Trend Micro OfficeScan

- What is Trend Micro OfficeScan?
- Features
- How Do I Get Trend Micro OfficeScan?
- What are the Licensing Rights?
  - University Computers
  - 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?
  - Can I create my own groups or sub-groups in the admin console?
  - Should we manually turn off the Windows Firewall?
  - Are there additional Trend features that can be installed or turned on?
  - What do the different Trend icons in the system tray mean?
  - Can I hide the Trend icon in the system tray?
  - Do the OfficeScan clients pull or are they pushed to?
  - How many Trend servers are there, and which ones do I need to use?
  - 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 departmental firewall in order for the Trend clients to communicate with the Trend server?
  - I am having issues running Windows 10 and Trend. Why is my computer running so slow?
- 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?

University Computers

Trend Micro OfficeScan is currently licensed for UGA-owned computers. Our license allows for IT departments to set up their own OfficeScan servers if they so desire, and to enable additional features that may not be installed by default in the campus-wide service. DNLS interested in creating their own instances of OfficeScan should submit a ticket to the EITS Help Desk.

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 can obtain access to the OfficeScan management console, which will allow them to configure options for the agents installed on endpoints in their respective departments. Staff can log in with their MyID username and password here (Make sure to choose the myid.uga.edu domain):

• https://antivirus.uga.edu:4343/officescan/

If you have never logged in to that page, you will need to request access by submitting a ticket to the EITS Help Desk. In your request, make sure to specify what department you work for. If you have endpoints that are not joined to the myid.uga.edu Active Directory domain, you will also need to include the IP ranges where those machines reside.

Note: Machines that are not joined to the myid.uga.edu Active Directory domain, and that are also not part of the general campus network, cannot be managed from this console even if those machines are on campus and can otherwise communicate with the network. For example, if you have a private network 10.0.0.0/8 behind a router that is doing NAT with a public address of 128.192.x.x, and the machines on that private network are not joined to the MyID directory, then the machines in the 10.0.0.0/8 range will not appear in the console. If you do not wish to change
these conditions, you will need to stand up your own OfficeScan server in order to manage endpoints in that scenario - please see "Licensing" above for more information.

**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 unable to uninstall the client because it is asking for a password to unload the agent first, type in "p@$$word".
- 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.

**Can I create my own groups or sub-groups in the admin console?**

Yes and no.

For computers joined to the MyID domain, their groupings in Trend are based on their Organizational Unit (OU) groupings in Active Directory (AD). If you would like to make different groupings with different settings, you will first need to create those OUs in AD and move the clients to the appropriate OU. It may take a few hours before Trend syncs with the new AD structure and for the OUs to replicate into the Trend client groups.

For computers that are not joined to the MyID domain, we have to create the groups for you and the groupings will need to be IP-based. Please open a ticket with the EITS Help Desk requesting a group to be made in Trend, and make sure to include what department you work for as well as all of the IP addresses of the clients that need to be in the group (if at all possible, please use consecutive IP addresses for members in a group).

**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.

**Are there additional Trend features that can be installed or turned on?**

Yes. Because we want to provide an installer that causes the least amount of interference to business process and does not risk interrupting critical systems, there are a number of features that are turned off by default. DNLs are free to turn on these features for their clients in the management console, and those options can be configured differently for each individual client or for entire AD OUs. Additional features that must be implemented at the server-level can still be implemented, but DNLs would need to stand up their own OfficeScan servers to do so (see Licensing above).
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="icon1.png" alt="Icon" /></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="icon2.png" alt="Icon" /></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="icon3.png" alt="Icon" /></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="icon4.png" alt="Icon" /></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="icon5.png" alt="Icon" /></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>

Can I hide the Trend icon in the system tray?

Yes. In the admin console, go to Networked Computers, Client Management, and select the group, sub-group, or client you want to apply this to. Then click Settings, Privileges and Other Settings, go to the Other Settings tab, and check “Do not allow users to access the client console from the system tray or Windows Start menu”.

Do the OfficeScan clients pull or are they pushed to?

Both. They pull signature updates, but any configuration changes or software updates are pushed to them.

How many Trend servers are there, and which ones do I need to use?

There are five: the main server is the OfficeScan server - antivirus.uga.edu - this is where the console resides and what does most of the updating. This is the only one you would need to access, as it contains the installation files and hosts the web console for client administration. The main server works with three Smart Protection servers that run the web reputation service, file reputation service, and load balances the signature updating with the OfficeScan server, as well as load balance with each other. The fifth server is the Control Manager. All the other servers point here for licensing and reporting.

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 departmental firewall in order for the Trend clients to communicate with the Trend server?

Yes. In order for the clients to be managed via the admin console, you’ll need to open ports 443, 5274, 8080 and 31525 for ingress to your clients from 128.192.1.2.

If you restrict egress traffic (not typical), you will also need to open those ports to 128.192.1.2, 128.192.11.144, 128.192.11.147, and 128.192.11.165.

I am having issues running Windows 10 and Trend. Why is my computer running so slow?

There have been many reported issues with the latest version of Windows Defender clashing with Trend Antivirus. If you are noticing your computer running abnormally slow and it appears as though both Trend Antivirus and Windows Defender are running you can disable Windows Defender via global policy by following the steps listed on this page: https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10#disable_windows_defender_globalpolicy

External Links

- Office of Information Security Homepage