Disks** confirmation message appears.

9. Click **Continue**.

The installation starts.

Configuring Network Addresses on the Preconfiguration Console

Procedure

1. Open the Deep Discovery Director virtual machine console.
2. Log on to the preconfiguration console using the following default credentials:
 - User name: admin

- Password: admin

The **Main Menu** screen appears.

3. Select **Configure network settings** and then press **ENTER**.

The **Configure Network Settings** screen appears.

4. Configure the following required settings:

- IPv4 address
- Subnet mask
- IPv4 gateway

**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 6-6](#).

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

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

Logging on to the Management Console

Procedure

1. Open a browser window and connect to the server address provided on the pre-configuration console.

The management console logon screen appears.

2. Type the following default credentials:

- User name: admin

- Password: admin

3. Click **Log on**.

The **Directory** screen appears.

Chapter 4

Directory

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

- Left pane: Appliance tree with groups (represented by folders) and appliances (identified by display names, initially identical to their host names)
- 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 from a designated repository server
- **Unmanaged:** Appliances placed in this group cannot receive plan information and updates.


Appliances can register to Deep Discovery Director on their respective management consoles. Newly registered appliances first appear in the Unmanaged group but can be moved to the Managed group at any time.


Directory Tasks

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

The following table describes the three object types and the available information for each object.

TABLE 4-1. Directory Object Types

OBJECT	DISPLAYED INFORMATION
Appliances	<ul style="list-style-type: none"> • Plans: 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 updates from • Updates: Build number and installation date of all installed updates <hr/> <div>  Note For Deep Discovery Analyzer clusters, Deep Discovery Director also displays the following: <ul style="list-style-type: none"> • 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) </div>


OBJECT	DISPLAYED INFORMATION
Local Repository servers	<ul style="list-style-type: none"> • Plans: Plans that were or will be deployed to the server • Server: Identifiers such as IP address, host name and display name, and other information such as the address of the Central Repository server • Updates: Build number and installation date of all installed updates • Repository: Update files that it hosts and IP address of the Central Repository server • Deep Discovery appliances: Appliances that are configured to download updates from it <hr/> <div>  Note You can assign a maximum of three repository servers per appliance. </div> <hr/>
Groups	Overview of appliances and plans associated with that group, including statuses and connection information.


Other Directory Tasks

You can also perform the following actions:

TABLE 4-2. Other Directory Tasks

ACTION	DESCRIPTION
Add groups	<p>Add groups to better organize appliances, such as by location or business unit.</p> <p>To add a group:</p> <ol style="list-style-type: none"> 1. Click the menu icon beside the group name and then select Add. 2. In the text box, type a name with a maximum of 256 characters.

ACTION	DESCRIPTION
Edit group or appliance names	<p>To edit a group or appliance name:</p> <ol style="list-style-type: none"> 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.
Move groups or appliances	<p>To move a group or an appliance to a different group:</p> <ol style="list-style-type: none"> 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. <p>This function is disabled whenever:</p> <ul style="list-style-type: none"> • 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 groups	<p>Delete empty or unused groups to simplify the Directory.</p> <p>To delete a group, click the menu icon beside the group name and then select Delete.</p> <hr/> <p> WARNING!</p> <p>Deleting a group cancels the plans associated with that group, moves appliances to the Unmanaged group, and unregisters repository servers from Deep Discovery Director. Only groups without unfinished plans can be deleted.</p> <hr/> <p>This function is disabled whenever:</p> <ul style="list-style-type: none"> • 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.

ACTION	DESCRIPTION
Delete appliances	<p data-bbox="521 251 1147 305">To delete an appliance, click the menu icon beside the display name and then select Delete.</p> <p data-bbox="521 321 1184 406">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.</p> <hr data-bbox="521 438 1184 441"/> <div data-bbox="521 451 1184 576"> WARNING! Deleting an appliance unregisters it from Deep Discovery Director, stops all connections, and cancels all associated plans.</div> <hr data-bbox="521 576 1184 579"/>

Chapter 5

Appliance Updates

Plans

Plans define the scope and schedule of update deployment 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 update files to be deployed must match the product and language of the target appliances.

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

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



Important

Plans can expire. If one or more appliances do not execute the plan within the specified period, the plan is considered expired.

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

TABLE 5-1. Plans

ITEM	DESCRIPTION
Name	Specified during plan creation
Type	Type of file deployed to targets. Deep Discovery Director currently supports hotfixes, critical patches, and firmware upgrades.

ITEM	DESCRIPTION
Plan status	<p>A plan can have any of the following statuses.</p> <ul style="list-style-type: none"> • In progress: Deployment started at the specified time and at least one appliance has executed the plan. • Pending: Deployment has not started or no appliances have received plan information from Deep Discovery Director. • Expired: Deployment did not start at the specified time and no appliances received plan information from Deep Discovery Director. • Completed: Deployment started at the specified time and all appliances successfully executed the plan. • Unsuccessful: Deployment did not start at the specified time or at least one appliance was unable to execute the plan.
Deployed	Date and time deployment started
Created	Date and time plan was created
Description	Description of the plan
Creator	User account that created the plan

Plan Tasks

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

TABLE 5-2. Plan Tasks

TASK	DESCRIPTION
Plan information	Plan deployment status and schedule, update file details, and other related information
Appliance information	<p>Host name, appliance status, deployment start and completion, and appliance path</p> <p>For details, see Appliance Statuses on page 5-4.</p>

Appliance Statuses

Deep Discovery Director displays any of the following appliance statuses.

TABLE 5-3. Appliance Statuses




STATUS	DESCRIPTION
Pending	The appliance has not received the plan information from Deep Discovery Director.
In progress	Any of the following situations may apply. <ul style="list-style-type: none">• The appliance has acknowledged receipt of the plan information and has started downloading files.• The appliance has acknowledged receipt of the plan information and has started executing the plan.• The appliance is downloading the update files.• The appliance has downloaded the update files and is executing the plan.
Suspended	The appliance has temporarily stopped downloading files and will resume on the specified execution period.
Completed	The appliance executed the plan successfully.
Unsuccessful	Any of the following situations may apply. <ul style="list-style-type: none">• The appliance was unable to execute the plan.• The appliance is performing tasks that do not match the plan information.• The appliance is connected to a Local Repository server that is unavailable or does not exist.
Expired	The appliance did not receive the plan information during the specified execution period.


STATUS	DESCRIPTION
Unreachable	<p>Any of the following situations may apply.</p> <ul style="list-style-type: none">• The appliance has unregistered from Deep Discovery Director.• The appliance has been deleted from Deep Discovery Director.

Other Plan Tasks

You can also perform the following tasks:

TABLE 5-4. Other Tasks

TASK	DESCRIPTION
Add	<ol style="list-style-type: none"> 1. Type a plan name with a maximum of 256 characters. 2. Optional: Type a description. 3. Select an update file from the list. <hr/> <div data-bbox="477 451 1080 602">  Note Deep Discovery Director displays a list of files that are available on the designated repository server. Verify that the file matches the product and language of the target appliances. </div> <hr/> <ol style="list-style-type: none"> 4. Select target appliances. Deep Discovery Director displays the appliances that are compatible to the file that you selected. <hr/> <div data-bbox="477 753 1036 846">  Note Installing updates automatically restarts the target appliances. </div> <hr/> <ol style="list-style-type: none"> 5. Specify the deployment schedule. <ul style="list-style-type: none"> • Immediate: Starts deployment immediately after the plan is saved • Custom: Deploys the plan at the specified period <ul style="list-style-type: none"> • Plan deployment start and expiration (Deep Discovery Director server time) • Appliance execution period (appliance local time) 6. Click Save.
Edit	<p>Select a plan with the status Pending and then click Edit.</p> <hr/> <div data-bbox="431 1268 1040 1333">  Note Only plans that have not been deployed can be edited. </div>

TASK	DESCRIPTION
Copy	Select a plan in the list and click Copy .
Delete	<div>Select a plan in the list and click Delete.</div> <div> Note Only plans that have been unsuccessfully deployed can be deleted.</div>

Repository

The Repository screen displays all update files hosted by the server. The screen provides filters that you can use to search by update type, product, language, and file name or version. You can also upload and delete files.

Uploading Files

The Central Repository server supports uploading of multiple files through simultaneous single-file upload sessions. The server opens a browser tab for each upload session, allowing you to navigate away from the screen and perform other tasks while waiting for the upload to complete.

Procedure

1. Go to **Appliance Updates > Repository**.
 2. Click **Upload**.
 3. Click **Select** and then select a valid TAR file.
 4. (Optional) Type a description.
 5. Click **Upload**.
-

Connection Settings

Registering to the Deep Discovery Director Server

Procedure

1. Go to **Administration > Connect to Deep Discover Director**.
2. Under **Connection Settings**, type the **Server address** for Deep Discovery Director.
3. Under **Connection Settings**, type the **API key** for Deep Discovery Director.



Note

Log on to the Deep Discovery Director management console to obtain the API key.

4. Click **Register**.



Note

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

After the registration process is complete, the **Test Connection** button appears. You can click **Test Connection** to test the connection to Deep Discovery Director.

Connecting to the Central Repository Server



Note

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

For details, see [Proxy on page 6-7](#).

Procedure

1. Type the following:

- IPv4 address or FQDN of the Central Repository server
- API key of the Central Repository server

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



Important

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

2. Click **Connect**.

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

Managing Connections to Local Repository Servers

Procedure

1. Optional: Specify the preferred period for downloading updates.
2. Assign at least one repository server to each appliance.



Note

You can assign secondary repository servers only after selecting the primary repository server.

3. Click **Save**.
-


Chapter 6

Administration

Updates

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

TABLE 6-1. Hotfixes / Patches

SYSTEM UPDATE	DESCRIPTION
Hotfix	<p>A hotfix is a workaround or solution to a single customer-reported issue. Hotfixes are issue-specific, and are not released to all customers.</p> <hr/> <p> Note A new hotfix may include previous hotfixes until Trend Micro releases a patch.</p> <hr/>
Patch	<p>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.</p>

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

<http://downloadcenter.trendmicro.com/>

Installing a Hotfix / Patch

Procedure

- 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**.
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 will automatically restart after the update is complete.

6. Log on to the management console.
 7. Go back to the **Administration > Updates** screen.
 8. Verify that the hotfix / patch displays in the **History** section as the latest update.
-

Rolling Back a Hotfix / Patch

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

**Note**

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

Procedure

1. Go to **Administration > Updates**.
2. In the **History** section, click **Rollback**.

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

3. Log on to the management console.
 4. Go back to the **Administration > Updates** screen.
 5. Verify that the hotfix / patch no longer displays in the **History** section.
-

Microsoft Active Directory Integration

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

Configuring Microsoft Active Directory Integration

Procedure

1. Obtain the information required to configure Microsoft Active Directory integration from the server administrator.
2. Go to **Administration > Microsoft Active Directory Integration**.
3. Select the server type that is integrating.
 - Microsoft Active Directory
 - Microsoft AD Global Catalog
4. Type the server address.
5. Select the access protocol.
 - 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 6-6*
- *Proxy on page 6-7*
- *Time on page 6-8*

- [Certificate on page 6-9](#)
- [Session Timeout on page 6-10](#)

Network

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

Modify the IP address immediately after completing all deployment tasks.



Note

You can also use the **Preconfiguration Console** to modify the network settings.

For details, see [Configuring Network Addresses on the Preconfiguration Console on page 3-6](#).

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

Configuring Port Binding

Deep Discovery Director supports the binding of services to a second network port. When services are bound to eth0 and eth1, Deep Discovery Director directs all connections to the Central Repository server through eth1.



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.
 - 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.

A new **eth1** section to configure network settings for the second network port displays under the existing **eth0 (management)** section.
 2. Configure the IP address and other network settings of the second network port.
 3. Click **Save**.
-

Using IPv4 and IPv6 Dual Stack

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

Procedure

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

A new section to configure IPv6 settings displays between the existing IPv4 and DNS settings.
 2. Configure the IPv6 settings.
 3. Click **Save**.
-

Proxy

Specify proxy settings if Deep Discovery Director connects to the Central Repository through a proxy server.



Note

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

Procedure

1. Go to **Administration > System Settings > Proxy**.
The **Proxy** screen appears.
 2. Select **Connect to the Central Repository using a proxy server**.
 3. Select the protocol to use for proxying.
 - HTTP
 - SOCKS4
 - SOCKS5
 4. Type the IPv4 address or FQDN of the proxy server.
 5. Type the port number. The default port number is **80**.
 6. (Optional) If you selected **HTTP** or **SOCKS5** as protocol, and your proxy server requires authentication, select **Specify authentication credentials**, and then type the user name and password used for authentication.
 7. (Optional) Click **Test Connection** to verify the connection to the proxy server.
 8. Click **Save**.
-

Time

Configure date and time settings immediately after installation.

Procedure

1. Go to **Administration > System Settings > Time**.
The **Time** screen appears.
2. Select one of the following methods and configure the applicable settings.
 - Select **Connect to an NTP server** and type the FQDN or IP address of the NTP server.

- Select **Set manually** and configure the time.
3. Select the applicable time zone.

**Note**

Daylight Saving Time (DST) is used when applicable.

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

Certificate

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

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

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

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

Importing a Certificate

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

**Important**

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

Procedure

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

The **Certificate** screen appears.

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

The certificate will be imported immediately.

Session Timeout

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

Accounts

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

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

- [*Adding a Local User Account on page 6-11*](#)
- [*Adding an Active Directory User Account on page 6-12*](#)

**Note**

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

For details, see [Microsoft Active Directory Integration on page 6-4](#).

Adding a Local User Account

The **Add Account** screen appears when you click **Add** on the **Accounts** screen.

Procedure

1. Toggle the **Status** of this account.
 2. Select **Local user** as the **Type** of this account.
 3. Type a valid user name.
 4. Type a valid password.
 5. Type the password again to confirm it.
 6. Select a **Role** for this account. The role determines the level of access this account has.
 - **Administrator:** Users with this role have full access to all management console features.
 - **Operator:** Users with this role have read-only access to all management console features.
 7. (Optional) Type a description for this account.
 8. Click **Save**.
-

Adding an Active Directory User Account



Note

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

For details, see *Microsoft Active Directory Integration on page 6-4*.

The **Add Account** screen appears when you click **Add** on the **Accounts** screen.

Procedure

1. Toggle the **Status** of this account.
2. Select **Active directory user** as the **Type** of this account.
3. Type a user name and click **Search** to search the Active Directory for matching user accounts.

Matching user accounts are displayed in the results table.



Note

If an account's User Principle Name (UPN) is not specified on the Active Directory server, it will not be displayed in the search results.



4. Select the Active Directory account to add.
5. Select a **Role** for this account. The role determines the level of access this account has.
 - **Administrator:** Users with this role have full access to all management console features.
 - **Operator:** Users with this role have read-only access to all management console features.
6. (Optional) Type a description for this account.



7. Click **Save**.

Other Accounts Tasks

You can also perform the following tasks:

TABLE 6-2. Other Tasks

TASK	DESCRIPTION
Edit account	<p>Click on a user name to open the Edit Account screen and do the following:</p> <ul style="list-style-type: none"> • Toggle the account status • Change the password • Change the role • Modify the description <hr/> <p> Note</p> <ul style="list-style-type: none"> • The passwords of Microsoft Active Directory accounts cannot be changed from the management console. • Clicking on the user name of the logged-on account opens the Change Password screen instead.
Delete account	<p>Select one or more user accounts to delete and then click Delete.</p> <hr/> <p> Important</p> <ul style="list-style-type: none"> • There must be at least one local administrator account. • You cannot delete the logged-on account. • Other users who are currently logged on to the management console will be logged off automatically.
Change password	<p>Click on the user name of the logged-on account to open the Change Password screen and change the password.</p>

TASK	DESCRIPTION
View account lock status	<p>Deep Discovery Director includes a security feature that locks an account in case the user typed an incorrect password three times in a row. This feature cannot be disabled. Accounts locked this way, even administrator accounts, unlock automatically after ten minutes.</p> <hr/> <p> Note Microsoft Active Directory accounts are never locked.</p> <hr/>
Toggle account status	<p>Click on the toggle in the Status column to enable or disable the user account.</p> <hr/> <p> Important There must be at least one active local administrator account.</p> <hr/>

System Logs

Deep Discovery Director maintains system logs that provide summaries about user access, setting changes, and other configuration modifications that occurred using the management console.

Deep Discovery Director stores system logs in the appliance hard drive. The system logs can be exported in CSV format for offline viewing.

Power Off / Restart

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

- **Power Off:** All active tasks are stopped, and then the appliance gracefully shuts down.

- **Restart:** All active tasks are stopped, and then the appliance is restarted.

Integrated products may queue data while the appliance is unavailable.

Index



TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM17452/160713