About Trend Micro Web Protection Add-On

Trend Micro™ Web Protection Add-On is a thin client solution that complements existing antivirus solutions by providing a glimpse of some of Trend's leading-edge technologies. Trend Micro Web Protection Add-On includes Trend Micro Web Threat Protection and “in-the-cloud” bot behavior analysis capabilities.

Trend Micro Web Threat Protection monitors outbound Web requests to protect your computer against malicious threat payloads hosted on infiltrated or specially crafted Web sites. Web Threat Protection includes in-the-cloud bot behavior analysis capabilities that monitor your computer for suspicious behavior associated with bots. Bots can secretly take control of your computer for criminal purposes.

In addition, Trend Micro Web Threat Protection technology is designed to block access attempts to potentially malicious Web sites in real-time. If evidence of potential bot infection is detected, Trend Micro Web Protection Add-On will direct you to Trend Micro™ HouseCall™ for a full system scan and clean.

Trend Micro Web Protection Add-On is highly proactive because it is designed to intercept initial malware payload delivery at the earliest possible point of infection—“in the cloud”. The payload delivery does not reach and infect your computer. By intercepting malware “in the cloud”, the need for resource-intensive threat scanning and clean up on your computer is greatly reduced.

Using Web Protection Add-On

To take advantage of the features available with Web Protection Add-On your computer must be connected to the Internet. If your computer connects to the Internet through a home network, Web Protection Add-On can use your current network settings automatically. If you use a proxy server, configure proxy settings to use Web Protection Add-On.

Configuring Proxy Settings

Click **Settings** from the Web Protection Add-On main screen and click the **Proxy Settings** tab to configure proxy server settings.

*Note: You can specify a proxy server name or IP address in the **Proxy server** field.*

Configuring Security Settings

Click **Settings** from the Web Protection Add-On main screen to display the **Security Settings** screen.

The core protection features are configurable from the **Security Settings** tab. Configure Web Threat Protection Add-On to benefit from the protection provided by Web Threat Protection, Bot Scan, and notifications.

Web Threat Protection

Select this option to detect and block Web-based security risks like phishing scams based on a “reputation score”. Trend Micro calculates this score using heuristic analysis and a database of known threats. Two detection options and three protection levels determine whether Web Protection Add-On will allow or block access to a website.

Query Method

- Encrypted HTTP – This option queries the path/file level (HTTP) and encrypts all queries, making this the more secure option.
- DNS and Encrypted HTTP – This option increases query performance by querying the domain level (DNS) first and then the path/file level (HTTP). However, query results are sent in plain text. Encrypted HTTP is used if the DNS query is unsuccessful.

Protection Level

- High - Blocks a greater number of Web threats but increases the risk of false positives.
- Medium - Blocks most Web threats while keeping the false positive count low. This is the Trend Micro recommended protection level and also the default setting.
- Low - Blocks fewer Web threats but reduces the risk of false positives.

Bot Scan

Select this option to monitor your computer for suspicious activities. This feature regularly checks with an online service to identify behavior associated with bots.

- Monitor incoming HTTP requests – Select this feature to detect if a bot is receiving commands on your computer.
- Monitor SMTP traffic – Select this feature to detect if your computer has become an open relay and a bot is using your computer to send phishing or spam messages.
- Monitor IRC requests – Select this feature to detect if a bot is receiving commands on your computer.
- Monitor DNS queries – Select this option to detect if a bot is installed on your computer.

Display notifications when threats are detected

Select this option to display pop-up notifications to help you quickly take action against threats as they are detected.

Upgrading to the Latest Web Protection Add-On Version

Click **Settings** from the Web Protection Add-On main screen to display the **Security Settings** screen. Then, click **Update Now** to download the latest version of Web Protection Add-On.

Viewing Logs

Click **Logs** from the Web Protection Add-On main screen. Events are added every 15 seconds and are automatically deleted after 45 days. You can export log information to a CSV file by clicking the **Export to CSV** button.

Sending Feedback to Trend Micro

Click **Logs** from the Web Protection Add-On main screen and click the **Feedback** button at the bottom of this screen. You can select to send Trend Micro diagnostic information or proceed directly to the Feedback Web site.

Removing Web Threats and Bots

The Web Protection Add-On system tray icon changes to alert you when Web threats or bots are detected.

Web Protection Add-On will block access attempts to potentially malicious Web sites in real-time. If evidence of potential bot infection is detected, scan and clean your computer with an effective antivirus program to remove them.

To scan and clean your computer for free, visit HouseCall online. If you have an antivirus program installed, download the latest update and scan your computer.

System Requirements

Operating System:

- Microsoft™ Windows™ 2000 Professional/Server (with the latest Service Pack)
- Microsoft Windows XP Home or Professional (with the latest Service Pack)
- Microsoft Windows Vista (with the latest Service Pack) (32-bit versions only)
- Microsoft Windows 2003 Server
- Microsoft Windows Server 2008

Hardware:

- Intel™ Pentium™ 350MHz and above (Windows Vista requires at least Intel Pentium 800MHz)
- At least 128MB RAM (Windows Vista requires at least 512MB RAM)
- At least 250MB free disk space
- IPv4 Internet connection