Combining Web and Data Endpoint Clients

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x	◆ *System requirements*, page 4 ◆ *Creating installation packages*, page 7 ◆ *Deploying endpoint software to client machines*, page 14 ◆ *Uninstalling endpoint software*, page 19

Websense® offers solutions for securing client workstations, laptops, and other endpoint machines from data loss and inbound web threats when the machines are outside the corporate network.

The solutions are endpoint client software applications that run on the endpoint machines 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 deploy endpoint client software that includes both the *Web Endpoint* and *Data Endpoint* features for customers with Websense Web Security Gateway Anywhere.

You can also deploy the Web or Data Endpoint alone, or you can deploy the Remote Filtering Client (with or without the Data Endpoint). See the following articles for instructions:

- Installing and Deploying Data Endpoint Clients
- Installing and Deploying Web Endpoint Clients
- Installing and Deploying Remote Filtering Client

Websense endpoint solutions include both server and client components. See *System requirements*, page 4 for information about the hardware requirements and supported operating systems for endpoint components.

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 has 2 operation modes:

- In **Web scanning and filtering** mode, the endpoint client 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.

  The endpoint client can be used with both full-tunnel and split-tunnel VPNs, ensuring that all web traffic is managed properly.
- In **proxy manipulation** mode, for supported browsers, the endpoint client manipulates proxy settings in real time. For example, if the 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 whose traffic is managed by the hybrid service.

Data Endpoint

Data Endpoint is designed for organizations concerned about data loss originated at the endpoint, whether malicious or inadvertent. For example, if you want to prevent employees from taking sensitive data home on their laptops and printing it, posting to the Web, copy and pasting it, etc., you would benefit from this endpoint solution.

Websense Data Endpoint is a comprehensive, secure and easy-to-use endpoint data loss prevention (DLP) solution. It monitors real-time traffic and applies customized DLP policies over application and storage interfaces. You can also apply discovery policies to endpoints to determine what sensitive data they hold.

Data Endpoint can analyze files when they are opened by endpoint applications. It can monitor cut, copy, paste, print, and print screen operations. It can analyze endpoint Web activities. And it can analyze data that users copy to external drives and endpoint client machines.

Multiple agent limitations

Just as you can install Data and Web Endpoint together, you can install them with third-party agents, such as an antivirus agent, as well.

There are limitations in all multi-agent deployments to be aware of.

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.

System requirements

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x	◆ *Hardware requirements*, page 4 ◆ *Operating system requirements*, page 4 ◆ *Browser support*, page 5

Hardware requirements

Windows

Windows clients must meet the following minimal hardware requirements.

- 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

Mac clients must meet the following minimal requirements.

- 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

Data Security

When the Data Endpoint analyzes data via the Web > Endpoint HTTP/HTTPS destination, it intercepts HTTP(S) posts as they are being uploaded within the browser. (It does not monitor download requests.)

For both Mac and Windows-based endpoints, Data Security analyzes posts from the following browsers:

Version 7.8.4

- Internet Explorer versions 7 to 11
- Firefox versions up to 30
- Google Chrome 26 to 36. Windows endpoints using Chrome 33 or later must belong to a domain for the Data Endpoint Chrome extension to function.

Version 7.8.3

- Internet Explorer versions 7 to 11
- Firefox versions up to v28
- Google Chrome 26 to 34

Version 7.8.2

- Internet Explorer versions 7 to 11
- Firefox versions up to v26
- Google Chrome 26 to 31

Version 7.8.1

- Internet Explorer versions 7 to 11

- Firefox 3 to 22
- Google Chrome 26 to 28

For Mac only

- Safari 7.0.3 (v7.8.3 and beyond) on Mac OS X.

  Prior to that, it analyzed posts from supported Safari versions on Mac OS X 10.7 or above.

Data Security does not support the HTTP/HTTPS destination channel on Linux.

Web Security

In addition, 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 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 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 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.

Creating installation packages

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x	◆ *Websense Data Endpoint*, page 10 ◆ *Websense Web Endpoint*, page 12

You use the Websense Endpoint Package Builder to create a combined installation package for the combined Web and Data Endpoints. The combined installation package (a single executable file) is used to deploy the endpoint clients to user machines.

The Endpoint Package Builder is a Windows utility that can be used to create 32- and 64-bit Windows packages and/or Mac packages endpoint clients.

The utility can be found on any Windows server that includes a Websense Web Security or Data Security component.

Note

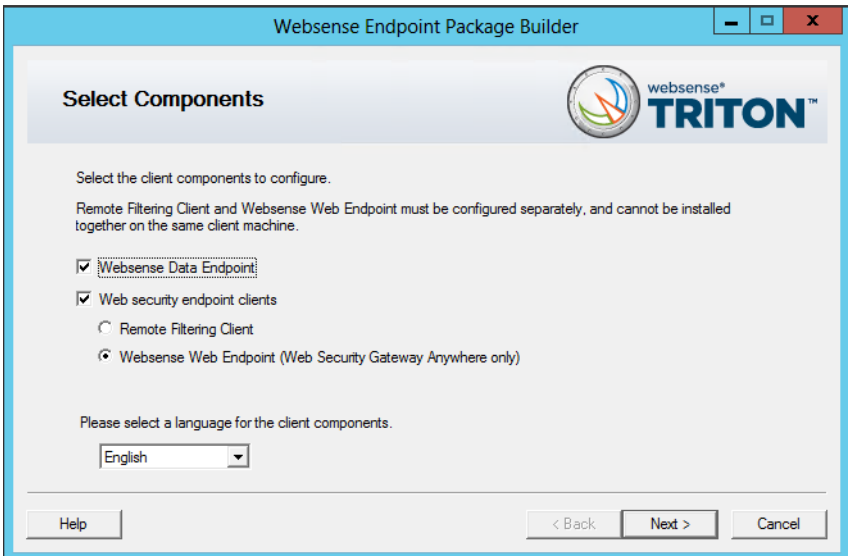
The packages created by the Websense Endpoint Package Builder are backwards compatible with previous endpoint versions.

1. To launch the Websense Endpoint Package Builder, do one of the following on the TRITON management server:
   - Navigate to **Start** > **All Programs** > **Websense** > **Data Security** > **Endpoint Package Builder**.
   - On Windows Server 2012, browse to the Start page and select **Endpoint Package Builder**.

   The Websense Endpoint Package Builder utility extracts required files and launches.
2. On the **Select Components** screen, select:

- Websense Data Endpoint
- Web security endpoint clients

3. Under Web security endpoint clients, select Websense Web Endpoint (Web Security Gateway Anywhere only).

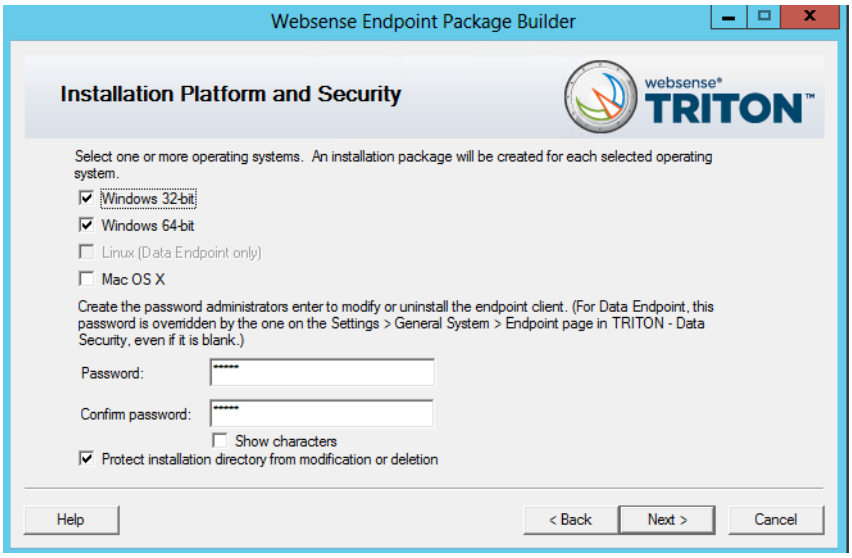


Also select a language for the client components.

In the TRITON console, you can change the language used for displaying messages to Data Endpoint users, but the language displayed in the user interface (buttons, captions, fields, etc.) can only be set during packaging.

Click **Next** when you're done.

4. On the **Installation Platform and Security** screen, select the operating system or systems for which you want to create an installation package, create the administrator password that will be used to uninstall or modify endpoint client software, and configure anti-tampering settings. When you are finished, click **Next**.



- You can create Windows (32-bit or 64-bit) or Mac OS X installation packages. Linux is not supported for combined Web and Data Endpoint packages. It is for stand-alone Data Endpoints. Do not choose Linux.
- For security purposes, anyone who tries to modify or uninstall endpoint software is prompted for a password.

  Once the endpoint client contacts the server, this password is overwritten with the password specified by a TRITON administrator. Set this password in one of the following places (it is not necessary to do it in both):

  - Data Endpoint: Go to **Settings > General > System > Endpoint**, then on the General tab, select **Enable endpoint adminitrator password** and enter and confirm a password.
  - Web Endpoint: Go to **Settings > Hybrid Configuration > Hybrid User Identification**, then enter and confirm an anti-tampering password.

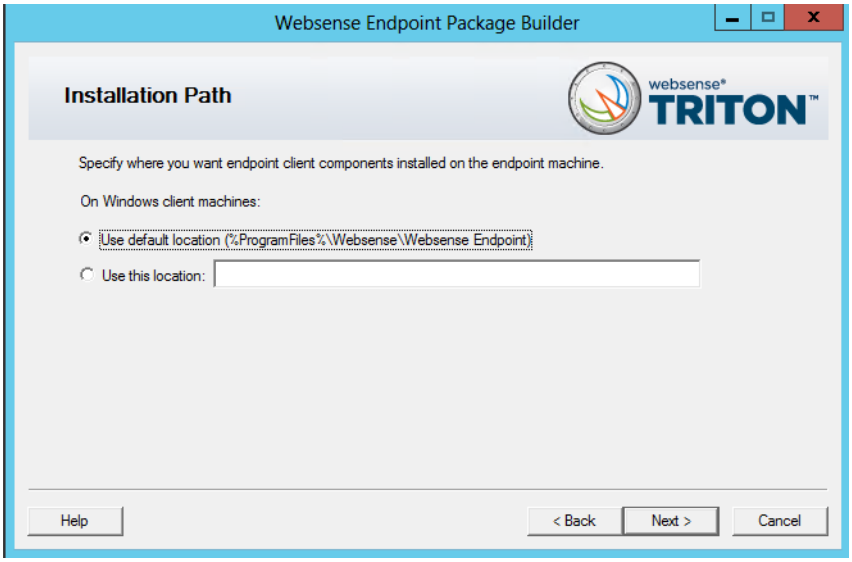
  If no password is specified, every user is able to uninstall the endpoint software from their computer.

  Click **Show characters** to display the password characters while you type.
- Sometimes when users cannot modify or uninstall the endpoint software, they try to delete the directory where the software is installed.

  Click **Protect installation directory from modification or deletion** if you do not want users to be able to perform these functions.

5. On the **Installation Path** screen, specify the directory to use for installing endpoint software on each endpoint machine. The directory path must contain only English characters.

Note that this screen does not appear if you are creating only a Mac OS X endpoint package. On Mac OS X machines, the endpoint client is installed in the /Applications directory.

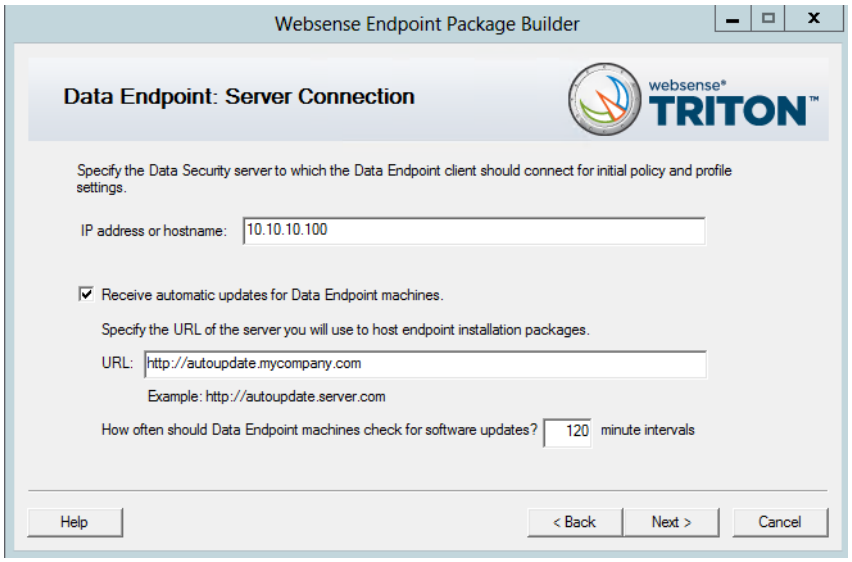


- **Use default location**: The endpoint software is installed in a default directory: \Program Files\Websense\Websense Endpoint (*Windows*) or /opt/websense/LinuxEndpoint (*Linux*).
- **Use this location**: Manually specify the installation path for the endpoint software. Environment variables are supported.

6. Click **Next**.

Websense Data Endpoint

1. The Data Endpoint Server Connection screen appears:



IP address or hostname: Provide the IP address or hostname of the Data Security server that endpoint machines should use to retrieve initial profile and policy information. (Once configured, endpoints retrieve policy and profile updates from the endpoint server defined in their profiles.)

Receive automatic updates for Data Endpoint machines (Windows only): When new versions of the endpoint are released, you may upgrade the software on each endpoint—this can be done via GPO or SMS—or you can configure automatic updates on this screen.

You cannot use the auto-update feature in the Web Security manager to automate updates for combined Web and Data Endpoints.

This option does not apply to Linux or Mac endpoints.

To automate software updates for combined endpoints:

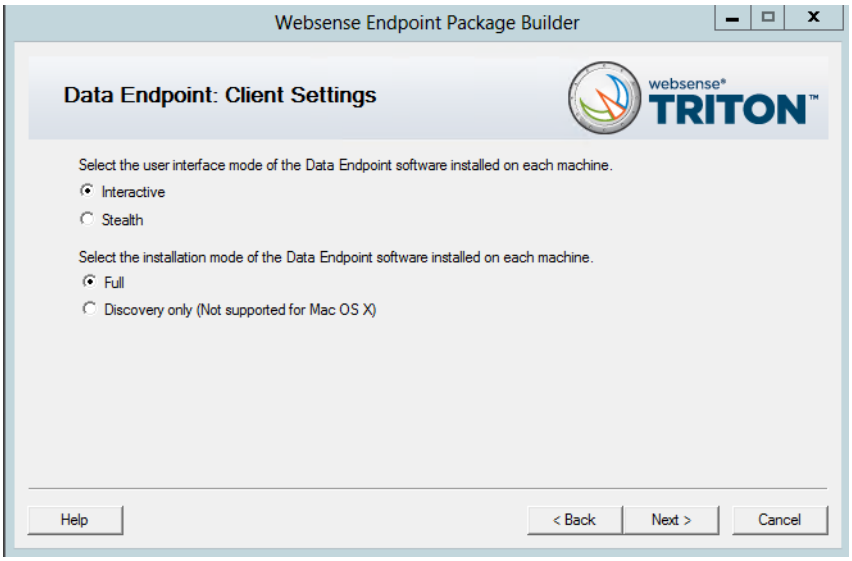
a. Prepare a server with the latest updates on it (see "Automatic Updates for Websense data endpoints" for details).

b. Select **Receive automatic updates for Data Endpoint machines**.

c. Specify the URL of the server you created. (It cannot be secure http (https).)

d. Indicate how often you want endpoint machines to check for updates.

2. Click **Next** and the Client Settings screen appears:



Complete the fields as follows:

User interface mode	Select from the following 2 options: • **Interactive**: A user interface is displayed on all endpoint machines. Users know when files have been contained and have the option to save them to an authorized location. • **Stealth**: The Websense Data Endpoint user interface is not displayed to the user. Note that reinstallation is required to switch user interface modes.

Installation Mode	Applies to Windows only. Select from the following 2 options: • **Full**: Installs the endpoint with full policy monitoring and blocking capabilities upon a policy breach. All incidents are reported in the TRITON console. Endpoints that are installed in Full Mode require a reboot. • **Discovery Only**: Configures the endpoint to run discovery analysis but not DLP. Discovery Only installation does not require a reboot.

3. Click **Next**. If you chose no other endpoints, skip to *Global settings*, page 13 for instructions. Otherwise, continue to *Websense Web Endpoint*, page 12

Websense Web Endpoint

1. Use the **Proxy Settings** screen to specify the URL for your organization's PAC file.
   - Replace the default URL with the customized URL for your deployment, which can be found on the **Settings > Hybrid Configuration > User Access** page in the Web Security manager.

     The custom PAC file string looks something like this:

     ```
     http://hybrid-web.global.blackspider.com:8082/
     proxy.pac?p=<alphanumeric_string>
     ```

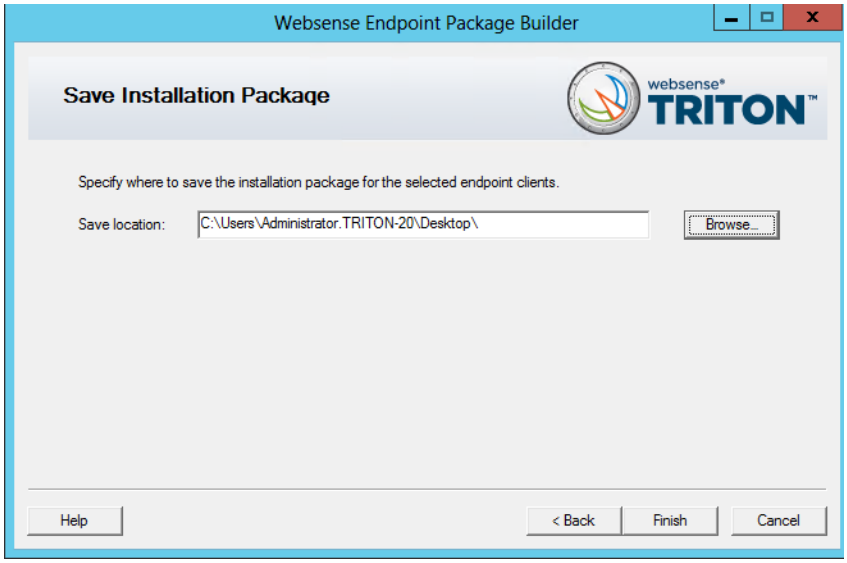
     In this example, **<alphanumeric_string>** is a unique identifier for your organization.

     Note the difference between the subdomains of the default PAC file URL and the sample customized URL. The "hybrid-web" subdomain is used for Web Security Gateway Anywhere deployments that use Web Endpoint. The "webdefence" subdomain is used by Cloud Web Security.
   - Check **Enable local user-defined Proxy Setting** if you want to allow users to edit local proxy settings if a network event prevents access to the hybrid service.

     Note that should a network change occur and an endpoint can no longer reach the cloud service, an automatic override takes effect. You don't need to enable the automatic override feature. It is on by default.
2. Click **Next**.

Global settings

1. When you're done configuring your endpoint selections, use the **Save Installation Package** screen to enter a directory path to use for storing the installation package before it is deployed to client machines.



   Either manually enter a path or click **Browse** to find the location.

2. Click **Finish**.

   You'll see a system message if the package is created successfully. If the creation of the package fails, you'll see an error message. If this happens, contact Websense Technical Support for assistance.

3. Click **OK**.

   Once the packaging tool has finished, the packages are created in the designated path. Refer to *Deploying endpoint software to client machines*, page 14 for instructions on distributing the package to the endpoint machines.

Deploying endpoint software to client machines

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x	◆ *Before you begin*, page 14 ◆ *Deploying Windows endpoints*, page 15 ◆ *Deploying Mac endpoints*, page 17

Before you begin

- Check that your endpoint machines meet the minimum system requirements. See *System requirements*, page 4, for details.
- See *Multiple agent limitations*, page 2, if you are deploying the endpoints on Windows clients.
- Exclude the following directories from any antivirus software that is deployed to endpoint clients:
  - The endpoint installation folder
  - Endpoint processes: **wepsvc.exe** and **dserui.exe**.
  - **EndpointClassifier.exe** and **kvoop.exe**
- Ensure the endpoint installation path is not being encrypted by disk encryption software.
- Ensure that the auto-update feature in the Web Security manager is disabled. If you want auto-updates, you can use the Data Security method described below.

Disabling automatic updates for Web Endpoint

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

Enabling automatic updates for combined endpoints

To deploy endpoint updates automatically, you must create an update server that hosts endpoint installation packages. See "Automatic Updates for Websense data endpoints" for details.

You must also select **Receive automatic updates for data endpoints** on the Websense Endpoint Package Builder "Server Connections" screen. On this same screen, specify the URL of the server you created and indicate how often you want endpoint machines to check for updates (every 2 hours by default).

When configured properly, your update server pushes software updates out to endpoint machines and installs the packages in the background silently.

Note

If you want to change the components installed on an endpoint with components of the same version (for example, switch from a Data and Web Endpoint combination to a stand-alone Date Endpoint), you must use the package builder to generate a new package and use one of the other deployment options to deploy it. You cannot use the auto-update feature to update endpoints with the same version.

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, including virtual desktop clients running Windows:

- Manually on each endpoint device

  See *Manual deployment*, page 16.
- Using System Center Configuration Manager (SCCM) or Systems Management Server (SMS)

  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. If you need assistance, contact Websense Technical Support.

Manual deployment

Windows packages contain a single executable file: **WebesenseEndpoint_32bit.exe** or **WebesenseEndpoint_64bit.exe**.

Copy this self-extracting executable file to the client machine, then run the following command:

```
WebsenseEndpoint_64bit.exe /v"XPSWD=<password>
WSCONTEXT=<token>"
```

where:

- <password> is the anti-tampering password used by the previous-version endpoint client (if upgrading) or to be used by the new endpoint.
- <token> is the WSCONTEXT value displayed in the GPO command string on the **Settings > Hybrid Configuration > Hybrid User Identification** page in the Web Security manager. The WSCONTEXT argument used to identify your organization to the hybrid service must be included in the command string.
- All arguments passed via the **/v** parameter must be enclosed in straight quotes, as shown in the example.

You must provide both the XPSWD and WSCONTEXT arguments.

To perform a silent install, add the /qn" parameter as follows:

```
WebsenseEndpoint_64bit.exe /v"/qn XPSWD=<password>
WSCONTEXT=<token>"
```

The MSI command switches are summarized below:

Function	MSI Switch
Silent install	WebsenseEndoint_32bit /v"/qn"
Set WSCONTEXT	WebsenseEndoint_32bit /v"WSCONTEXT=xxxx"
Set uninstall password	WebsenseEndoint_32bit /v"XPSWD=xxxx"
Set WSCONTEXT and silent install	WebsenseEndoint_32bit /v"/qn WSCONTEXT=xxxx"

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.

Testing deployment

To confirm that the endpoint is installed and running on a machine:

- For Web Endpoint, go to **Start > Administrative Tools > Services**. Check that **Websense SaaS Service** is present in the Services list, and is started.

  The installed Websense Web Endpoint on the Windows operating system also 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.

- When the Data Endpoint is installed in interactive mode, an icon ( ) appears on the endpoint machine's task bar. Click the icon for status information. (No icon shows in stealth mode.)

Deploying Mac endpoints

There are a few ways to distribute the endpoint software:

- Manually on each endpoint device

  See *Manual deployment*, page 17.
- Using Remote Desktop (Mac OS X only)

  See Installing Mac endpoints with Remote Desktop for details.

Manual deployment

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.

Testing deployment

To confirm that the endpoint is installed and running on a machine:

- For Web Endpoint, look under Launchpad or the applications directory for the client software. It is typically located in the /Library/Application Support/ Websense Endpoint/ directory.
- When the Data Endpoint is installed in interactive mode, an icon ( ) appears on the endpoint machine's task bar. Click the icon for status information. (No icon shows in stealth mode.) See Installing and Deploying Data Endpoint Clients for more details.

Configuring endpoint software

Applies to:

- Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x
- Data Security, v7.8.x

Once the endpoint software is deployed, the Web Endpoint is ready for use. The policies and exceptions you created for users whose requests are managed by the hybrid service are applied automatically.

The Data Endpoint requires configuration in the TRITON console, however. This entails:

1. Adding an endpoint profile to the Data Security manager or using the default. A default profile is automatically installed with the client package. (**Settings > Deployment > Endpoint**.)
2. Rearranging endpoint profiles. (**Settings > Deployment > Endpoint**.)
3. Configuring endpoint settings. (**Settings > General > System > Endpoint**.)
4. Creating endpoint resources. (**Main > Policy Management > Resources > Endpoint Devices/Endpoint Applications/Application Groups.**
5. Creating or modifying a rule for endpoint channels. (**Main > Policy Management > DLP / Discovery Policies**, Destination tab.)
6. Defining the type of endpoint machines to analyze, as well as the network location. (**Main > Policy Management > DLP / Discovery Policies**, Custom Policy wizard, Source tab.) Use the Network Location field to define the behavior of the endpoint on and off the network.

See the Data Security Manager Help for specific instructions.

Uninstalling endpoint software

Applies to:	In this topic
◆ Web Filter, Web Security, Web Security Gateway, and Web Security Gateway Anywhere, v7.8.x ◆ Data Security, v7.8.x	◆ *Windows uninstallation*, page 19 ◆ *Mac uninstallation*, page 21

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. It is different for each version and bit type (32- versus 64-bit).
- `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.
8. 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]
```