

Installing and Deploying Data Endpoint Clients

Applies to:	In this topic
<ul style="list-style-type: none">◆ Data Security, v7.8.x	<ul style="list-style-type: none">◆ System requirements, page 2◆ Creating installation packages, page 8◆ Deploying endpoint software to client machines, page 14◆ Uninstalling endpoint software, page 17

Websense Data Endpoint is a solution for securing client workstations, laptops, and other endpoint machines from data loss when the machines are outside the corporate network and for identifying sensitive data on the clients themselves.

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

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

Web endpoint solutions are also available. You can install these along with Data Endpoint to protect your endpoint machines from inbound web threats. This includes the Web Endpoint and the Remote Filtering Client. You cannot deploy both web endpoint solutions with the Data Endpoint at one time.

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 Data Endpoint component.

Why 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.

System requirements

Applies to:	In this topic
<ul style="list-style-type: none">◆ Data Security, v7.8.x	<ul style="list-style-type: none">◆ Hardware requirements, page 2◆ Port requirements, page 3◆ Operating system requirements, page 4◆ Windows 7 , page 5

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

Linux

- ◆ At least 1 GB RAM
- ◆ 1 GB free hard disk space (not including contained files and temporary buffers; see the TRITON - Data Security Help for information about contained files and allocating enough disk storage for them)

Mac

- ◆ At least 1 GB RAM

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

Port requirements

The following ports must be kept open for Data Endpoint operation:

Data Endpoint client

Outbound

To	Port	Purpose
Data Security Server	443*	Connect to Endpoint Server
Data Security Server	80**	Connect to Endpoint Server

* You can choose between secured and unsecured connection. The default is secured (HTTPS, port 443).

** Optional

Inbound

None

Data Endpoint server

Outbound

To	Port	Purpose
Data Security Management Server	443	Retrieve fingerprints and natural language processing scripts
Data Security Management Server	17443	Incidents

Inbound

From	Port	Purpose
Data Security Management Server	443	Retrieve fingerprints and natural language processing scripts
Endpoint Client	80	Incidents
Supplemental Data Security Server	17444	Retrieve fingerprints and natural language processing scripts

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	✓	✓
VMware View Horizon VDI v5.2 running Windows 7 (v7.8.3 and beyond)	✓	✓
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		✓
VMware View Horizon VDI v5.2 running Windows Server 2008 (v7.8.3 and beyond)		✓
Windows Server 2012 R2		✓
Mac OS X 10.7, 10.8 Mac OS X 10.9 (v7.8.2 and beyond)		✓
Red Hat Enterprise Linux/CentOS 5.1 with stock kernel 2.6.18-53****	✓	✓

Red Hat Enterprise Linux/CentOS 5.5 with stock kernel 2.6.18-194****	✓	✓
---	---	---



Note: by default, Windows Server 2003 or XP support only 3 agents per client. If your endpoint clients will be running multiple agents—for example the endpoint agent, an antivirus agent, and an antispam agent—they should be updated to Windows XP SP3 or Windows Server 2003 SP2. In addition, you must modify their registry entries.

****The Linux endpoint requires FUSE support to enable USB detection. If you are running CentOS 5.1, FUSE support is configured upon installation. If you are running CentOS 5.5, FUSE support is built into the kernel. If you have upgraded from CentOS 5.1 to CentOS 5.5, you may not have FUSE support in your running kernel. If this is the case, please install the relevant FUSE packages before running the endpoint installer.

Virtualized environments

Data Endpoint can be installed on endpoint clients running Windows in Citrix XenDesktop Virtual Desktop Infrastructure (VDI) environments. The following operating systems are supported:

- ◆ Citrix XenDesktop 5.6
 - Windows XP
 - Windows 7
- ◆ Citrix XenDesktop 7.1
 - Windows Server 2008 R2
 - Windows XP
 - Windows 7

Browser support

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 endpoints.

Email clients

Data Security analyzes all email messages sent from endpoint users, even if they send them to external Web mail services such as Yahoo.

For Windows, Websense Data Security can analyze endpoint email generated by Microsoft Outlook and IBM Lotus Notes. It supports the desktop version of Outlook 2003, 2007, and 2010, but not the Windows 8 touch version . If you are using Outlook 2003, then Office 2003 SP3 must be installed. Data Security supports IBM Lotus Notes version 8.5.1, 8.5.2 FP4, and 8.5.3.

For Mac OS X, Data Security can analyze endpoint email generated by Outlook 2008, Outlook 2011, and Apple Mail.

Printer drivers

You can monitor data being sent from an endpoint machine to a local or network printer. Data Security supports drivers that print to a physical device, not those that print to file or PDF.

Applications and controls

You can monitor or prevent sensitive data from being copied and pasted from an application such as Microsoft Word or a Web browser. This is desirable, because endpoint clients are often disconnected from the corporate network and can pose a security risk.

Data Security can monitor copy and paste operations on most browsers, such as Internet Explorer, Firefox, Safari, and Opera.

The applications that Data Security supports out of the box are found in the Technical Library article, [Data Security Endpoint Applications](#). You can also add custom applications.

Supported removable media

You can monitor or prevent sensitive data from being transferred to removable media. Data Security monitors unencrypted data being copied to native Windows and Mac CD/DVD burner applications. It monitors non-native Windows CD/DVD burner applications as well, but only blocks or permits operations without performing content classification.

Non-native CD/DVD blocking applies to CD, DVD, and Blue-ray read-write devices on Windows 7, Windows 8, Windows Server 2008 R2, and Windows Server 2012 endpoints.

Linux endpoint does not support CD/DVD burners.

On Windows 7, Data Security can also monitor unencrypted data being copied to Android devices through the Windows Portable Devices (WPD) protocol.

LAN control

Users commonly take their laptops home and then copy data through a LAN connection to a network drive or share on another computer. They also commonly take data from a shared folder (at work) to copy onto their laptop. With Data Security you can control LAN operations to protect your data.

Endpoint LAN control is applicable to Microsoft sharing only.

Destination channels by operating system

All the destination channels shown below are supported on Windows endpoints.

On Linux endpoints, only removable media is supported. The HTTP/HTTPS and email channels are not supported on Linux, nor are the print or LAN channels or endpoint applications.

On Mac, all destination channels except the print channel are supported, with the exceptions noted below.

Destination Channel	Windows	Mac OS X	Linux
Email	✓	✓	
Web HTTP/HTTPS	✓	✓	
Printing	✓		
Applications*	✓	✓	
Removable media	✓	✓	✓
LAN	✓	✓	

*Cloud apps and screen capture operations are not supported on Mac endpoints. Cloud apps cannot be launched using Windows Store browsers on Windows endpoints.

Creating installation packages

Applies to:	In this topic
<ul style="list-style-type: none"> ◆ Data Security, v7.8.x 	<ul style="list-style-type: none"> ◆ Websense Data Endpoint, page 11 ◆ Global settings, page 13

You use the Websense Endpoint Package Builder to create an installation package for data endpoints. The installation package (a single executable file) is used to deploy the endpoint client to user machines.

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

The utility can be found on machines with a Data Security server or TRITON management server installed.



Note

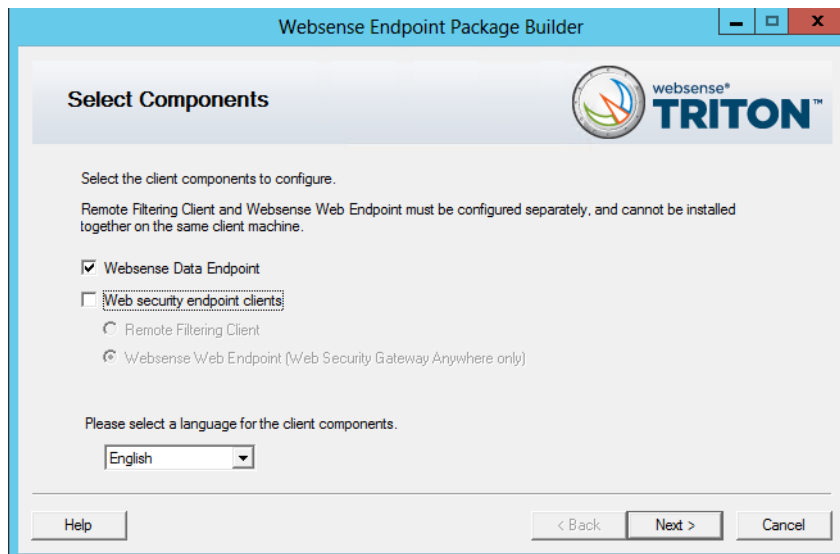
If existing versions of Data Endpoint are running on client machines, you can install the new package on top of them. (You do not have to uninstall them first.)

Version 7.7.x endpoints are fully compatible with the v7.8.x management server and can take advantage of the new predefined policies. To gain access to new endpoint features, however, you should upgrade your endpoints to v7.8.x.

1. To launch the Websense Endpoint Package Builder, 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**.

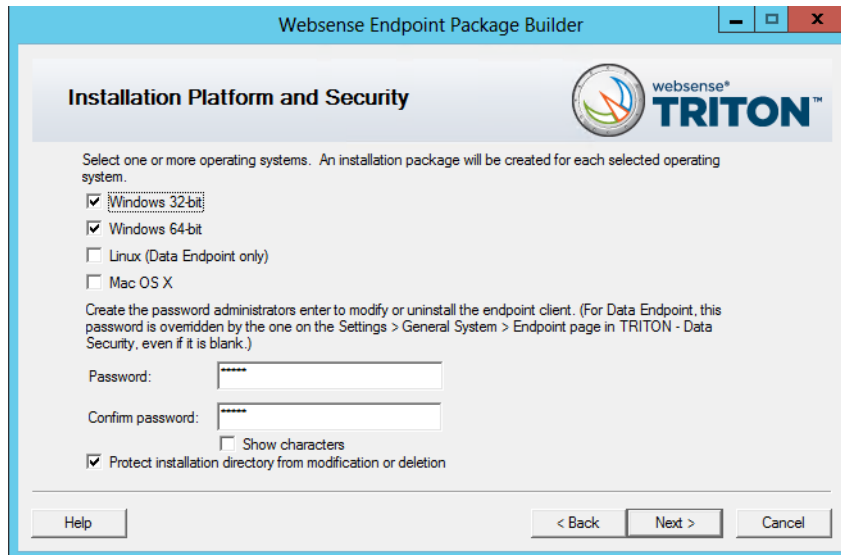


Also select a language for the client components.

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.

3. 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), Mac OS X, and/or Linux installation packages.
- 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. In Data Security manager, you can set this password on the General tab under **Settings > General > System > Endpoint**.

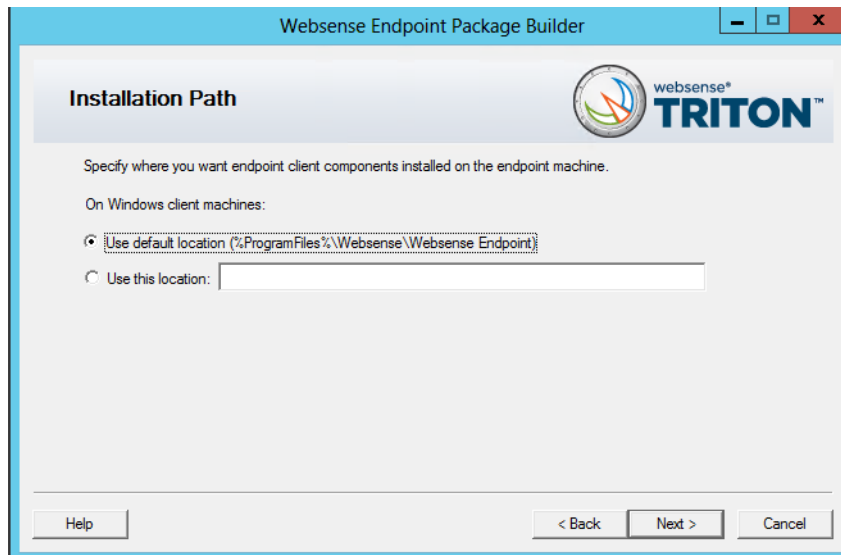
If no password is specified, every user is able to uninstall the endpoint software from their computer.

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.

4. 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.

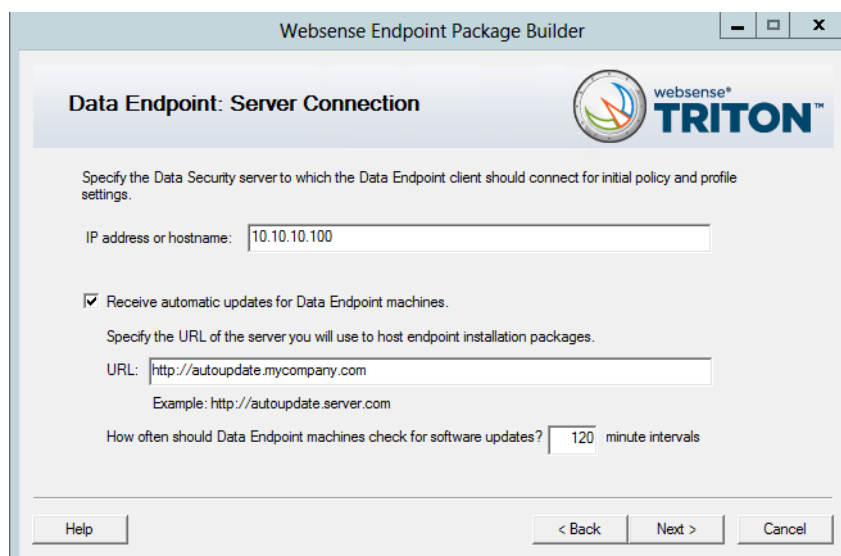


- **Use default location:** The endpoint software is installed in a default directory: \Program Files\Websense\Websense Endpoint (*Windows*) or /opt/websense/LinuxEndpoint (*Linux*).
- **Use this location:** Manually specify the installation path for the endpoint software. Environment variables are supported.

5. Click **Next**.

Websense Data Endpoint

1. The Data Endpoint Server Connection screen appears:



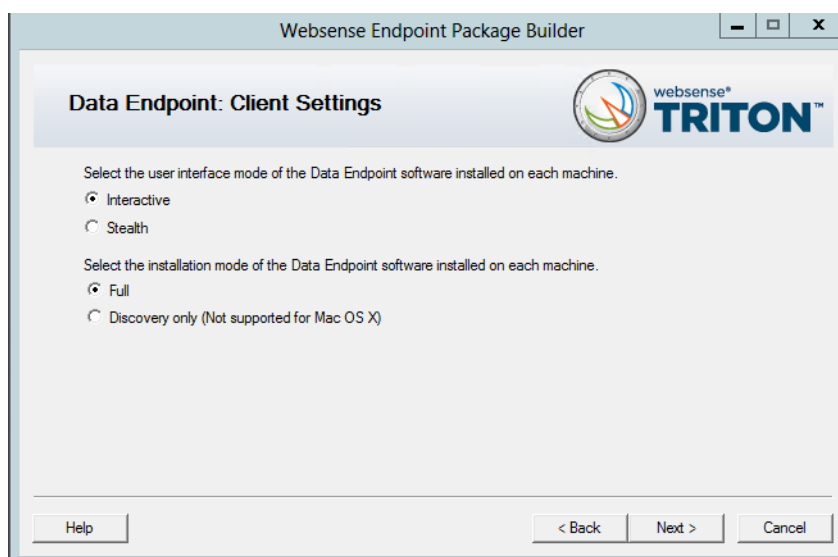
IP address or hostname: Provide the IP address or host name of the Data Security server that endpoint machines should use to retrieve initial profile and policy information. (Once configured, endpoints retrieve policy and profile updates from the endpoint server defined in their profiles.)

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.

This option does not apply to Linux or Mac endpoints.

To automate software updates for 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:

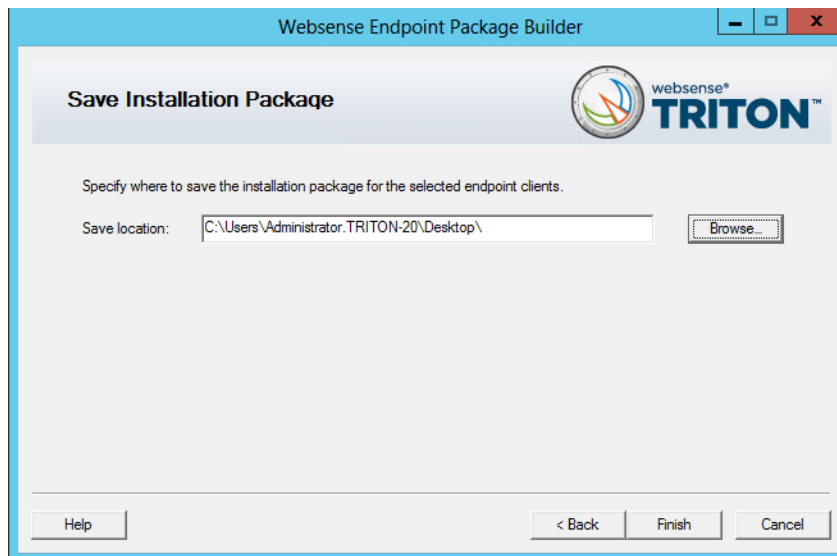
User interface mode	<p>Select from the following 2 options:</p> <ul style="list-style-type: none"> • Interactive: A user interface is displayed on all endpoint machines. Users know when files have been contained and have the option to save them to an authorized location. • Stealth: The Websense Data Endpoint user interface is not displayed to the user. <p>Note that reinstallation is required to switch user interface modes.</p>
---------------------	--

Installation Mode	<p>Applies to Windows only. Select from the following 2 options:</p> <ul style="list-style-type: none"> • 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**.

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
◆ Data Security, v7.8.x	◆ Before you begin , page 14 ◆ Deploying Windows endpoints , page 15 ◆ Deploying Mac endpoints , page 15 ◆ Deploying Linux endpoints , page 16

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 the endpoint
 - 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.

If you plan to use one, create an auto-update server to host endpoint installation packages. This option applies only to Windows endpoints. 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 a data endpoint with components of the same version (for example, switch from a data and web endpoint combination to a data only 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:

- ◆ Manually on each endpoint machine. Windows packages contain a single executable file, **WebesenseEndpoint_32bit.exe** or **WebesenseEndpoint_64bit.exe**. Copy the self-extracting file to the client machine, double-click it, and step through the installation wizard.
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). 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.

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

Deploying Mac endpoints

There are a few ways to distribute the endpoint software:


- ◆ Manually on each endpoint machine. See [Manual deployment](#), page 15.
- ◆ Using Remote Desktop (Mac OS X only). See [Installing Mac endpoints with Remote Desktop](#) for details.

Manual deployment

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

1. Copy **WebesenseEndpoint_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 **WebesenseEndpoint.pkg**.
3. Double-click **WebesenseEndpoint.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.

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

Deploying Linux endpoints

Linux packages contain the following installer: **LinuxEndpoint_SFX_installer_el5**. Use this installer with Red Hat Enterprise Linux version 5.x.

To install Data Endpoint software on a Linux computer, copy the installer to the machine and run it in the terminal console. Reboot the machine when done.

Configuring endpoint software

Installing and Deploying Data Endpoint Clients | Data Security Solutions | Version 7.8.x

Once the endpoint software is deployed, log on to the TRITON console to configure it. 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
<ul style="list-style-type: none">◆ Data Security, v7.8.x	<ul style="list-style-type: none">◆ Windows uninstallation, page 17◆ Mac uninstallation, page 18◆ Linux uninstallation, page 19

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*	<code>misexec /x{ProductCode} XPSWD=xxxx /qn</code>
Silent uninstall without reboot*	<code>misexec /x{ProductCode} XPSWD=xxxx /norestart /qn</code>

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.

Linux uninstallation

Run the **ep-uninstall** script (located by default at `/opt/websense/LinuxEndpoint/ep-uninstall`). You may be prompted for an administrative password, if one was defined by your system administrator.

