Installing and Deploying Web Endpoint

Websense Web Security Solutions | v7.8.x | Updated 29-Sept-2014

In this topic

Websense® Web Endpoint is a solution for securing endpoint client machines such as laptops from inbound Web-based threats when they are outside the corporate network.

Web Endpoint is a software application that runs on the endpoint client machine to block, monitor, and log transactions (like Internet requests) according to the organization's security and acceptable use policies. Administrators can create policies that provide full visibility into inbound and outbound traffic, but that don't restrict use of the endpoint machine.

This article describes how to install and deploy Web Endpoint client software.

A Data Endpoint client is also available. You can install it in combination with Web Endpoint client to prevent data loss from endpoint machines. See Combining Web and Data Endpoint Clients for more information.

Websense endpoint solutions include both server and client components. See *System requirements*, page 2, for information about the hardware requirements and supported operating systems for the Web Endpoint component.

Why Web Endpoint

In Websense Web Security Gateway Anywhere deployments, Websense Web Endpoint can be used to secure client machines whose Internet activity is managed by the hybrid service. Web Endpoint provides transparent authentication and enforces the use of hybrid web security policies.

Web Endpoint routes Internet requests to the hybrid service so that the appropriate web security policy can be applied.

- Web Endpoint redirects HTTP and HTTPS traffic to the hybrid service with an encrypted token that identifies the user, enabling the correct policy to be applied and reporting data to be correctly logged. No password or other security information is included.

  Web Endpoint can be used with both full-tunnel and split-tunnel VPNs, ensuring that all web traffic is monitored and managed.
- For supported browsers, the Web Endpoint manipulates proxy settings in real time. For example, if Web Endpoint detects it is at a hotspot, but the user has not finished registration, it removes its proxy settings until the gateway has successfully opened.

You can enable Web Endpoint for some or all machines managed by the hybrid service.

System requirements

In this topic

Hardware requirements

Windows

- Pentium 4 (1.8 GHz or above)
- At least 850 MB free hard disk space (250 MB for installation, 600 MB for operation)
- At least 512 MB RAM on Windows XP
- At least 1GB RAM on Windows Vista, Windows 7, Windows 8, Windows Server 2003, Windows Server 2008, Windows Server 2012

Mac

- At least 1 GB RAM
- At least 500 MB free hard disk space (375 MB for installation, 125 MB for operation)

Operating system requirements

Endpoint clients must be running one of the following operating systems:

Operating System	32-bit	64-bit
Windows 7 with Service Pack 1	✓	✓
Windows 8 Windows 8.1 (v7.8.2 and beyond) and Windows 8.1, Update 1 (v7.8.4 and beyond)	✓	✓
Windows Vista with Service Pack 1 or higher	✓	✓
Windows XP with Service Pack 2 or higher	✓	✓
Windows Server 2003 with Service Pack 2	✓	✓
Windows Server 2008 with Service Pack 2	✓	✓
Windows Server 2008 R2 with Service Pack 1		✓
Windows Server 2012 R2		✓
Mac OS X 10.7, 10.8 Mac OS X 10.9 (v7.8.2 and beyond)		✓

Browser support

The following web browsers support the endpoint client on both 32-bit and 64-bit Windows operating systems and the 64-bit Mac operating system:

Version 7.8.4

- Internet Explorer 7 to 11 on Windows
- Firefox 3.x to 30 on Windows and Mac
- Safari 5.x on Windows
- Safari 5.x, 6.x, 7.x on Mac
- Google Chrome from 15 to 36 on Windows and Mac
- Opera 11 to 21 on Windows and Opera 11 to 20 on Mac

Version 7.8.3

- Internet Explorer versions 7 to 11
- Firefox 3.x to 28 on Windows and Mac

- Safari 5.x on Windows
- Safari 5.x, 6.x, 7.x on Mac
- Google Chrome from 15 to 34 on Windows and Mac
- Opera from 11 to 15 Windows and Mac

Version 7.8.2

- Internet Explorer versions 7 to 11
- Firefox 3.x to 22 on Windows and Mac
- Safari 5.x on Windows
- Safari 5.x, 6.x on Mac
- Google Chrome from 15 to 31 on Windows and Mac
- Opera from 11 to 15 Windows and Mac

Version 7.8.1

- Internet Explorer versions 7 to 11
- Firefox 3.x to 22 on Windows and Mac
- Safari 5.x on Windows
- Safari 5.x, 6.x on Mac
- Google Chrome from 15 to 28 on Windows and Mac
- Opera from 11 to 15 Windows and Mac

Full support means that the browser supports all installation methods, and both policy enforcement and proxy manipulation.

Obtaining the endpoint installation package

Navigate to the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web Security manager to obtain the endpoint installation package for standalone Web Endpoints deployments.

- Different endpoint packages are available for 32-bit and 64-bit clients; select the appropriate package (or combination of packages) from the list provided.
- When you select an endpoint package, a GPO command is displayed on the page. Use the command provided if you intend to deploy the Web Endpoint MSI package to client machines via GPO.

See the Web Security Help for more information about downloading and deploying Web Endpoint.

If you plan to use Web Endpoint with Data Endpoint, use the Websense Endpoint Package Builder to create an installation package. See Combining Web and Data Endpoint Clients for more information.

Deploying endpoint software to client machines

In this topic

Before you begin

- Check that your endpoint machines meet the minimum system requirements. See *System requirements*, page 2, for details.
- Exclude the following directories from any antivirus software that is deployed to endpoint clients:
  - The folder where you will install Web Endpoint
  - Endpoint processes: **wepsvc.exe** and **dserui.exe**.
  - **EndpointClassifier.exe** and **kvoop.exe**
- Ensure the Web Endpoint installation path is not being encrypted by disk encryption software.

Deploying Windows endpoints

Important

After deploying the installation package, you must restart the endpoint software to complete the installation process.

There are a few ways to distribute the endpoint software on Windows clients:

- Manually on each endpoint machine. Windows packages contain a single executable file, **WebesenseEndpoint_32bit.exe** or **WebesenseEndpoint_64bit.exe**.
  1. Copy the self-extracting file to a temporary folder on the client machine, then unzip the file.
  2. Open a command prompt, then navigate to the location of the unzipped installation files.
  3. Enter the following command:

     ```
     msiexec /package "Websense Endpoint.msi" /norestart
     WSCONTEXT=xxxx
     ```

     Replace “xxxx” with the unique configuration code shown on the Settings > Hybrid Configuration > Hybrid User Identification page in the Web Security manager. The code is shown as part of the **GPO command** string.

In virtual desktop (VDI) environments, install the endpoint software as if the client machine were a physical machine, while taking into consideration any additional steps required by the infrastructure for third-party installations.

- Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS) (Windows only). See Creating and distributing Websense endpoints using SCCM or SMS for details.
- Using a Microsoft Group Policy Object (GPO) or other third-party deployment tool for Windows.

  The GPO command for deploying Web Endpoint is displayed on the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web Security manager. Note that the command includes a WSCONTEXT parameter that is required to ensure that your organization's policies are applied to user requests.

  See Manually deploying Web Endpoint for Windows in the Web Security Help for details.

To confirm that Web Endpoint is installed and running on a Windows machine, use the Windows Services tool. Check that **Websense SaaS Service** is present in the Services list, and is started.

Deploying Mac Web Endpoint

There are a few ways to distribute the endpoint software:

- Manually on each endpoint machine. See *Manual deployment of Mac Web Endpoint*, page 6.
- Using Remote Desktop (Mac OS X only). See Installing Mac endpoints with Remote Desktop for details.

Manual deployment of Mac Web Endpoint

Mac packages contain a zip file, **WebsenseEndpoint_Mac.zip**.

1. Copy **WebsenseEndpoint_Mac.zip** to the client machine, and double-click the file.
2. Mac OS X versions 10.6.7 through 10.8 automatically create a directory named "EndpointInstaller," which contains a file called **WebsenseEndpoint.pkg**.
3. Double-click **WebsenseEndpoint.pkg** to start the installation process.
4. Click **Continue**, and agree to the license agreement.
5. Click **Install**.
6. Enter a user name and password for a user with administrator rights to install the software.

   You'll receive a confirmation message if the endpoint was successfully installed.

Enabling automatic updates for Web Endpoint

Once you have deployed your endpoint package to end users, Web Endpoint can be updated for some or all of your users directly from the hybrid service. If you use the Data Endpoint auto-update feature for endpoints with both data and web security capabilities, however, endpoints receive updates from your auto-update server instead.

To enable automatic Web Endpoint updates to client machines:

1. Go to the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web Security manager.
2. Mark **Enable installation and update of Web Endpoint on client machines**.

   This defines whether automatic updates are deployed to the client machines that you specify. If you uncheck this option at a later date, no further automatic updates occur. However, the installed endpoint software continues to run until it is uninstalled from the client machines.
3. Mark **Automatically update endpoint installations when a new version is released**.
4. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

> ✓ **Note**
>
> At the completion of any endpoint update, you must restart the endpoint for the updates to take effect.

Note that while a Web Endpoint update is taking place (which can take several minutes), end users are unable to browse, but are shown a Web page explaining that the update is occurring. This page continues to retry the requested Web page every 10 seconds until the endpoint software has finished updating. The request is then submitted, and either the page or a block page is displayed.

Configuring endpoint software

Once the endpoint software is deployed, the Web Endpoint is ready for use. The policies and exceptions you created for all clients are applied to the endpoint client as well.

Endpoint status icons, override and disable features, and diagnostics

The installed Websense Web Endpoint on the Windows operating system displays one of three possible status icons in the end-user’s task bar. The icon serves as both a status indicator, such as if the endpoint is working, overridden, or disabled, and as an access point to additional diagnostic information.

See the Web Endpoint features article for more details about endpoint icons, diagnostics, and the override and disable features. A guide that explains the icons and their features is available for end users as well.

Uninstalling endpoint software

In this topic

Windows uninstallation

You can uninstall endpoint software 2 ways:

- Locally on each endpoint agent
- Remotely through a deployment server or distribution system

> ✓ **Note**
> If you configured an administrative password, you must supply it to uninstall the software.

Local uninstallation

1. Go to **Start > Control Panel > Add/Remove Programs**.
2. The Add/Remove Programs screen is displayed.
3. Scroll down the list of installed programs, select **Websense Endpoint** and click **Remove**.
4. Click **Yes** in the confirmation message asking if you are sure you want to delete the Websense Endpoint.
5. You may be prompted to provide an administrative password, if you defined one. If so, enter the password in the field provided and click **OK**.
6. You’ll see a system message indicating you must restart your system. Click **Yes** to restart or **No** to restart your system later. Once the computer has been restarted, the configuration changes apply.

Remote uninstallation with deployment server

If you use a deployment server, you can perform a silent uninstall by running the following command:

```
msiexec /x {product_code} XPSWD=password /qn
```

where:

- `{product_code}`is a unique identifier (GUID) that can be found in the **setup.ini** file of each installation package or the system registry.
- `password` is the administrator password that you entered when creating the installation package.

To find the **setup.ini** file, use a file compression tool like WinZip or 7-Zip to extract the contents of the installation package executable

To perform a silent uninstall that doesn't require a reboot, add the /norestart parameter as follows:

```
misexec /x{ProductCode} /qn /XPSWD=xxxx /norestart
```

The MSI command switches are summarized below

Function	MSI Switch
Silent uninstall*	misexec /x{ProductCode} XPSWD=xxxx /qn
Silent uninstall without reboot*	misexec /x{ProductCode} XPSWD=xxxx /norestart /qn

Remote uninstallation using distribution systems

You can uninstall endpoint software remotely by using distribution systems. If you used an SMS distribution system to create packages for installation, those packages can be reused, with a slight modification, for uninstalling the software. If a package was not created for deployment of the endpoint software, a new one needs to be created for uninstalling.

To uninstall with package:

1. Follow the procedure for Creating and distributing Websense endpoints using SDCCM or SMS.
2. In step 1, select **Per-system uninstall**.
3. Complete the remaining procedures.
4. After deploying the package, the Websense Endpoint will be uninstalled from the defined list of computers.

Mac uninstallation

1. Go to **System Preferences.**
2. In the **Other** section, click the icon for the **Websense** endpoint software.

3. Click **Uninstall Endpoint**.
4. Enter the local administrator name and password.
5. Click **OK**.
6. If you created an anti-tampering password to block attempts to uninstall or modify endpoint client software, enter that password.
7. Click **OK** to begin uninstalling the endpoint.

   You'll receive a confirmation message if the endpoint was successfully uninstalled.

To uninstall the Mac endpoint remotely, you can use the following command line option with Apple Remote Desktop:

```
wepsvc --uninstall [--password pwd]
```

Third-party agents

By default, Windows XP and Windows Server 2003 limit the number of concurrent agents in a system. As a result, a fatal (BSOD) error may occur when users try to access files via DFS (Distributed File System) and Websense endpoint software is installed with more than 2 other agents.

To overcome this limitation, update client operating systems to Windows XP SP3 or Windows Server 2003 SP2 and follow the procedures below.

For further details, please refer to: http://support.microsoft.com/kb/906866.

On all relevant endpoint (client) machines:

1. Make a backup copy of your Windows registry before you continue. See support.microsoft.com for details.
2. Click **Start > Run** and type **regedit**, then click **OK**.
3. Locate and then click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Mup\
   Parameters
   ```
4. In the right pane, right-click **DfsIrpStackSize**, then click **Modify**.

> **Note**
>
> If the DfsIrpStackSize registry entry does not exist, you must create it. To do this:
>
> a. Go to **Edit > New**, then click **DWORD Value**.
>
> b. Type **DfsIrpStackSize**, then press **Enter**.

5. In the Base box, click **Decimal**, then type **10** in the Value data box and click **OK**.
6. Exit the Registry Editor.
7. Restart the computer.