Trend Micro™ OfficeScan XG

Best Practice Guide for Malware

Anti-Spyware Anti-Spam Antivirus Anti-Phishing Content & URL Filtering

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Author: Mark Tongco

Released: October 05, 2016

Table of Contents

OfficeScan XG Best Practice Guide for Malware Protection

1.1 > Enable Smart Scan Agents

Ensure that OfficeScan agent can query at least two Smart Protection Servers

This guidance avoids the creation of a single-point of failure for anti-malware security. If the lone Smart Protection Server on the network crashes, this has repercussions for desktop security throughout the network.

Adding a second Smart Protection Server on the network, or ensuring that all File Reputation-enabled agents can connect to the Trend Micro scan service if the primary Scan Service fails, results in a more robust security implementation.

Options:

- Enable the Integrated Smart Protection Server on multiple OfficeScan servers
- Install VMWare-based Standalone Smart Protection servers

There are two types of local Smart Protection Servers:

- Integrated Smart Protection Server
- Standalone Smart Protection Server

Both essentially work the same way, but are ported for different software platforms.

Integrated Smart Protection Server

The Integrated Smart Protection server is automatically installed on the OfficeScan server. It can be installed during OfficeScan server installation or at later point.

Standalone Smart Protection Server

The Standalone Smart Protection Server is recommended to large networks. At this point, this server is only available as a VMWare image that runs CentOS.

For more information regarding image compatibility on virtual servers, refer to: http://docs.trendmicro.com/en-us/enterprise/smart-protection-server.aspx

When opting to use the Integrated Smart Protection server, make sure it is installed.

To verify if the Integrated Smart Protection server is installed and accessible from a particular desktop, enter the following URL in the desktop‘s browser:

https://<OSCE_Server>:<https_port>/tmcss/?LCRC=08000000AC41080092000080C4F01936B21D9104

-Or-

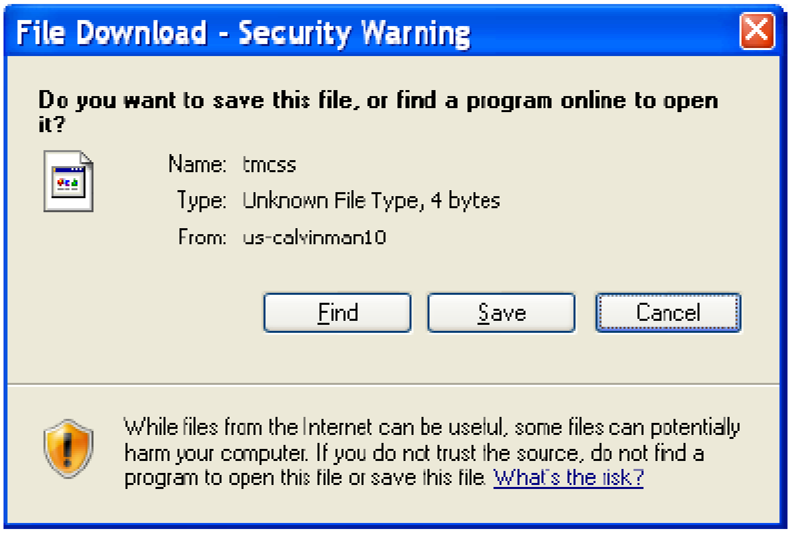
http://<OSCE_Server>:<http_port>/tmcss/?LCRC=08000000AC41080092000080C4F01936B21D9104

Examples:

https://OSCE11:4343/tmcss/?LCRC=08000000AC41080092000080C4F01936B21D9104

http://OSCE11:8080/tmcss/?LCRC=08000000AC41080092000080C4F01936B21D9104

If the browser returns the following, the Integrated Smart Protection Server is both enabled and accessible.



File Download - Security Warning

Do you want to save this file, or find a program online to open it?

Name: tmcss

Type: Unknown File Type, 4 bytes

From: us-calvinman10

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

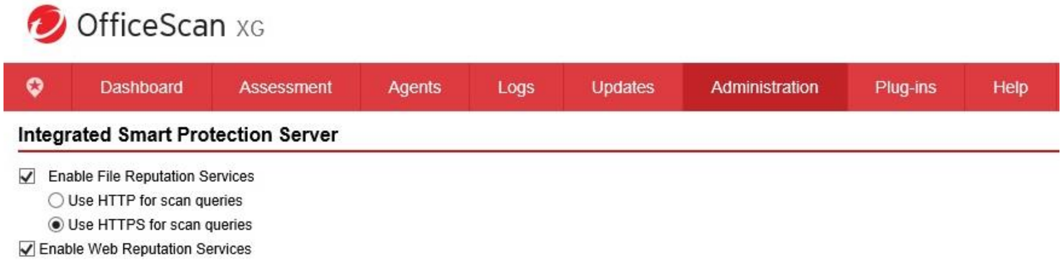
Figure 1 Integrated Smart Protection Server warning

Enable Smart Scan

The smart scan solution makes use of lightweight patterns that work together to provide the same protection provided by conventional anti-malware and anti-spyware patterns. A Smart Protection Server hosts the Smart Scan Pattern. This pattern is updated hourly and contains the majority of pattern definitions. Smart scan agents do not download this pattern. Agents verify potential threats against the pattern by sending scan queries to the Smart Protection Server.

In the smart scan solution, clients send identification information determined by Trend Micro technology to Smart Protection Servers. Clients never send the entire file and the risk of the file is determined using the identification information. This method minimizes the amount of pattern download by relying on cloud technology. Thus, Smart scan agents benefit from local scans and in-the-cloud queries provided by File Reputation Services.

Before including Integrated Smart Protection Server in Smart Protection Sources, make sure it is enabled using the following checkbox on the OfficeScan management console.



Integrated Smart Protection Server

☑ Enable File Reputation Services

○ Use HTTP for scan queries

● Use HTTPS for scan queries

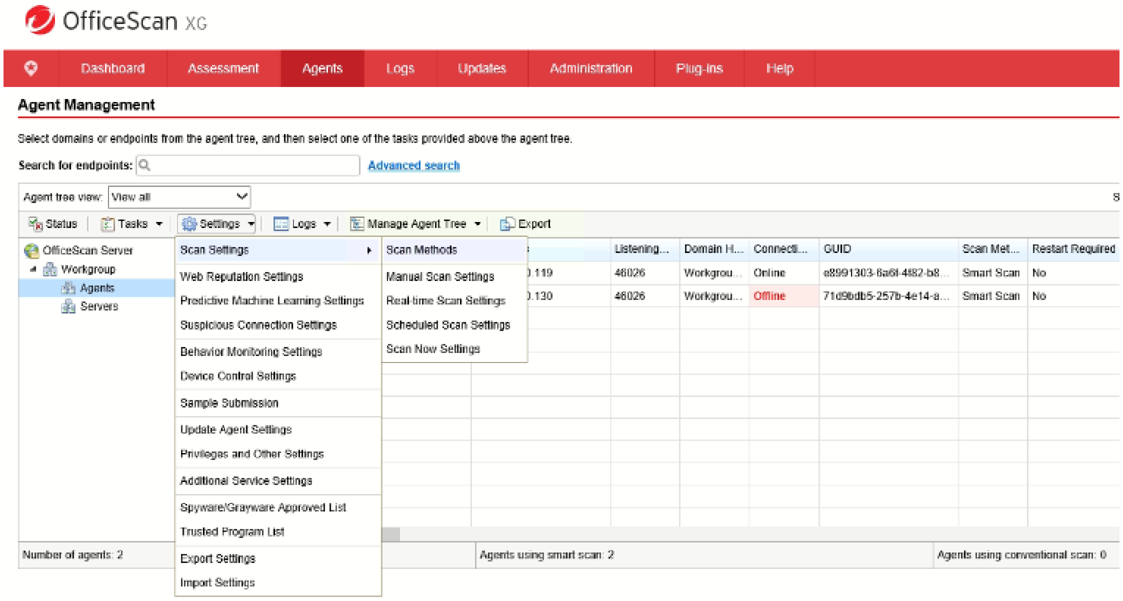
☑ Enable Web Reputation Services

When using File Reputation functionality with an Integrated Smart Protection server, make sure that the Smart Protection server is enabled before switching scan types. This is an important step because the mechanism for switching from conventional scanning to File Reputation does not include automatic verification of Smart Protection server functionality.

It is, therefore, possible to assign a File Reputation-enabled OfficeScan agent to a non-functional Smart Protection server.

1. Create separate domains for Smart and Conventional agents

Upon installation, the default scan mode for the OfficeScan network is called – Smart Scan. As with other OfficeScan agent settings, since this is set at the root of the OfficeScan agent tree, this will affect all future agents, in addition to existing agents that are not already assigned agent-specific scan-method settings.



Agent Management

Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree.

Search for endpoints:

Agent tree view: View all

	Listening...	Domain H...	Connecti...	GUID	Scan Met...	Restart Required
).119	48026	Workgrou...	Online	e8991303-8a6f-4482-b8...	Smart Scan	No
).130	48026	Workgrou...	Offline	71d9bdb5-257b-4e14-a...	Smart Scan	No

Number of agents: 2

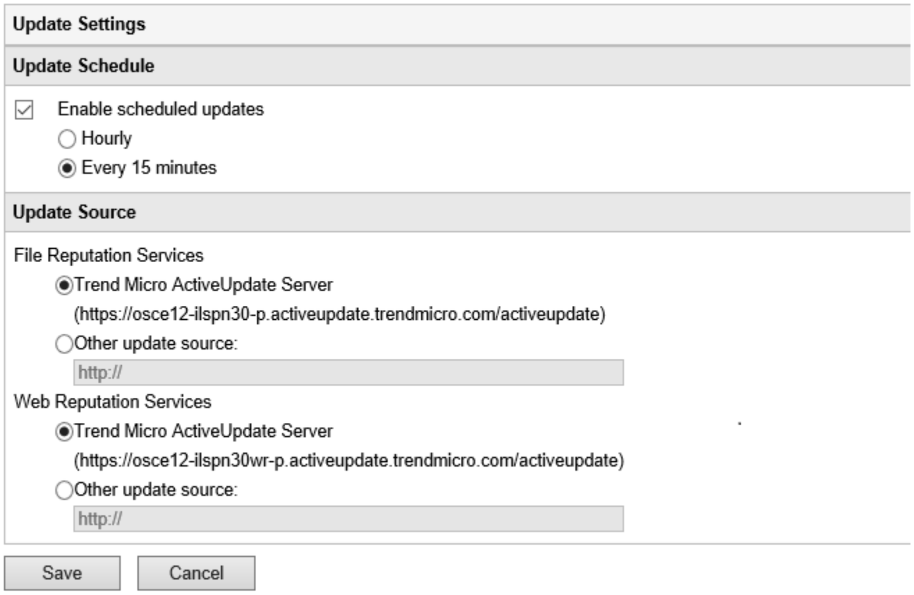
Agents using smart scan: 2

Agents using conventional scan: 0

Figure 2 Agent Management settings window

To separate conventional agents, create OfficeScan domains that have Conventional scan enabled, and then migrate to the created domain.

2. Schedule Smart Protection Server to update on every 15 minutes basis.



Update Settings

Update Schedule

☑ Enable scheduled updates

○ Hourly

● Every 15 minutes

Update Source

File Reputation Services

● Trend Micro ActiveUpdate Server (https://osce12-ilspn30-p.activeupdate.trendmicro.com/activeupdate)

○ Other update source: http://

Web Reputation Services

● Trend Micro ActiveUpdate Server (https://osce12-ilspn30wr-p.activeupdate.trendmicro.com/activeupdate)

○ Other update source: http://

Figure 3 Update Settings window

1.2 > Configuring Manual Scan Settings

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**
3. Select the group/domain you wish to apply the settings to
4. Click **Settings** > **Scan Settings** > **Manual Scan Settings**
5. Configure the Target tab
6. Files to Scan > All Scannable files
7. Scan Settings

   7.1. Scan hidden folders

   7.2. Scan network drive

   7.3. Scan compressed files

   7.4. Scan OLE objects

   - Detect exploit code in OLE files
8. Virus /Malware Scan Settings Only > Scan boot area
9. CPU Usage > Medium: pause slightly between file scans
10. Scan Exclusion > Enable scan exclusion

    10.1. Scan Exclusion list (Directories)

    - Exclude directories where Trend Micro products are installed

- Retains OfficeScan agent's exclusion list

10.2. Scan Exclusion list (Files)

- Retains OfficeScan agent's exclusion list

11. Configure the Action tab
12. Virus/Malware > Use a specific action for each virus/malware type:

    12.1. Joke: Quarantine

    12.2. Trojans: Quarantine

    12.3. Virus: Clean & Quarantine

    12.4. Test Virus: Quarantine

    12.5. Packer: Quarantine

    12.6. Probable Malware: Quarantine

    12.7. Other Malware: Clean & Quarantine

13. Back up files before cleaning
14. Damage Cleanup Services

    14.1. Cleanup type: Advanced cleanup

    14.2. Enable > Run cleanup when probable virus/malware is detected

15. Spyware/Grayware > Clean: OfficeScan terminates processes or delete registries, files, cookies and shortcuts.

1.3 > Configuring Real-time Scan Settings

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**
3. Select the group/domain you wish to apply the settings to
4. Click on **Settings** > **Scan Settings** >> **Real-time Scan Settings**
5. Enable virus/malware scan and Enable spyware/grayware scan
6. Configure the Target tab.
7. User Activity on Files > Scan files being: created/modified and retrieved
8. Files to Scan > All Scannable files
9. Scan Settings >

    9.1. Scan network drive

    9.2. Scan the boot sector of the USB storage device after plugging in

    9.3. Scan all files in removable storage device after plugging in

    9.4. Quarantine malware variants detected in memory

9.5. Scan compressed files

9.6. Scan OLE objects

- Detect exploit code in OLE files

10. Virus/Malware Scan Settings Only > Enable Intellitrap
11. Enable CVE exploit scanning for files downloaded through web and email channels
12. Configure Scan Exclusion Tab > Enable scan exclusion

12.1. Scan Exclusion list (Directories)

- Exclude directories where Trend Micro products are installed
- Retains OfficeScan agent's exclusion list

12.2. Scan Exclusion list (Files)

- Retains OfficeScan agent's exclusion list

13. Configure the Action tab
14. Virus/Malware > Use a specific action for each virus/malware type:

14.1. CVE exploit: Quarantine

14.2. Joke: Quarantine

14.3. Trojans: Quarantine

14.4. Virus: Clean & Quarantine

14.5. Test Virus: Quarantine

14.6. Packer: Quarantine

14.7. Probable Malware: Quarantine

14.8. Other Malware: Clean & Quarantine

15. Back up files before cleaning
16. Damage Cleanup Services

16.1. Enable > Run cleanup when probable virus/malware is detected

17. Spyware/Grayware > Clean: OfficeScan terminates processes or delete registries, files, cookies and shortcuts.

1.4 > Configuring Scheduled Scan Settings

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**
3. Select the group/domain you wish to apply the settings to
4. Click on **Settings** > **Scan Settings** >> **Scheduled Scan Settings**
5. Enable virus/malware scan and Enable spyware/grayware scan

6. Configure the Target tab
7. Configure the Schedule scan to run at least once a week.
8. Files to Scan > All Scannable files
9. Scan Settings >
   9.1. Scan compressed files
   9.2. Scan OLE objects
   - Detect exploit code in OLE files
10. Virus/Malware Scan Settings Only > Scan boot area
11. CPU Usage > Medium: pause slightly between file scans
12. Scan Exclusion > Enable scan exclusion
    12.1. Scan Exclusion list (Directories)
    - Exclude directories where Trend Micro products are installed
    - Retains OfficeScan agent's exclusion list Scan Exclusion list (Files)
    - Retains OfficeScan agent's exclusion list
13. Configure the Action tab
14. Virus/Malware > Use a specific action for each virus/malware type:
    14.1. Joke: Quarantine
    14.2. Trojans: Quarantine
    14.3. Virus: Clean & Quarantine
    14.4. Test Virus: Quarantine
    14.5. Packer: Quarantine
    14.6. Probable Malware: Quarantine
    14.7. Other Malware: Clean & Quarantine
15. Back up files before cleaning
16. Damage Cleanup Services
    16.1. Cleanup type: Advanced cleanup
    16.2. Enable > Run cleanup when probable virus/malware is detected
17. Spyware/Grayware > Clean: OfficeScan terminates processes or delete registries, files, cookies and shortcuts.

1.5 > Configuring Scan Now Settings

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**

3. Select the group/domain you wish to apply the settings to
4. Click on **Settings** > **Scan Settings** >> **Scan Now Settings**
5. Enable virus/malware scan and Enable spyware/grayware scan
6. Configure the Target tab
7. Files to Scan > All Scannable files
8. Scan Settings

   8.1. Scan compressed files

   8.2. Scan OLE objects

   - Detect exploit code in OLE files

9. Virus /Malware Scan Settings Only > Scan boot area
10. CPU Usage > **Medium**: pause slightly between file scans
11. Scan Exclusion > Enable scan exclusion

    11.1. Scan Exclusion list (Directories)

    - Exclude directories where Trend Micro products are installed
    - Retains OfficeScan agent's exclusion list

    11.2. Scan Exclusion list (Files)

    - Retains OfficeScan agent's exclusion list

12. Configure the Action tab
13. Virus/Malware > Use a specific action for each virus/malware type:

    13.1. Joke: Quarantine

    13.2. Trojans: Quarantine

    13.3. Virus: Clean & Quarantine

    13.4. Test Virus: Quarantine

    13.5. Packer: Quarantine

    13.6. Probable Malware: Quarantine

    13.7. Other Malware: Clean & Quarantine

14. Back up files before cleaning
15. Damage Cleanup Services

    15.1. Cleanup type: Advanced cleanup

    15.2. Run cleanup when probable virus/malware is detected

16. Enable Spyware/Grayware > Clean: OfficeScan terminates processes or delete registries, files, cookies and shortcuts.

1.6 > Table Summary

	Real-time Scan	Manual Scan	Scheduled Scan	Scan Now
Files to scan	All Scannable	All Scannable	All Scannable	All Scannable
Scan hidden folders		✓		
Scan network drive	✓	✓		
Scan boot sector of USB storage device after plugging in	✓			
Scan all files in removable storage devices after plugging in	✓			
Quarantine malware variants detected in memory	✓			
Scan compressed files	✓	✓	✓	✓
Scan OLE objects	✓	✓	✓	✓
Detect exploit code in OLE files	✓	✓	✓	✓
Enable Intellitrap	✓			
Scan boot area		✓	✓	✓
CPU usage		Medium	Medium	Medium
Cleanup type for Damage Cleanup Services		Advanced Cleanup	Advanced Cleanup	Advanced Cleanup
Run cleanup for probable virus	✓	✓	✓	✓
Clean action for detected Spyware	✓	✓	✓	✓

1.7 > Enable Web Reputation

Web Reputation Service (WRS) allows OfficeScan to detect and block access to sites that harbor Web-based threats. When an agent requests a URL, it first checks the "reputation score" of the URL by querying the Trend Micro reputation servers. Access to the URL is then allowed or denied depending on the score and the security level you configured.

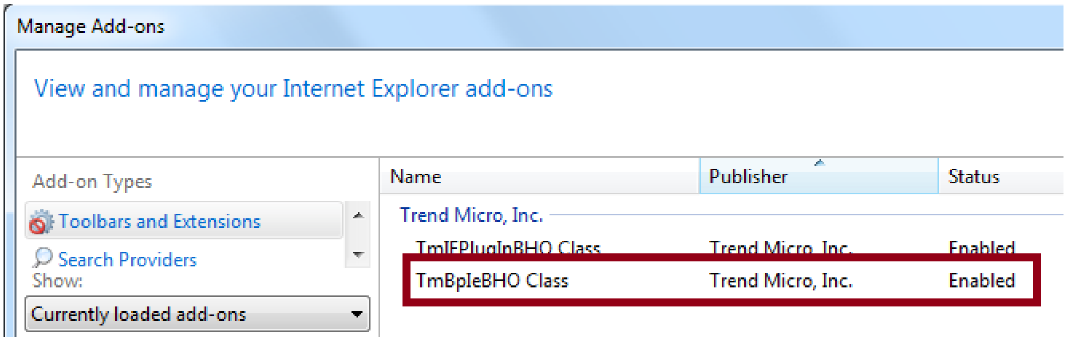
To configure WRS, please do the following:

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**
3. Select the group/domain you wish to apply the settings to
4. Click **Settings** and select **Web Reputation Settings**
5. For both External and Internal Agents, Enable **Web Reputation Policy**
6. Enable **Check HTTPS URLs**
7. Select the **Medium** security level for the policy.
8. Browser Exploit Prevention > **Enable Block pages containing malicious script**
9. Approved/Block URL list

   You may add the URLs of the Web sites you want to approve or block. By default, Trend Micro and Microsoft Web sites are included in the Approved list.

10. Select whether to allow agents to send logs to the OfficeScan server. You can use this option to **analyze URLs blocked by WRS.**
11. **Click Apply to All Agents**.

In Internet Explorer, enable TmBpIeBHO Class.



Name	Publisher	Status
Trend Micro, Inc.		
TmIEPlugInBHO Class	Trend Micro, Inc.	Enabled
TmBpIeBHO Class	Trend Micro, Inc.	Enabled

Figure 4 Enabled TmBpIeBHO Class

1.8 > Configure Global C&C Callback Settings

Administrators can configure OfficeScan to log all connections between agents and confirmed C&C IP addresses. The Trend Micro Command & Control (C&C) Contact Alert Services provides enhanced detection and alert capabilities to mitigate the damage caused by Advanced Persistent Threats (APT) and targeted attacks.

These are the steps on how to do it:

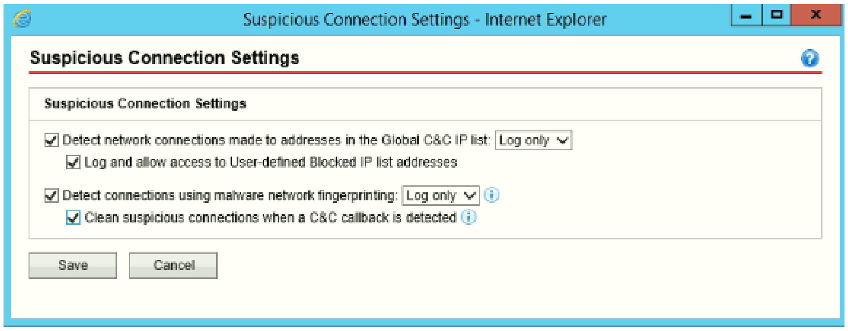
1. Navigate to **Agents** > **Agent Management**
2. Select the group/domain you wish to apply the settings to
3. Click on **Settings** > **Suspicious Connection Settings**
4. Enable the following:

Log network connections made to addresses in the Global C&C IP list

Log and allow access to User-defined Blocked IP list addresses

Log connections using malware network fingerprinting

Clean suspicious connections when a C&C callback is detected



Suspicious Connection Settings - Internet Explorer

Suspicious Connection Settings

Suspicious Connection Settings

☑ Detect network connections made to addresses in the Global C&C IP list: Log only

☑ Log and allow access to User-defined Blocked IP list addresses

☑ Detect connections using malware network fingerprinting: Log only

☑ Clean suspicious connections when a C&C callback is detected

5. Click **Apply to All Agents**. Click **Close**.
6. Click on **Settings > Additional Service Settings**
7. Under **Suspicious Connection Service**, select **Enable service on the following operating systems**
8. Click **Apply to All Agents,** then Click **Close**.

1.9 > Enable Smart Feedback

The Trend Micro Smart Protection Network provides a feedback mechanism to minimize the effort of threats harvesting, analysis and resolving. It not only helps increase the detection rate but also provides a quick real-world scenario. It also benefits customers to help ensure they get the latest protection in the shortest possible time.

To configure Smart Feedback, please do the following:

1. On the OfficeScan Server, login to the Management Console
2. Click **Administration > Smart Protection >> Smart Feedback**
3. Check Enable **Trend Micro Smart Feedback** option box
4. Click **Save**.

1.10 > Enable Behavior Monitoring/Ransomware Protection Feature

OfficeScan constantly monitors computers (or endpoints) for unusual modifications to the operating system or on installed software.

Administrators (or users) can create exception lists that allow certain programs to start despite violating a monitored change, or completely block certain programs. In addition, programs with a valid digital signature or have been certified are always allowed to start.

To configure Behavior Monitoring and Ransomware Protection features, please do the following:

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management** > **Settings** > **Behavior Monitoring Settings**

Malware behavior blocking

Malware Behavior Blocking provides a necessary layer of additional threat protection from programs that exhibit malicious behavior. It observes system events over a period of time. As programs execute different combinations or sequences of actions, Malware Behavior Blocking detects known malicious behavior and blocks the associated programs. Use this feature to ensure a higher level of protection against new, unknown, and emerging threats.

- Check to enable **Malware Behavior Blocking**
- Under **Threats to block:** Recommend to select **Known and potential threats**

Ransomware Protection

Ransomware Protection prevents the unauthorized modification or encryption of files on OfficeScan agents by "ransomware" threats. Ransomware is a type of malware which restricts access to files and demands payment to restore the affected files.

- Check enable **Protect documents against unauthorized encryption or modification**
- Check enable **Automatically backup and restore files changed by suspicious programs**
- Check enable **Block processes commonly associated with ransomware**

> NOTE 🗎 To reduce the chance of OfficeScan detecting a safe process as malicious, ensure that the agent has internet access to perform additional verification processes using Trend Micro servers.

- Check enable **Enable program inspection to detect and block compromised executable files.**

```
NOTE 🗎 Program inspection provides increased security if you select
"Known and potential threats" in the Threats to block drop-down.
```

Anti-Exploit Protection

Anti-exploit protection works in conjunction with program inspection to monitor the behavior of programs and detect abnormal behavior that may indicate that an attacker has exploited program vulnerability. Once detected, Behavior Monitoring terminates the program processes.

- Check enable **Terminate programs that exhibit abnormal behavior associated with exploit attacks**

```
NOTE 🗎 Anti-exploit Protection requires that you select Enable program
inspection to detect and block compromised executable files.
```

Newly Encountered Programs

Trend Micro classifies a program as newly encountered based on the number of file detections or historical age of the file determine by the Smart Protection Network

- Check enable **Monitor newly encountered programs downloaded through HTTP or email applications**

Recommended to select **Prompt user**

```
NOTE 🗎 This notification requires that Administrators enable Real-time
Scan and Web Reputation.
```

3. On the bottom of the window, click **Save.**

1.11 > Enable Predictive Machine Learning

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features.

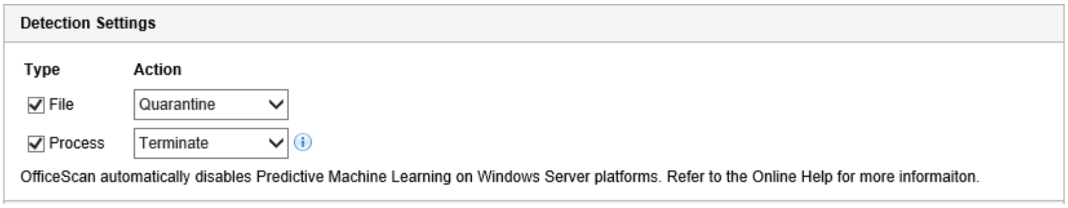
Predictive Machine Learning also performs a behavioral analysis on unknown or low-prevalence processes to determine if an emerging or unknown threat is attempting to infect your network.

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

To enable Predictive Machine Learning Feature, please do the following;

1. On the OfficeScan Server, log-in to Management Console.
2. Go to **Agents** > **Agent Management** > **Settings** > **Predictive Machine Learning Settings**
3. Check **Enable Predictive Machine Learning**

4. Under **Detection Settings**, select the following;



Detection Settings

Type	Action
☑ File	Quarantine
☑ Process	Terminate

OfficeScan automatically disables Predictive Machine Learning on Windows Server platforms. Refer to the Online Help for more informaiton.

- Select to automatically **Quarantine** files that exhibit malware-related features based on the Predictive Machine Learning analysis

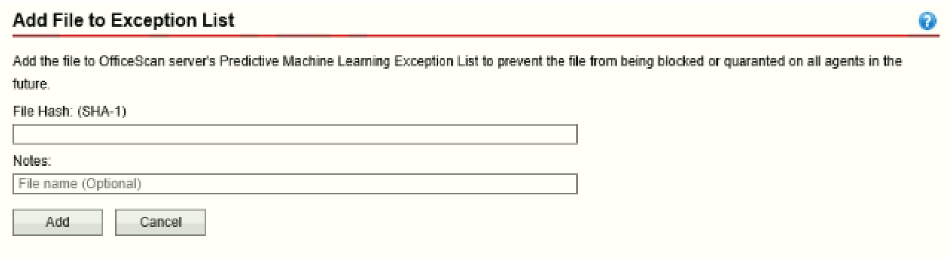
- Select to automatically **Terminate** processes that exhibit malware-related behaviors based on the Predictive Machine Learning analysis

Note: Predictive Machine Learning attempts to clean the files that executed the malicious processes. If the clean action is unsuccessful, OfficeScan quarantines the affected files.

5. Under **Exceptions**, configure the global Predictive Machine Learning file exceptions to prevent all agents from detecting a file as malicious.

a. Click **Add** File Hash.

The Add File to Exception List screen appears.



Add File to Exception List

Add the file to OfficeScan server's Predictive Machine Learning Exception List to prevent the file from being blocked or quaranted on all agents in the future.

File Hash: (SHA-1)

Notes:

File name (Optional)

b. Specify the file SHA-1 hash value to exclude from scanning.
c. Optionally provide a note regarding the reason for the exception or to describe the file name(s) associated with the hash value.

d. Click **Add**.

OfficeScan adds the file hash to the Exceptions list.

6. On the bottom of the window, click **Save.**

1.12 > Enable Sample Submission Feature

You can configure OfficeScan agents to submit file objects that may contain previously unidentified threats to a Virtual Analyzer for further analysis. After assessing the objects, Virtual Analyzer adds any objects found to contain unknown threats to the Virtual Analyzer Suspicious lists and distributes the lists to other OfficeScan agents throughout the network.

Sample Submission Feature requires the following:

- You must register the OfficeScan server with TrendMicro Control Manager server (6.0 Sp3 patch 2 or later)
- You must subscribed Suspicious Object List Settings
- The Trend Micro Control Manager server must have an active connections to a Trend Micro Deep Discovery Analyzer server (5.1 or later)
- Configure OfficeScan to add Deep Discovery Analyzer Server information and its API Key.

1.12.1 Registering OfficeScan to Control Manager

1. Go to **Administration** > **Settings** > **Control Manager**
2. Specify the entity display name, which is the name of the OfficeScan server that will display in Control Manager.

   By default, entity display name includes the server computer's host name and this product's name (for example, Server01_OfficeScan).

   > NOTE 🗎 In Control Manager, OfficeScan servers and other products managed by Control Manager are referred to as "entities"

3. Specify the Control Manager server FQDN or IP address and the port number to use to connect to this server. Optionally connect with increased security using HTTPS.
   - For a dual-stack OfficeScan server, type the Control Manager FQDN or IP address (IPv4 or IPv6, if available).
   - For a pure IPv4 OfficeScan server, type the Control Manager FQDN or IPv4 address.
   - For a pure IPv6 OfficeScan server, type the Control Manager FQDN or IPv6 address

   > NOTE 🗎 Only Control Manager 5.5 SP1 and later versions support IPv6.

4. If the IIS web server of Control Manager requires authentication, type the user name and password.
5. If you will use a proxy server to connect to the Control Manager server, specify the following proxy settings:
   - Proxy protocol
   - Server FQDN or IPv4/IPv6 address and port
   - Proxy server authentication user ID and password
6. Decide whether to use one-way communication or two-way communication port forwarding, and then specify the IPv4/IPv6 address and port.

7. To check whether OfficeScan can connect to the Control Manager server based on the settings you specified, click **Test Connection**

   Click **Register** if a connection was successfully established.

8. If the Control Manager server is version 6.0 SP1 or later, a message appears prompting you to use the Control Manager server as the update source for the OfficeScan integrated Smart Protection Server. Click **OK** to use the Control Manager server as the integrated Smart Protection Server update source or **Cancel** to continue using the current update source (by default, the ActiveUpdate server).

9. If you change any of the settings on this screen after registration, click **Update Settings** after changing the settings to notify the Control Manager server of the changes.

10. If you no longer want the Control Manager server to manage OfficeScan, click **Unregister**.

1.12.2 Configuring Suspicious Object List Settings

To enable Suspicious Objects List Settings, please do the following;

1. Go to **Administration** > **Settings** > **Suspicious Object List.**

2. Select which list to enable on agents.

   - Suspicious URL List

   - Suspicious IP List (only available when subscribing to the registered Control Manager server)

   - Suspicious File List (only available when subscribing to the registered Control Manager server)

   Administrator can manually synchronize the Suspicious Object lists at any time by clicking the **Sync Now** button.

3. In the **Agent Update Settings** section, specify when agents update the Suspicious Object lists.

   - **Notify OfficeScan agents based on the agent component update schedule.** OfficeScan agents update the Suspicious Objects lists based on the current update schedule.

   - **Automatically notify OfficeScan agents after updating the Suspicious Objects on the server.** OfficeScan agents automatically update the Suspicious Object lists after the OfficeScan server receives updated lists.

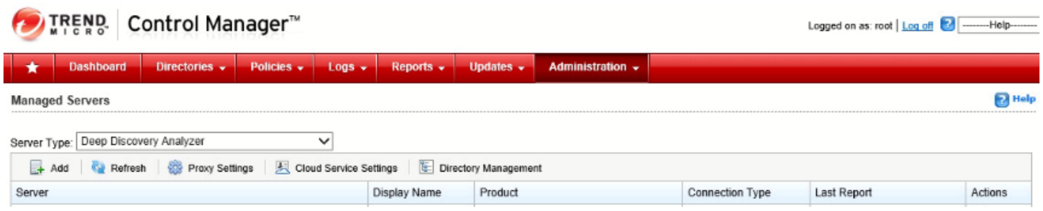
   > NOTE 🗎 OfficeScan agents not configured to receive update from Update Agents perform incremental updates of the subscribe Suspicious Object lists during synchronization.

4. Click **Save.**

1.12.3 Adding Deep Discovery Analyzer to Control Manager

To add Deep Discovery Analyzer to Control Manager, please do the following;

1. On the Control Manager Server console >Go to **Administration** > Select **Manager Server**

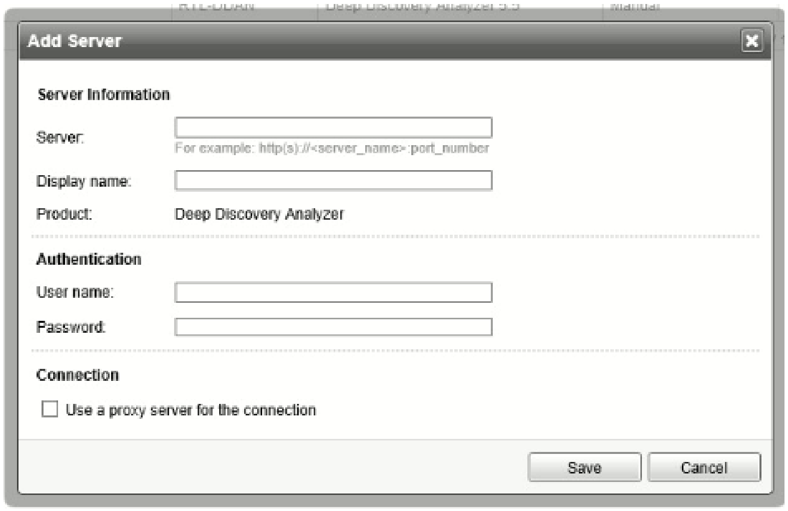


Managed Servers

Server Type: Deep Discovery Analyzer

Server	Display Name	Product	Connection Type	Last Report	Actions

2. Click **Add,** and **Add server** window will appear.



Server Information

Server: For example: http(s)://<server_name>:port_number

Display name:

Product: Deep Discovery Analyzer

Authentication

User name:

Password:

Connection

☐ Use a proxy server for the connection

3. Enter the Deep Discovery Analyzer **Server Information**

4. Click **Save**

1.12.4 Enabling Sample Submission Feature

To enable Sample Submission Feature, please do the following;

1. Log-in to OfficeScan Management Console

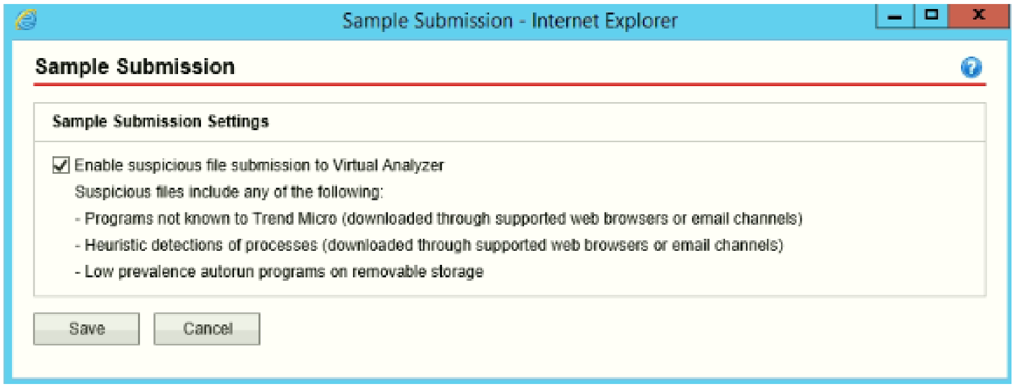
2. Go to **Agents** > **Agent Management**

3. Select the group/domain you wish to apply the settings to

4. Select **Sample Submission**

5. **Sample Submission Settings** will appear.

6. Select to **Enable suspicious file submission to Virtual Analyzer**



Sample Submission - Internet Explorer

Sample Submission

Sample Submission Settings

☑ Enable suspicious file submission to Virtual Analyzer

Suspicious files include any of the following:

- Programs not known to Trend Micro (downloaded through supported web browsers or email channels)
- Heuristic detections of processes (downloaded through supported web browsers or email channels)
- Low prevalence autorun programs on removable storage

7. Click **Save**

1.13 > Configure Global Agent Settings

Advance settings that will apply to all the OfficeScan agents on your network.

To configure Global Agent Settings, please do the following:

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Global Agent Settings**
3. Under **System** tab > Go to **Service Restart** area
4. Select to **Automatically restart any OfficeScan agent service if the service terminates unexpectedly.**
5. Click **Save**.

1.14 > Configure Agent Self-protection

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**
3. Select the group/domain to apply the settings
4. Click **Settings** and select **Privileges and Other Settings**
5. Click **Other Settings** tab
6. Enable all Agent Self-protection
   - 6.1. Protect OfficeScan agent services
   - 6.2. Protect files in the OfficeScan agent installation folder
   - 6.3. Protect OfficeScan agent registry keys
   - 6.4. Protect OfficeScan agent processes
7. Click **Apply to All Agents**. Click **Close**.

1.15 > Configure Device Control

Device Control provides control feature that regulates access to external storage devices and network resources connected to computers. It helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

By default, Device Control feature is enabled but ALL devices have FULL ACCESS. Block AutoRun functions on USB devices are also enabled.

1. On the OfficeScan Server, login to the Management Console
2. Go to **Agents** > **Agent Management**
3. Select the group/domain you wish to apply the settings to
4. Click **Settings** and select **Device Control Settings**
5. Check **Enable Device Control** for both External and Internal Agents
6. Enable **Block the AutoRun function on USB storage devices**

1.15.1 Permissions for Storage Devices

- Allow access to USB storage devices, CD/DVD, floppy disks, and network drives. You can grant full access to these devices or limit the level of access. Limiting the level of access brings up "Program lists" which allows programs on storage devices to have Modify, Read and execute, Read and List device content only.

- Configure the list of approved USB storage devices. Device Control allows you to block access to all USB storage devices, except those that have been added to the list of approved devices. You can grant full access to the approved devices or limit the level of access.

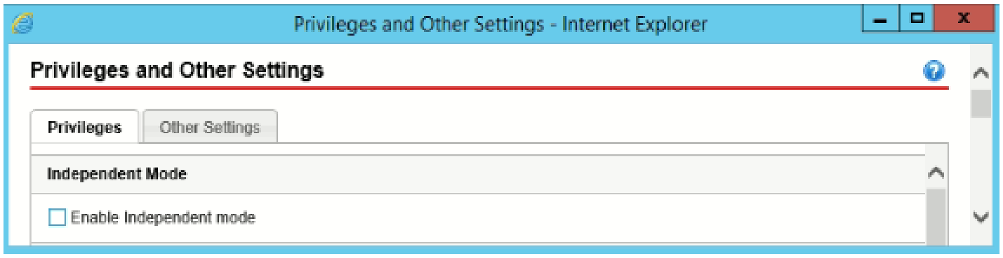
Configure the settings according to your preference.

1.16 > Disabling Independent Mode for Machines in the Network

Trend Micro recommends disabling Independent mode for the machines that are in the Local Area Network.

1. Login to the OfficeScan Management Console

2. Go to **Agents** > **Agent Management**
3. Select the group/domain you wish to apply the settings to
4. Click **Settings** > **Privileges and Other Settings**
5. On the **Privileges** tab >**Independent Mode**



Privileges and Other Settings

Independent Mode

□ Enable Independent mode

6. Uncheck **Enable Independent mode** option if enabled for LAN machines. Otherwise, leave it as is.

1.17 > Install Intrusion Defense Firewall (IDF) plug-in

```
NOTE 🗎 Intrusion Defense Firewall (IDF) is part of the OfficeScan plug-
in manager.  This requires a new activation code. Please contact sales to
obtain a license.
```

↳ More information can be found **here**.

1. Login to the OfficeScan Management Console
2. Click **Plug-ins**
3. Under **Intrusion Defense Firewall**, click Download

1.18 > Anti-threat Tool Kit

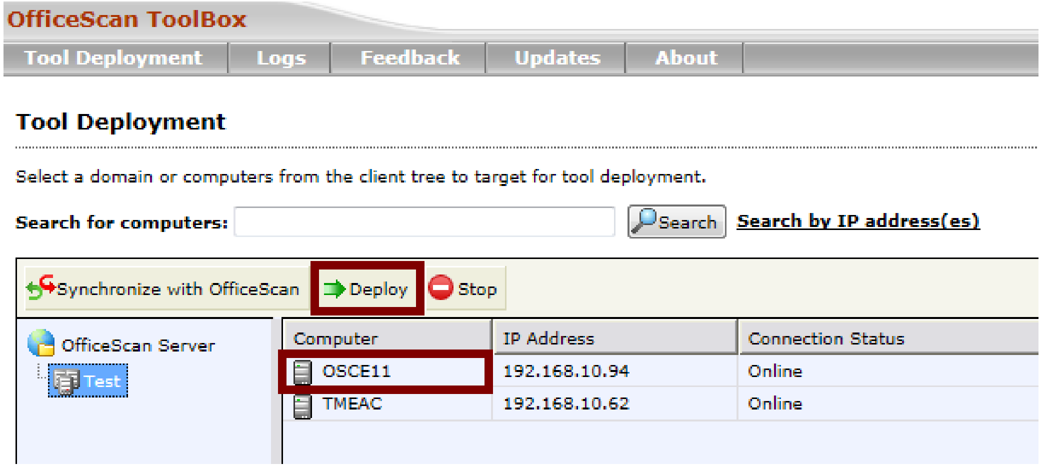
Trend Micro Anti-Threat Toolkit (ATTK) is a collection of tools including general on-demand scanner, suspicious file collector, specific malware cleaner, etc. The on-demand scanner supports both online and offline detection and removal of viruses, Trojans, worms, unwanted browser plugins, and other malware.

The ATTK Tool can be deployed via the OfficeScan toolbox for ease and convenience. Alternatively, it can be downloaded from https://spnsupport.trendmicro.com/

1.19 > Install OfficeScan ToolBox plug-in

OfficeScan Toolbox manages, deploys, executes, and consolidates logs for a variety of standalone Trend Micro tools.

1. Login to the OfficeScan Management Console
2. Click **Plug-ins**
3. Under **Trend Micro OfficeScan ToolBox**, download and install the plug-in
4. After installing the plug-in, click **Manage Program** to access the OfficeScan ToolBox console.
5. Select which OfficeScan agents to deploy the Anti-Threat Tool Kit (ATTK) package then click **Deploy**.



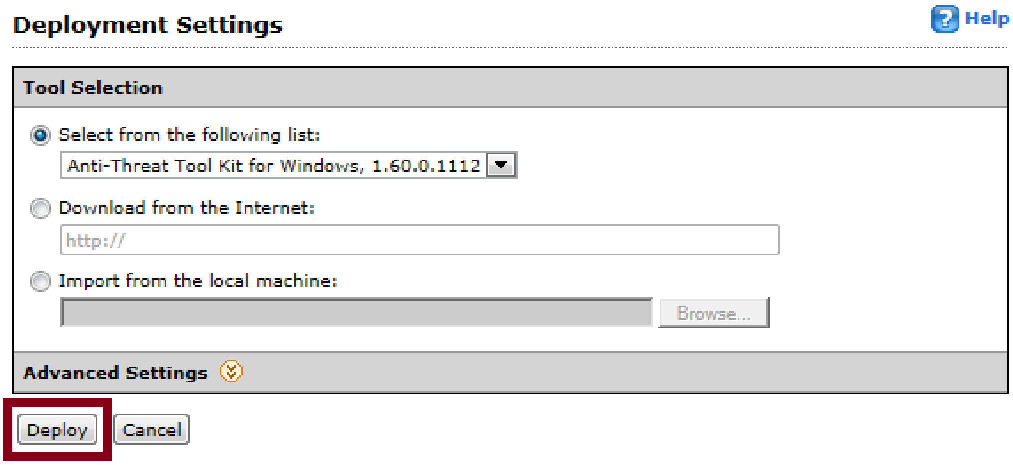
Tool Deployment

Select a domain or computers from the client tree to target for tool deployment.

Search for computers:

Computer	IP Address	Connection Status
OSCE11	192.168.10.94	Online
TMEAC	192.168.10.62	Online

6. On the Deployment Settings window, the ATTK toolkit is already selected by default. Click **Deploy**.



Deployment Settings

Tool Selection

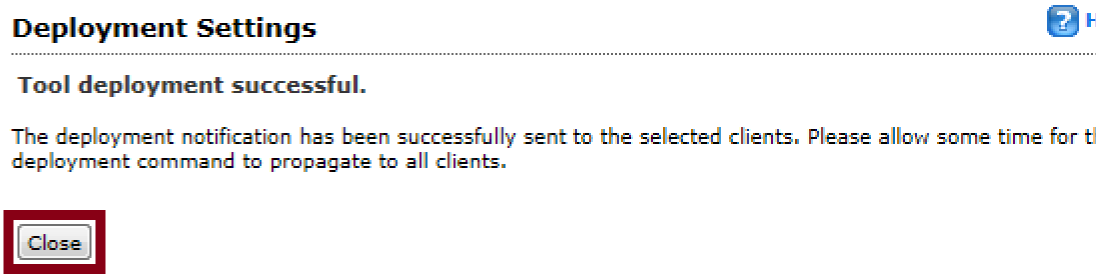
● Select from the following list:
Anti-Threat Tool Kit for Windows, 1.60.0.1112

○ Download from the Internet:
http://

○ Import from the local machine:

Advanced Settings

7. A confirmation that the tool deployment is successful will appear. The ATTK package will be deployed on the agent in a few minutes.

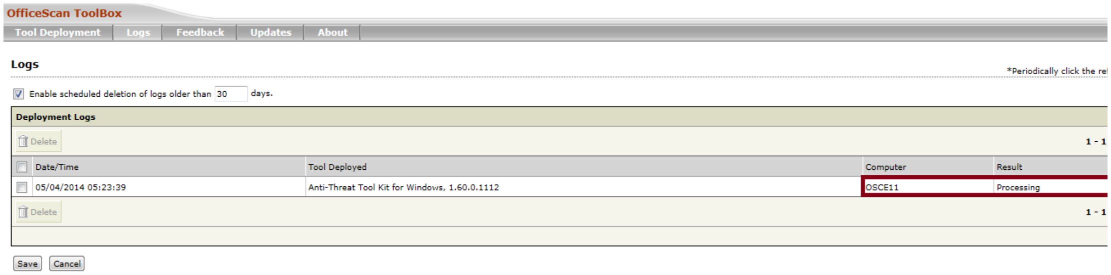


Deployment Settings

Tool deployment successful.

The deployment notification has been successfully sent to the selected clients. Please allow some time for t deployment command to propagate to all clients.

8. On the Logs tab, the ATTK deployment is being processed appears.



Logs

*Periodically click the re

☑ Enable scheduled deletion of logs older than 30 days.

Deployment Logs

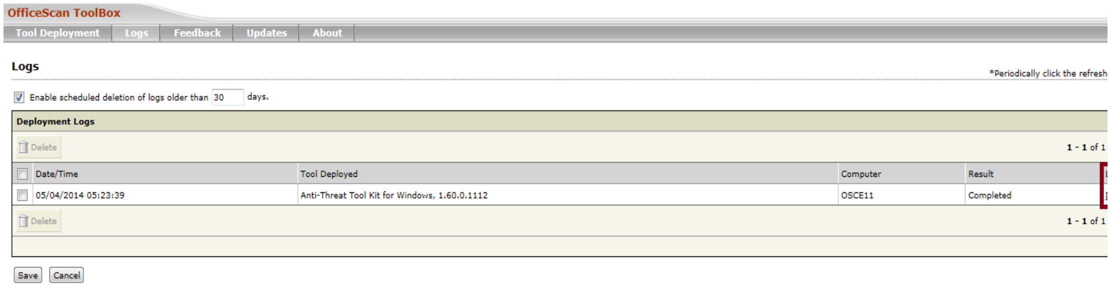
1 - 1

□	Date/Time	Tool Deployed	Computer	Result
□	05/04/2014 05:23:39	Anti-Threat Tool Kit for Windows, 1.60.0.1112	OSCE11	Processing

1 - 1

9. Once the deployment is finished, it will indicate on the Tool Deployment page that it is complete.

10. Go to the Logs tab and the result would be **Completed**. The file can be downloaded and sent to Trend Micro Technical Support for analysis.



Logs

*Periodically click the refresh

☑ Enable scheduled deletion of logs older than 30 days.

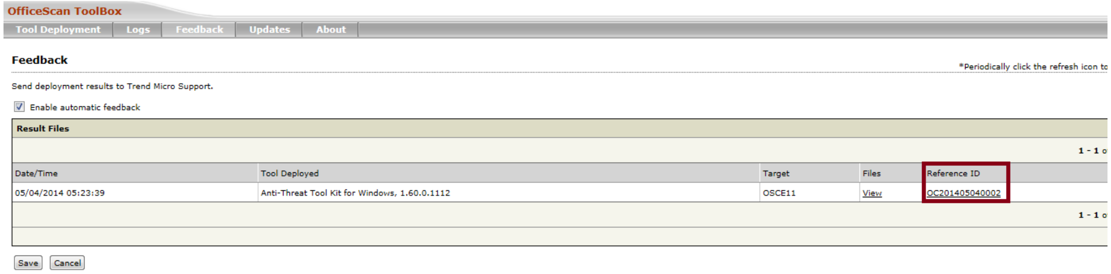
Deployment Logs

1 - 1 of 1

□	Date/Time	Tool Deployed	Computer	Result
□	05/04/2014 05:23:39	Anti-Threat Tool Kit for Windows, 1.60.0.1112	OSCE11	Completed

1 - 1 of 1

11. The Feedback tab can be accessed and send the Reference ID to Trend Micro Technical Support for analysis.



Feedback

*Periodically click the refresh icon to

Send deployment results to Trend Micro Support.

☑ Enable automatic feedback

Result Files

1 - 1 o

Date/Time	Tool Deployed	Target	Files	Reference ID
05/04/2014 05:23:39	Anti-Threat Tool Kit for Windows, 1.60.0.1112	OSCE11	View	OC201405040002

1 - 1 o

1.20 > Using the Security Compliance

Security Compliance allows you to detect agent computers that do not have antivirus software installed within your network environment, by scanning your Active Directory Scope and connecting to port(s) used by OfficeScan server(s) to communicate with the OfficeScan agents.

Security Compliance can then install the OfficeScan agent on unprotected computers.

1. Login to the OfficeScan Management Console
2. Click on **Assessment > Unmanaged Endpoints**
3. In line with **Active Directory Scope / IP Address Scope**, click **Define Scope** button
4. If you have more than one (1) OfficeScan server, click the link for **Specify Ports** under
5. A**dvanced Settings** then click **Save**.
6. Click **Save and Reassess**.
7. The assessment result of the machines within your Active Directory Scope appears. Highlight the machines you wish and click **Install** to deploy OfficeScan agent program to them.

NOTE 🗎 • If more than one (1) OfficeScan servers installed within the environment, specify each communication port being used by OfficeScan agents to connect to the respective OfficeScan server.

•This feature can only validate machines with OfficeScan agent software installed. If a machine is running other anti-virus program, assessment will return a BLANK result for the queried

NOTE 🗎 The suggested solutions are not OfficeScan specific but are helpful in maintaining a secure network.

1.21 > Disable System Restore

1. In Active Directory Users and Computers, navigate to Computer Configuration, Administrative Templates | System | System Restore.
2. Double-click "Turn off System Restore," set it to Enabled. Click OK.
3. Close the policy and exit Active Directory Users and Computers.
4. The changes will take effect on the next policy refresh.

1.22 > Disable Autorun

1. Click **Start** then **Run**
2. Type “GPEDIT.MSC” then press **Enter**.
3. Go to Local Computer Policy | Administrative Template | System
4. On the right pane, double-click Turn off Autoplay
5. When you are in the properties dialog box, click enabled
6. Choose All drives from the drop-down list underneath.
7. Click **OK**.

1.23 > Run Microsoft Baseline Security Analyzer monthly

1.23.1 Check Unpatched PC

1. Download the tool on the link below

http://www.microsoft.com/en-us/download/details.aspx?id=7558

2. See more information on the link below

http://technet.microsoft.com/en-au/security/cc184924.aspx

1.24 > Educate users not to click on links they do not trust

Do not open suspicious links or files especially from instant messengers, emails from unidentified users and from pop-up windows.