Trend Micro OfficeScan

- What is Trend Micro OfficeScan?
- Features
- How Do I Get Trend Micro OfficeScan?
- What are the Licensing Rights?
  - Personally Owned Computers
  - Cloud Licensing
- What is the OfficeScan Management Console?
- Known Issues and Frequently Asked Questions
  - When attempting to install the OfficeScan client, there appears an error saying "Unable to upgrade the OfficeScan Agent. The installation package was created from an Trend Micro OfficeScan server that does not manage the agent installed on this endpoint."
  - Can OSX and Linux machines be managed in the same console as PCs?
  - Should we manually turn off the Windows Firewall?
  - What do the different Trend icons in the system tray mean?
  - Do I need to do anything special when deploying an image with the OfficeScan client on it?
  - Do I need to open any ports on my firewall in order for the Trend clients to communicate with the Trend server?
- External Links

What is Trend Micro OfficeScan?

Trend Micro OfficeScan is an antivirus program developed by Trend Micro. Enterprise Information Technology Services (EITS) provides OfficeScan to all departments who require anti-virus software. It is compatible with Windows and Mac OS. Trend Micro OfficeScan is available for UGA-owned computers only.

Features

- OfficeScan offers a conventional signature-based scan engine as well as a reputation-based in-the-cloud scanning. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment and significantly reduces the overall client footprint.
- Web Reputation blocks clients from known malicious sites.
- Intrusion Defense Firewall supplements highly effective OfficeScan client-level security with network-level Host Intrusion Prevention System (HIPS). Intrusion Defense Firewall acts as a virtual patch to shield vulnerabilities in Operating Systems and common client applications, delivering true zero-day protection from known and unknown threats.

How Do I Get Trend Micro OfficeScan?

Trend Micro OfficeScan can be obtained from the OfficeScan server directly - these links will always be the most updated version of the installer.

Windows:

- **64-bit (Recommended installer for both workstations and servers)**
- **32-bit (Not recommended unless the above installer fails)**

Mac OSX:

- **OSX Installer**
Note: OSX requires a special uninstaller to remove Trend. That uninstaller can be found here.

Linux:

ServerProtect for Linux 3 is available from TrendMicro for UGA owned machines running a Linux operating system (e.g. RHEL, SUSE, CentOS, Asianux). Linux clients can be downloaded directly from TrendMicro.

When you install any of the Linux products, you will be prompted for three items, one of which is the activation key. You will need to open a ticket with the EITS Help Desk to get this key. The other two items are:

- IP of the Control Manager: 128.192.1.100
- HTTP or HTTPS?: HTTPS

Once installation is complete, you can manage these clients locally.

What are the Licensing Rights?

Personally Owned Computers

Computers that are not owned by the University are not licensed to use our instance of OfficeScan. We do not recommend you pay for a personal antivirus software license as plenty of free options are available, such as Avira or Bitdefender.

Cloud Licensing

The University does not have a central license for cloud use, but departments are free to purchase Trend for their cloud deployments as needed. Trend has a page dedicated to Amazon AWS deployments here.

What is the OfficeScan Management Console?

DNLS and other departmental IT support staff may view policies for the agents installed on endpoints in their respective departments. They may also create reports for security events that have occurred within their domain. Staff members who have not yet done so can obtain access to the OfficeScan management console by making a request to the InfoSec Office via Team Dynamix.

Note: When requesting access staff will need to include their department. If this is the first user for a given department, IP addresses (or IP address ranges) will need to be included as well.

Known Issues and Frequently Asked Questions

When attempting to install the OfficeScan client, there appears an error saying "Unable to upgrade the OfficeScan Agent. The installation package was created from an Trend Micro OfficeScan server that does not manage the agent installed on this endpoint."

- You will need to uninstall the client that is already installed on that machine before you can install the newest client.
- If you are running OSX, you will need to uninstall the client using the uninstall package (see above).
- Users who upgraded to Windows 10 without first updating their installed OfficeScan agent may be unable to uninstall the program. In those cases, please contact the Office of Information Security (soc@uga.edu) and request the Trend Windows Uninstaller package.

Can OSX and Linux machines be managed in the same console as PCs?
No, they are managed through the Mac plugin manager in the OfficeScan admin console, and through the separate (local) Linux Server Protect console, respectively. Access to the Mac console is not available to DNLs and policies for such clients need to be created by us. You can put in a ticket with the EITS Help Desk to request configuration changes for these types of clients.

**Should we manually turn off the Windows Firewall?**

No. Currently the default setup is to use the Windows firewall. Per Trend's recommendation, this runs in conjunction with the Trend Intrusion Defense Firewall.

**What do the different Trend icons in the system tray mean?**

These icons are used in our setup:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon 1" /></td>
<td>The client can connect to a Smart Protection Server and/or the Smart Protection Network. All services work properly.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon 2" /></td>
<td>The client cannot connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is enabled and the client is still protected from viruses whose signatures exist locally to the client and from new viruses whose signatures are pushed out from the OfficeScan server.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon 3" /></td>
<td>The client cannot connect to an OfficeScan Server, but can connect to a Smart Protection Server and/or the Smart Protection Network. Real-time Scan is enabled and the client is still protected.</td>
</tr>
<tr>
<td><img src="image4.png" alt="Icon 4" /></td>
<td>The client cannot connect to an OfficeScan Server or a Smart Protection Server and/or the Smart Protection Network. The client is still protected from viruses whose signatures exist locally to the client.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Icon 5" /></td>
<td>If you are using Conventional Scan rather than SmartScan, you may see this icon which indicates that all components are up-to-date and services work properly.</td>
</tr>
</tbody>
</table>

**Do I need to do anything special when deploying an image with the OfficeScan client on it?**


You will need to download this executable to complete the above instructions: Trend Micro OfficeScan

**Do I need to open any ports on my firewall in order for the Trend clients to communicate with the Trend server?**

Yes. In order for the clients to reach the OfficeScan server, you'll need to allow traffic to 40.113.218.209 and 40.113.220.196 over port 443 (egress).
External Links

- Office of Information Security Homepage