Your organization uses Websense Data Endpoint to protect sensitive information stored on your computer when it is disconnected from the network. Depending on your corporate policy, data could be quarantined or encrypted when you try to email it, print it, or copy it to removable media such as thumb drives, CD/DVD burners, and Android devices. (CD/DVD and Android support depends on your operating system.)

Data Endpoint includes server software installed on corporate servers and client software installed on your computer.

This guide tells you how to use the endpoint client software to view status information, set encryption passwords, release files from quarantine, and view logs. It also tells you how to disable the client in extreme cases and update the client software to the latest version.
Viewing status information

To view the Websense Data Endpoint status information, click the Websense Data Endpoint icon on your task bar.

On the Websense Data Endpoint screen, you can:

- See whether your machine is connected to an endpoint server
- Check the IP address of the Data Security server hosting the endpoint server software
- View your endpoint profile name, and when it was last updated
- Determine if endpoint protection is enabled or bypassed
- View discovery status and details of the last and next discovery scans
Disabling the endpoint client

1. On the Websense Data Endpoint screen, click **Disable**.

2. Report the bypass ID to your Data Security administrator.
3. Enter the bypass code supplied by the administrator.
4. Click **Enter**.

The endpoint client is disabled for the length of time specified when the bypass code was created. The button on the task bar updates from the **Disable** button with the red X icon to an **Enable** button with a green check mark icon.

Related topics:
- *Disabling the endpoint client*, page 3
- *Viewing contained files*, page 7
- *Viewing logs*, page 8
- *Updating the endpoint client*, page 9
Setting encryption passwords

Some corporate policies dictate that sensitive data be encrypted before being copied to a removable media device such as a USB drive. If this is the case for your organization, you cannot copy files to such media until you set the password to use to decrypt them.

Set the password one time, then any time you copy sensitive data to removable media, it is encrypted and copied along with a Websense Decryption Utility to the device.

You, or any other user accessing the files on endpoints where the Websense Data Endpoint is not installed, or where the password configured for encryption is different than yours, must enter this password.

To specify the encryption password:

1. Right-click the Websense Data Endpoint icon on your task bar, and select Set Encryption Password.
2. Enter your password, then re-enter your password.
3. Click OK.

Note

The password should be at least 8 characters in length (maximum is 15 characters), and it should contain:
- At least one digit
- At least one symbol
- At least one capital letter
- At least one lowercase letter

The following example shows a strong password:

8%w@s1*F
See *Decrypting files on a removable media device, page 5* for information on using the Websense Decryption Utility.

## Decrypting files on a removable media device

To decrypt the content on your removable media device, you must run a Websense Decryption Utility. Content that was encrypted on Windows can be encrypted on any Windows or Mac machine. (Content cannot be encrypted on Mac, however.)

The Websense Decryption Utility is copied to your removable media device along with the encrypted files. It is also available on [www.websense.com](http://www.websense.com).

**Decrypting files on Windows:**

1. Insert the removable device into a Windows laptop or desktop.
2. Double-click `wsdecrypt.exe`.
3. Enter the encryption password when prompted. A dialog appears and displays lists of subdirectories and files on your system.

4. Navigate to the folder containing the encrypted files. By default, the files are on your removable media device.
5. Select the folders and files to decrypt, right-click, and select **Save As**.

6. Select the folder in which to save the decrypted files.

**Decrypting files on Mac**

1. Insert the removable device into a Mac laptop or desktop.

2. Double-click **Websense Decryption Utility.dmg** and mount it as a disk volume.

3. Launch the application **Websense Decryption Utility** in the disk volume.

4. Drag and drop the encrypted files from the removable media device into the application's list window.

5. Select the file to decrypt, and select "Decrypt File As...". If the file selected is not encrypted by the Websense endpoint, the operation is disabled.

6. Enter the encryption password when prompted. A file save dialog appears if the correct password is entered.
7. Enter the file name that you want to save the decrypted file as.

![Websense Decryption Utility](image)

8. If necessary, select the next file to decrypt. No prompt appears as long as it is encrypted by the same password.

The Websense Decryption Utility decrypts the files using the password you provided and places them in this path.

Files that were encrypted with a different password are not decrypted.

**Viewing contained files**

Contained files are those that are held in temporary storage on an endpoint.

Files are contained if your organization chose to prevent sensitive information from being written from an endpoint to a removable device—such as a USB flash drive, CD/DVD, or external hard disk—and you try to copy a file to a forbidden device. If the file has been modified, the contained file includes the modifications, but the changes are not written to the original file location. This prevents work from being lost, but does not jeopardize the original file.

You can view the contents of contained files from the endpoint client, and choose to save them to an authorized location instead.

Related topics:

- Disabling the endpoint client, page 3
- Viewing contained files, page 7
- Viewing logs, page 8
- Updating the endpoint client, page 9
1. On the Websense Data Endpoint screen, click **Contained Files**.

![Image of Contained Files window](image)

2. To see the contents of a file, select the file and click **Open**.

3. To save a file to an authorized location, select the file and click **Save As**, then browse to the new location.

4. Click **Close** when done.

### Viewing logs

There are two logs available in the endpoint client:

- The system log contains information about changes on your machine, for example:
  - Changes of connection status, such as your computer moving from an office to a remote location
  - When the Websense Data Endpoint is enabled or disabled
  - When endpoint profiles are applied and updated
  - When the client is connected to or disconnected from the endpoint server

The content log contains details of file operations that have been picked up by the endpoint policy, and any actions taken by the endpoint as a result.

**Related topics:**
- *Disabling the endpoint client*, page 3
- *Viewing contained files*, page 7
- *Viewing logs*, page 8
- *Updating the endpoint client*, page 9
To see the log details, on the Websense Data Endpoint screen, click **View logs**.

To see the latest log information, click **Refresh**.

### Updating the endpoint client

Periodically, your corporate policies and endpoint profile are pushed to your machine to keep them up to date. To update them manually, click **Update** on the Websense Data Endpoint screen.