Aspera Connect 3.1.1

Debian/RHEL/CentOS/Ubuntu (GLIB 2.9+)

Document Version: V1

Contents

Introduction

Introducing the Aspera Connect install-on-demand Web browser plugin.

Aspera Connect is an install-on-demand Web browser plugin that powers high-speed uploads and downloads with an Aspera server. Compatible with most standard browsers depending on your Operating System, Aspera Connect integrates all of Aspera's high-performance transport technology in a small, easy-to-use package that provides unequaled control over transfer parameters. Aspera Connect includes the following features:

Feature	Description
fasp file transport	High-performance transport technology.
Browser Plug-in	Uploads and downloads are launched transparently by a Web browser.
Flexible Transfer Types	Easily transfer single files, multiple folders or entire directories.
Resume transfers	Automatically retries and resumes partial and failed transfers.
Browser-independent transfer	Web browser can be closed during transfer operation.
Transfer Monitor	Built-in transfer monitor for visual, rate control and monitoring.
HTTP Fallback	HTTP fallback mode for highly restrictive network environments.
Proxy Support	Input HTTP fallback and *fasp* proxy settings.
Content Protection	Password-protect files that are being transferred and stored on the remote server.
Queuing	Allow a fixed number of concurrent transfers and place the rest in a queue.

System Requirements

System requirements for installing/running Connect.

The following requirements are applicable when installing and running the Connect application:

- (*GLIB 2.9 and higher*) Debian 6.0+, RHEL/Centos 6.0+ or Ubuntu 8.04+.
- Firefox 4+ *(32-bit only)*

Setting up Connect

Install Aspera Connect and configure your computer for *fasp* file transfers.

Part 1: Installation

Instructions for installing Aspera Connect on your system.

This topic explains the installation process for Aspera Connect on your system. Connect can be installed on your system via the Web installer or downloadable package. Please refer to corresponding the sections below.

WARNING: Before installing Connect, ensure that you are running Debian 6.0+, RHEL/Centos 6.0+ or Ubuntu 8.04+. Connect 3.X supports GLIB 2.9 and higher.

IMPORTANT NOTE: For Connect to function correctly, you must have *cookies enabled* within your browser. Please review your browser help for instructions on verifying this setting.

Aspera Connect Web Installer

Use your browser to navigate to your Aspera Web application (i.e. Faspex Server, Connect Server or Shares). Once you have reached the server's webpage, you will 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 on this button will either launch the automatic installer or redirect you to the Aspera Connect download page (for *manual installation*). Follow the on-screen instructions to complete the installation process. If your browser displays a security prompt/warning, click **Allow** or **Continue** to proceed.

Aspera Connect Desktop Installer

You can download the Aspera Connect package directly from *http://beta-www.asperasoft.com/download_connect/*. Once downloaded, close your web browser and run the following commands in the installer's directory (replace the version number accordingly):

```
# tar -zxvf aspera-connect-<version>.tar.gz
# sh aspera-connect-<version>.sh
```

Post Installation

Once Aspera Connect has finished installing, it will execute automatically when connecting to a Connect, Faspex or Shares Server webpage. Look for the Connect icon in your system tray to confirm that it is running.

If Connect does not start automatically (or you need to restart it), you can execute the application manually with the following command:

```
# ~/.aspera/connect/bin/asperaconnect
```

Part 2: Network Environment

If required, configure network proxies or override network speeds via the Aspera Connect GUI.

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

Network Requirements

Your SSH outbound connection may differ based on your organization's unique network settings. Although **TCP/22** is the default setting, refer to your IT Department for questions related to which SSH port(s) are open for file transfer. Please also consult your specific Operating System's help documentation for specific instructions on configuring your firewall. If your client host is behind a firewall that does not allow outbound connections, you will need to allow the following:

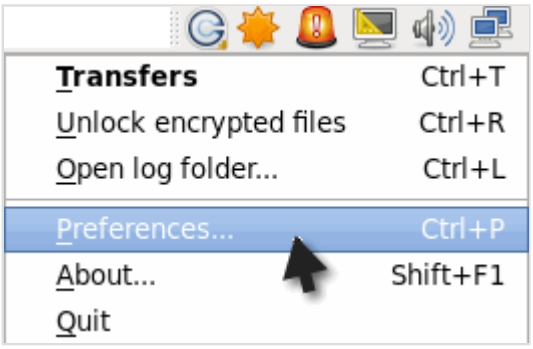
- Outbound connections for SSH, which is **TCP/22** by default, although the server side may run SSH on another port (please check with your IT Department for questions related to which SSH port(s) are open for file transfer).
- Outbound connections for *fasp* transfers, which is **UDP/33001** by default,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

Limit Transfer Rates

IMPORTANT NOTE: Unless you need to limit the bandwidth used by Aspera Connect, you should not set any values in these fields.

If Aspera Connect is already running, go to **System Tray** > **Right-click Aspera Connect** > **Preferences** . If it is not running, you can execute the application manually with the following command:

```
# ~/.aspera/connect/bin/asperaconnect
```



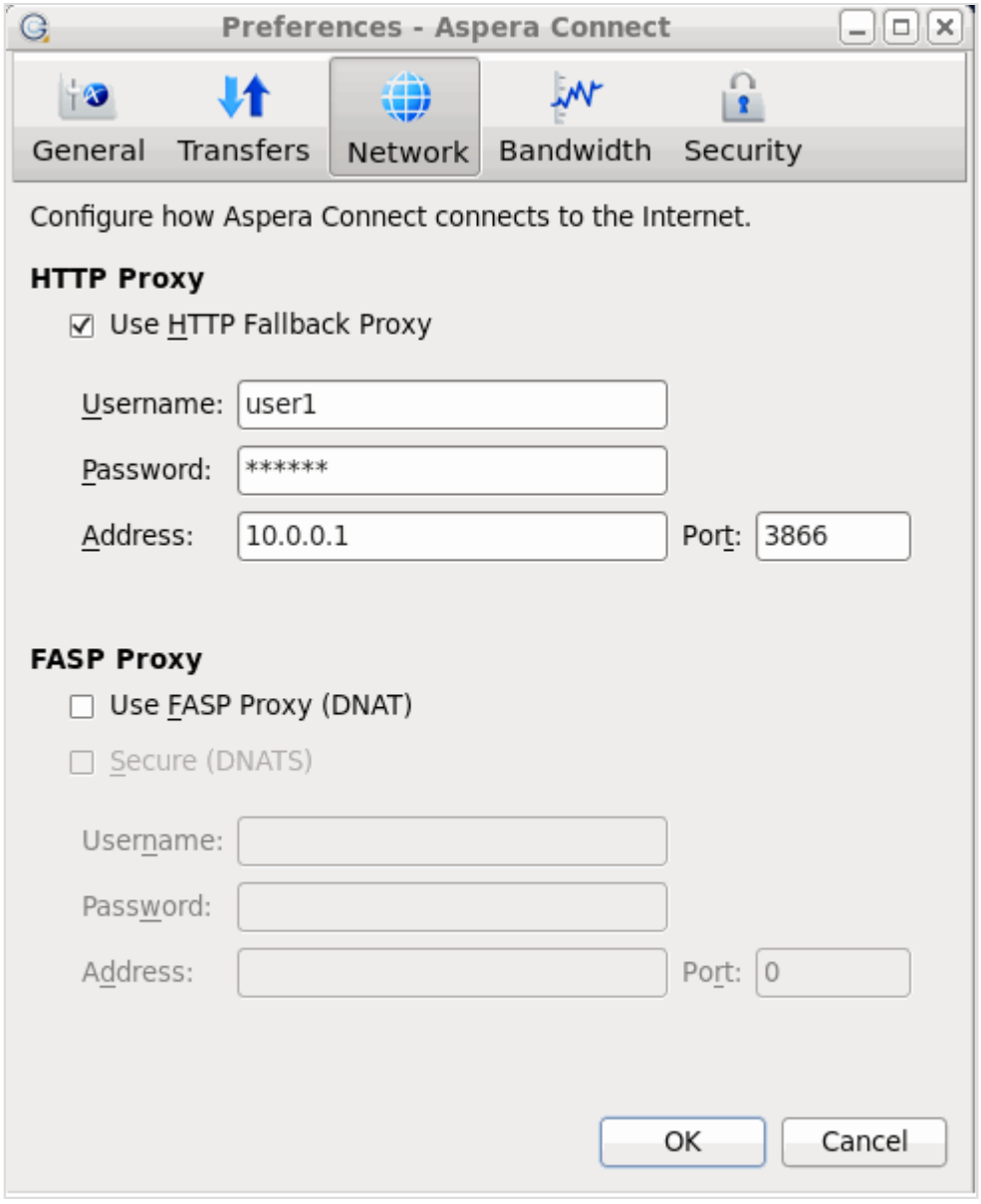
You can limit Aspera Connect's transfer rates via the **Bandwidth** option.

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

1. **Your network's bandwidth. If your bandwidth doesn't allow you to reach these limits, then they will not be enforced.**
2. **Your Aspera transfer server settings. Settings on your server may prohibit you from reaching transfer rates inputted into these fields.**

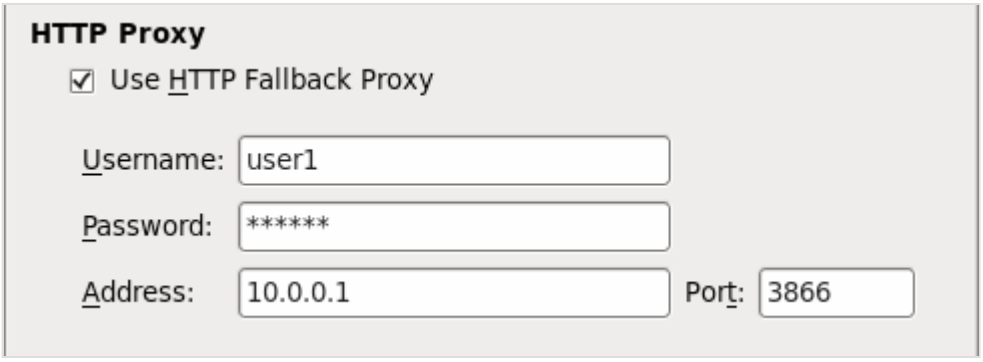
HTTP Fallback Proxy

The HTTP fallback proxy should only be used for fallback transfers, **not** for *fasp* transfers. To set up an HTTP fallback proxy, go to Aspera Connect **Preferences** > **Network** .



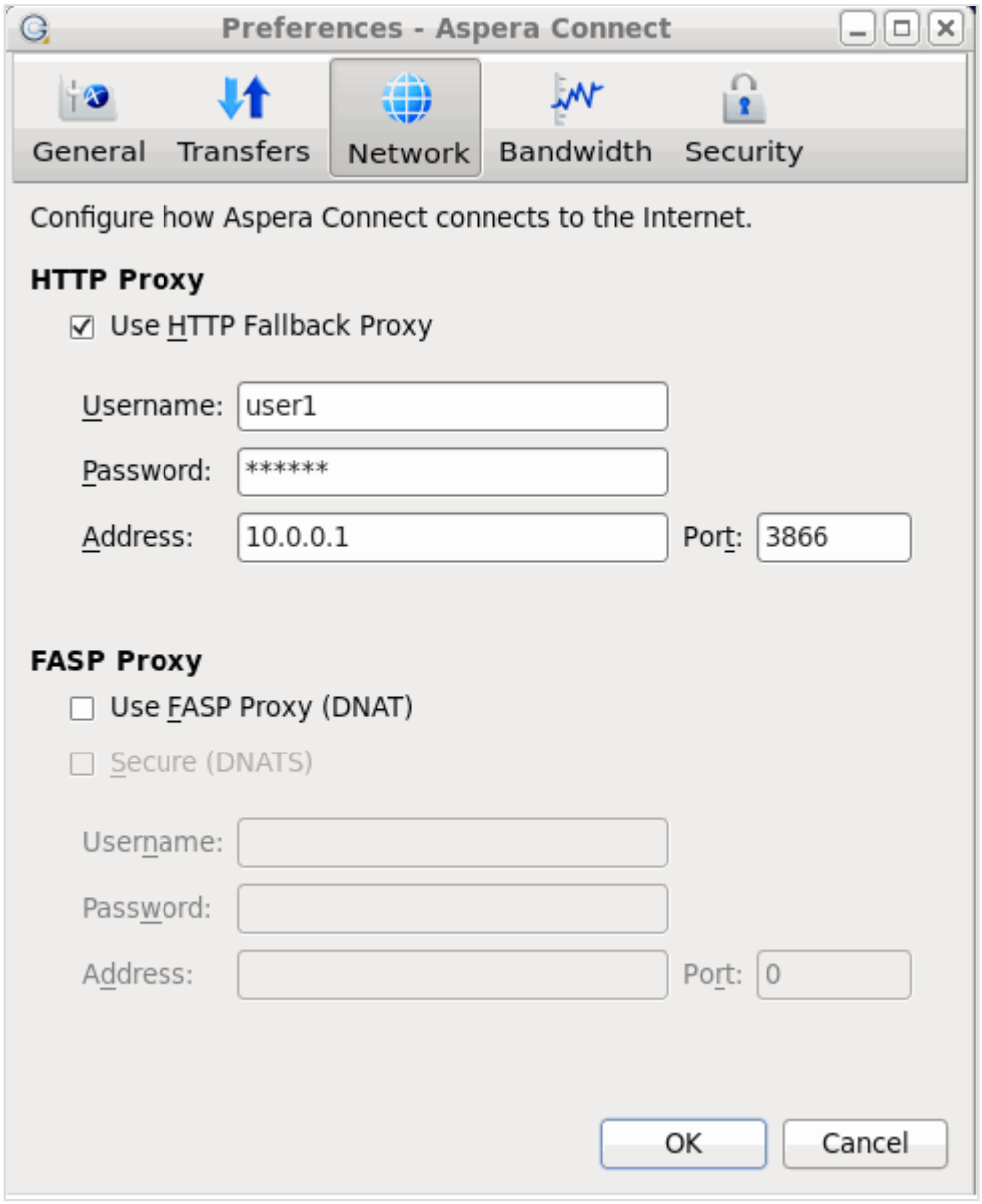
Under the **HTTP Proxy** section, you can modify the proxy configuration for the server handling HTTP fallback. HTTP fallback serves as a secondary transfer method when the Internet connectivity required for Aspera accelerated transfers (i.e., UDP port 33001, by default) is unavailable. If UDP connectivity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

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



FASP Proxy

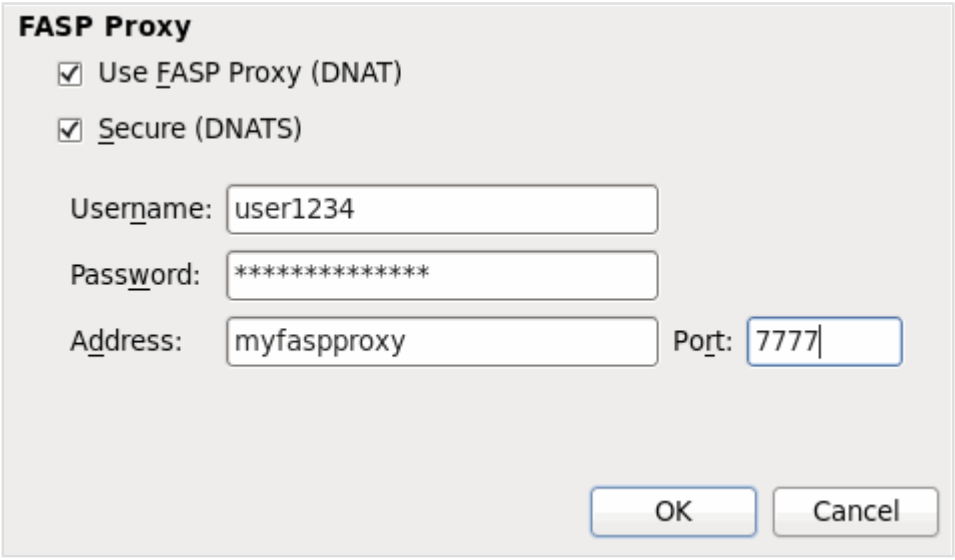
When *fasp* proxy is enabled, Aspera will pass the DNAT or DNATS (secure) username, server address and port to **ascp**. To set up a *fasp* proxy, go to Aspera Connect **Preferences** > **Network** .



To configure a *fasp* proxy, enable the following checkbox(es):

- Use FASP Proxy (DNAT)
- Secure (DNATS)

Upon selecting the checkbox(es), input your proxy server username, password, address and port number.

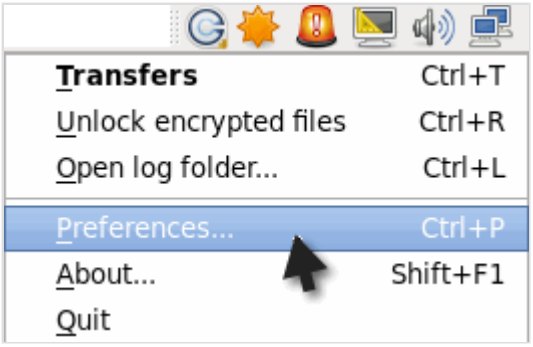


Part 3: Basic Configuration

Changing Aspera Connect's default settings via the "Preferences" option.

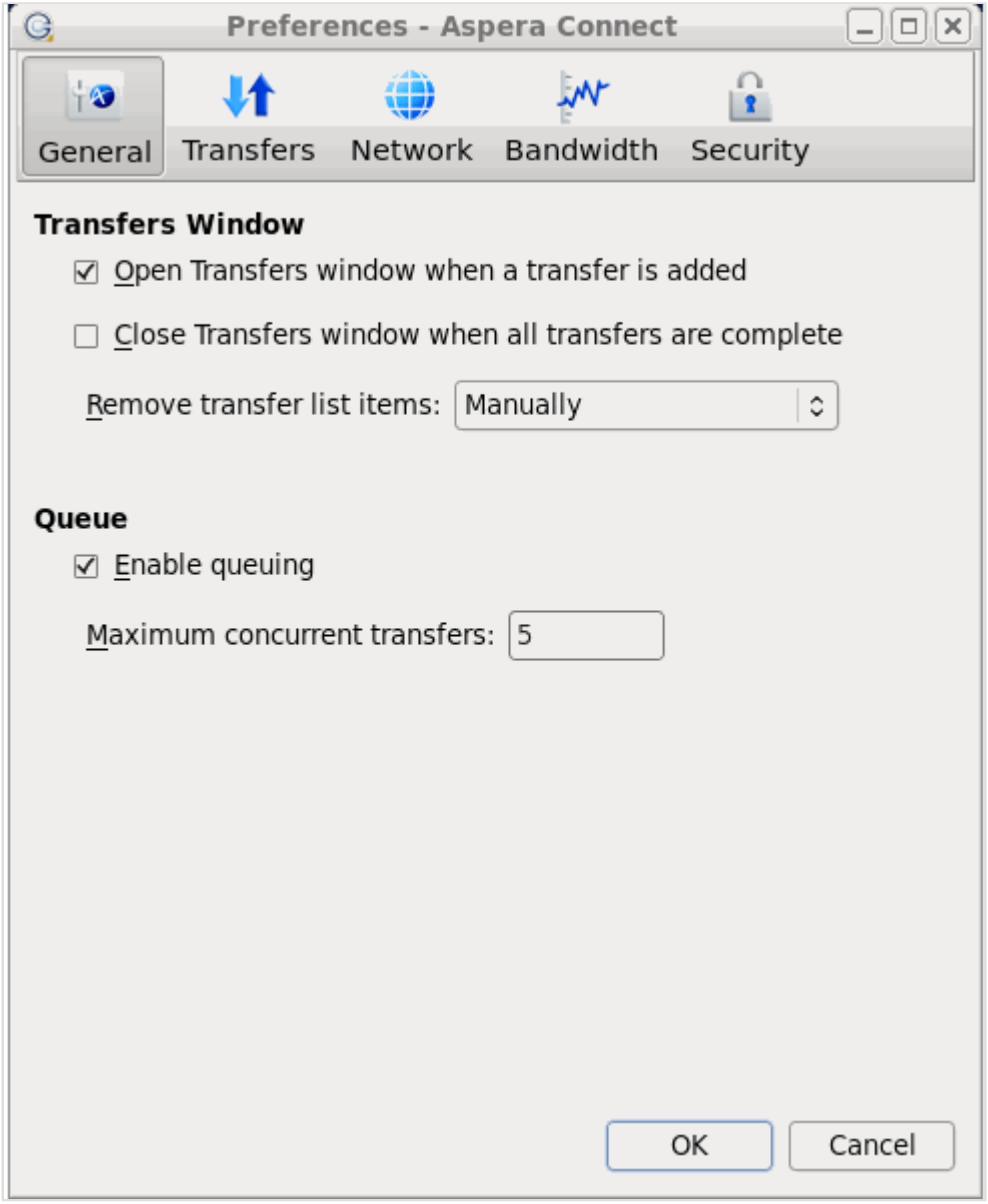
If Aspera Connect is already running, go to **System Tray** > **Right-click Aspera Connect** > **Preferences** . If it is not running, you can execute the application manually with the following command:

```
# ~/.aspera/connect/bin/asperaconnect
```



General Preferences

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

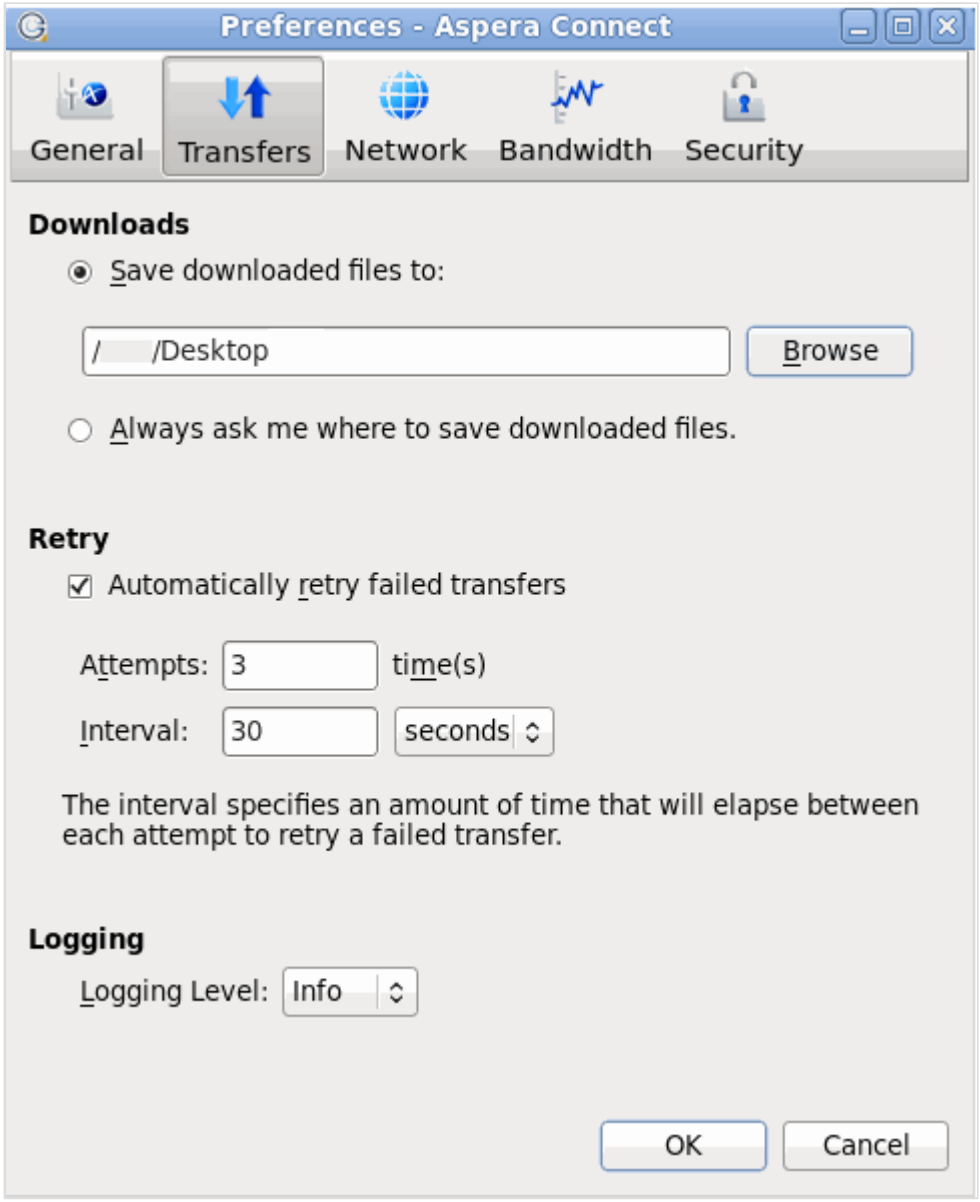


Under the **General** option, you can modify the following settings:

- 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

Aspera Connect's transfer behavior can be configured under the **Transfers** preference option.



By default, Connect downloads files to the current user's desktop. To change this setting, set the download rule within the *Downloads* section as follows:

- **Save downloaded files to**: Specify the path to save the downloaded files.
- **Always ask me where to save downloaded files**: 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

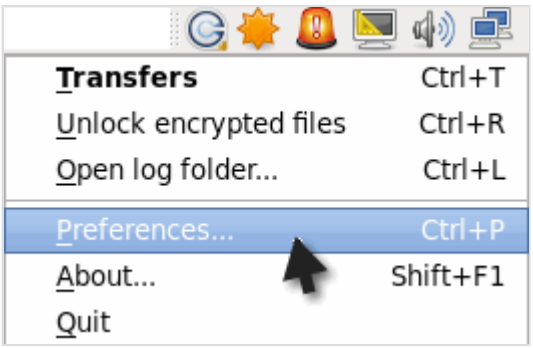
Configuring Aspera Connect's security preferences.

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.

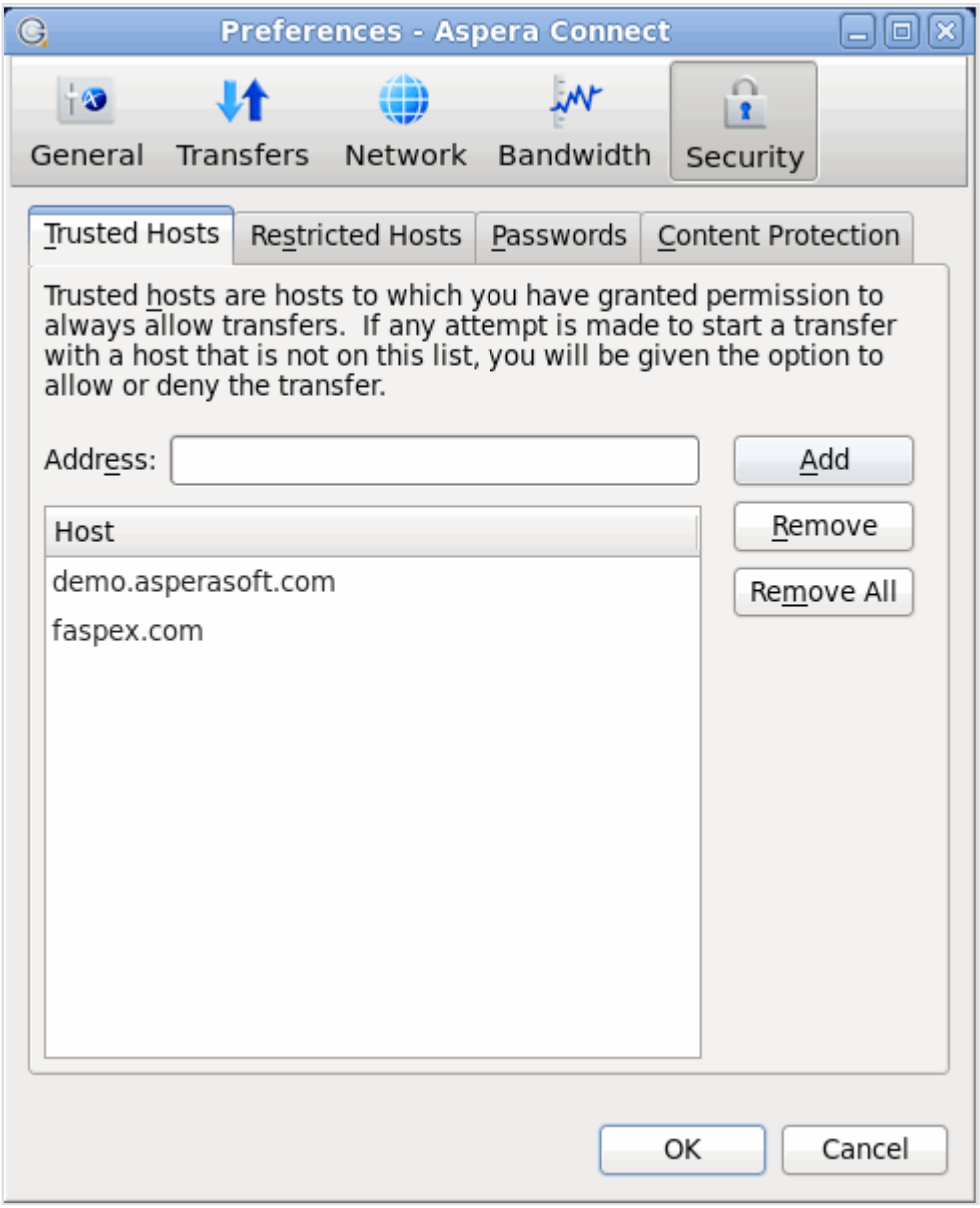
The settings above can be configured via the the Aspera Connect **Preferences** dialog box. If Aspera Connect is already running, go to **System Tray** > **Right-click Aspera Connect** > **Preferences** . If it is not running, you can execute the application manually with the following command:

```
# ~/.aspera/connect/bin/asperaconnect
```

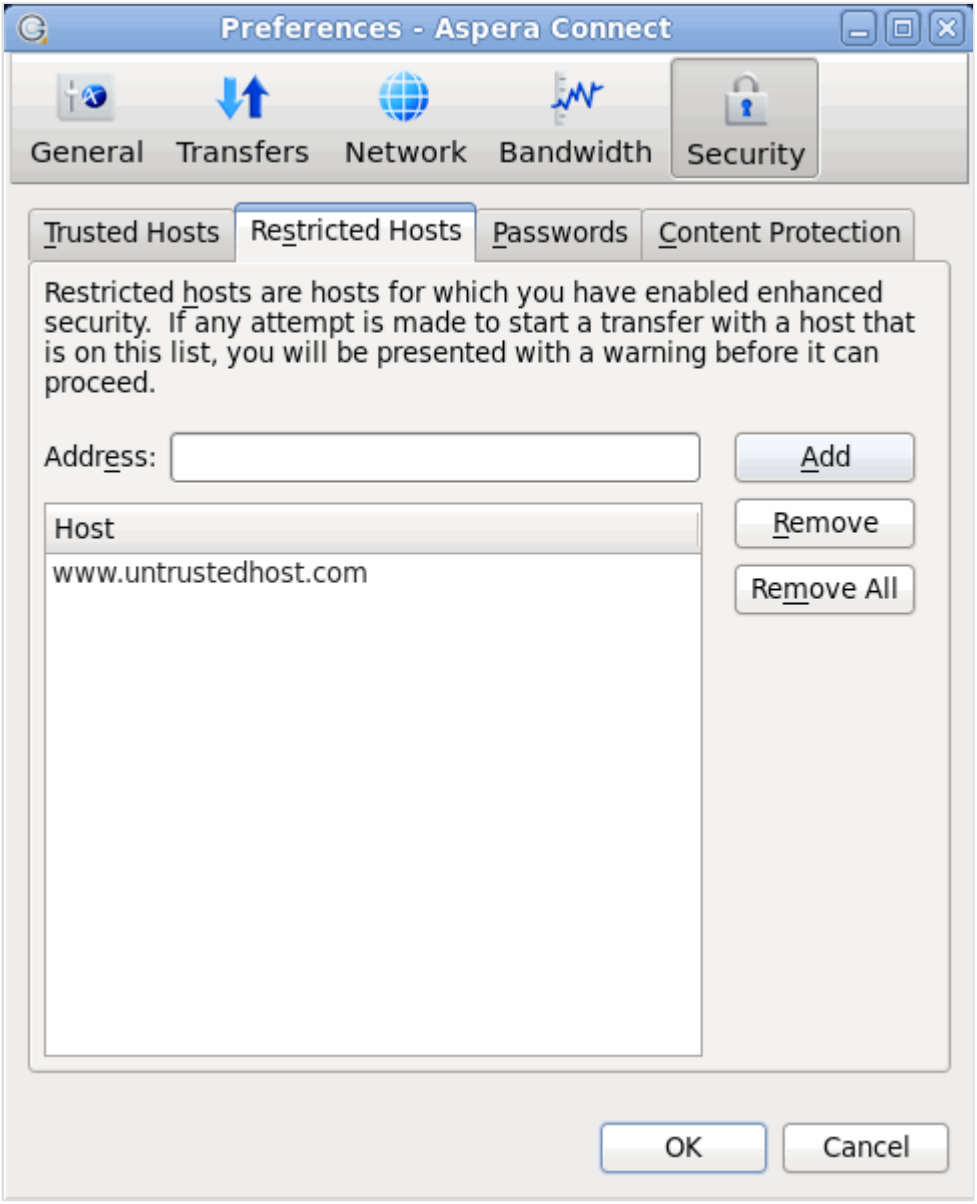


Managing Hosts

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**.

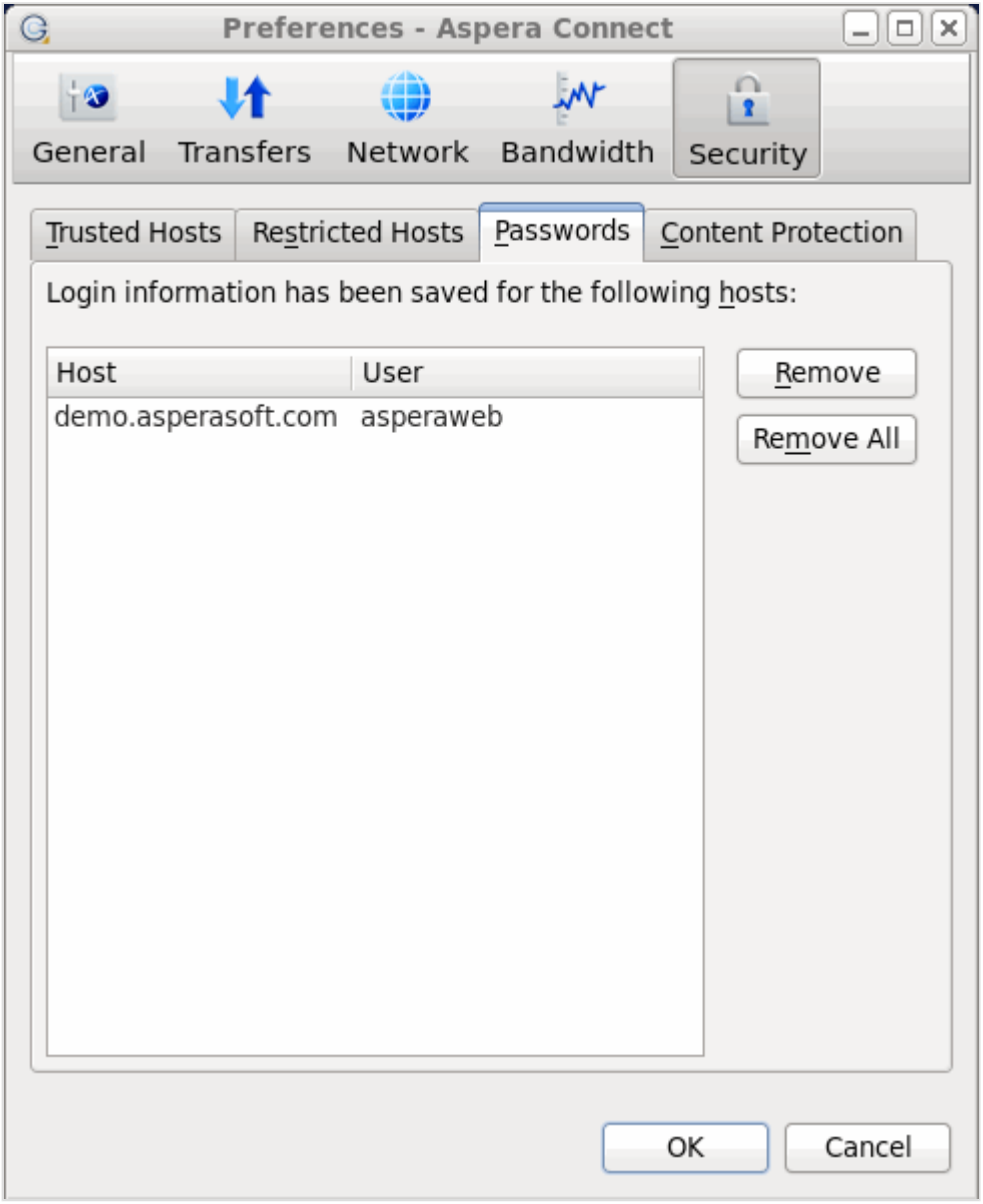


To view, add or remove restricted hosts, go to **Security** > **Restricted Hosts** . Here, enter the host's address in the specified text field and click **Add**.



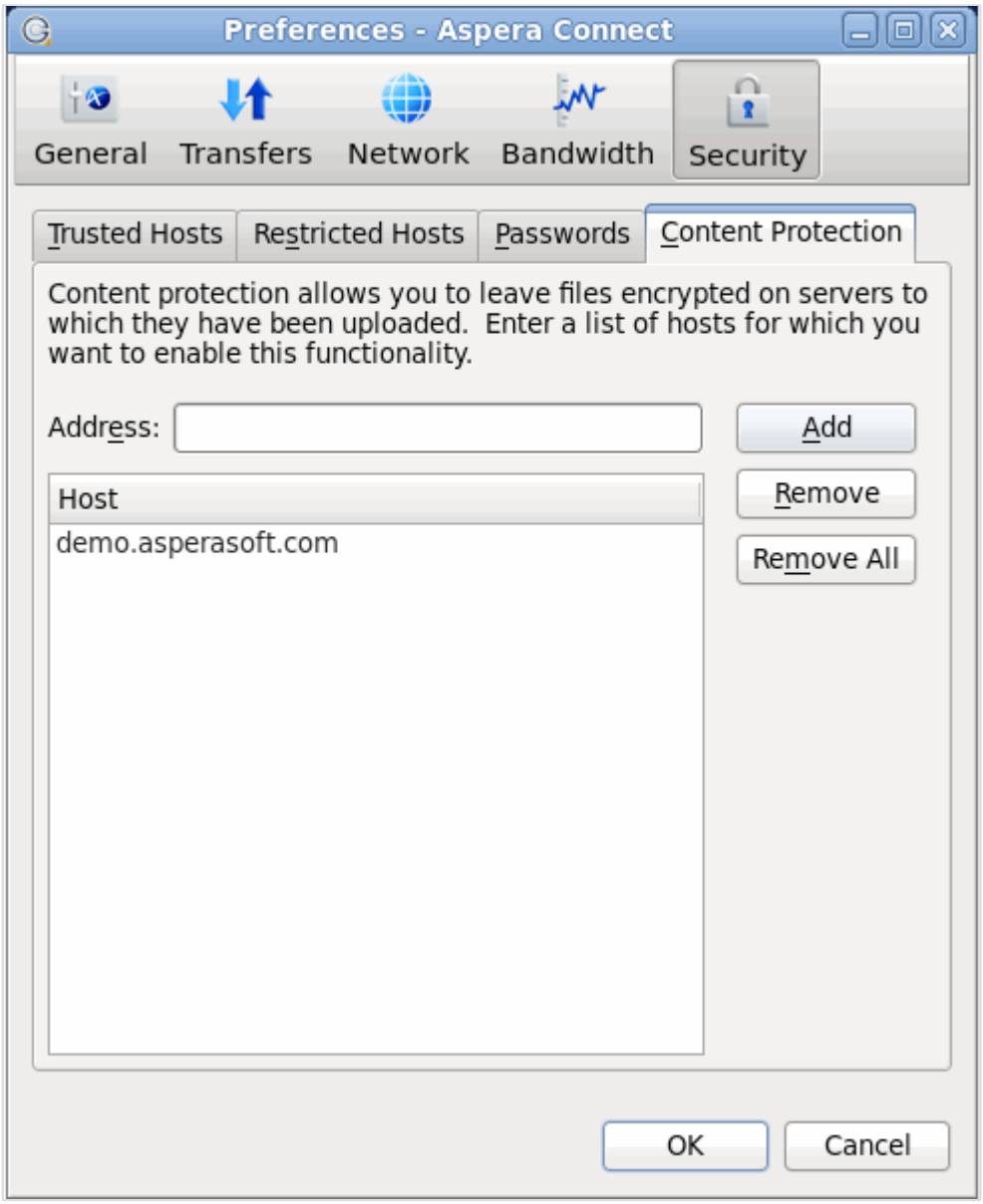
IMPORTANT NOTE: By adding a host to the restricted list, you will be required to provide confirmation every time you attempt to initiate a transfer with that host.

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

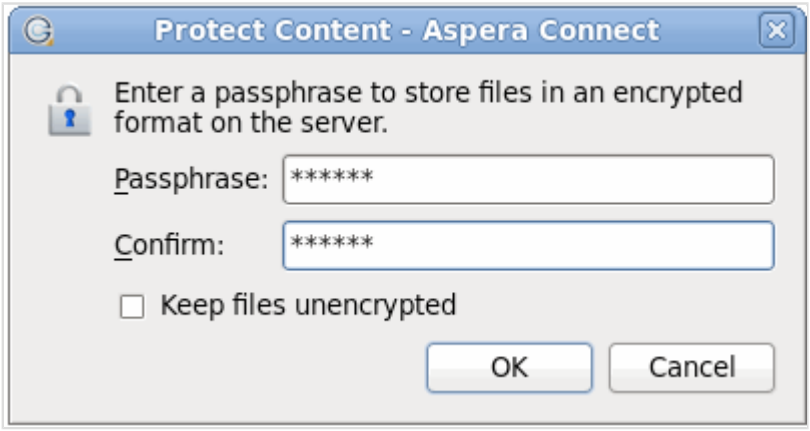


Content Protection

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.

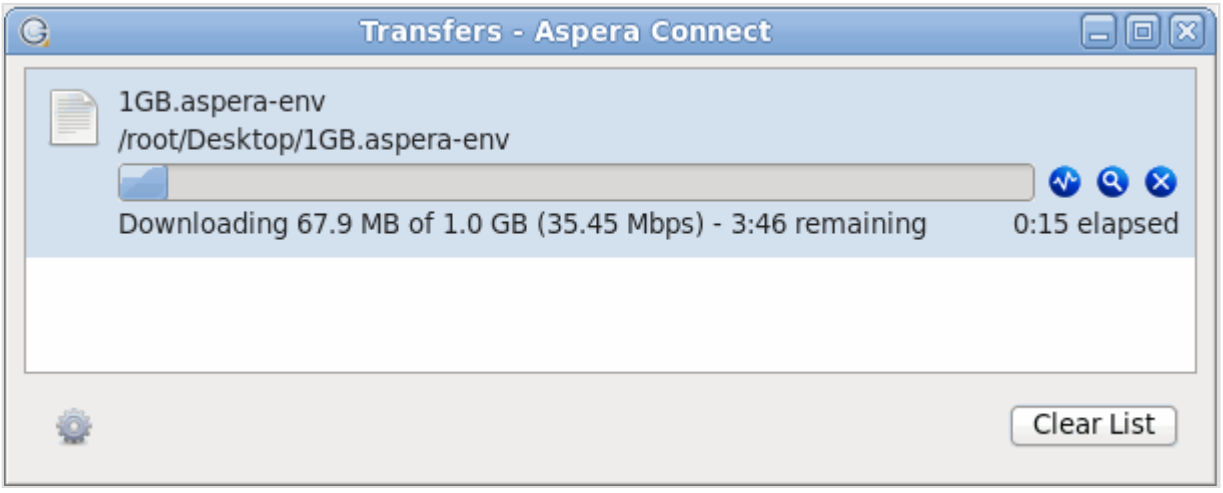


Once content-protected files have been uploaded to your server, they will appear with an *aspera-env* suffix (Aspera Security Envelope).

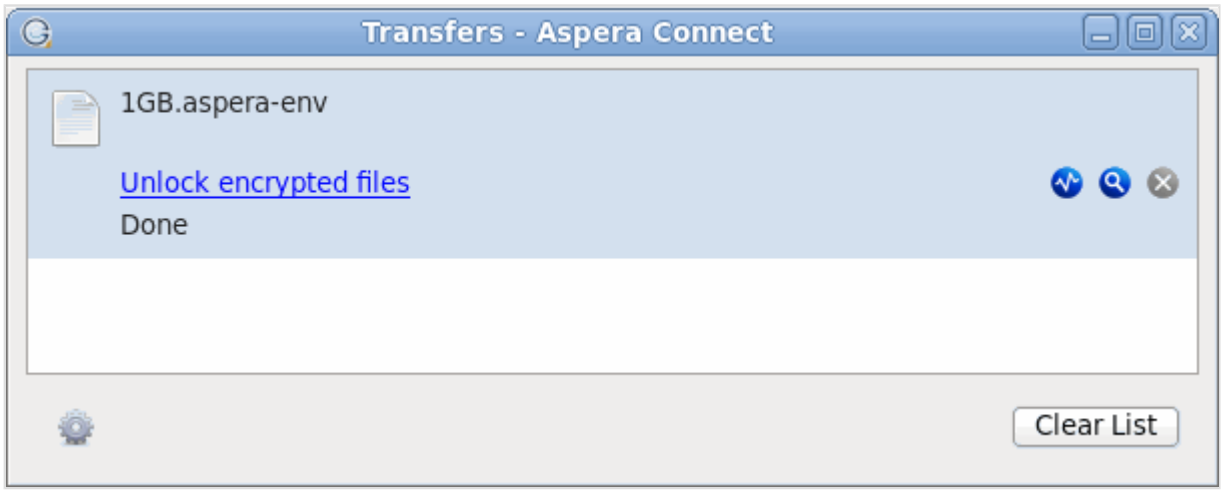
When using Aspera Connect to download a content-protected file, you have two decryption options.

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. Please refer to the topic "*Decrypting Local Files*" for details.**

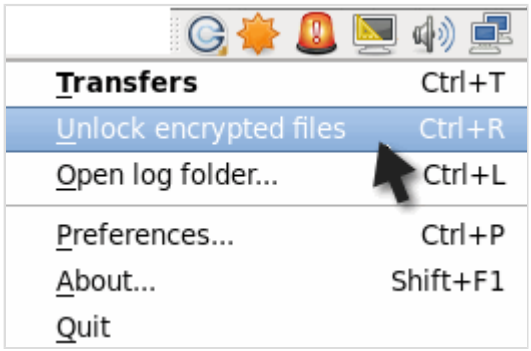
As the content-protected file is being downloaded to your computer, the file suffix is displayed as *aspera-env* in the Aspera Connect **Transfers** window.



Once downloading has completed, check your Aspera 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 Aspera Connect application menu (select the **Unlock encrypted files** option shown below).



For instructions on using the decryption utility, refer to the topic "*Decrypting Local Files*."

Connect Functionality

Transfer files using Aspera Connect.

Initiating a File Transfer

Testing and initiating file transfers with Aspera Connect.

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 Aspera Connect.

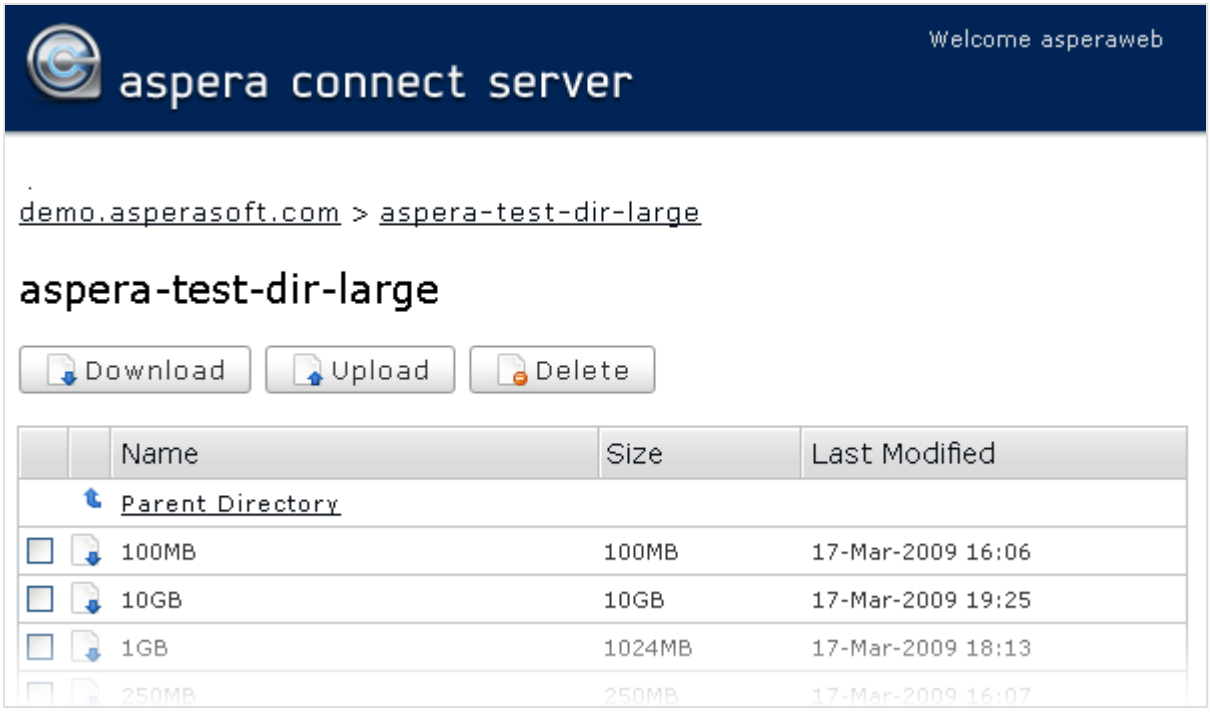
1. Open your web browser and log in to Aspera's test transfer server at *http://demo.asperasoft.com/aspera/user*.

   Enter the following credentials when prompted:

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

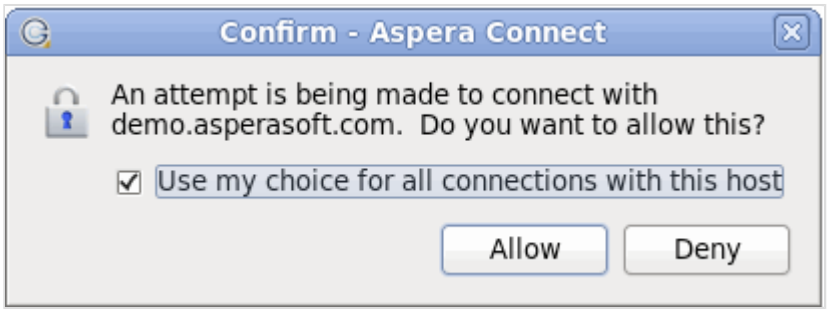
2. On the Aspera Connect server web page, browse into the folder */aspera-test-dir-large*

   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 Aspera 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.

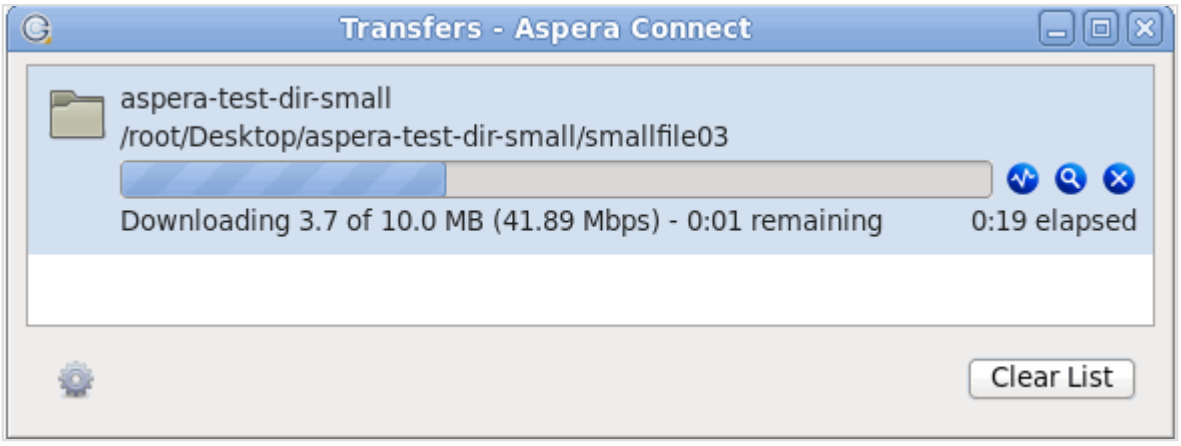
Note that when uploading, you should **avoid transferring files with the following characters** in the file name:

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

The Transfer Manager

A detailed look at the Aspera Connect "Transfer Manager."

You may view and manage all transfer sessions within the Aspera Connect **Transfers** window.

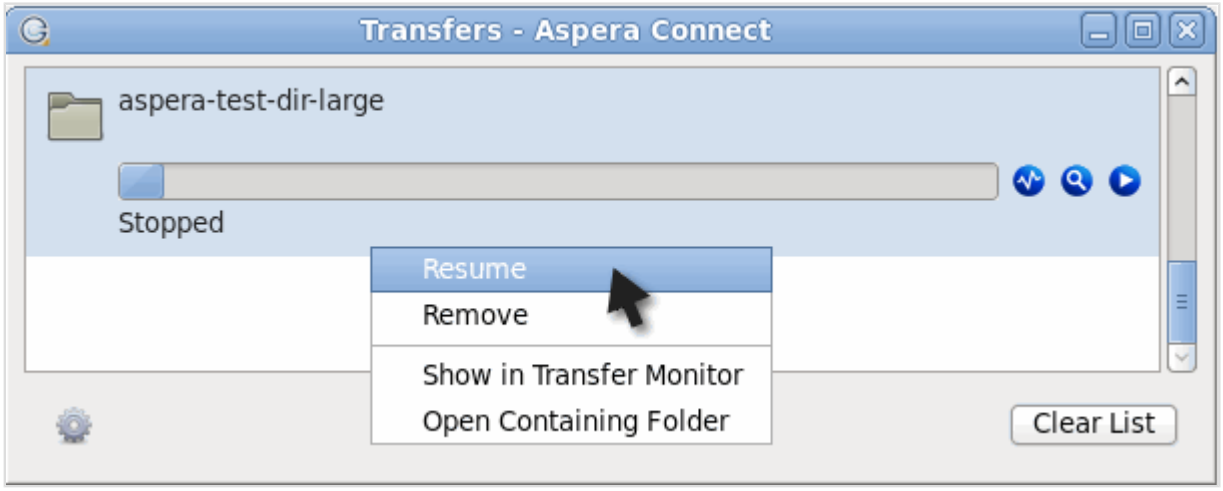


The Aspera Connect **Transfers** window contains the following controls:

- Open the Transfer Monitor. For more information on using this feature, please refer to the topic "*Transfer Monitor*."
- Reveal the file on your computer.

- 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.

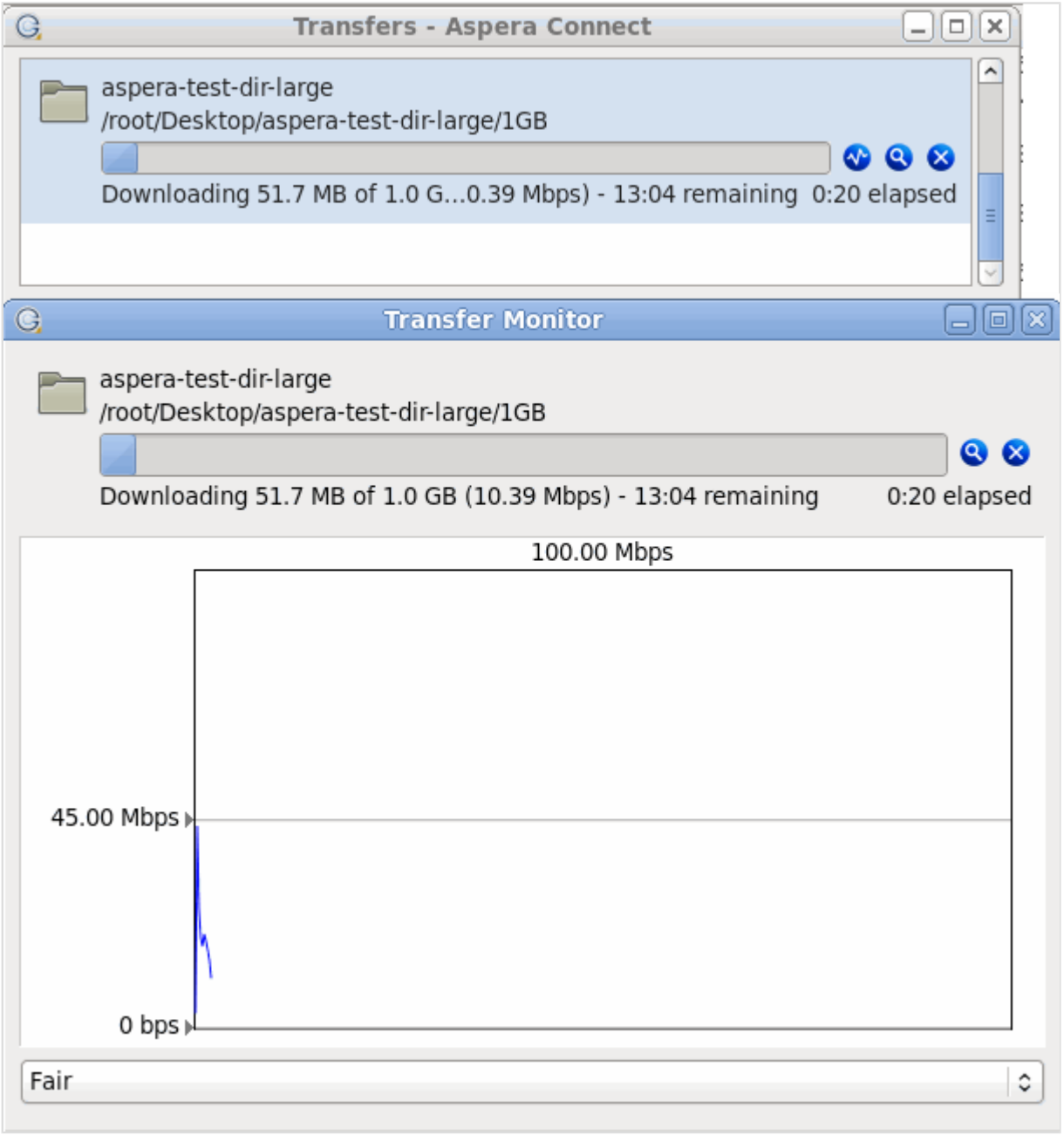


The Transfer Monitor

Monitor transfer status via the Aspera Connect "Transfer Monitor."

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

- Adjust the **file transfer speed** using the vertical slider.
- Change the **transfer policy** (fixed, high, fair and low). If allowed by the transfer server, you can specify which rate policy the transfer should utilize.



- Under the *fixed* rate policy, the transfer will transmit data at a rate equal to the target rate (although this may impact the performance of other traffic present on the network).
- Under the *fair* rate policy, the transfer will attempt to transmit data at a rate equal to the target rate. If network conditions do not permit that to be achieved, it will transfer at a rate lower than the target rate, but not less than the minimum rate.
- Under the *high* rate policy, the transfer rate will be adjusted to fully utilize the available bandwidth (up to the maximum rate).

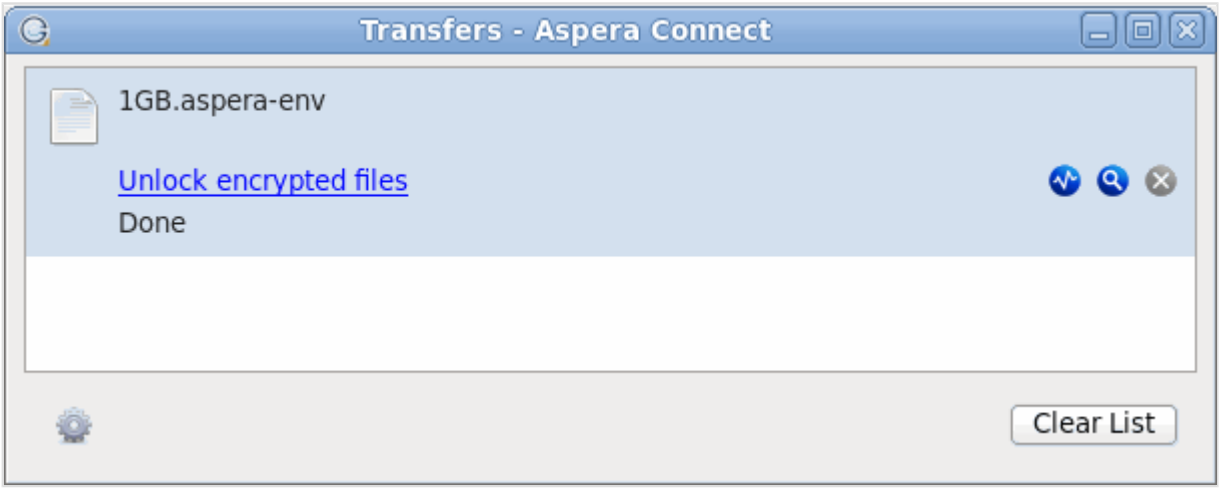
- Under the *low* rate policy, the transfer rate is less aggressive than *fair* when sharing bandwidth with other network traffic. When congestion builds up, the transfer rate is decreased all the way down to the minimum rate, until other traffic retreats.

IMPORTANT NOTE: Users can only switch between High and Fair transfer policies if the host is Enterprise Server v3.0+.

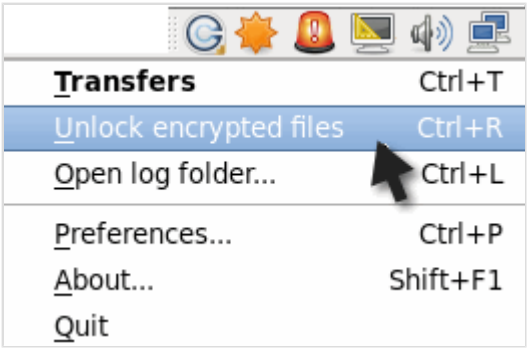
Decrypting Local Files

Decrypt content-protected files on your local system.

If you elected to download the content-protected file(s) and decrypt the file(s) *after* the download has completed, then you will receive a status message in the Connect **Transfers** window telling you to **Unlock encrypted files**, along with a link to the Aspera decryption utility.



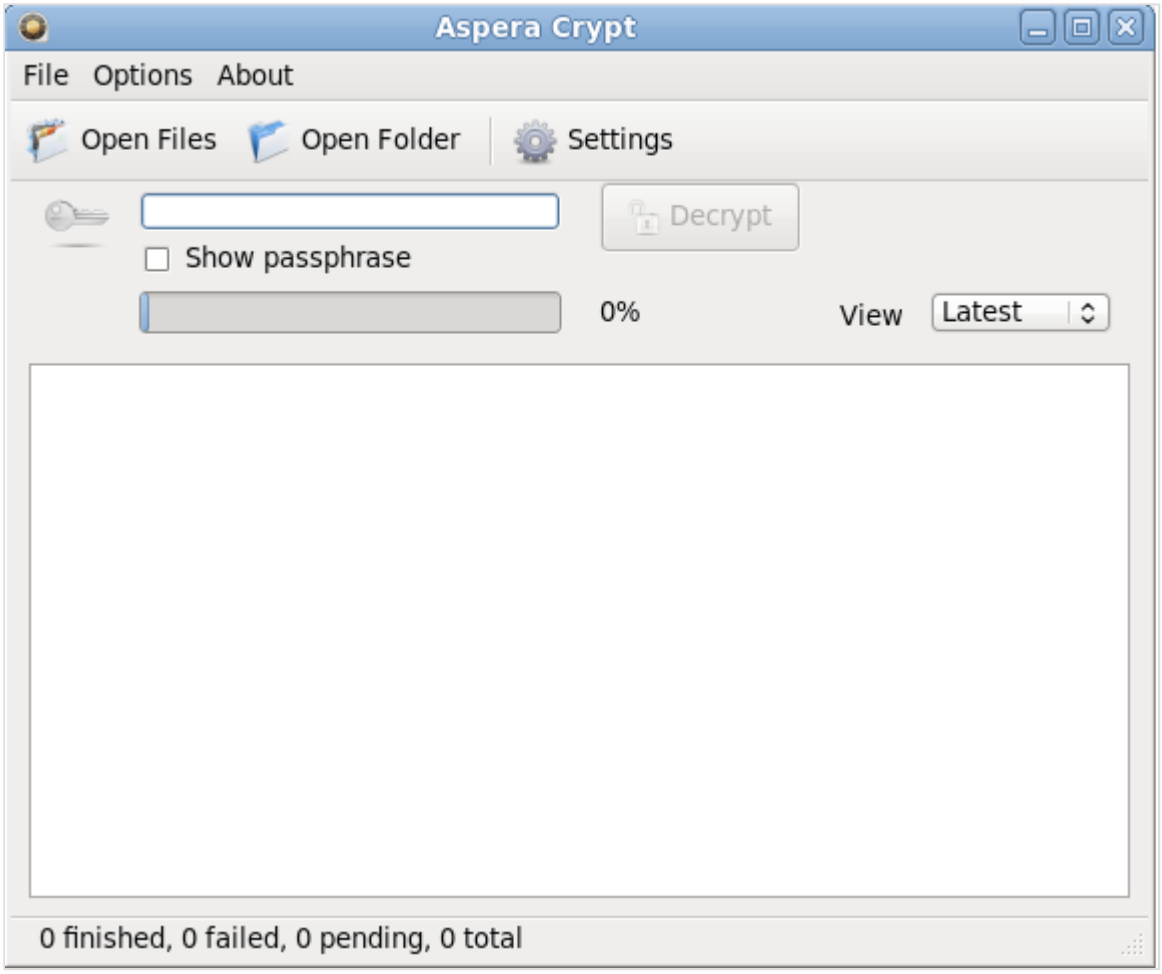
Note that when encrypted items have been downloaded to your computer, they will display the extension *aspera-env* (Aspera Security Envelope). You may also access this utility by going to **System Tray** > **Right-click Aspera Connect** > **Unlock encrypted files** .



If you launch this utility from the Aspera Connect menu, you must follow Step 1, below. If you launch the utility from the **Transfers** window, then skip to Step 2.

1. *(Skip if launching from the Transfers window)* Select the **Unlock encrypted files** option from the Aspera Connect application menu.

   After clicking this option, the decryption utility window will appear (called **Aspera Crypt**).



   After launching Crypt, click the **Open Files** or the **Open Folder** button to browse for your file(s). Use the **Open Files** button to locate your content-protected file(s), and the **Open Folder** button to locate a folder containing content-protected file(s). When your encrypted contents are loaded into Crypt, a status message will appear at the bottom of the application that displays the number of items ready for decryption.

2. Adjust settings, if needed.

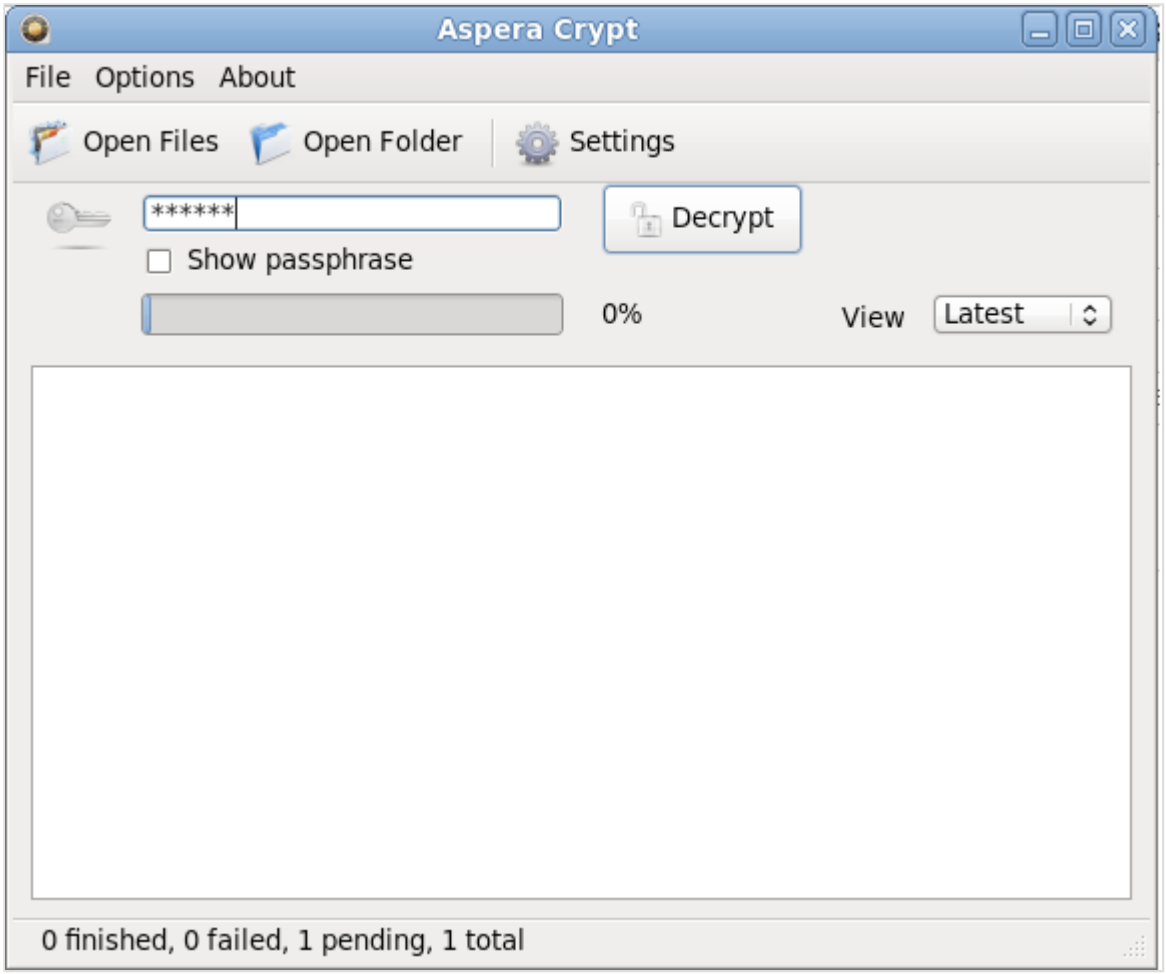
   The Aspera Crypt **Settings** button enables you to modify the following settings:

   - **Delete encrypted files when finished (checkbox)**: When enabled (i.e., checked), Aspera Crypt will remove the encrypted files from your system after the destination (decrypted) content has been created.

- **Number of concurrent threads for decryption (drop-down list)**: Select from 1 (default), 2, 4 and 8, which determines the number of threads that are being decrypted at any given time (i.e., queuing).

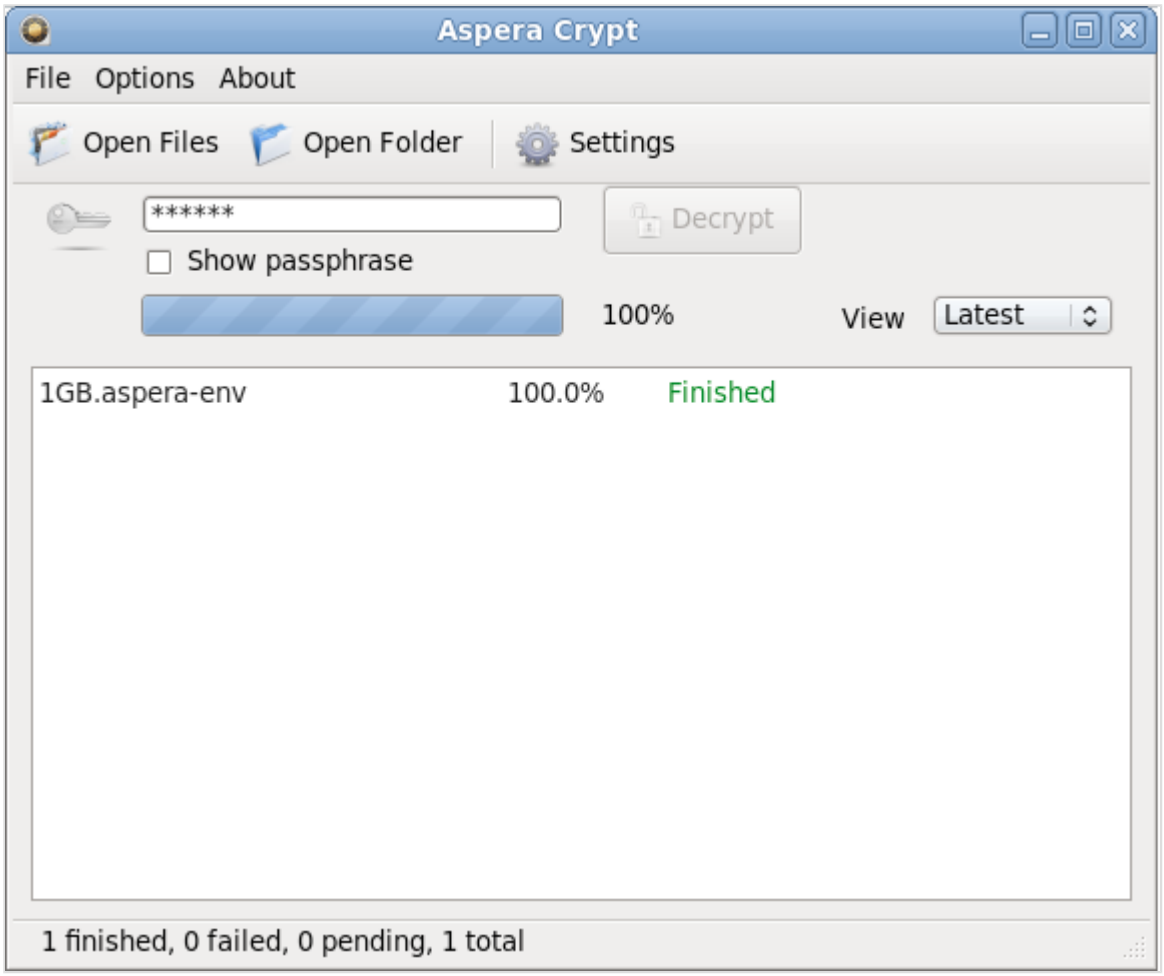
3. Input your passphrase and click the **Decrypt** button

   After browsing for your contents, enter your passphrase in the text field. Your passphrase will be masked, unless you enable the **Show Passphrase** checkbox. Once files are loaded and the **Decrypt** button is activated, click it to decrypt your content.

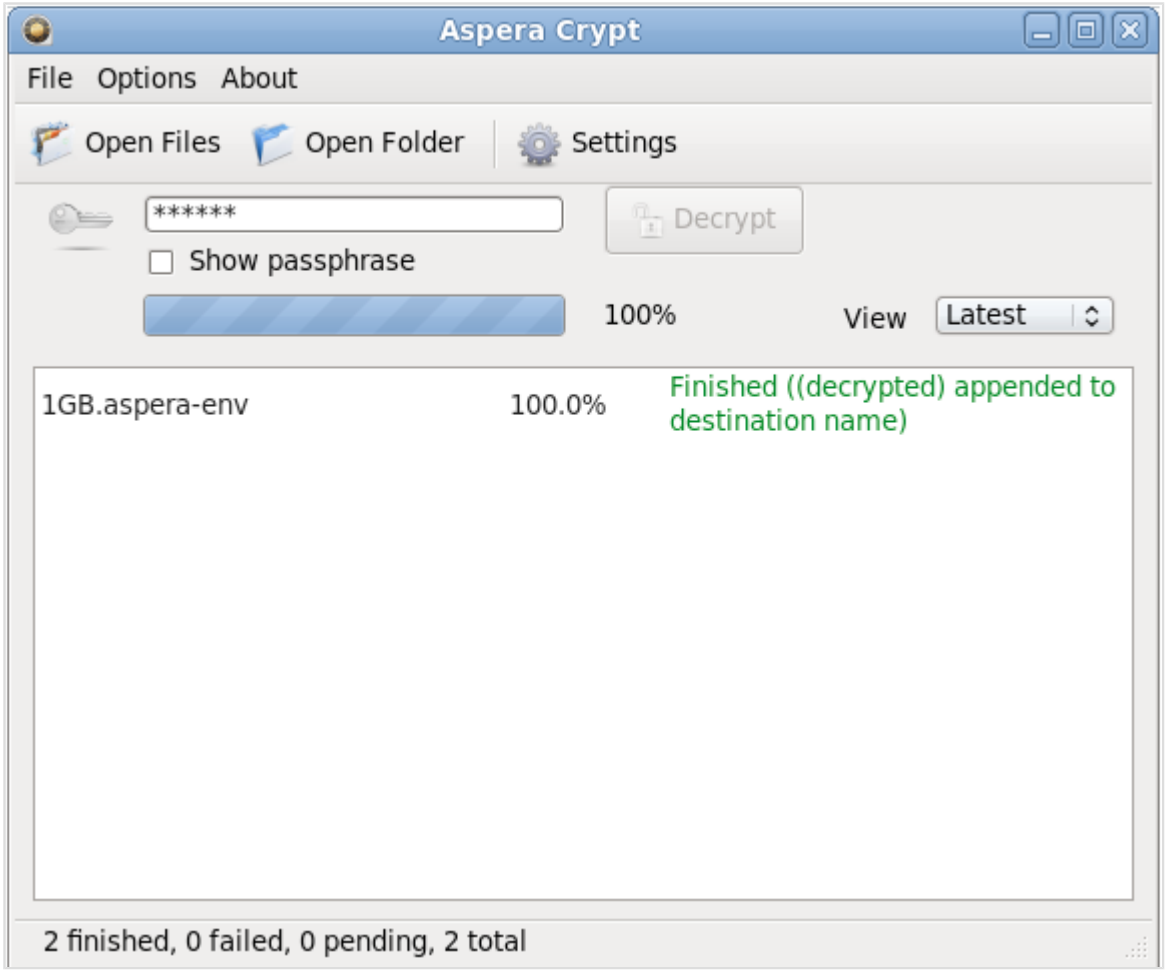


4. View output and confirm decryption

   Once your file(s) 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. Note that "*(decrypted)*" is added to the file name any time the decrypted file (without the *.aspera-env* extension) already exists in the same folder.



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*.

Uninstalling

Remove Aspera Connect from your computer.

IMPORTANT NOTE: Before proceeding with uninstalling Aspera Connect, be sure to **quit** any open browsers.

Aspera Connect installs the following files and folders to your computer:

- `~/.mozilla/plugins/libnpasperaweb.so` Firefox browser plugin
- `~/.aspera/connect` Application files, preferences

To uninstall Aspera Connect, first quit the Aspera Connect application and any open web browsers. Then, use the following commands to delete the installed files:

```
# rm ~/.mozilla/plugins/libnpasperaweb.so
# yes|rm -r ~/.aspera/connect
```

Appendix

Log Files

Locate Aspera Connect's log files.

Log Files

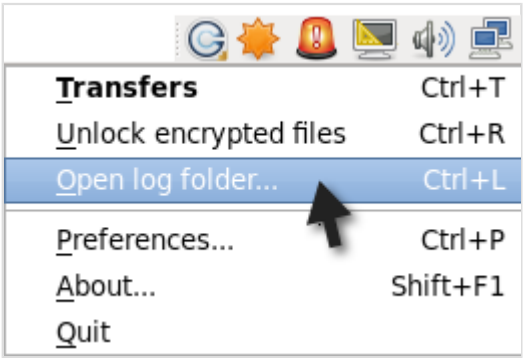
- aspera-connect.log
- aspera-connect-browser-plugin.log
- aspera-scp-transfer.log
- aspera-webinstaller-plugin.log

Log File Location

Log files are located in the following directory:

```
~/.aspera/connect/var/log
```

You may also utilize Connect's log folder shortcut by going to **System Tray** > **Right-click Aspera Connect** > **Open log folder...** .



Troubleshooting

Troubleshooting Connectivity

Connectivity errors and potential solutions.

SSH Connectivity Errors

This section applies to timeouts that occur in the middle of transfers (which results in error codes 13, 15 or 40). It addresses the case when Aspera Connect is unable to connect to the server and receives the error "Timeout establishing connection." This case is due to blocked TCP connectivity. Aspera Connect is attempting to contact the server on the designated TCP port (typically configured to be 33001) and either the client-side firewall is preventing outbound TCP access or a misconfiguration of the server side firewall is not allowing inbound TCP traffic to the Aspera server. To address this issue, attempt to connect to the server's TCP port through the command-line terminal on your client machine (the machine that Aspera Connect is installed on). To do so, run the following command to connect to the server on **port 33001** (or the configured TCP port, if other than 33001).

```
# telnet server-ip-address 33001
```

Note that you should replace server-ip-address with the IP address of the Aspera server.

If the error received is "Connection refused," the Aspera server is not running the SSHD service and you will need to contact your server administrator. If the error received is "Timeout," then the problem is the client-side firewall, which is likely disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound **TCP traffic on port 33001** (or the configured TCP port, if other than 33001).

UDP Connectivity Errors

This section applies when Aspera Connect appears to successfully connect to the server; however, the transfer progress reads 0% and eventually the error "Data transfer timeout" is received (error codes 14, 15 or 18). Although the files to be transferred appear at the destination, they are 0 bytes in size. This is is due to blocked UDP connectivity. The control connection over TCP is established, but the data connection--using UDP--cannot be established. UDP problems are generally caused by firewall configuration. To address this issue, check that **UDP port 33001** is opened for outbound traffic.

Technical Support

For further assistance, you may contact us through the following methods:

Contact Info	
Email	support@asperasoft.com
Phone	+1 (510) 849-2386
Request Form	*http://support.asperasoft.com/home*

The technical support service hours:

Support Type	Hour (Pacific Standard Time, GMT-8)
Standard	8:00am – 6:00pm
Premium	8:00am – 12:00am

We are closed on the following days:

Support Unavailable Dates	
Weekends	Saturday, Sunday
Aspera Holidays	Please refer to our *Website*.

Feedback

The Aspera Technical Publications department wants to hear from you on how Aspera's user manuals can be improved. To submit feedback about this manual, or any other Aspera product document, please visit the *Aspera Product Documentation Feedback Forum*.

Through this forum, you can let us know if you find content that isn't clear or appears incorrect. We also invite you to submit ideas for new topics, as well as ways that we can improve the documentation to make it easier for you to read and implement. When visiting the Aspera Product Documentation Feedback Forum, please remember the following:

- You must be registered to use the Aspera Support Website at *https://support.asperasoft.com/*.
- Be sure to read the forum guidelines before submitting a request.

Legal Notice