IBM Aspera Connect User Guide 3.7.4

Mac OS X

Revision: 193 Generated: 04/23/2018 09:47

Contents

Introduction

Connect is an install-on-demand Web application that facilitates high-speed uploads and downloads with an Aspera transfer server.

Depending on your operating system, Connect is compatible with most standard Web browsers. It integrates all of Aspera's high-performance transport technology in a small, easy-to-use package that provides unequaled control over transfer parameters. Connect includes the following features:

Feature	Description
FASP file transport	High-performance transport technology.
Browser interface	Uploads and downloads are launched transparently by a Web browser.
Flexible transfer types	Easily transfer single files, multiple folders or entire directories.
Transfer retry and resume	Automatically retries and resumes partial and failed transfers.
Browser-independent transfer	The Web browser can be closed during transfer operations.
Transfer monitor	A built-in transfer monitor for visual rate control and monitoring.
HTTP fallback	HTTP fallback mode for highly restrictive network environments.
Proxy support	HTTP fallback and FASP proxy settings.
Content protection	Password-protect files that are being transferred and stored on the remote server.
Queueing	Allow a fixed number of concurrent transfers and place the rest into a queue.

System Requirements

For supported operating systems and browsers, see the release notes for this release of Connect.

Setting Up Connect

Part 1: Installation

This section explains the installation process for the IBM Aspera Connect on your system. Connect can be installed on your system through the Web installer or downloadable DMG. See the corresponding sections below.

CAUTION:

- Before performing a system-wide installation (all users of the machine), uninstall any per-user installations. For details, see Uninstalling on page 24.
- Eject all previous Connect installers before downloading the new installer.

Important: In order for Connect to function correctly, *you must have cookies enabled* within your browser. For instructions on verifying this setting, see the Help documentation for your browser.

The Connect Web Installer

1. Use your browser to navigate to your Aspera Web application (IBM Aspera Faspex, IBM Aspera Connect Server or IBM Aspera Shares).

2. Once you have reached the server's Web page, you see an **Install Now** button (or **Upgrade Now** button if you have an older version of Connect installed on your system).

   Depending on your operating system and browser, clicking this button either launches the automatic installer or redirects you to the Connect download page (for manual installation).
3. Follow the on-screen instructions to complete the installation process.
4. If your browser displays a security prompt or warning, click **Allow** or **Continue** to proceed.

The Connect Desktop Installer

You can download the Connect DMG directly from http://downloads.asperasoft.com/connect2/. Once downloaded, close your Web browser and run the installer on your machine. You will need to accept the terms and conditions and click **Install**.

After Installation

Once Connect has finished installing, you can open it from the following location:

Macintosh HD > Applications > Aspera Connect

OR

Macintosh HD > Users > *home_directory* **> Applications >Aspera Connect**

Note: In addition to the Connect application, the Aspera encryption/decryption utility (IBM Aspera Crypt) is also installed on your system.

Part 2: Network Environment

If you need to configure any network proxies or override network speeds, you can do so through Connect's **Network** option. Before modifying Connect's network configuration, review the network requirements below, which describe ports that may need to be open on your network (such as ports 22 and 33001).

Network Requirements

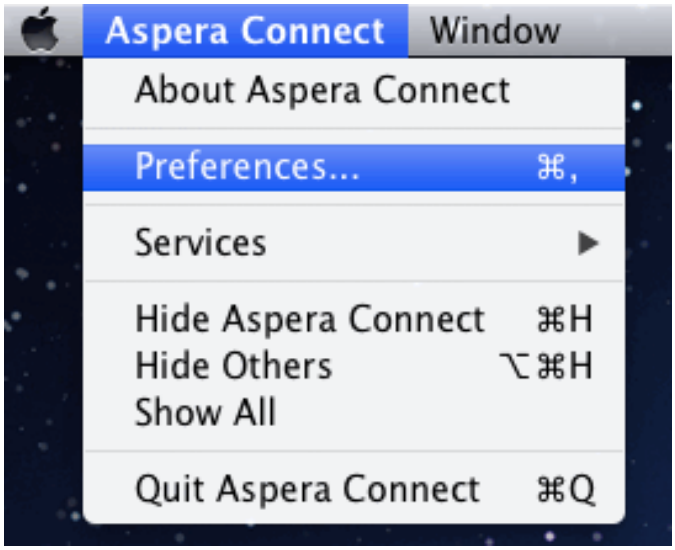
Your SSH outbound connection may differ based on your organization's unique network settings. Although **TCP/22** is the default setting, consult your IT department for questions related to which SSH port(s) are open for file transfer. Also see the Help documentation for your particular operating system, for specific instructions on configuring your firewall. If your client host is behind a firewall that does not allow outbound connections, you must allow the following:

- Outbound connections for SSH, which is **TCP/22** by default, although the server side may run SSH on another port (check with your IT department for questions related to which SSH port(s) are open for file transfer).
- Outbound connections for FASP transfers, which is **UDP/33001** by default, although the server side may run FASP transfers on one or more other ports (check with your IT department for questions related to which port(s) are open for FASP transfers).

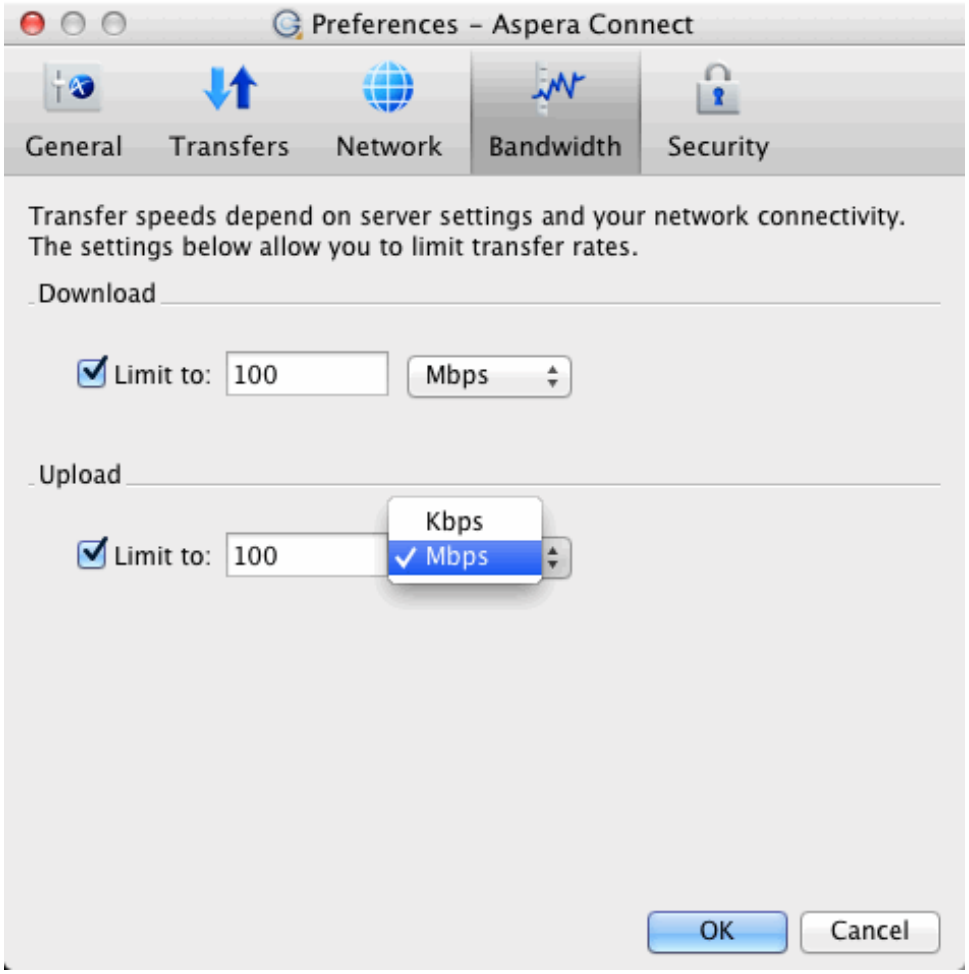
Limit Transfer Rates

Important: Do not set any values in these fields unless you need to limit the bandwidth that Connect uses.

Launch Connect (**Macintosh HD > Applications > Aspera Connect** *OR* **Macintosh HD > Users >** *home_directory* **> Applications > Aspera Connect**) and open **Preferences** (**Menu bar > Aspera Connect > Preferences**).



You can limit Connect's transfer rates via the **Bandwidth** option.



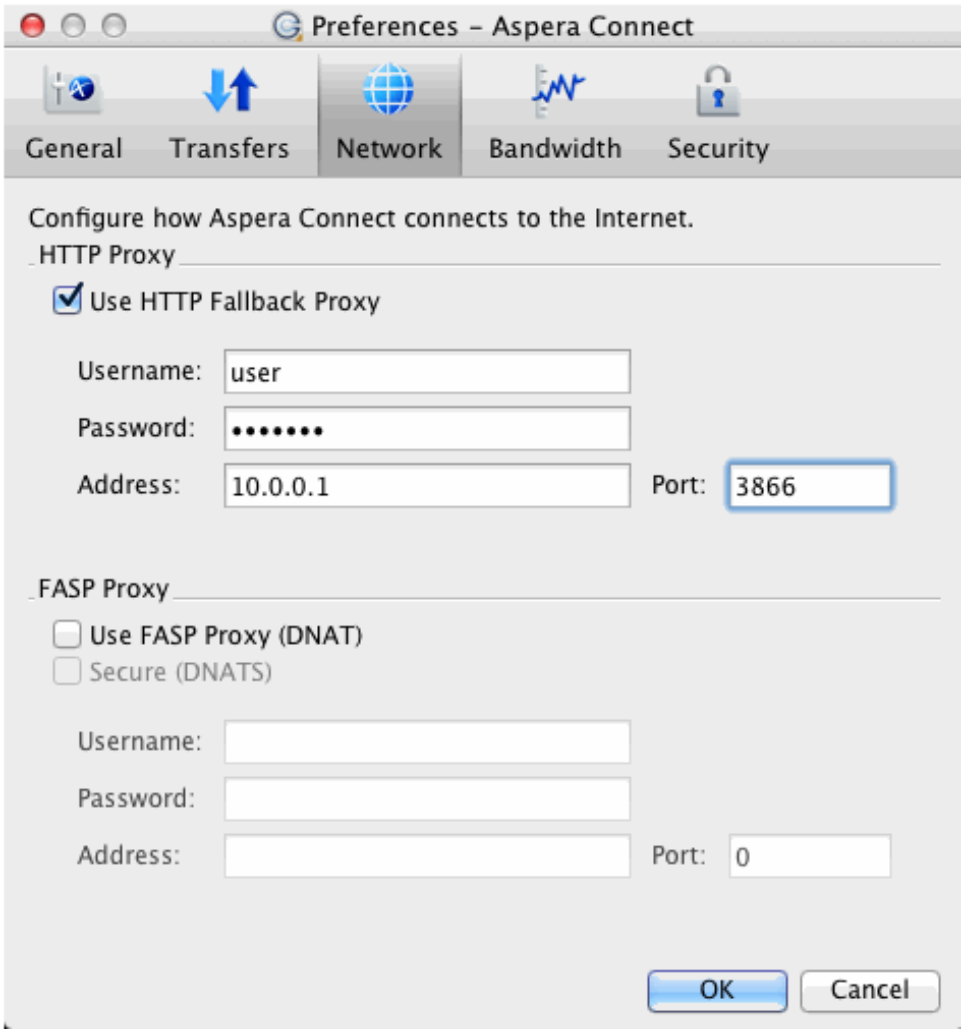
You can limit the download and upload transfer rates by enabling the respective checkboxes and entering a rate in either Mbps or Kbps. Note that your ability to limit these rates depends on the following factors:

- Your network's bandwidth: Available bandwidth on your network may limit your transfer rate, even if you enter larger numbers into these fields.
- Your Aspera server transfer settings: Settings on your server may limit your transfer rate even if your network bandwidth and the numbers you enter are larger.

HTTP Fallback Proxy

The HTTP fallback proxy should be used for fallback transfers only, *not* for FASP transfers.

To set up an HTTP fallback proxy, go to **Preferences > Network** in Connect.



Under the **HTTP Proxy** section, you can modify the proxy configuration for the server handling HTTP fallback. HTTP fallback serves as a secondary transfer method when the Internet connectivity required for Aspera accelerated transfers (that is, UDP port 33001, by default) is unavailable. If UDP connectivity is lost or cannot be established, if you have configured an HTTP fallback proxy, the transfer will continue over the HTTP protocol based on this proxy configuration.

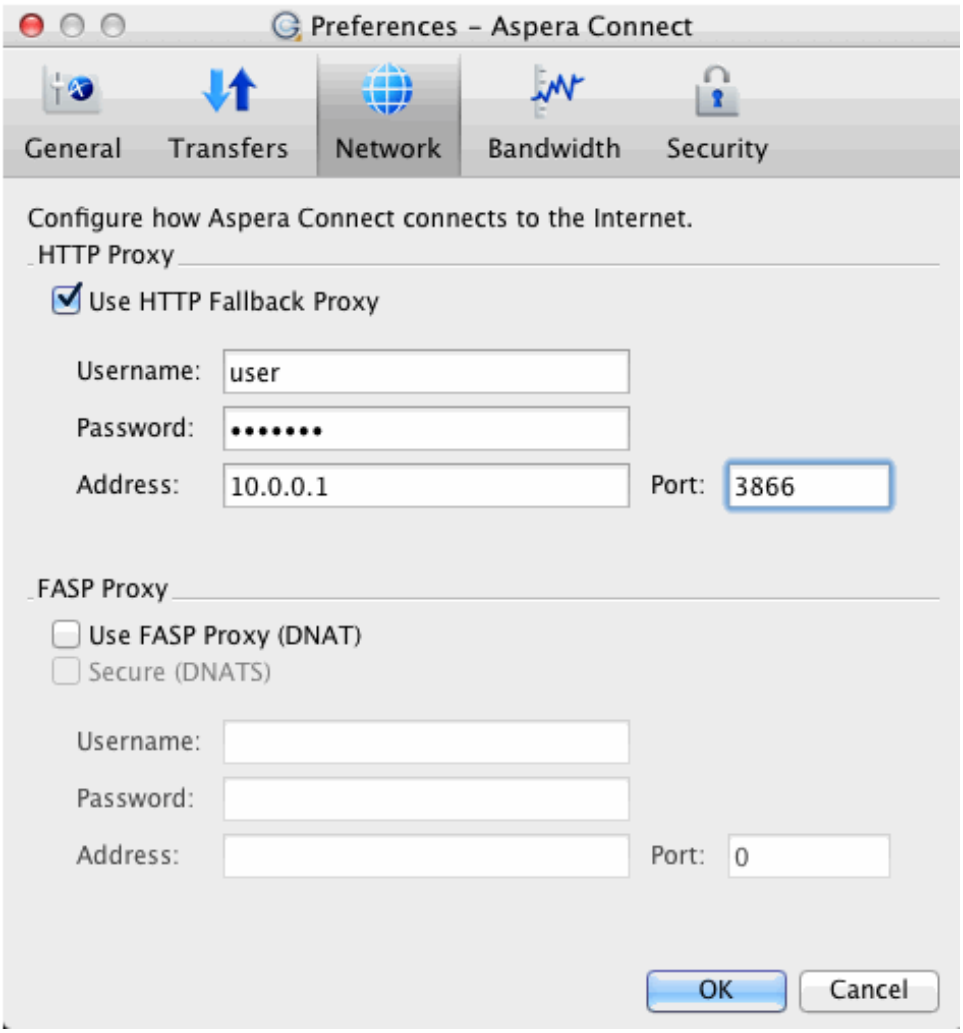
To configure an HTTP fallback proxy, select **Use HTTP Fallback Proxy** and enter your settings. These settings include NTLM authentication credentials (username and password), as well as the host name/IP address and port number.

FASP Proxy

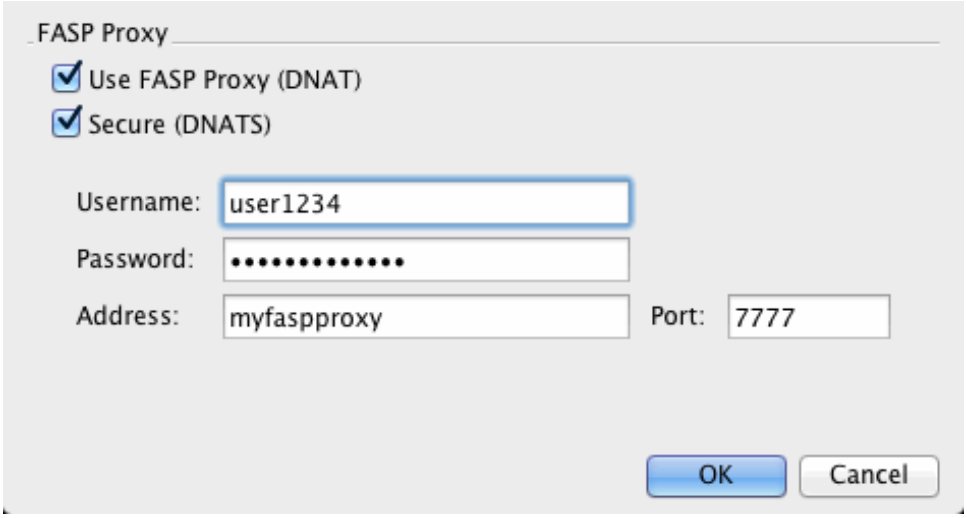
When FASP proxy is enabled, Aspera will pass the DNAT or DNATS (secure) username, server address, and port to **ascp**.

To set up a FASP proxy, do the following:

1. go to **Preferences > Network** in Connect.

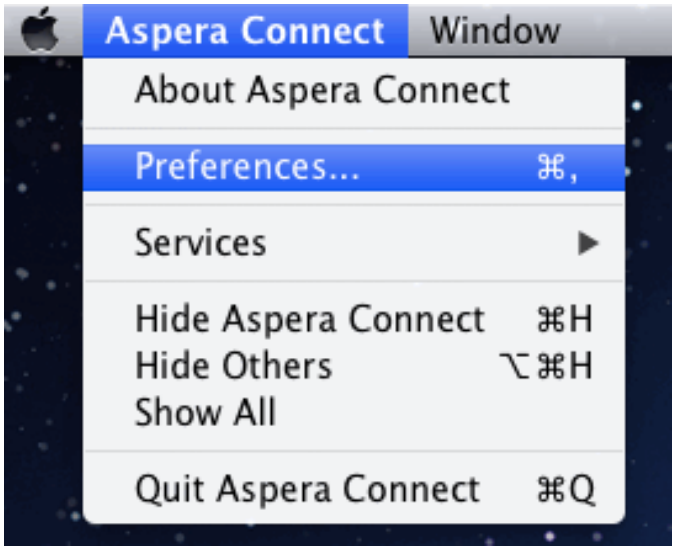


2. Enable the following checkbox(es):
   - **Use FASP Proxy (DNAT)**
   - **Secure (DNATS)**
3. Enter your proxy server username, password, address and port number.



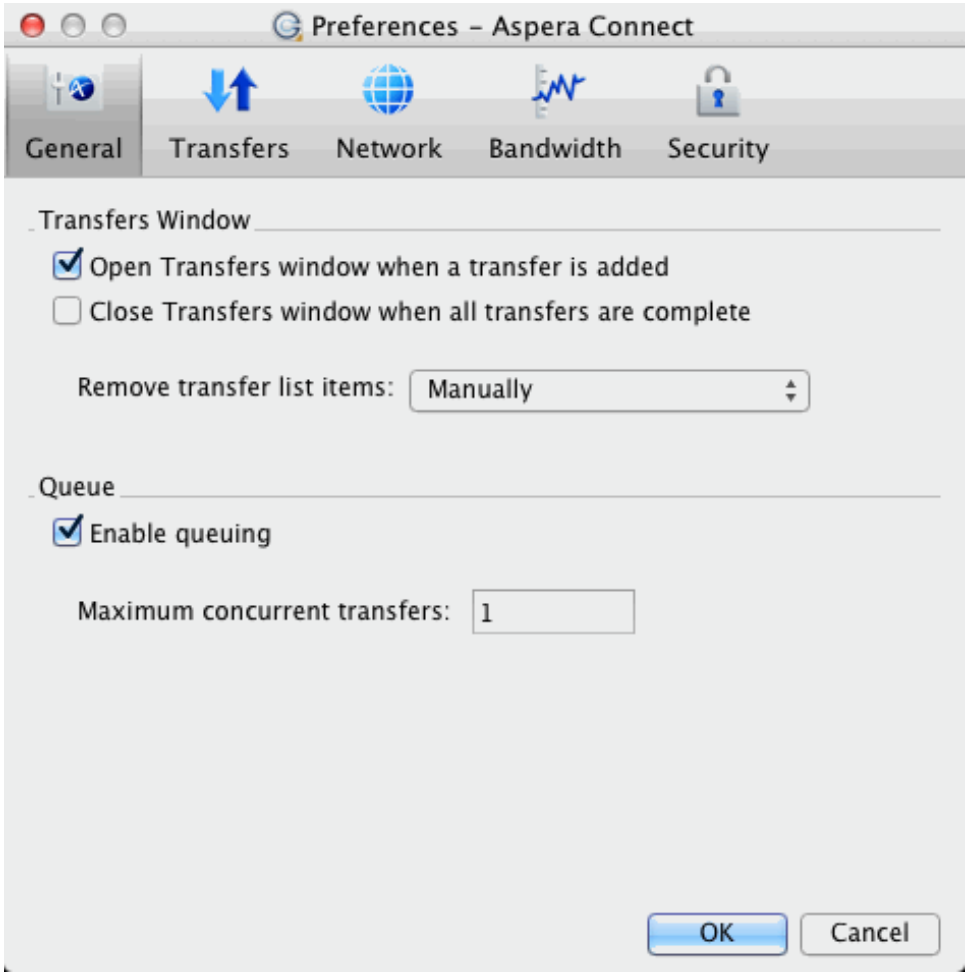
Part 3: Basic Configuration

To change the application's default settings before transferring files, launch IBM Aspera Connect (**Macintosh HD > Applications > Aspera Connect** *OR* **Macintosh HD > Users > (Home Directory) > Applications > Aspera Connect**) and open **Preferences** (**Menu bar > Aspera Connect > Preferences**).



General Preferences

Connect's general application behavior can be configured via the **General** option.



Under the **General** option, you can modify the following settings:

- Specify how the **Transfers** window should behave when a transfer begins and completes (via the checkboxes).
- Specify how transfer list items should be removed from the **Transfers** window (via the drop-down list).
- Enable or disable transfer queuing via the checkbox (which allows a fixed number of concurrent transfers and places the rest in a queue) and identify the maximum number of concurrent transfers via the text box.

Transfer Preferences

Connect's transfer behavior can be configured under **Preferences > Transfers**.

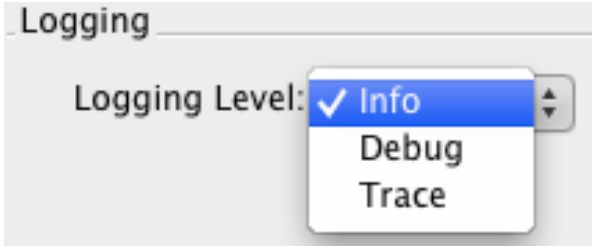
By default, Connect downloads files to the current user's **Downloads** folder. To change this setting, adjust the following settings:

- **Save downloaded files to**: Specify the path to save the downloaded files.
- **Always ask me where to save downloaded files**: Opt to select an ad-hoc location for each download.

You can also set a retry rule if a transfer fails. Set the retry rule within the **Retry** section as follows:

- **Automatically retry failed transfers**: Enable or disable.
- **Attempts**: Specify how many times Connect should attempt to retry the transfer.
- **Interval**: Specify the amount of time that should elapse between each attempt (in seconds, minutes or hours).

Lastly, you may configure a logging level that can be used to control the logging output when troubleshooting a transfer issue.



Note that this feature is typically utilized only when contacting Aspera Support. Select from one of the following options:

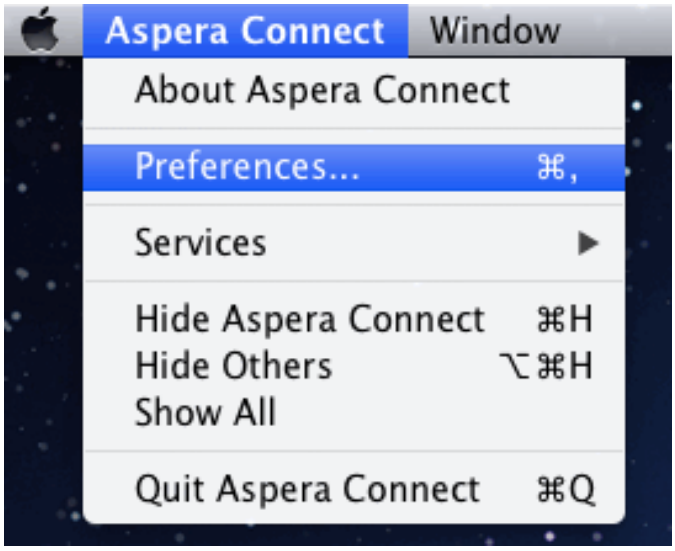
- **Info**: Displays general messages about requests, **ascp** spawn options and transfer status changes.
- **Debug**: Verbose (i.e., request validation and FASP management messages. **-D** will also be passed to **ascp**.
- **Trace**: Extra verbose. **-DD** will also be passed to **ascp**.

Part 4: Security Configuration

IBM Aspera Connect features the following capabilities for minimizing security risks when uploading or downloading files:

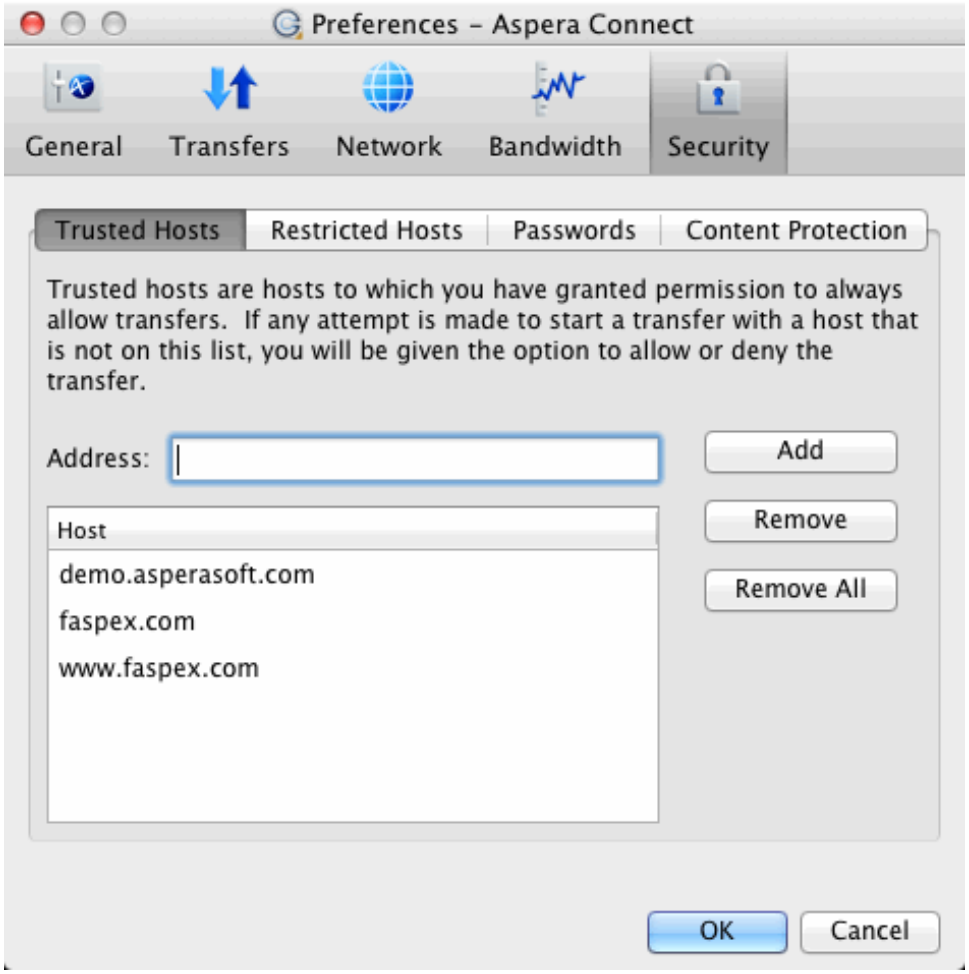
- You can add Aspera servers as **Trusted Hosts** to avoid the recurring security prompt, or add servers to the **Restricted Hosts** list to require confirmation every time you attempt to initiate a transfer with that host.
- You have the option of saving your authentication credentials when you connect to a server, as well as removing them from the **Passwords** tab.
- **Content protection** is a feature that allows uploaded files be encrypted during a transfer for the purpose of protecting them while stored on a remote server. The uploader sets a password while uploading the file, and the password is required to decrypt the protected file.

The settings above can be configured in the Connect **Preferences** dialog. To open the Connect **Preferences** dialog, launch Connect (**Macintosh HD > Applications > Aspera Connect** *OR* **Macintosh HD > Users > {Home Directory} > Applications > Aspera Connect**) and open **Preferences** (**Menu bar > Aspera Connect > Preferences**).

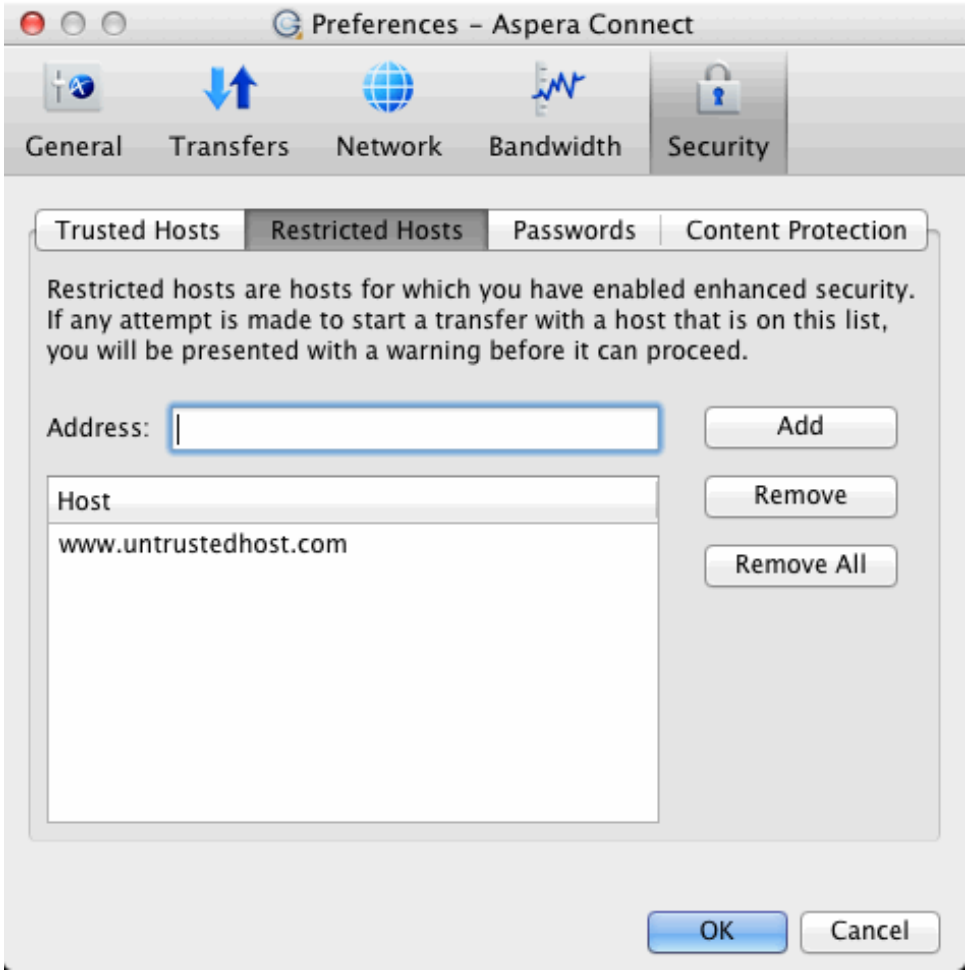


Managing Hosts

When a transfer is initiated and the **Use my choice for all transfers with this host** option is enabled in the confirmation dialog, the server that you are allowing or denying will be added to the **Trusted Hosts** or **Restricted Hosts** list, respectively. To view, add or remove additional trusted hosts, go to **Security > Trusted Hosts**. Enter the host's address in the specified text field and click **Add**.

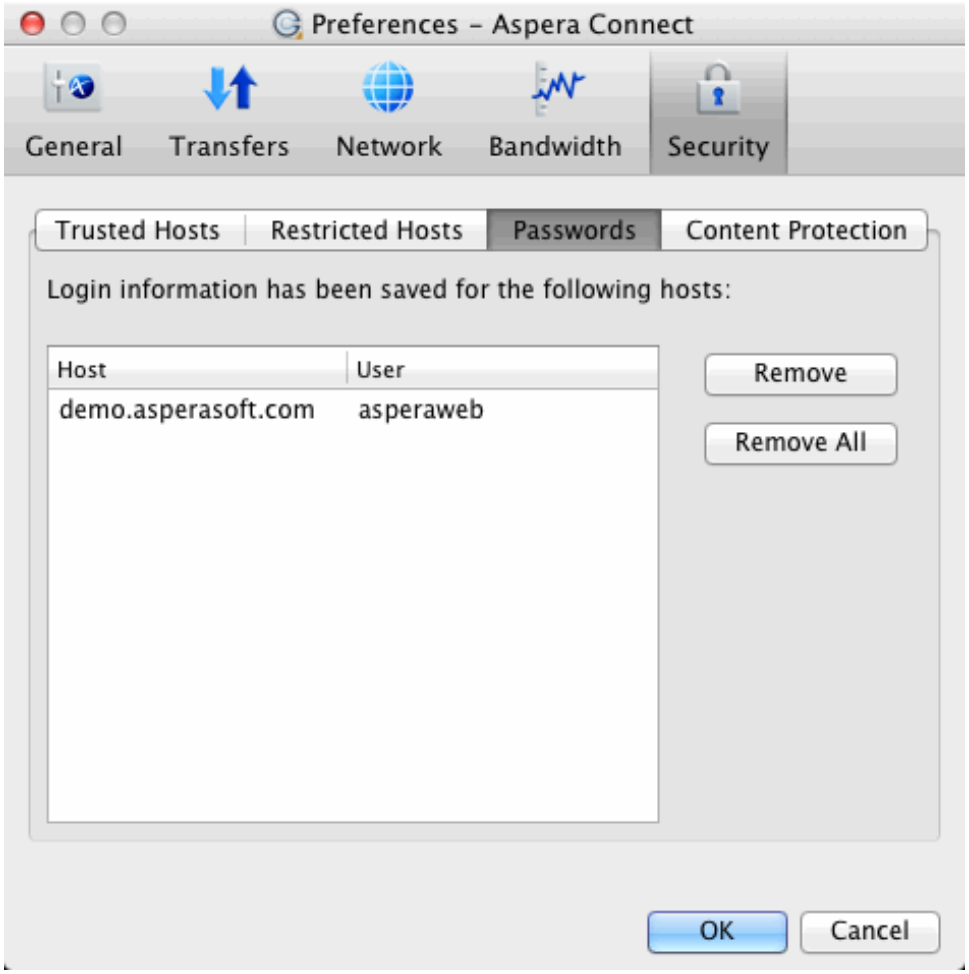


To view, add or remove restricted hosts, go to **Security > Restricted Hosts**. Here, enter the host's address in the specified text field and click **Add**.



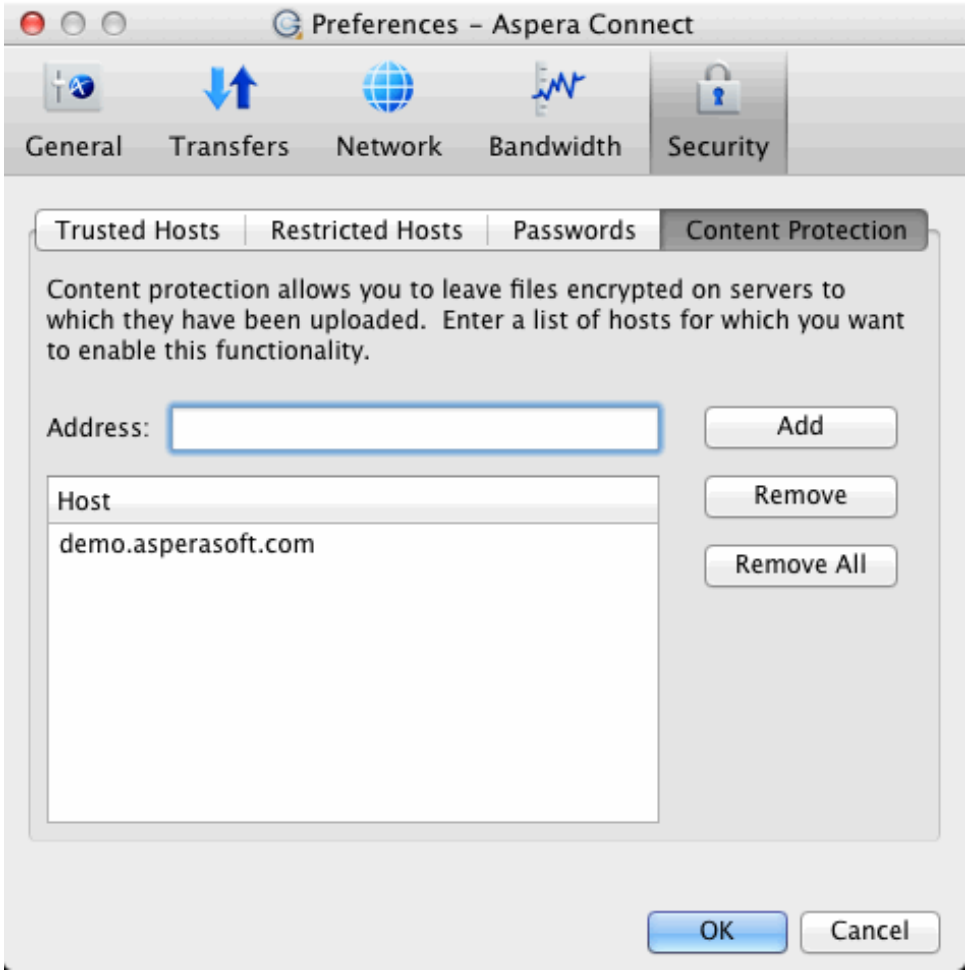
Important: By adding a host to the restricted list, you will be required to provide confirmation every time you attempt to initiate a transfer with that host.

To view, add or remove saved information for a host, go to **Security > Passwords**. Here, you can remove saved credentials.



Content Protection

To add hosts that require uploaded files to be encrypted during a transfer, click the **Content Protection** tab under the **Security** option. Enter your Aspera server address in the Address text field and click **Add**. The server will be added to the host list.



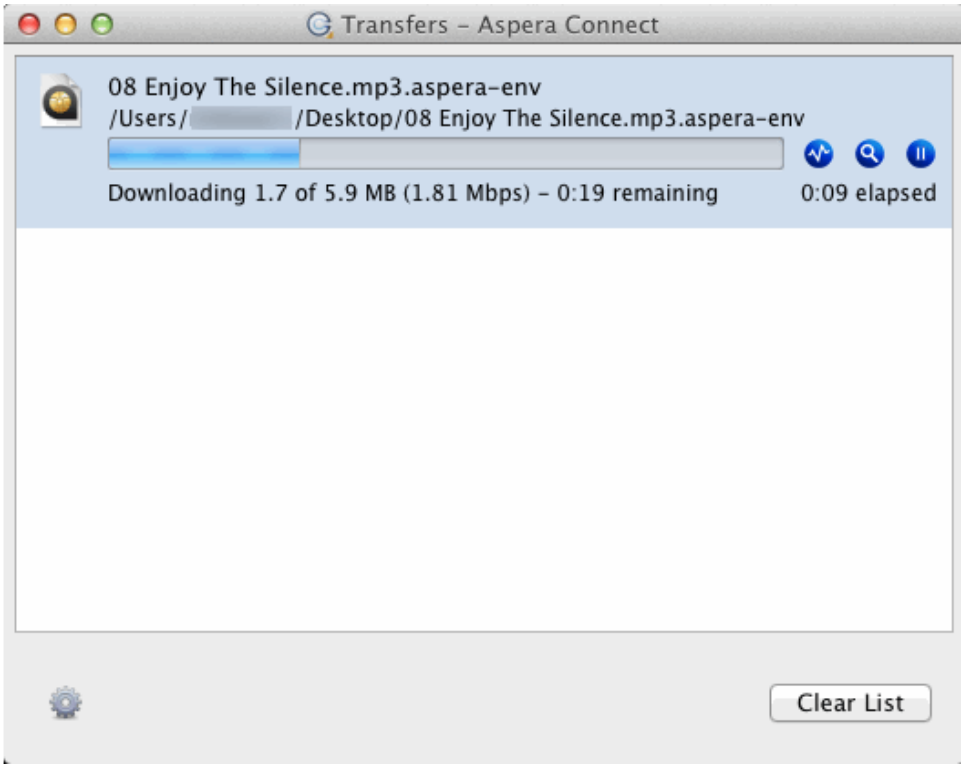
When uploading files to a server that is configured as a content-protected host, a confirmation window will appear and prompt you for a passphrase to encrypt the file. You can enter the passphrase in the text field, or check **Leave uploaded files unencrypted** *(if allowed by the server)* to proceed without using this feature. Click **OK** to start the transfer.

Once content-protected files have been uploaded to your server, they will appear with an *aspera-env* suffix (Aspera Security Envelope).

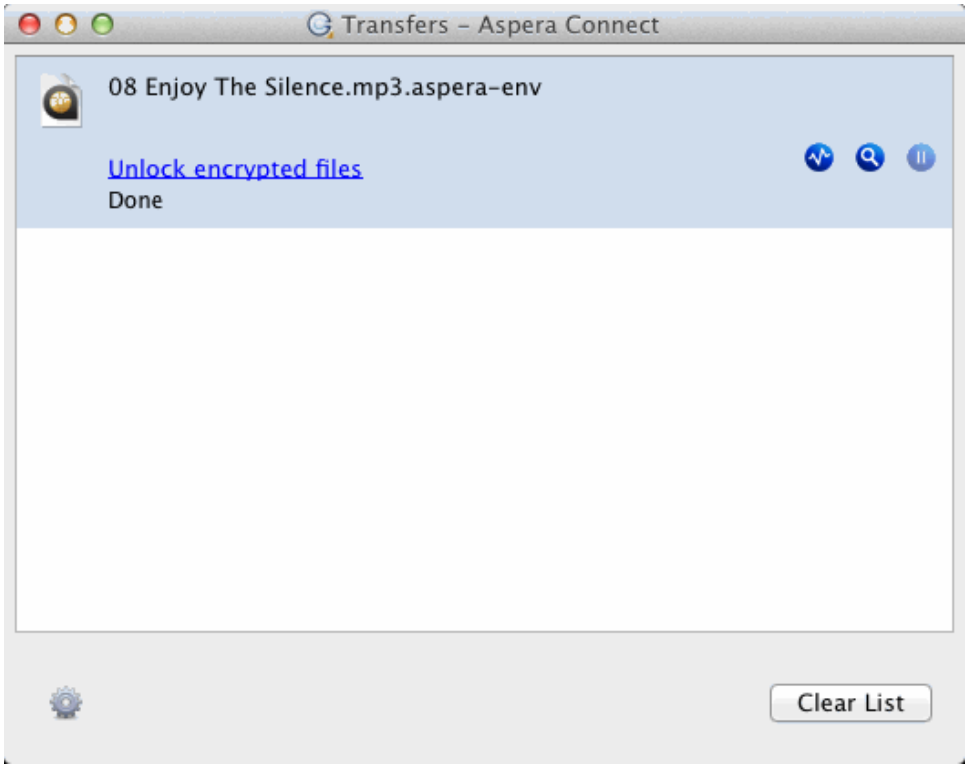
When you use Connect to download a content-protected file, you have two decryption options.

1. You can input and confirm your passphrase to decrypt the files *during* the download.
2. **OR**, you can enable the **Keep downloaded file encrypted** checkbox to download the content-protected files, and decrypt the files *after* the download has completed. When you select this option, you don't need to input your passphrase into the dialog box; however, you will need to take additional steps to decrypt the files on your local computer. See Decryption for details.

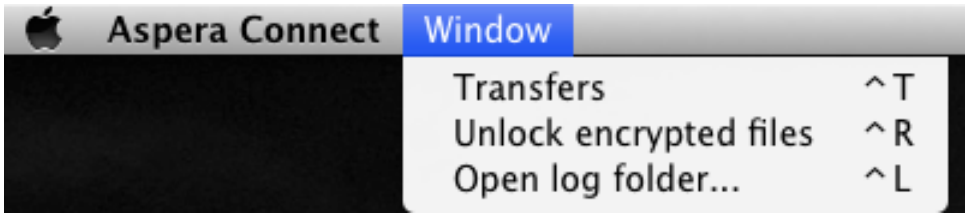
As the content-protected file is being downloaded to your computer, the file icon will change to that of the *aspera-env* file type in the Connect **Transfers** window.



Once downloading has completed, check your Connect **Transfers** window. If you inputted your passphrase to decrypt the files *during* the download (*Option 1*, above), you will be able to open the unlocked files without taking further action. If you elected to download the content-protected files and decrypt the files *after* the download has completed, you will receive a status message telling you to **Unlock encrypted files**, along with a link to the Aspera decryption utility.



Note that you can also unlock encrypted files from the Connect application menu (select the **Unlock encrypted files** option shown below).



For instructions on using the decryption utility, see Decryption.

Connect Functionality

Initiating a File Transfer

The following steps describe (1) how to perform a download test using Aspera's test server and (2) how to initiate a common file transfer using IBM Aspera Connect.

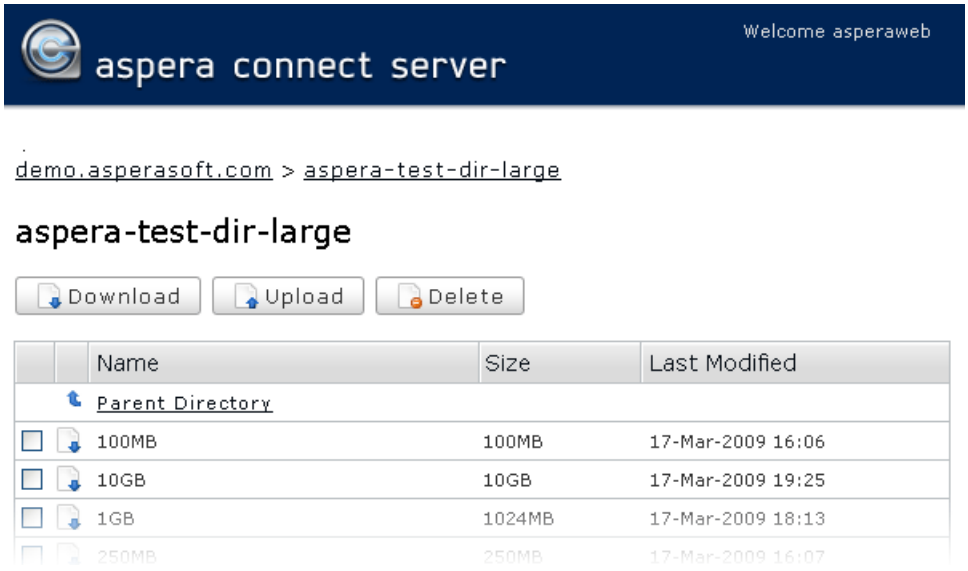
1. Open your Web browser and log in to Aspera's test transfer server at http://demo.asperasoft.com/aspera/user.

   Enter the following credentials when prompted:

   - **User:** asperaweb
   - **Password:** demoaspera

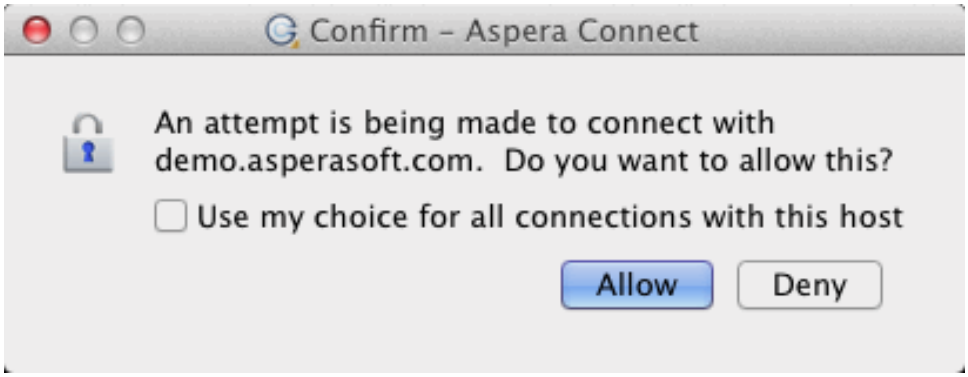
2. On the IBM Aspera Connect Server, browse into the folder */aspera-test-dir-large*

   Click any icon to download the corresponding file or folder. You may also checkmark multiple boxes and click **Download** to download more than one file or folder at a time.



3. Confirm the transfer.

   Select **Allow** to begin. Enable the **Use my choice for all connections with this host** checkbox to skip this dialog in the future.



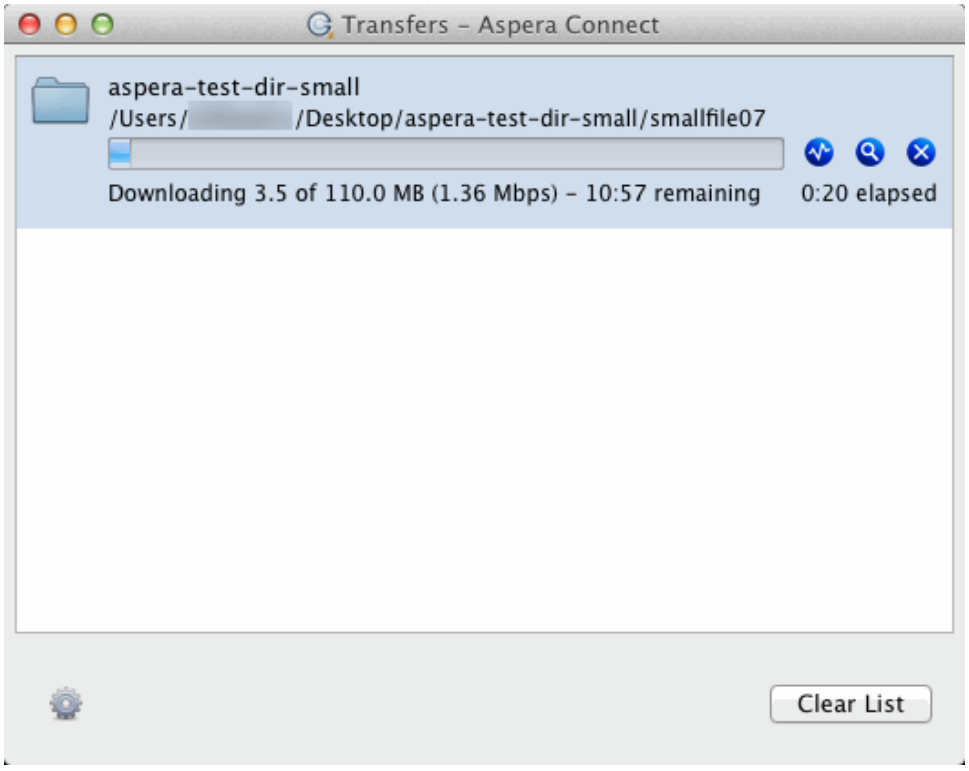
Once you confirm that the configuration settings are correct and that Connect is working properly, you can begin transferring with your organization's Aspera server. Simply point your browser to your server's address (e.g., *http://companyname.com/aspera/user*) to get started.

Note that when uploading, you should **avoid transferring files with the following characters** in the file name:

```
Characters to avoid: /   \   "  :   '   ?   >   <   & *  |
```

The Transfers Window

You can view and manage all transfer sessions within the **Transfers** window.

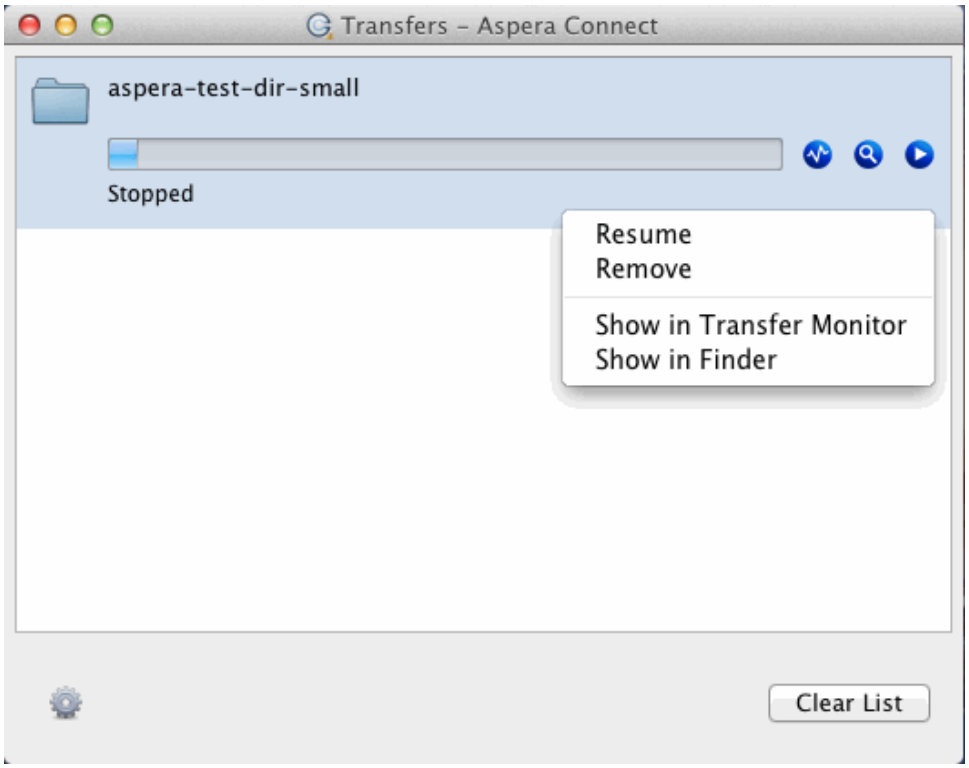


The **Transfers** window contains the following controls:

- Open the Transfer Monitor. For more information on using this feature, see Monitoring Transfers.
- Open the folder on your computer that contains this content.

- Stop the transfer session.
- Resume transfer.
- Retry a failed transfer.

When the queuing option is enabled, only a certain number of concurrent transfers are allowed. The additional transfers will be queued in the **Transfers** window and initiated when a transfer is finished. You can manually start a queued transfer by clicking the button. You can also right-click on a started or stopped transfer to access various controls. The example below shows the right-click options for a stopped transfer.



Monitoring Transfers

You can monitor and adjust file transfer speed by clicking to open the IBM Aspera Connect **Transfer Monitor** dialog. If you have sufficient server privileges and your transfer server is configured to allow it, you may modify the following in this dialog:

Field	Value
Transfer progress bar	Adjust the file transfer speed by clicking and sliding the transfer progress bar.
	Click to view the destination folder of the transferred files.
	Click to stop the transfer session.
Transfer policy: • Fixed • High	Select the transfer policy from the drop-down list: • The transfer transmits data at a rate equal to the target rate, although this may impact the performance of other traffic present on the network.

Field	Value
• Fair • Low	• The transfer rate is adjusted to use the available bandwidth up to the maximum rate. • The transfer attempts to transmit data at a rate equal to the target rate. If network conditions do not permit that, it transfers at a rate lower than the target rate, but not less than the minimum rate. • The transfer rate is less aggressive than Fair when sharing bandwidth with other network traffic. When congestion occurs, the transfer rate is decreased to the minimum rate, until other traffic retreats.

Note: You can only switch between High and Fair transfer policies if the host is IBM Aspera Enterprise Server version 3.0 or later.

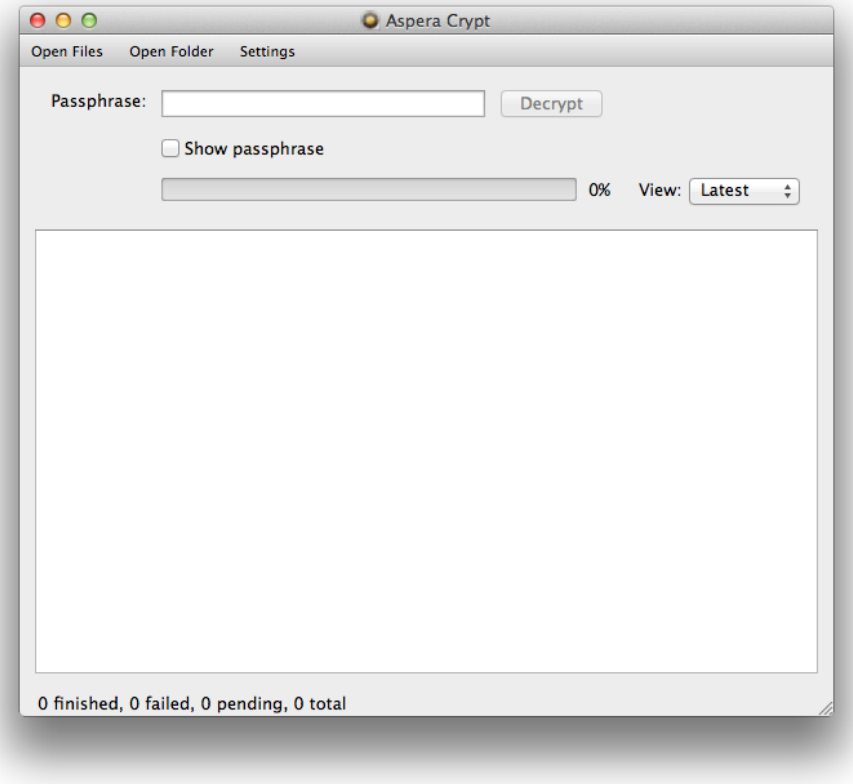
Decrypting Encrypted Files

Once you have downloaded an encrypted package, file or directory, Aspera Crypt makes it simple to browse for it in your file system, enter your passphrase and decrypt the contents.

Note: When an encrypted item has been downloaded to your computer, it will have the extension **.aspera-env** (Aspera Security Envelope).

1. Launch Aspera Crypt and browse for your package, file or directory.

   To launch Aspera Crypt, go to **Macintosh HD > Applications > Aspera Crypt**.



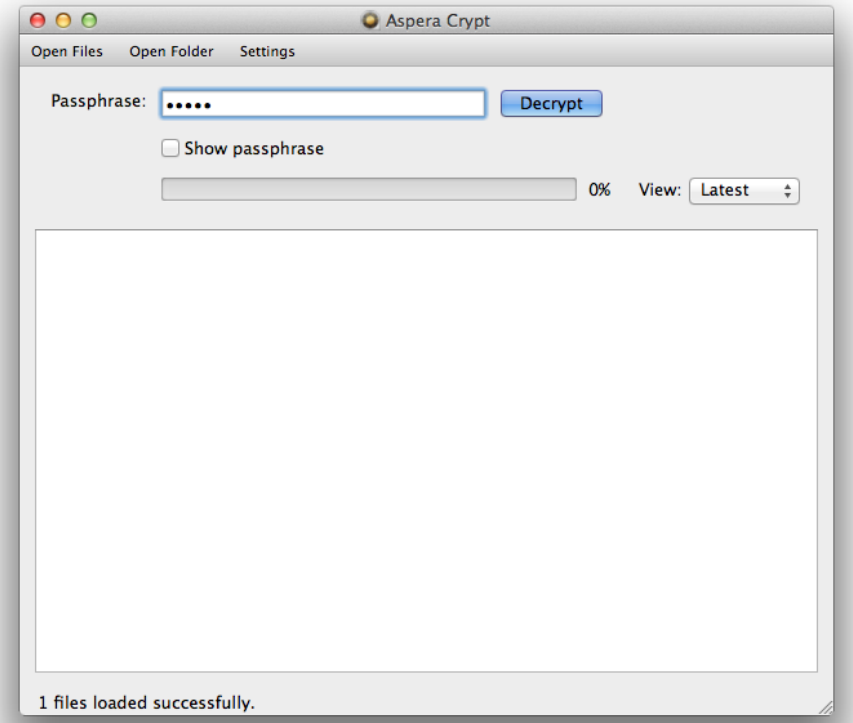
2. Browse for your package, file, or folder:

   - Click **Open Files** to locate a IBM Aspera Faspex package or an Enterprise/Connect server file.
   - Click **Open Folder** to locate an Enterprise/Connect server folder.

When your encrypted contents are loaded into Crypt, a status message appears at the bottom of the application, displaying the number of items ready for decryption.

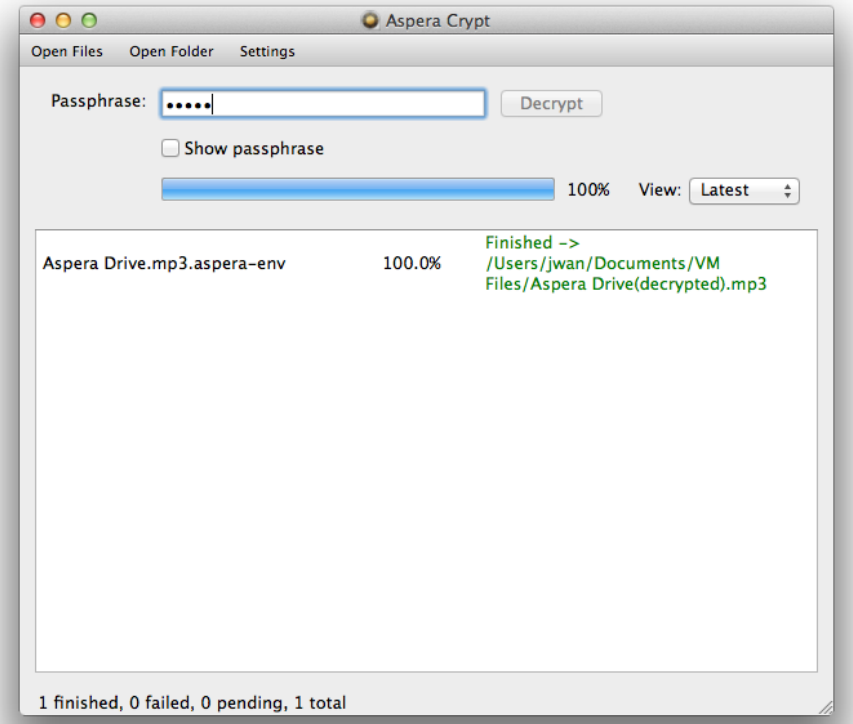
3. Input your passphrase and click the **Decrypt** button.

   After browsing for your contents, enter your passphrase in the text field. Your passphrase will be masked, unless you enable the **Show Passphrase** checkbox. Note that you must input the correct passphrase in order to activate the **Decrypt** button. Once the **Decrypt** button is activated, click it to decrypt your package, file or folder.

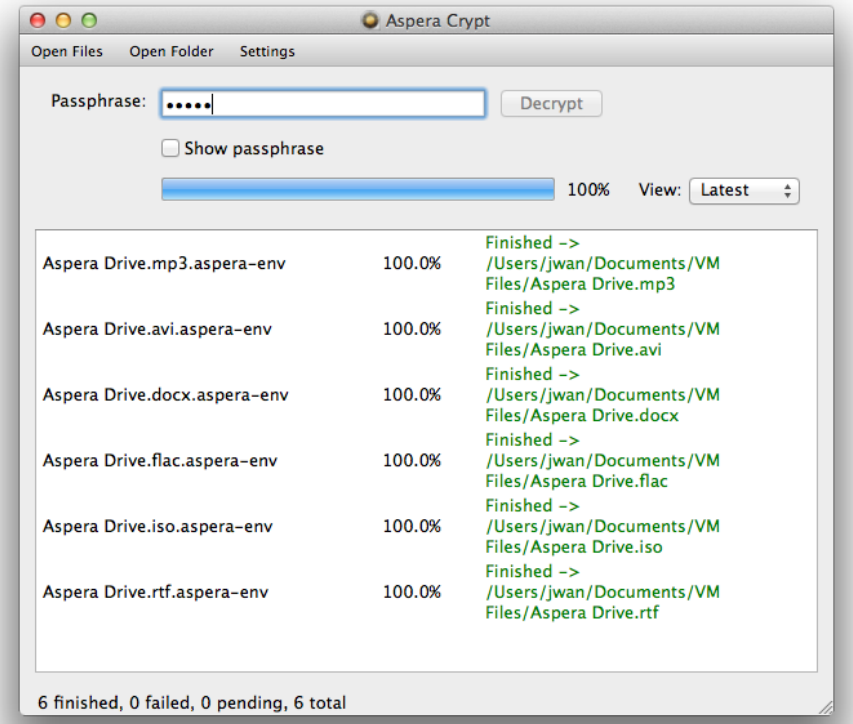


4. View output and confirm decryption.

   Once your package, file or folder contents have been successfully decrypted, you can view the output in the Aspera Crypt viewing window.



The decrypted contents will appear in the same directory as the original encrypted contents.



If your Crypt viewing window has multiple decrypted items listed, you can use the **View** drop-down list to sort the items by **latest**, **finished** or **failed**.

Maintaining Your Connect Installation

Upgrading

When a new version becomes available, Connect upgrades itself automatically.

If Connect does not upgrade automatically (for example, because the system does not have Internet access), you can fetch the latest version explicitly. To do so, go to http://downloads.asperasoft.com/connect2. Click **Upgrade Now** and follow the on-screen instructions. This process will either initiate auto-upgrade or download the latest installer.

Download Location

If you are upgrading an existing installation for which you changed the default download location, that custom location is preserved after you upgrade. Connect will continue to save your downloaded content to the location you specified.

Uninstalling

Important: Before proceeding with uninstalling Connect, you must quit any open browsers.

To uninstall the Connect Browser Plug-in, quit both the Connect application and any open Web browsers. Then, run the corresponding uninstall script below (based on how you installed Connect on your system).

Installation Method	Path
System-wide installation (all users)	**/Library/Application Support/Aspera/Aspera Connect/uninstall_connect.sh**
Per-user installation	**~/Library/Application Support/Aspera/Aspera Connect/uninstall_connect.sh**

File Cleanup

After uninstalling IBM Aspera Connect, old Connect files can be safely removed from your system.

Log Files

```
~/Library/Logs/Aspera_Connect
```

Database File

If you previously installed Connect for all users (that is, system-wide), then when *uninstalling*, you will only be able to remove the Connect database for the current user. Thus, to remove this database file (**connectdb.data**), you need to locate the following directory for each additional user account:

```
/Users/username/.aspera/connect/
```

You may alternatively delete the entire **.aspera** directory after uninstalling Connect, if desired.

Appendices

Log Files

Log Files

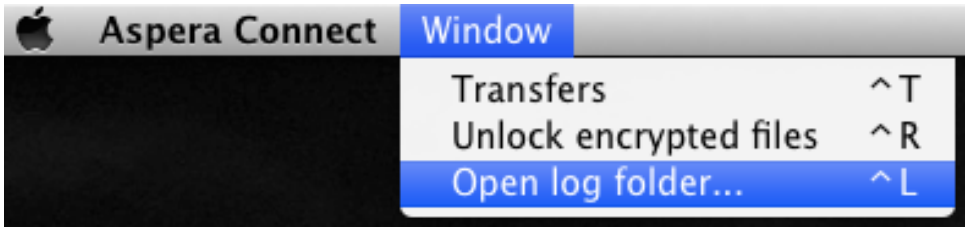
- **aspera-connect.log**
- **aspera-connect-browser-plugin.log**
- **aspera-scp-transfer.log**
- **aspera-webinstaller-plugin.log**

Log File Location

Log files are located in the following directory:

```
~/Library/Logs/Aspera_Connect
```

You can also use Connect's log folder shortcut by going to **Menu bar > Aspera Connect > Window > Open log folder**.



For information on removing old log files, see File Cleanup.

Plug-In Locations

Plug-In Location

Installation Type	Connect Browser Plug-In Location
User	**~/Library/Internet Plug-Ins**
System	**/Library/Internet Plug-Ins**

Web Installer Plug-In Locations

Browser	Web Installer Plug-In Location
Chrome	**~/Library/Application Support/Google/Chrome/Default/Extensions/aljbeaimggdioicepilcjnkphjobddok**
Firefox	**~/Library/Application Support/Firefox/Profiles/extensions/awi@asperasoft.com**
Safari	**~/Library/Internet Plug-Ins**

Troubleshooting

Connectivity Issues

SSH Connectivity Errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between the IBM Aspera Connect and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (the machine that Connect is installed on). Use `telnet` to test the connection to the server:

```
$ telnet server-ip-address 33001
```

where *server-ip-address* is the IP address of the Aspera server (ex. 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused":** The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.

- **"Timeout":** The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP Connectivity Errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

Aspera Connect Diagnostic Tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

```
https://test-connect.asperasoft.com/
```

Technical Support

Support Websites

For an overview of IBM Aspera Support services, go to http://asperasoft.com/company/support/.

To view product announcements, webinars, and knowledgebase articles, as well as access the Aspera Support Community Forum, sign into the IBM Aspera Support site at support.asperasoft.com using your email address (not your company Aspera credentials), or set up a new account. You can click on a heading then click **Follow** to receive notifications when new knowledgebase articles are available; if you follow **RELEASE NOTES** under a specific product, you will be automatically notified of new releases.

Personalized Support

You may contact an Aspera support technician 24 hours a day, 7 days a week, through the following methods, with a guaranteed 4-hour response time.

If you have an emergency, create a ticket using the **Support Request Form** with as many details as you have available and then **call**. If you are asked to leave a voice message, include the ticket number.

Email	support@asperasoft.com
Phone (North America)	+1 (510) 849-2386, option 2
Phone (Europe)	+44 (0) 207-993-6653 option 2
Phone (Singapore)	+81 (0) 3-4578-9357 option 2
Support Request Form	https://support.asperasoft.com/anonymous_requests/new/

Legal Notice