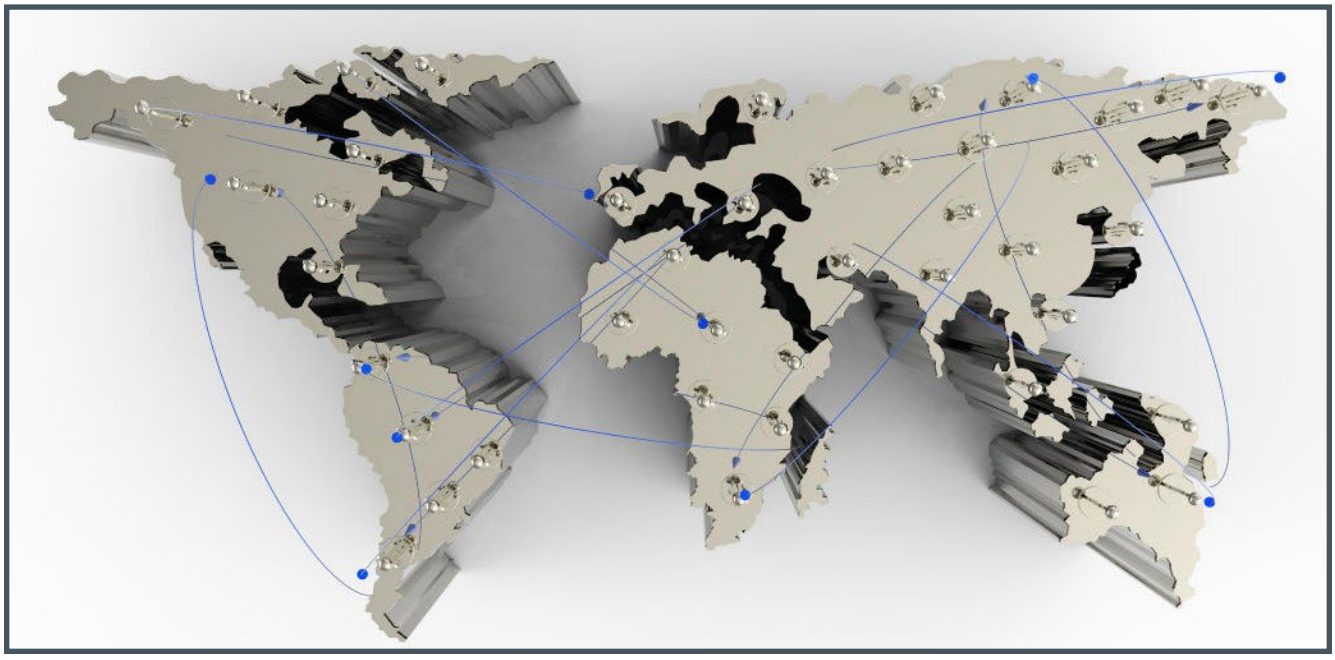
CyberVault Send-To
Version 3.2

Installation, Configuration and Use



Contents

Introduction

CyberVault Send-To is a client-based software program that seamlessly integrates CyberVault™
Secure Data Room into your Windows desktop. CyberVault™ Send-To is especially useful for uploading large documents and complex folder hierarchies easily and securely. It is also a reliable tool for downloading Data Room contents securely to your local or network drive.

CyberVault Send-To makes collaborating with others easy and just as secure as with CyberVault™
Secure Data Room. When you share a document, a link to this document is added to an e-mail. This link grants the invited persons a time-limited access to this document.

In addition to a graphical user interface client, the program is available as an executable version that may be called in a command line mode or from another program. In this way, the CyberVault Send-To functions can be integrated with a standard application for planning and executing recurring jobs and processes. It can also be used to synchronize a file system area with a Data Room.

This document describes the installation, configuration and use of CyberVault Send-To.

2 Before You Install

2.1 Check the Prerequisites

CyberVault Send-To requires the following prerequisites:

- **Permission to install software on the respective client computer:** Users must have the permission to install software on their client computers or an administrative user must install the software for the user on their client computer.

- **Supported operating systems:**
  - Windows 10 (32-bit and 64-bit)
  - Windows 8.1 (32-bit and 64-bit)
  - Windows 8 (32-bit and 64-bit)
  - Windows 7 (32-bit and 64-bit)
  - Windows Server 2008 R2
  - Windows Server 2012 R2
  - Windows Server 2012

- **Client computer compatible with:**
  - Microsoft .Net Framework 4.5 or newer
  - Microsoft Visual C++ 2012 Redistributable (x86) – 11.0.610.30
  - Optional: Microsoft Visual C++ 2012 Redistributable (x64) – 11.0.610.30
  - Note that all required software components are included in the installation package and herefore do not need to be installed separately.

- **CyberVault™ Secure Data Room:**
  - CyberVault Send-To requires a Data Room where API access is enabled. Please contact your Data Room manager if you have any questions about this.
  - As of CyberVault Send-To version 3.1.1, users of CyberVault Send-To can log in using SAML authentication with the SAML 2.0 protocol. This option requires CyberVault™ Secure Data Room version 8.30.701 or newer.

2.2 Download the MSI Installation File for CyberVault Send-To

The installation of CyberVault Send-To on a client computer can be done through an MSI instal-
lation file. This installation file is compatible with both 32-bit and 64-bit operating systems.

3 Install CyberVault Send-To

To install CyberVault Send-To, use the Microsoft installation file (*.msi). Choose the advanced installation if you want to customize the location where CyberVault Send-To is installed.

3.1 Perform a Standard Installation

1. Double-click the **CyberVault Send-To Installer.msi** installation file.
2. Accept the CyberVault License Agreement and click **Install**.
3. In the **User Account Control** window, click **Yes** to allow the program to make changes to your computer. CyberVault Send-To is now being installed on the given computer.
4. Once the installation is complete, click **Finish** to exit the Installation Wizard.

3.2 Perform an Advanced Installation

1. Double-click the **CyberVault Send-To Installer.msi** installation file.
2. Accept the CyberVault License Agreement and click **Advanced**.
3. Change the default installation location to a different location.
4. Click **Next**.
5. In the **User Account Control** window click **Yes** to allow the program to make changes to your computer. CyberVault Send-To is now being installed on the given computer.
6. Once the installation is complete, click **Finish** to exit the Installation Wizard.

3.3 Upgrade CyberVault Send-To From Version 2.x to Version 3.x

If you are running CyberVault Send-To from the command line via an XML file, you have to make the following adjustments to the XML file after an upgrade of a CyberVault Send-To version 2.x to version 3.x (for more information, please refer to the chapter “Run CyberVault Send-To as an an fi from the Windows command line", page 15

1. Open your XML file in a text editor.
2. Remove the line **<EncryptedPassword>EncryptPasswordSetBySoftware</EncryptedPassword>.**
3. Enter the initial password between the “Password” tags **<Password>Password</Password>.**
4. Save your XML file. The password is encrypted immediately after you run the XML file containing your changes. As of then, the encrypted password is displayed between the “EncryptedPassword” tags.

4 Configure CyberVault Send-To

4.1 Configure a Data Room Server Connection

To add a Data Room server:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the **Data Room Folder** area, click **Browse**.
3. Click **Add Server**.
4. Open the **Server URL** drop-down list, and select a Data Room server, or type the server's URL into the field. Enter your **Username** (the e-mail address you defined during your first registration to the Data Room server).
5. Enter your **Password**.
6. Enable the **Remember my Password** option, if you want CyberVault Send-To to remember your login information.
7. Click **OK.**

To change the Data Room server:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the **Data Room Folder** area, click **Browse**.
3. Select the server you want to change.
4. Click **Modify Server**.
5. Change the **Server URL** or your **Username** and **Password.**
6. Click **OK.**

To remove a Data Room server:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the **Data Room Folder** area, click **Browse**.
3. Select the server you want to remove.
4. Click **Remove Server.**
5. Confirm the security prompt with **Yes.**

4.2 Use the Full Integrity Check

The full integrity check is an option to calculate and validate checksums for files that you download and upload. The full integrity check thus ensures that only the latest versions of the documents are downloaded and uploaded. The integrity check is enabled by default and should not be disabled!

To verify that the full integrity check is enabled:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the lower left corner, click **Options**.
3. Make sure that the A**lways use full integrity check (document fingerprint)** option is enabled.
4. Click **OK.**

4.3 Configure Connection Options

To configure the connection options:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the lower left corner, click **Options.**
3. Specify this information:
    - **Timeout:** Enter a time after which the Send-To operation is canceled. The default value is 60 seconds.
    - **Buffer Size:** A file will be split and transferred in smaller pieces. The Buffer Size value specifies themsize of the packet for the file transfer. The default value is 1 megabyte.
4. Click **OK.**

4.4 Configure Proxy Settings

To enable the proxy server:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the lower left corner, click **Options.**
3. Enable the **Enable Proxy?** option.
4. Click **Settings.** The **CyberVault Send-To - Proxy Configuration** window is displayed.
5. Select **Automatically detect settings** to apply the proxy settings from your Internet Ex-plorer.
6. You can also select **Manual configuration** and enter the **Host, Port, Username** and **Pass-word.**
7. Click **OK.**

To modify the proxy server configuration:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the lower left corner, click **Options.**
3. Enable the **Enable Proxy?** option.
4. Click **Settings.** The **CyberVault Send-To - Proxy Configuration** window is displayed.
5. Make your changes as described under “To enable a proxy server”.
6. Click **OK.**

To disable the proxy server:

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the lower left corner, click **Options.**
3. Disable the **Enable Proxy?** option.
4. Click **OK.**

5 Functionalities Available with Send-To

5.1 Upload Files to a PIN-Protected Data Room

1. In Windows Explorer, select documents or folders you want to upload to the Data Room.
2. Right-click the selected items.
3. Select **Send-To > CyberVault Secure Data Room.** The CyberVault Send-To dialog window is displayed.
4. In the Data Room Folder area, click Browse. By default the last folder you have uploaded to is displayed in the **Data Room Folder** dialog. The **SMS Login** window is displayed.
5. Enter the PIN you received by e-mail.
6. Click **OK.**

5.2 Upload Files to DRs Without Additional Authentication

1. In Windows Explorer, select the documents or folders you want to upload to the Data Room.
2. Right-click the selected items.
3. Select **Send-To > CyberVault Secure Data Room**. The CyberVault Send-To dialog window is displayed.
4. In the **Data Room Folder** area, click **Browse**. By default the last folder you have uploaded to is displayed in the **Data Room Folder** dialog.
5. Click **OK.**

5.3 Simulate a File Upload

To check if an upload of large documents will be successful you can simulate the upload be-forehand. The simulation verifies the accuracy of names and paths, and the accessibility of files and folders.

1. In Windows Explorer, select the documents or folders you want to upload to a Data Room.
2. Right-click the selected items.
3. Select **Send-To > CyberVault Secure Data Room.** The CyberVault Send-To dialog window is displayed.
4. In the **Data Room Folder** area, click **Browse**. By default the last folder you have uploaded to is displayed in the **Data Room Folder** dialog.
5. Click **Simulate** to check if files are correctly uploaded. After the simulation is complete, a dialog window is displayed. You can verify if the simulation was successful and open the report file.
6. Click **OK.**

5.4 Download Files from a Data Room

As of version 3.0, you can download files from your Data Room to a destination folder on your local disk also by using the graphical user interface of CyberVault Send-To.

1. Start **CyberVault Send-To** via your Windows Start menu. The CyberVault Send-To dialog win-dow is displayed.
2. In the **Data Room Folder** area, click **Browse.** By default the last folder you have down-loaded from is displayed in the **Data Room Folder** dialog.
3. Enable the **Download folder contents** option.
4. In the **Local Folder** area, click **Browse** to select a local target folder.
5. Click **OK.**

5.5 Send a Document Securely

You can also use CyberVault Send-To for securely sending a document that is not stored in the Data Room but locally, e.g. on your hard disk or a network drive. The document is then also saved to your Data Room. The shared document is added as a secure link to a new e-mail and is sent in an encrypted format to the selected recipients. You can only send one document
as a secure link at once. The type of delivery (Send To External Users (Anonymous), Send To External Users, Send To External Users (PIN), Send To Data Room Members) is defined by the security configuration of the target Data Room, or the security category of the document or folder, and cannot be changed.

To send a document securely:

1. In Windows Explorer, right-click the document you want to send securely.
2. Select Send-To > **CyberVault Secure Data Room.** The CyberVault Send-To dialog window is displayed.
3. In the **Data Room Folder** area, click **Browse**. By default the last folder you have uploaded to is displayed in the Data Room Folder dialog.
4. Specify this information:
   - **Recipient:** Click **To...** to enter a recipient you have already sent a secure link to. Alternatively enter the e-mail address.
   - **Subject:** The name of the item is entered as the subject by default. Overwrite this default text, if applicable.
   - **Message:** Enter a message text (maximum 3,000 characters).
   - **Pickup period (days):** Select the link validity period. The maximum validity period of a link to a document is 30 days. If required, overwrite the displayed default value with a lower value. Once the given period has expired, recipients can no longer access the document.

5. From the **Type of delivery** drop-down list, select which recipients may receive the document and which document format is used. The following options are available:

- **Send To External Users (Anonymous):** The link can be used without having to authenticate with a one-time PIN.
- **Send To External Users:** Recipients can download the document without having to authenticate with a one-time PIN. Every download is logged in the item history with the e-mail address of the recipient.
- **Send To External Users (PIN):** Recipients must authenticate themselves in the Data Room with a one-time PIN, which they receive in a separate e-mail. Every download is logged with the e-mail address of the recipient in the item history.
- **Send To Data Room Members:** The item can only be sent to Data Room members. Before downloading the document, recipients must authenticate themselves in accordance with the Data Room settings.

6. Click **OK.**

5.6 Create a New Data Room Folder

1. Start **CyberVault Send-To** via your Windows Start menu. The **CyberVault Send-To** dialog win-dow is displayed.
2. In the **Data Room Folder** area, click **Browse.**
3. Select the Data Room in which you want to create a new folder.
4. Click **Create New Folder.** The **New Folder** dialog window is displayed.
5. Enter a folder name.
6. Click **OK.** The new folder is created in the Data Room.

5.7 View Folders and Documents in the Web Browser

1. Start **CyberVault Send-To** via your Windows Start menu. The **CyberVault Send-To** dialog win-dow is displayed.
2. In the **Data Room Folder** area, click **Browse**.
3. Select the folder you want to view in the web browser.
4. Click **View In Web Browser**. You are directed to the login page of CyberVault Secure Data Room.
5. Enter your username and password, and click **Login**.
6. If the Data Room is PIN-protected, enter the PIN you received by e-mail and click **OK**. In the Data Room, you are directed to the **Folders** view.

6 Run Send-To from Windows Command Line

CyberVault Send-To can also be run from the Windows command line or another shell program. This enables CyberVault Send-To to be integrated in a standard job scheduling application. With
CyberVault Send-To in the command line you can download and upload documents and simulate the upload. You can also configure an XML file with all parameters and run it from the command line. The following chapters provide information on the syntax in the DOS command line, optional parameters, scenarios, and a step-by-step description of the procedure.

6.1 Syntax to Be Used in the Windows Command Line

SendToShell requires the following syntax:

SendToShell.exe [/?] /s SERVER (/u USERNAME /p PASSWORD | /winlogin | /certissuer "CERTISSUER" /certname "CERTNAME") /l "LOCAL PATH" [/o OBJECT ID | /t "TARGET PATH"] [/d DATAROOM ID] [/m MODE] [/simulate] [/r "REPORT PATH"] SendToShell.exe /i "OPTIONS PATH"

6.2 Parameters for CyberVault Send-To in the Command Line

You can also use CyberVault Send-To for securely sending a document that is not stored in the

Parameter	What Can Be Configured?	Which Values Can Be Used?
/?	Displays syntax explanations	Example: /?
/s	Must be followed by the URL of the server that the Send-To tool connects to	Example: /s secure.CyberVault.gov
/u	A username to be used for the server connection specified.	Example: /u user@domain.com
/p	To authenticate with the username, enter the password.	Example: /p Password
/winlogin	Select this option to authenticate via your Windows login.	To enable Windows login. /winlogin
/r	The path specifies where the report file will be saved along with its name and format. The report file can be saved as .xml or .xls	Example: /r c:\temp\report.xml
/i	Must be followed by a valid path to an XML file listing all input parameters to be used for the call to SendToShell.	Example: /i c:\temp\Send-ToShell.XML

Parameter	What Can Be Configured?	Which Values Can Be Used?
/certissuer	Select this option, to authenticate with a certificate. Enter the issuer of the certificate.	Example: /certissuer CN=QMCA, DC=qmserver, DC=local
/certname	Select this option, to authenticate with a certificate. Enter the name of the certificate.	Example: /certname E=xxx@CyberVault.com, CN=stag800p_Uxxxx, CN=Users, DC=qmserver, DC=local
/l	Must be followed by a local path. It specifies the location to which or from which Send-To should upload or download documents. A path with blanks must be quoted. **Note:** Do not select the system root folder, e.g. C:\, because this folder will contain protected files and/ or folders that cannot be accessed by Send-To and will cause an error to occur.	Example: /l c:\temp
/o	Enter a folder Object ID to which or from which Send-To should upload or download documents.	Example: /o 123456789
/t	Enter a target path to which or from which CyberVault Send-To should upload or download documents.	Example: /t /My DRC/My Dataroom/ Documents/My Folder
/d	Enter a valid Data Room ID to which or from which Send-To should upload or download documents.	Example: /d 123456789
/m	By default, CyberVault Send-To uploads files and folders to the Data Room. Select if you want to upload or download files and folders.	To upload files and folders: /m UPLOAD To download files and folders: /m DOWNLOAD
/simulate	To check if an upload of large documents will be successful you can simulate the upload beforehand. The simulation verifies the accuracy of names and paths, and the accessibility of files and folders. The detailed results of the simulation will be written to the report file.	To simulate the document upload: /simulate
/move	If activated, source files will be deleted after the transfer is complete.	To remove the files after upload: /move
/ignoreroot	The system root folder may contain protected files or folders that cannot be accessed by Send-To. If /IgnoreRoot is activated, only files below the source root folder will be transferred but not the root folder itself.	To ignore the document root folder: /ignoreroot

7 Run CyberVault Send-To as an XML File From the Windows Command Line

You can also create an XML file for running CyberVault Send-To from the command line. Copy the text and save it as a text file (*.txt). Adjust the parameters to meet your requirements. In the following chapters, you can find detailed information on the available parameters and their effects.

7.1 Exclude Certain File Types or Filenames From the Upload

You can exclude certain file types or filenames from the upload when running CyberVault Send-To from the command line using an XML file. For this, the following tag must be added to the XML file used: <ExclusionFilter></ExclusionFilter>. The text between the tags must be a regu-lar expression that defines which filenames (or parts of it) or extensions are to be ignored.

7.2 Example of an XML File for Running CyberVault Send-To From the Command Line

```
<CyberVault>
<option>
<Server>secure.gov.CyberVault.net</Server>
<LocalPath>c:\temp</LocalPath>
<Username>user@domain.com</Username>
<Password>Password</Password>
<CertIssuer>CN=QMCA, DC=qmserver, DC=local</CertIssuer>
<CertName>E=xxx@CyberVault.com, CN=stag800p_Uxxxx, CN=Users,
DC=qmserver, DC=local</CertName>
<WindowsLogin>true</WindowsLogin>
<ObjectID>201201</ObjectID>
<TargetPath>/My DRC/My Dataroom/Documents/My Folder</TargetPath>
<DataroomID>1111</DataroomID>
<DataroomName>My Dataroom</DataroomName>
<Mode>UPLOAD</Mode>
<Simulation>false</Simulation>
<IgnoreRoot>true</IgnoreRoot>
<Move>false</Move>
<ReportPath>c:\Report Files\report.xls</ReportPath>
```

<SendSubject>The message subject to be sent to the recipients</SendSubject>
<SendMessage>The message body to be sent to the recipients</SendMessage>
<SendRecipient>a.user@domain.com</SendRecipient>
<SendRecipient>b.user@domain.com</SendRecipient>
<SendRecipient>c.user@domain.com</SendRecipient>
<ExclusionFilter>.*\.pdf?$</ExclusionFilter>
<ExclusionFilter>.*\.log?$</ExclusionFilter>
<ExclusionFilter>.*\.db?$</ExclusionFilter>
</option>
</CyberVault>

7.3 Parameters Available in the CyberVault Send-To XML File

Parameter	What Can Be Configured?	Which Values Can Be Used?
<server>	Must be followed by the URL of the server that the Send-To tool connects to, e.g. secure.gov. CyberVault.net	Example: <Server>secure.gov.CyberVault.net</Server>
<LocalPath>	Must be followed by a local path. It specifies the location to which or from which CyberVault Send-To should upload or download documents. A path with blanks must be quoted. **Note:** Do not select the system root folder, e.g. C:\ because this folder will contain protected files and/or folders that cannot be accessed by Send-To and will cause an error to occur.	Example: <LocalPath>c:\temp</LocalPath>
<Username>	A username to be used for the server connection specified.	Example: <Username>user@domain.com</Username>
<Password>	To authenticate with the username, enter the password.	Example: <Password>Password</Password>
<CertIssuer>	Select this option, to authenticate with a certificate. Enter the issuer of the certificate.	Example: <CertIssuer>CN=QMCA, DC=qmserver, DC=local</CertIssuer>
<CertName>	Select this option, to authenticate with a certificate. Enter the name of the certificate.	Example: <CertName>E=xxx@CyberVault.com, CN=stag800p_Uxxxx, CN=Users, DC=qmserver, DC=local</CertName>

Parameter	What Can Be Configured?	Which Values Can Be Used?
<Windows Login>	Select this option, to authenticate via your Windows login.	Enter true to enable: <WindowsLogin>true</ WindowsLogin> Enter false to disable: <WindowsLogin>false</ WindowsLogin>
<ObjectID>	Enter a folder Object ID to which or from which CyberVault Send-To should upload or download documents.	Example: <ObjectID>123456789</ ObjectID>
<TargetPath>	Enter a target path to which or from which CyberVault Send-To should upload or download documents.	Example: <TargetPath>/My DRC/My Dataroom/Documents/My Folder</TargetPath>
<DataRoom ID>	Enter a valid Data Room ID to which or from which CyberVault Send-To should upload or download documents.	Example: <DataRoomID>123456789</ DataRoomID>
<Mode>	By default, CyberVault Send-To uploads files and folders to the Data Room. Select if you want to upload or download files and folders.	To upload files and folders: <Mode>Upload</Mode> To download files and folders: <Mode>Download</Mode>
<Simulation>	To check if an upload of large documents will be successful you can simulate the upload beforehand. The simulation verifies the accuracy of names and paths, and the accessibility of files and folders. The detailed results of the simulation will be written to the report file.	To enable the simulation: <Simulation>True</Simulation> To disable the simulation: <Simulation>False</Simulation>
<IgnoreRoot>	The system root folder may contain protect-ed files or folders that cannot be accessed by Send-To. If <IgnoreRoot> is activated, only files below the source root folder will be transferred but not the root folder itself.	To ignore the root folder: <IgnoreRoot>True</IgnoreRoot> To transfer all files: <IgnoreRoot>False</IgnoreRoot>
<Move>	If activated, source files will be deleted after the transfer is complete.	To remove files after the upload: <Move>True</Move> To save the files after the upload: <Move>False</Move>
<ReportPath>	The path specifies where the report file will be saved along with its name and format. The report file can be saved as .xml or .xls.	Example: <ReportPath>c:\temp\report. xml</ReportPath>

Parameter	What Can Be Configured?	Which Values Can Be Used?
<ExclusionFilter>	You can exclude certain file types or file names from the upload. The text between the tags must be a regular expression that defines which file names (or parts of it) or extensions are to be ignored.	Example: To exclude *.PDF files: <ExclusionFilter>.*\.pdf?$</ExclusionFilter> To exclude *.LOG files: <ExclusionFilter>.*\.log?$</ExclusionFilter> To exclude *.DB files: <ExclusionFilter>.*\.db?$</ExclusionFilter>

8 Create and Open the Send-To Report File

CyberVault Send-To records every document transfer in a report file. A new report is created af-
ter every Send-To operation and one line is entered for each document processed. If an error occurs while an item is being processed, CyberVault Send-To continues with the next item on the list. If connection issues arise during the transfer, CyberVault Send-To tries to re-establish the connection several times and continues with the transfer if possible.

By default the report file is stored in the user's **Temp** directory. Access to this directory is easy by using the **%temp%** environmental variable. If required, a different location can be specified in the graphical user interface.

To define a different location for the report file:

1. Start **CyberVault Send-To** via your Windows Start menu. The **CyberVault Send-To** dialog win-dow is displayed.
2. In the **Report File** area, click **Browse**.
3. Select the folder in which you want to save the report file.
   The filename is **SendTo-Report.xls** by default.
   The file can be saved as a pure XML file or in an XML format that can be opened with Mic-rosoft Excel (.xls, .xlsx). This offers various convenient functions like filters, for example.
4. Click **OK.**

The report file provides the following details:

Item	Value
Type	Displays the item type processed. Possible values: • **Document** • **Folder**
Status	Displays the status of the item processed: Possible values: • **Created** • **Already existed and nothing needed to be transferred** • **New document version was created** • **Error occurred**
Start	Displays the time the upload started.
End	Displays the time the upload was completed.
Bytes	Displays the volume of the data transferred
Object ID	Displays the Item ID of the file or folder in CyberVault™ Secure Data Room.
Fingerprint	Displays the unique document ID.
Source	Displays the folder path from where the document was uploaded.
Destination	Displays the folder path to where the document was uploaded.
Error	Displays the description of the error.

9 Open the CyberVault Send-To Log File

The **sendTo.log** file records the events which happen while CyberVault Send-To is used, e.g. download and upload of documents, API details, file locations, etc. As of version 3.0, errors that occur during batch downloading of files are also written in detail into the **sendTo.log** file which is located under **...\AppData\Local\Temp**. To access this folder type **%Temp%** into the address line of your browser. For each file that could not be downloaded, the error code and description is written into the log file. If an error occurs during batch processing, the download process continues with the next available file.

10 Frequently Asked Questions

The **sendTo.log** file records the events which happen while CyberVault Send-To is used, e.g. download and upload of documents, API details, file locations, etc. As of version 3.0, errors that occur during batch downloading of files are also written in detail into the **sendTo.log** file which is located under **...\AppData\Local\Temp**. To access this folder type **%Temp%** into the address line of your browser. For each file that could not be downloaded, the error code and description is written into the log file. If an error occurs during batch processing, the download process continues with the next available file.

10.1 What is Contained in the Send-To Installation Package?

The installation package (*.msi) contains the following software components:

- CyberVault Send-To
- Microsoft .Net Framework 4.5 Client

10.2 Known Restrictions

Issues when sending e-mails:

- A message with more than 2,000 characters is stored in a shortened version in the Data Room. However, the recipient receives the complete message.
- You cannot send CC e-mails with CyberVault Send-To.
- The delivery format (Brainmark, Original, or Edit) is defined by the security configuration of the target folder and cannot be changed.
- You cannot send multiple secure document links in one e-mail.

Further issues:

- For using Send-To, the Data Room Manager has to deactivate the options **Only allow access for trusted applications** (under **Data Room Administration > Security > Device Management > Edit > Only allow access for trusted applications**).
- Windows only supports path names up to 260 characters. If the path length of a selected folder or document exceeds the maximum, the CyberVault Send-To function is unavailable and displayed as deactivated. In this case, try to process the documents and folders in smaller units or move or rename the files respectively. Document and folder names with special characters will extend the path length significantly. Every special character adds three characters and every space adds six characters to the path.
- The local file structure from the root folder (typically C:) cannot be compared to the file structure of the Data Room when using CyberVault Send-To from the command line. Therefore some files may not be downloaded or uploaded.
- Currently, previous document versions can only be displayed in and downloaded from CyberVault™ Secure Data Room.
- You can restore deleted files in CyberVault™ Secure Data Room only.

11 Appendix: Document Revision History

Version	Date of Change	Revision
1.0	December 8, 2014	Update to version 3.0 added the following new chapters: • Download files from a Data Room (see page 10) • Exclude certain file types or filenames from the download (see page 14) • Open the CyberVault Send-To log file (see page 19)
1.1	December 16, 2014	Update to the supported operating systems (see page 4)
1.2	February 25, 2015	Correction in chapter "Exclude certain file types or file names from the download" which is now "Exclude certain file types or filenames from the upload" (see page 14)
1.3	March 25, 2015	Chapter "2.1 Check the Prerequisites": Updated the supported operating systems and versions (see page 4)
1.4	July 6, 2015	Update to version 3.1 • Chapter "2.1 Check the Prerequisites": Updated the supported operating systems and versions (see page 5) • New chapter 3.3 "Upgrade CyberVault Send-To from version 2.x to version 3.x" (see page 6)
1.5	August 19, 2015	Chapter "2.1 Check the Prerequisites": Added the possibility to use SAML authentication with SAML 2.0 protocol (see page 4)
1.6	October 12, 2015	Update to version 3.2 – no content changes
1.7	Novermber 11, 2015	Update of chapter 2.1 "Check the Prerequisites" (see page 5)
1.8	October 13, 2017	Known restriction added: **"deactivate the option Only allow access for trusted applications"**