1 Using Websense Web Endpoint

Endpoint User's Guide | Web Endpoint | Version 7.8.x

Your organization uses Websense® Web Endpoint to secure your workstation or laptop from inbound web threats. Your laptop is secured even when outside the corporate network.

This guide explains how to do the following:

- *View endpoint status*
- *Automatic temporary override*
- *Disable endpoint protection*
- *Diagnose system problems*

View endpoint status

Endpoint User's Guide | Web Endpoint | Version 7.8.x

Related topics:

- *Automatic temporary override*, page 2
- *Disable endpoint protection*, page 3
- *Diagnose system problems*, page 4

To view the status of Websense Web Endpoint for Windows, hover over the Web Endpoint icon in your task bar. Each icon serves as both a status indicator and an access point to additional diagnostic information. You'll see one of three possible icons:

Icon	Hover Text	Description
	Websense: Enabled	The Web Endpoint software is successfully configured, connectivity to the cloud service exists, and the cloud proxy auto-configuration or PAC file is correct and accessible.
	Websense: Override	The Websense cloud service cannot be reached. The Web Endpoint is automatically overridden. See *Automatic temporary override*.
	Websense: Disabled	This icon displays if your organization has allowed you to disable the endpoint and you then disable it. See *Disable endpoint protection*.

Important
Note that if you disable the Web Endpoint service, a reboot will always enable it.

If you see this icon,  , it means Data Endpoint is also installed. See the Data Endpoint User's Guide for more information on what this means and the features available to you via this icon.

Automatic temporary override

Related topics:

- *View endpoint status*, page 1
- *Disable endpoint protection*, page 3
- *Diagnose system problems*, page 4

When a network change or other event occurs that keeps the endpoint from reaching the cloud service, an automatic temporary override of the endpoint takes effect. This means the endpoint is temporarily not available.

Examples of network change events include the following:

- Changing from Wi-Fi to an Ethernet network connection

- Assigning a new IP address to your laptop
- Connecting to a virtual private network (VPN)

Endpoint override allows you to continue using the Internet even during technical difficulties (provided Internet access is available), although there will be no endpoint protection during this time.

When the endpoint is overridden and the endpoint cannot reach the cloud service, you can change the proxy settings on your endpoint client machine in Internet Explorer. This could be useful if you are using a client network and are positioned behind a proxy server or other network device that prevents access to Internet resources. Contact your system administrator for assistance with making this change.

Once connectivity to the cloud service resumes, the endpoint is automatically re-enabled.

Disable endpoint protection

Related topics:

- *View endpoint status*, page 1
- *Automatic temporary override*, page 2
- *Diagnose system problems*, page 4

Sometimes, it may be useful to manually disable the endpoint to troubleshoot issues with the assistance of your system administrator. Be aware that disabling the endpoint introduces possible vulnerabilities, because you are no longer receiving the protection provided by the Web Endpoint service.

If your organization allows you to disable the endpoint, when you right click the endpoint icon, you'll see the option to **Disable** it. Select **Disable** to disable the endpoint at any time.

Disabling the endpoint:

- Stops it from intercepting traffic and securing your workstation from web threats.
- Turns off anti-tampering controls, so that you can manually change your proxy auto-config (PAC) file settings in Internet Explorer.

If you disable the endpoint, it is a best practice to change your PAC file settings. If you don't, depending on your system configuration, you may see an authentication page asking for your username and logon credentials. Contact your system administrator for assistance with changing your PAC file settings.

To re-enable the endpoint, click **Enable**.

> **Important**
> Note that if you disable the Web Endpoint service, a reboot will always enable it.

Diagnose system problems

Endpoint User's Guide | Web Endpoint | Version 7.8.x

Related topics:

- *View endpoint status*, page 1
- *Automatic temporary override*, page 2
- *Disable endpoint protection*, page 3

Windows Web Endpoint offers a three-part Diagnostic Dialog that you can access by double-clicking any of the three possible endpoint status icons that display in the task bar. The Diagnostic Dialog provides information that can assist with troubleshooting if an endpoint machine is not behaving as expected.

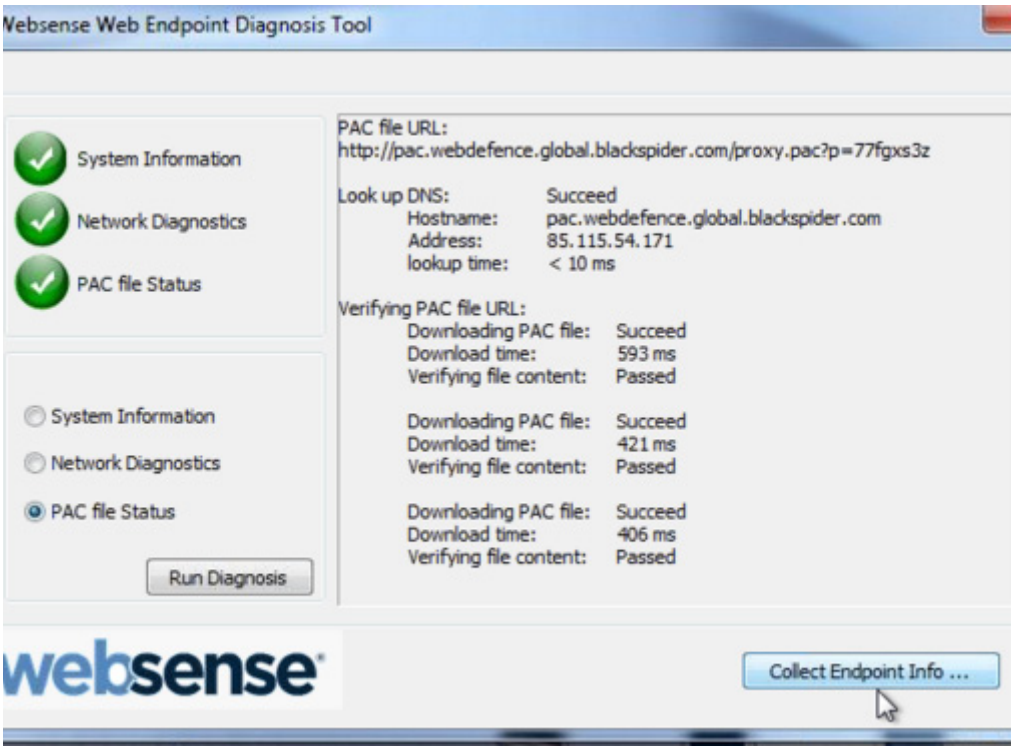
To access the Diagnostic Dialog, simply double-click on the endpoint status icon in the task bar.

When the dialog is launched, each of the diagnostic tests is executed in sequence. If one of the tests results in a failure, the subsequent tests are not automatically run.

Three diagnostic tests are accessed from this dialog:

1. **System Information** - collects basic information related to the specific system on which the endpoint software is installed
2. **Network Diagnostics** - collects information related to basic network connectivity
3. **PAC File Status** - collects information to determine if the PAC file is accessible

NOTE: Corresponding log files generated from these new diagnostics can easily be collected with the existing **CLIENTINFO.EXE** tool. Your Help Desk may ask you to run this tool to collect these files. To run it, click the **Collect Endpoint Info...** button on the diagnostics screen, as shown below.



The resulting file is placed onto the desktop. Attach the file to an email to Websense Technical Support or your authorized Websense Reseller.

For more information about the endpoint, contact your system administrator.