OfficeScan ToolBox 1.0

Administrator's Guide

TREND MICRO™ SMART PROTECTION NETWORK™

Endpoint Security

Protected Cloud

Web Security

Document Part No.: OSEM15312_120106

Release Date: January 2012

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6.119,165

Related Documents

Use this Administrator's Guide to upgrade, install and/or configure Trend Micro ToolBox in conjunction with Trend Micro OfficeScan.

For related information, see:

- **OfficeScan 10.6 Administrator's Guide**: Contains client deployment strategies, installation instructions, and common configuration tasks.

Feedback

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.

Please evaluate this documentation on the following site:

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

Table of Contents

Appendix A: Status Information

Index

Chapter 1

Introducing the OfficeScan ToolBox

The chapter introduces the OfficeScan™ ToolBox and provides an overview of its features and benefits.

Topics include:

- *About OfficeScan ToolBox on page 1-2*
- *Key Features and Benefits on page 1-2*

About OfficeScan ToolBox

The OfficeScan™ ToolBox is a plug-in program that functions as a framework which manages and deploys a variety of standalone Trend Micro tools. This framework triggers logging, and consolidates logs. The ToolBox leverages the client tree hierarchy of the OfficeScan server to remotely deploy these tools on clients managed by the OfficeScan server.

Administrators can silently deploy and log the operations of these standalone tools on clients. Each tool addresses a specific security or network concern. Detailed information regarding the function and use of a tool is available in a readme file that the ToolBox downloads with the tool.

After the ToolBox has successfully deployed a tool, administrators can choose to send all or part of the information gathered by the tool to Trend Micro for analysis. Trend Micro uses the information garnered from the analysis to develop new solutions that address the constantly changing threat landscape for all Trend Micro customers.

Note

All information sent to Trend Micro is strictly confidential.

Key Features and Benefits

The OfficeScan ToolBox provides the following features and benefits:

- **Standalone Tool Management**

  The ToolBox allows administrators to manage a variety of tools designed by Trend Micro to enhance the security of the customer's computing environment. The ToolBox provides a convenient framework to manage and deploy tools to multiple OfficeScan clients.

- **Log Consolidation and Management**

  The ToolBox automatically collects the logs generated by tools for easy access and viewing by administrators. Administrators can view the tool deployment history and results, and automatically or manually manage the size of the log database.

See *Log Settings on page 4-2*.

- **Anti-Threat Toolkit™ Feedback to Trend Micro**

  The ToolBox allows the Anti-Threat Toolkit to send scan-related information to Trend Micro. Administrators can choose whether to send this information automatically or manually. Trend Micro uses the information garnered from its analysis of this information to develop new solutions that address the constantly changing threat landscape for all Trend Micro customers.

  Note

  All information sent to Trend Micro is strictly confidential.

  See *Feedback Settings on page 4-3*.

- **Tool Updates**

  Administrators can automatically or manually download the latest updates for previously downloaded tools.

  See *Update Settings on page 4-5*.

Chapter 2

Managing the OfficeScan ToolBox

Install and activate the OfficeScan ToolBox independently of OfficeScan. The ToolBox provides its own console for product management. The management console is accessible from the OfficeScan web console.

Topics include:

ToolBox Installation

The OfficeScan ToolBox displays on the Plug-in Manager console. Use the console to download, install, and manage the program. Plug-in Manager downloads the installation package for the ToolBox from the Trend Micro ActiveUpdate server or from a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts the installation, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program installation or management from Trend Micro Control Manager's single sign-on function.

System Requirements

OfficeScan Server Requirements

TABLE 2-1. OfficeScan Server with Windows Server 2008 (including R2 with or without SP1)

HARDWARE	SPECIFICATIONS
Processor	Minimum: • 1GHz Intel™ Pentium™ processor or equivalent for x86 processors • 1.4 GHz Intel™ Pentium™ processor or equivalent for x64 processors Recommended: 2GHz Intel™ Pentium™ processor or equivalent for all processors
RAM	Minimum: 512MB Recommended: 2GB
Disk space	Minimum: 1GB

HARDWARE	SPECIFICATIONS
Other	Gigabit Network Interface Card (NIC) supported
Display	Monitor that supports 1024 * 768 resolution at 256 colors or higher

TABLE 2-2. OfficeScan Server with Other Platforms (Pentium processors)

HARDWARE	SPECIFICATIONS
Processor	Minimum: 800MHz Intel™ Pentium™ processor or equivalent
RAM	Minimum: 512MB Recommended: 1GB
Disk space	Minimum: 1GB
Other	Gigabit Network Interface Card (NIC) supported
Display	Monitor that supports 1024 * 768 resolution at 256 colors or higher

TABLE 2-3. OfficeScan Server with Other Platforms (Core 2 Duo processors)

HARDWARE	SPECIFICATIONS
Processor	Minimum: 2.13GHz Intel™ Core 2 Duo E6420 processor or equivalent
RAM	Minimum: 4GB
Disk space	Minimum: 2GB
Other	Gigabit Network Interface Card (NIC) supported
Display	Monitor that supports 1024 * 768 resolution at 256 colors or higher

Web Console Requirements

Hardware /Software	Specifications
Processor	Minimum: 300MHz Intel™ Pentium™ processor or equivalent
RAM	Minimum: 128MB
Disk space	Minimum: 30MB
Display	Monitor that supports 1024 * 768 resolution at 256 colors or higher
Browser	Internet Explorer™ 7.0 or higher

OfficeScan Client Requirements

Table 2-4. Windows XP/Server 2003 Client

Hardware/ Software	Specifications	
	32-bit	64-bit
Processor	300MHz Intel™ Pentium™ processor or equivalent (AMD64 processor architectures also supported)	Intel64 or AMD64 architecture processor
RAM	Minimum: 256MB Recommended: 512MB	
Disk space	Minimum: 350MB	
Display	Monitor that supports 800 x 600 resolution at 256 colors or higher	
Browser	Internet Explorer™ 7.0 for web setup	

TABLE 2-5. Windows Server 2008 Client

HARDWARE/ SOFTWARE	SPECIFICATIONS	
	32-BIT	64-BIT
Processor	Minimum: 1GHz Intel™ Pentium™ processor or equivalent; (AMD64 processor architectures also supported) Recommended: 2GHz Intel™ Pentium™ processor or equivalent	Minimum: 1.4 GHz Intel™ Pentium™ processor or equivalent for x64 processors Recommended: 2GHz Intel™ Pentium™ processor or equivalent for all processors
RAM	Minimum: 512MB Recommended: 2GB	
Disk space	Minimum: 350MB	
Display	Monitor that supports 800 x 600 resolution at 256 colors or higher	
Browser	Internet Explorer™ 7.0 for web setup	

TABLE 2-6. Windows Vista Client for 32-bit and 64-bit

HARDWARE /SOFTWARE	SPECIFICATIONS
Processor	Minimum: 800MHz Intel™ Pentium™ processor or equivalent (AMD64 processor architectures also supported)
RAM	Minimum: 1GB Recommended: 1.5GB
Disk space	Minimum: 350MB
Display	Monitor that supports 800 * 600 resolution at 256 colors or higher
Browser	Internet Explorer™ 7.0 for web setup

TABLE 2-7. Windows 7 Client for 32-bit and 64-bit

HARDWARE /SOFTWARE	SPECIFICATIONS
Processor	1GHz Intel™ Pentium™ processor or equivalent (AMD64 processor architectures also supported)
RAM	Minimum: 1GB Recommended: 1.5GB
Disk space	Minimum: 350MB
Display	Monitor that supports 800 * 600 resolution at 256 colors or higher
Browser	Internet Explorer™ 8.0 for web setup

Installing OfficeScan ToolBox

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the Plug-in Manager screen, go to the OfficeScan ToolBox section and click **Download**. The size of the plug-in program package displays beside the **Download** button.

   The Trend Micro OfficeScan ToolBox License Agreement screen appears.

   > **Note**
   >
   > If you encounter problems downloading the package, check the server update logs on the OfficeScan product console. On the main menu, click **Logs** > **Server Update Logs**.

3. After the download completes, click **Install** to begin the installation.

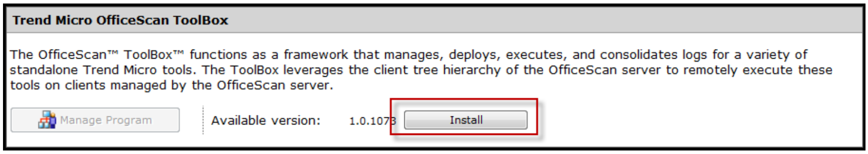

FIGURE 2-1. Install button for OfficeScan ToolBox

4. Click **Agree** to continue the installation. Click **Decline** to exit the screen without installing the ToolBox.

5. Monitor the installation progress. You can navigate away from the screen during the download. I

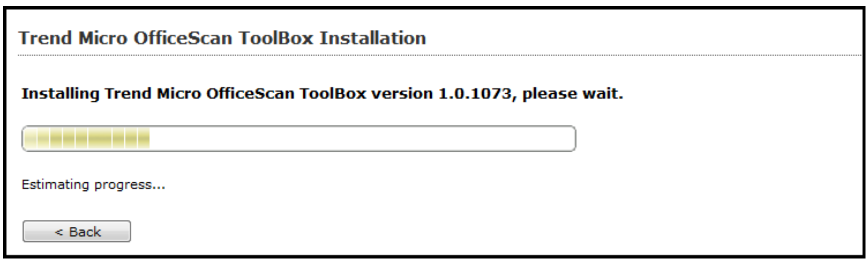

FIGURE 2-2. Installation progress for OfficeScan ToolBox

After Plug-in Manager installs the package, the Plug-in Manager screen appears.

After the installation, the current plug-in program version displays. You can then start managing the plug-in program.

Managing OfficeScan ToolBox

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** from the main menu.

2. On the Plug-in Manager screen, go to the OfficeScan ToolBox section and click **Manage Program**.

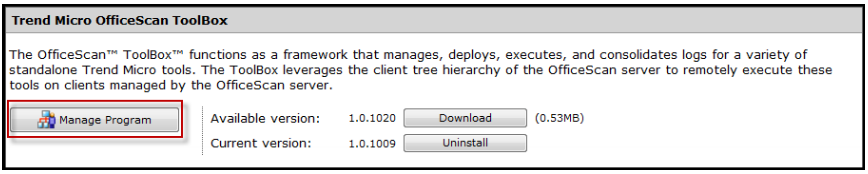

FIGURE 2-3. Manage Program button for OfficeScan ToolBox

OfficeScan ToolBox Upgrades

A new version of the ToolBox displays on the Plug-in Manager console. On the console, you can download the upgrade package and then upgrade the program. Plug-in Manager downloads the package from the Trend Micro ActiveUpdate server or a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts the upgrade, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program upgrading from Trend Micro Control Manager's single sign-on function.

Upgrading OfficeScan ToolBox

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.

2. On the Plug-in Manager screen, go to the OfficeScan Toolbox section and click **Download**. The size of the upgrade package displays beside the **Download** button.

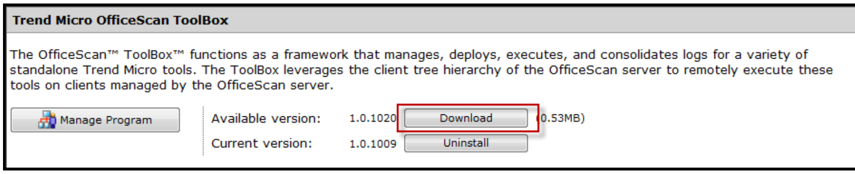

FIGURE 2-4. Download button for OfficeScan ToolBox

3. Monitor the download progress. Navigating away from the screen during the download does not affect the upgrade.

Note

If problems occur while downloading the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Update Logs**.

---

4. After Plug-in Manager downloads the package, a new screen displays.

After the upgrade, the Plug-in Manager service may need to restart, causing the Plug-in Manager screen to be temporarily unavailable. When the screen becomes available, the current plug-in program version displays.

OfficeScan ToolBox Uninstallation

There are several ways to uninstall the OfficeScan ToolBox program.

- Uninstall OfficeScan ToolBox from the Plug-in Manager console.
- Uninstall the OfficeScan server, which uninstalls Plug-in Manager and all installed plug-in programs. For instructions on uninstalling the OfficeScan server, see the OfficeScan Installation and Upgrade Guide.

Uninstalling OfficeScan ToolBox from the Plug-in Manager Console

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the Plug-in Manager screen, go to the OfficeScan ToolBox section and click **Uninstall**.

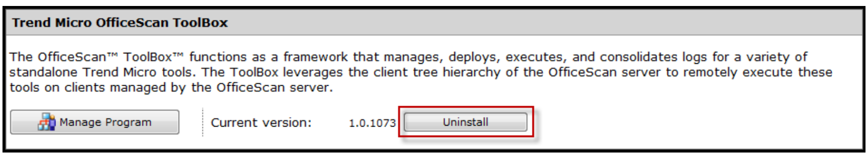

FIGURE 2-5. Uninstall button for OfficeScan ToolBox

3. Monitor the uninstallation progress. You can navigate away from the screen during the uninstallation.
4. After the uninstallation completes, the OfficeScan ToolBox is again available for installation.

Chapter 3

Deploying Tools

The chapter discusses the OfficeScan client tree and how to deploy tools to OfficeScan clients.

Topics include:

The Client Tree

The client tree displays all the clients (grouped into OfficeScan Domains) that the server currently manages. Clients are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

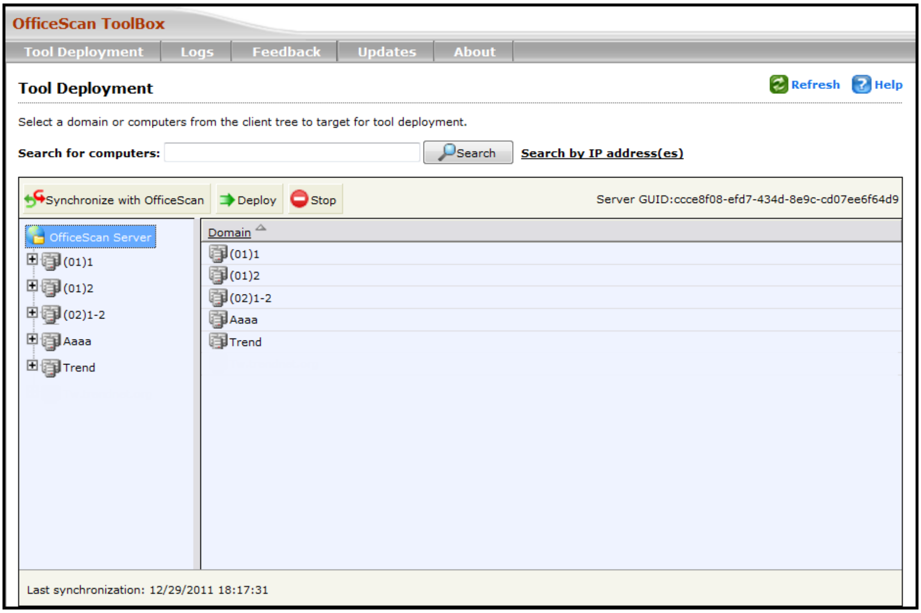

FIGURE 3-1. Client Tree

Client Tree Specific Tasks

The client tree displays when you manage the OfficeScan Toolbox on the web console. Above the client tree are menu items specific to the Toolbox. These menu items allow you to perform specific tasks, such as deploying a tool to a client. To perform any of the tasks, first select the task target (either a specific domain or one or several clients) and then select a menu item.

The client tree provides access to the following functions:

- **Search for computers**: Locate specific computers by typing search criteria in the text box.
- **Search by IP address(es)**: Click the hyperlink to display the **Search by IP Address(es)** screen. Locate specific computers by typing IP addresses in the text box. Use line breaks or commas to separate multiple IP addresses.
- **Synchronize with OfficeScan**: Synchronize the Toolbox's client tree with the OfficeScan server's client tree. See *Synchronizing the Client Tree on page 3-3* for details.
- **Deploy**: Deploy a tool to selected clients. See *Deploying a Tool on page 3-4* for details.
- **Stop**: Click to stop deploying a tool to the selected clients. Allow some time for the abort command to propagate to all clients.

Administrators can also manually search the client tree to locate computers or domains. Specific computer information displays in the table on the right (see *Deployment Information on page 3-5* for details).

Synchronizing the Client Tree

Before the ToolBox can deploy the tools to endpoints, administrators need to synchronize the client tree with the OfficeScan server.

Procedure

1. Open the ToolBox console.
2. In the Tool Deployment tab, click **Synchronize with OfficeScan**.

   A confirmation message screen appears.
3. Allow a few moments for the synchronization to complete. After the synchronization completes, the message "The client tree has been successfully synchronized with the OfficeScan server" appears.
4. Click **Close** to return to the **Tool Deployment** screen.

Deploying a Tool

The OfficeScan ToolBox can deploy a tool to one domain or many OfficeScan clients.

Procedure

1. Open the OfficeScan ToolBox console. The **Tool Deployment** screen appears.
2. Select domains or clients for the ToolBox to target by using:
   - **Search for computers**: Type the name of a domain or client in the text box and click **Search**.
   - **Search by IP address(es)**: See *Searching for IP Addresses on page 3-6* for details.
3. Click the domains or clients for the ToolBox to target. Select multiple clients by pressing the **Ctrl** or **Shift** keys.
4. Click **Deploy**.

   The **Deployment Settings** screen appears.
5. Select a tool to deploy by clicking:
   - **Select from the following list**: Select a pre-loaded tool from the drop-down list.
   - **Download from the Internet**: Type the URL from which to download the tool.
   - **Import a local copy**: Type the file path and file name of the pre-loaded tool.
6. (Optional) Expand the **Advanced settings** section by clicking the down arrows.
   - Click **Specify additional parameters for the selected tool**. Type the parameters that Trend Micro provided with the tool.

> **Note**
>
> Trend Micro provides additional parameters for custom-made tools. Standard tools do not require any additional parameters. Contact Support for further details regarding the use of any additional parameters provided with custom-made tools.

7. Click **Deploy**.

   The **Deploy Tool** screen appears.

8. Allow time for the ToolBox to deploy the tool to the selected domains and endpoints. Once the message “Deploy tool successfully” appears, click **Close** to return to the **Tool Deployment** screen.

9. Monitor the deployment of the tool under the **Deployment Status** column in the client list by occasionally clicking the **Refresh** button. Once the tool finishes its execution on the endpoints, the status changes from “Deploying” to “Completed”.

   > **Note**
   >
   > It is possible to cancel the deployment of a tool by clicking the **Stop** button located above the client list.

Deployment Information

The client tree table provides detailed information regarding specific clients and each client’s interaction with the OfficeScan ToolBox, if any. The ToolBox displays the following information in this table:

- **Computer**: The host name of the client
- **IP**: The IP address of the client
- **Connection**: The current connection status of the client
- **Last Tool Deployed**: Displays the most recent tool that the administrator deployed to the client
- **Deployment Status**: Displays the status of the most recently deployed tool

For details regarding the deployment status, see *Deployment Status of Tools on page A-1*.

- **Start Time**: The time that the administrator deployed the tool
- **End Time**: The time that the selected tool ceased its operations on the client

> **Note**
> Click a column heading to reorder the table.

- **Page**: Displays the current page of client search results. Click the arrow icons or type a page number to view more results.
- **Results per page**: Select the number of clients to display in the table

Searching for IP Addresses

Locate specific endpoints by typing IP addresses in the field.

Procedure

1. Open the ToolBox console. On the Tool Deployment screen, click the **Search by IP address(es)** link.

   The **Search by IP Addresses** screen appears.

2. Type the IP address(es) of the desired endpoint(s). Separate multiple IP addresses using line breaks, commas, semicolons, or spaces.

   > **Note**
   > The maximum length of the IP addresses text field is 2048 characters.

3. Click **Search**.

   The Search by IP Addresses screen closes and the IP search results display in the list beside the client tree.

Chapter 4

Administrative Settings

Administrators can manage the following settings to streamline the OfficeScan ToolBox functions.

Topics include:

Log Settings

The **Logs** screen allows administrators to define a scheduled deletion of logs, manually delete logs, and download the logs created after the deployment of a tool.

Configure the log settings using the following controls:

- **Enable scheduled deletion of logs older than ___ days**: Select this check box and specify the number of days that the ToolBox saves logs on the server. Click **Save** to retain this setting.
- **Delete**: Click to delete selected logs from the list.

> **WARNING!**
>
> The deletion (or scheduled deletion) of logs also deletes the same logs from the **Files to Send** list on the **Feedback** screen. After deleting all logs found in a Feedback entry, the Feedback entry disappears from the list. Save all desired feedback before deleting log files.

- **Deployment Logs** list: Select the check box next to the logs that require deletion. This list also provides the following information regarding existing logs:
  - **Date/Time**: The date and time that the tool started its execution
  - **Tool Deployed**: The name and version number of the deployed tool
  - **Computer**: The host name of the client on which the tool executed
  - **Result**: The current status of the tool's log files. A tool that has not completed its operations displays "Deploying" and then "Completed" once the operations are complete.

    For details regarding the result status, see *Result Status of Logs on page A-1*.
  - **Logs Files**: Click **Download** to download all the log information generated by the deployed tool.

> **Note**
>
> Each tool generates its own set of log files. The type of files and information contained in the logs differs for each tool.

- **Page**: Displays the current page number appearing in the list. Click the arrow icons or type a page number to view more logs.
- **Results per page**: Select the number of logs to display in the table
- **Save**: Click to save changes to the number of days that the ToolBox saves logs.

Feedback Settings

The feedback settings allow administrators to automatically send files generated by the Anti-Threat Toolkit to Trend Micro for analysis, select specific files to send to Trend Micro, and view the results of the analyses that Trend Micro performs on previously sent files.

WARNING!

The deletion (or scheduled deletion) of logs also deletes the same logs from the **Files to Send** list on the **Feedback** screen. After deleting all logs found in a Feedback entry, the Feedback entry disappears from the list. Save all desired feedback before deleting log files.

Configure the feedback settings using the following controls:

- **Enable automatic feedback**: Select to allow the ToolBox to automatically send Trend Micro feedback regarding the results of the tool deployments. Click **Save** to retain this setting.
- **Files to Send** list: This list also provides the following information regarding existing logs:
  - **Date/Time**: The date and time that the tool started its execution
  - **Tool Deployed**: The name and version number of the deployed tool
  - **Computer(s)**: The host name(s) of the client(s) on which the tool executed
  - **Files to Send**: View or edit the files sent to Trend Micro. See *Sending Feedback to Trend Micro on page 4-4* for details.

- **Reference ID**: Click the link (if available) to view detailed information about files previously sent to Trend Micro. If no link is available, contact Support and provide the displayed reference ID.
- **Send Feedback**: Click the **Send** button to send feedback regarding the tool operations. Allow time for the sending of files. Trend Micro has successfully received the files once the status under Send Feedback changes from "Sending" to "Sent".

> **Note**
>
> By default, the ToolBox sends all files generated by a deployed tool. Send specific files by selecting them under the **Files to Send** list column.

- **Page**: Displays the current page number appearing in the list. Click the arrow icons or type a page number to view more logs.
- **Results per page**: Select the number of logs to display in the table
- **Save**: Click to save changes to the automatic feedback option.

Sending Feedback to Trend Micro

View files previously sent to Trend Micro, or select specific files to send.

Procedure

1. Open the ToolBox console and click **Feedback**.
2. In the Files to Send list, under the Files to Send column, click one of the following:
    - **View**: Opens the **Files to Send** screen and displays files previously sent to Trend Micro.
    - **Edit**: Opens the **Files to Send** screen and displays a list of files generated by the deployed tool.
3. Select specific or all endpoints in the **View** drop-down list.
4. Select specific files to send to Trend Micro by selecting the check box to the left of the file name.

Note

Files that the ToolBox has already sent can be viewed on the **Files to Send** screen. The ToolBox does not send the files again.

5. Click **Save** to save the list of selected files and return to the **Feedback** screen.

Update Settings

The update settings allow administrators to configure the automatic update of tools, perform a manual update of tools, and view the product documentation for the tools that the ToolBox manages.

Configure the update settings using the following controls:

- **Enable automatic update of the tools**: Select to allow the ToolBox to automatically download updates for the existing tools as updates become available.
- Tools list: View the tools that the ToolBox currently manages. The Tools list provides the following information:
    - Tool: The name and version number of the tool
    - Description: Information regarding the purpose of the tool
    - **Readme**: Documentation released with the tool that contains late-breaking product news, known issues, installation tips, and other important information.
- **Save**: Click to save changes to the automatic update option.
- **Update Now**: Click to manually update all the tools that the ToolBox currently manages.

Note

The ToolBox requires an active Internet connection to perform both automatic and manual updates.

Appendix A

Status Information

Deployment Status of Tools

The following table provides details regarding the different status types for deployed tools.

TABLE A-1. Deployment Status Values for Tools

STATUS	DESCRIPTION
Deploying	The tool displayed under "Last Deployed Tool" is currently propagating to or running on the client.
Completed	The tool displayed under "Last Deployed Tool" successfully completed its operations on the client.
Stopped	The administrator stopped the tool displayed under "Last Deployed Tool" before it could complete its operations on the client or a system timeout occurred.
Download unsuccessful	The specified URL for downloading the tool was incorrect.
Import unsuccessful	The specified source or file format of the tool was invalid.
Interrupted	The tool was unable to complete its operations due to an internal error.

Result Status of Logs

The following table provides details regarding the different status types for logs.

TABLE A-2. Result Status Values for Logs

STATUS	DESCRIPTION
Deploying	The tool is currently propagating to or running on the client.
Completed	The tool successfully completed and collected logs about its operations on the client.
Stopped	The administrator stopped the tool before it could complete its operations on the client or a system timeout occurred.
Restart required	The client requires a system restart.
Clean successful	The tool successfully cleaned a threat from an endpoint.
Clean unsuccessful	The tool was unsuccessful while attempting to clean a threat from an endpoint.
Interrupted	The tool was unable to complete its operations due to an internal error.

Index