

Aspera Client 2.7.6

RedHat, Debian

Document Version: 1

Contents

Introduction.....	4
Installation.....	5
Requirements.....	5
Upgrade Note.....	5
Installing the Product.....	6
Configuring the Firewall.....	8
Testing Transfer.....	8
Transferring Files with the Application.....	11
Application Overview.....	11
Managing Connections.....	13
Creating SSH Keys.....	17
Transferring Files.....	21
Advanced Transfer Mode.....	25
Configuring Transfer Notifications.....	27
Using Transfer Notifications.....	35
Global Transfer Settings.....	39
Setting Global Bandwidth.....	39
Aspera Sync.....	42
asperasync Syntax.....	42
asperasync Examples.....	42
Transferring in Command-line.....	45
ascp Usage.....	45
ascp General Examples.....	50
ascp File Manipulation Examples.....	52
Creating Command Files.....	54
Frequently-Asked Questions.....	54
Creating SSH Keys (Terminal).....	56
Appendix.....	58

fasp Transfer Policies..... 58

Optimizing Transfer Performance.....58

Log Files..... 60

Updating Product License..... 60

Uninstall..... 62

Technical Support.....63

Feedback.....64

Legal Notice.....65

Introduction

Aspera Client is a file transfer client application built upon Aspera's *fasp* file transport technology. Aspera Client includes the following features:

Feature	Description
<i>fasp</i> transport technology	File transfer protocol that dramatically speeds transfers over IP networks by eliminating the fundamental bottlenecks in conventional technologies. <i>fasp</i> features bandwidth control, resume, transfer encryption, content protection, and data integrity validation.
Client application	A graphical file transfer application for initiating and managing transfers.
Aspera Sync	A command-line synchronization program.
ascp command	The command-line file transfer program.

Installation

Install the Aspera transfer product and set up your computer for *fasp* file transfers.

Requirements

Software and hardware requirements for optimal product functionality

System requirements for Aspera Client:

- Linux kernel 2.4 or higher. Linux distributions/kernels released after the product release date may not be compatible.
- Screen resolution 1024 x 768 or higher *for graphical user interface*.

Upgrade Note

Steps to safely upgrade from a previous version of the product.

If your computer has a previous version of the Aspera product installed, follow these steps to prepare it for the upgrade. Depending on the version of your product, the upgrade preparation procedure may differ. Skip any step that the version does not apply.

IMPORTANT NOTE: You cannot upgrade directly between different Aspera transfer products (e.g. From Point-to-Point to Client, or from Point-to-Point to Enterprise Server). To do so, you need to back up the configuration, uninstall the product, and perform a fresh install of the product to the newest version. .

1. *All Versions* - Verify existing product version

Depending on your current product version, the upgrade preparation procedure may differ. In a *Terminal window*, execute this command:

```
$ ascp -A
```

You can find the version number preceding the product name.

2. *All versions* - Stop all *fasp* transfer-related applications and connections.

Before upgrading the application, close the following applications and services:

- ascp connections

3. *All versions* - Backup the files

Depending on the version of your previous installation, backup the files in the specified locations:

Version	Folder
2.0.2 to 2.6+	<ul style="list-style-type: none">• /opt/aspera/etc/ (Server config, web config, user settings, license info)• /opt/aspera/var/ (Pre- and Post-Processing scripts, Connect Server)
2.0.1 and earlier	<ul style="list-style-type: none">• /var/opt/aspera/etc/ (Server config, web config, user settings, license info)• /usr/local/aspera/var/ (Pre- and Post-Processing scripts, Connect Server)

Installing the Product

A walkthrough of the installation and setup process.

To install Aspera Client, log into your computer with *root* permissions, and follow the steps below.

1. Download the Aspera product installer

Download the installer from the link below. Use the credentials provided to your organization by Aspera to access:

<http://asperasoft.com/en/downloads/2>

If you need help determining your firm's access credentials, contact [Technical Support](#) on page 63.

2. Run the installer

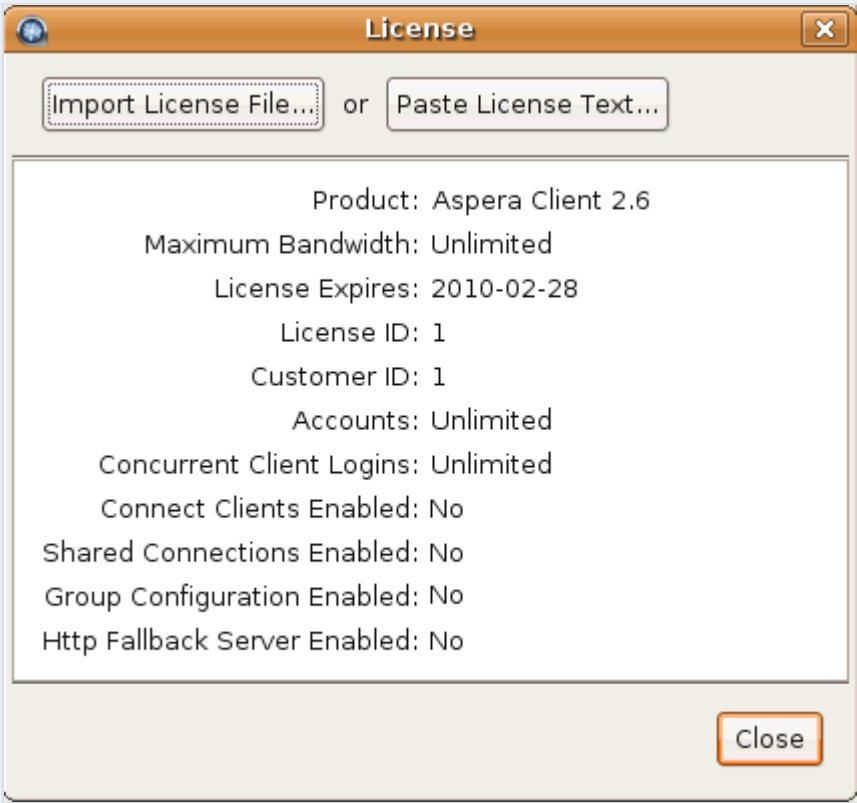
When downloaded, run the installer using the following commands and with the proper administrative permissions. Replace the file name accordingly.

OS	Commands
RedHat	<pre>\$ rpm -Uvh aspera-scp-client-[version].rpm</pre>
Debian	<pre>\$ dpkg -i aspera-scp-client-[version].deb</pre>

3. Install the license

There are two ways to install the license: through the GUI or via command line.

Method	Instructions
GUI	To install the license via the GUI, execute asperascp in a Terminal (as a root user) to launch the application. If this is a fresh install, an <i>Enter License</i> window will appear. You may click the Import License File... and select the license file, or Paste License Text... to copy-and-paste the license file's content. When finished, the license information will appear in the window. Verify that it is correct and click Close .

Method	Instructions
	
Terminal	<p>To install the license through command line, create the following file and paste your license key string into it:</p> <pre>/opt/aspera/etc/aspera-license</pre> <p>When finished, save and close the file. Use this command to verify the license info:</p> <pre>\$ ascp -A</pre>

If you are updating your product license after the installation, refer to [Updating Product License](#) on page 60.

4. Convert the old aspera.conf file manually (*Step necessary only when upgrading from product version 2.5 and earlier*)

In product version 2.6.3 and newer, the configuration file, "aspera.conf," contains the document root settings. When upgrading from product version 2.5 or earlier, the installer converts your old configuration files to the new format, using a "strict" method. If the old aspera.conf file has errors or unrecognized directives, the conversion will fail.

To review the errors, execute a manual strict conversion. Change the aspera.conf's path if it is not in the default location:

```
$ cd /opt/aspera/etc
```

```
$ sudo asconfigurator -T -F convert_conf_V1_data ./aspera.conf
```

If error occurs during the conversion, use the relaxed conversion method:

```
$ cd /opt/aspera/etc
$ sudo asconfigurator -F convert_conf_V1_data ./aspera.conf
```

5. **(For upgrades)** Check aspera.conf for errors

When upgrading your Aspera product to a newer version, it is recommended that you check the *aspera.conf* configuration file for errors. Run the following command in a *Terminal* window to validate aspera.conf:

```
$ /opt/aspera/bin/asuserdata -v
```

At this point, your Aspera transfer product is installed; however additional configuration steps are required to set up the application. . Please continue to the proceeding topics in this chapter.

Configuring the Firewall

Firewall settings required by the product.

Your Aspera transfer product requires access through the ports listed in the table below. If you cannot establish the connection, review your local corporate firewall settings and remove the port restrictions accordingly.

Product	Firewall Configuration
Client	<p>The following bullet points provide basic information for configuring your firewall to allow Aspera file transfers. Note that the outbound connection for SSH may differ based on your organization's unique network settings. Although TCP/22 is the default setting, please 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:</p> <ul style="list-style-type: none">• Allow outbound connections from the Aspera client on the TCP port (<i>TCP/33001</i>, by default, when connecting to a <i>Windows</i> server, or on another non-default port for other server operating systems).• Allow outbound connections from the Aspera client on the <i>fasp</i> UDP port (33001, by default).

Testing Transfer

Test client functionality by transferring with the Aspera Demo Server.

To make sure that the software is working properly, follow these steps to test download and upload transfers between your system and the Aspera Demo Server (Demo Server):

1. Download test files from the Demo Server

The first test is to download a test file from the Demo Server. The transfer command is based on the following settings:

Item	Value
Demo Server address	demo.asperasoft.com
Login account	aspera
password	demoaspera
Test file	/aspera-test-dir-large/100MB
Download location	/tmp/
Transfer settings	Fair transfer policy, target rate 10M, minimum rate 1M, encryption disabled.

Use the following command to download, press y to accept the server's key, and enter the password *demoaspera* when prompted:

```
$ ascp -QT -l 10M -m 1M aspera@demo.asperasoft.com:aspera-test-dir-large/100MB /tmp/
```

You should see the following session messages. The description from left to right is explained below:

```
Session Start...
100MB      23%    23MB  509Kb/s   11:59 ETA █
```

Item	Description
100MB	The name of the file that is being transferred.
23%	The percentage completed.
23MB	The amount transferred.
509Kb/s	Current transfer rate.
11:59 ETA	Estimated time remaining.

2. Upload test files to the Demo Server

10 Installation

When the file is downloaded, try uploading the same file back to the Demo Server. Use the command to upload the file (100MB) to the Demo Server's */Upload* directory. Enter the password *demoaspera* when prompted:

```
$ ascp -QT -l 10M -m 1M /tmp/100MB aspera@demo.asperasoft.com:Upload/
```

Transferring Files with the Application

Using the *Client* desktop application to transfer files.

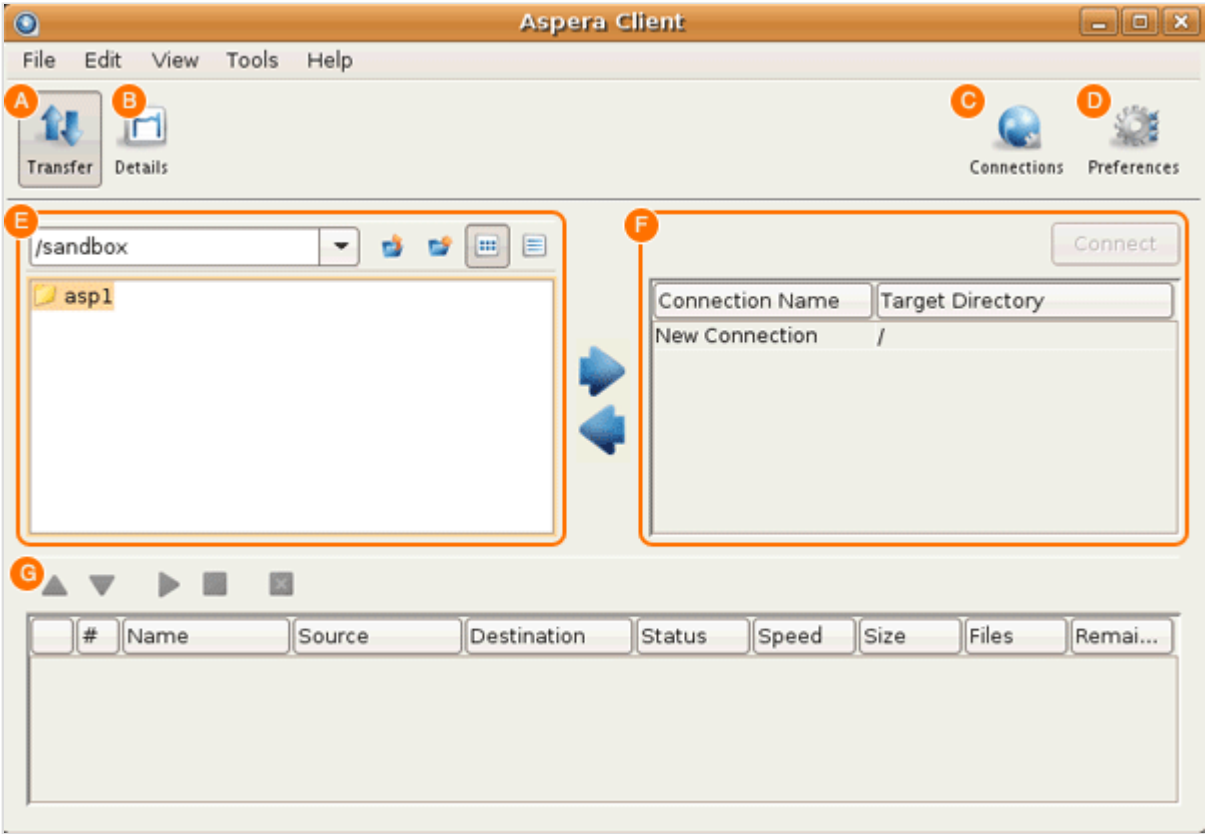
Application Overview

The *Client* application Overview.

To launch the application, execute the following command in a Terminal:

```
$ asperascp
```

Here is the application overview:

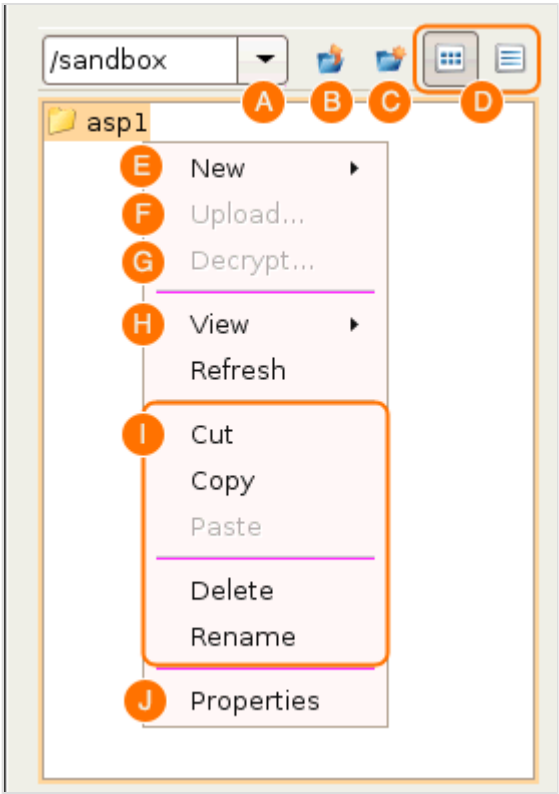


Item	Name	Description
A	Transfer	The transfer mode. Reveal the local/remote file browsers.
B	Details	The transfer details mode. Show the selected transfer session's details and the transfer control options.
C	Connections	Bring up the Connection Manager window to manage the remote endpoints.

12 Transferring Files with the Application

Item	Name	Description
D	Preferences	Set the local computer's default transfer settings such as the <i>fasp</i> global bandwidth and the number of simultaneous transfers in the queue, and the SMTP server's information for transfer notifications.
E	Local Browser	Browse the local file system to find files to transfer.
F	Connections/Remote Browser	When not connected, this panel shows connections that lists the saved connections. When connected, it becomes the remote file browser.
G	Transfers panel	Display previous, ongoing, and queued transfers. Manage the priority.

All options in the File Browser, including the file browser's contextual menu (Mouse right-click):



Item	Name	Description
A		Path indicator/selector.
B		Go to the parent directory.
C		Create a new folder.
D		Choose between the list views and the detail view.




Item	Name	Description
E	New	Create a new folder.
F	Upload... / Download...	Bring up the advanced upload or download window.
G	Decrypt...	Decrypt the selected file if it is encrypted with the content protection.
H	View / Refresh	Choose between the detail or the list views. Refresh the folder.
I	Cut / Copy / Paste / Delete / Rename	Options to manipulation the selected files.
J	Properties	Show the selected files' properties.

Managing Connections

Add and manage the remote *fasp* servers.

To connect to a remote computer, you need to add it into the *Connection Manager* before establishing the connection. In the application (**asperascp**), click **Connections** to begin.



In the Connection Manager, click  to create a new connection. When a connection is added, you can also use  and  to manage the connection profiles.

The Connection Manager includes the following configuration tabs:

Tab	Description
Connection	The basic host information, such as the address, login credentials, and connection ports.
Transfer	The transfer session-related options, such as the transfer speed and retry rules.
Tracking	Options for tracking the transfer session, including the confirmation receipt and the email notifications.
Filters	Create filters to skip files that match certain patterns.
Security	Enable the transfer encryption and the content protection.

Tab	Description
File Handling	Set up resume rule, preserve transferred file attributes, and remove source files.

The following tables detail all options in these tabs:

Connection

Option	Description
Host	Required The server's address, such as <i>192.168.1.10</i> or <i>companyname.com</i> .
User	The login user for the server.
Authentication	Choose either password or public key for authentication. To use the key-based authentication, refer to Creating SSH Keys on page 17.
Display Name	Enter a name for this connection.
Target Directory	The default directory when connecting to this computer. When leaving it blank, browsing the remote host brings up either the user account's document root (docroot), or the last-visited folder; when specifying a path, connecting to the host always brings up the exact directory. The default directory is shown in the <i>Connections</i> panel.
Advanced Settings: SSH Port (TCP)	The TCP network port. Default: 22
Advanced Settings: fasp PORT (UDP):	The UDP network port: Default: 33001
Advanced Settings: Connection Timeout	Timeout the connection attempt after the selected time.

Transfer

Option	Description
Transfer Name	Choose between the following option: Automatically generate allows the user interface to generate the transfer name; Automatically generate and add prefix uses auto-generated name with prefix; Specify uses the user-specified name.
Policy	Select the transfer policy. Refer to fasp Transfer Policies on page 58.
Speed	Check this option to specify the transfer rate. The target rate is constrained by the global bandwidth in the <i>Preferences</i> window. Refer to Setting Global Bandwidth on page 39.
Retry	Check this option to automatically retry the transfer after a recoverable failure. When checked, set the amount of time the transfer should be retried in seconds, minutes or hours. You may set the initial and maximum retry intervals by clicking the More Options... button.

Option	Description
	<ul style="list-style-type: none"> • Initial interval: The first retry waits for the initial interval. Input in seconds, minutes or hours. • Maximum interval: After the initial interval, the next interval doubles until the maximum interval is met, and then stops retrying after the retry time is reached. Input in seconds, minutes or hours. <p><i>Example 1:</i></p> <pre>10s initial interval, 60s maximum interval, retry for 180s Retry at (seconds): 10s 30s 70s 130s 180s Interval progression (seconds): 10s 20s 40s 60s 60s 50s</pre> <p><i>Example 2:</i></p> <pre>30s initial interval, 120s maximum interval, retry for 600s Retry at (seconds): 30s 90s 210s 330s 450s 570s 600s Interval progression (seconds): 30s 60s 120s 120s 120s 120s 30s</pre>
Advanced Setting	Click the button to reveal these options: Specify the fasp datagram size (MTU) and Disable calculation of source files size before transferring.

Tracking

Option	Description
Generate delivery confirmation receipt	Check the option to create the delivery receipt file in the specified location.
Send email notifications	Send out email notifications based on specified events (start, complete, and error). Refer to Using Transfer Notifications on page 35 for more information.

Filters

Click **Add** and enter the pattern to exclude files or directories with the specified pattern in the transfer. The exclude pattern is compared with the whole path, not just the file name or directory name. Two special symbols can be used in the setting of patterns:

Symbol	Name	Description
*	Asterisk	Represents zero to many characters in a string, for example *.tmp matches .tmp and abcde.tmp.
?	Question mark	Represents one character, for example t?p matches tmp but not temp.

Examples:

Filter Pattern	Matched files
*dirName	path/to/dirName, another/dirName
*1	a/b/file1, /anotherfile1
*filename	path/to/filename, /filename
path?/file?	path1/fileA, pathN/file5

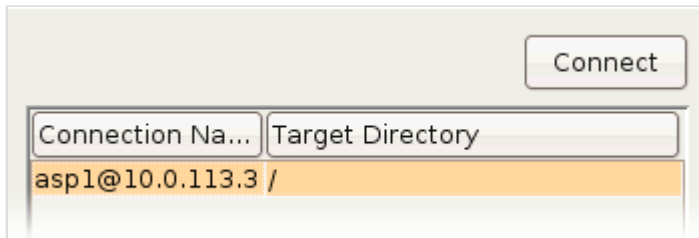
Security

Option	Description
Encryption	When checked, <i>fasp</i> encrypts files while transferring. Encryption may decrease performance, especially at higher transfer speeds and with slower computers.
Content Protection	Two options: Encrypt uploaded files with a password encrypts the uploaded files with the specified password. The protected file has the extension <i>.aspera-env</i> appended to the file name; Decrypt password-protected files downloaded prompts for the decryption password when downloading encrypted files.

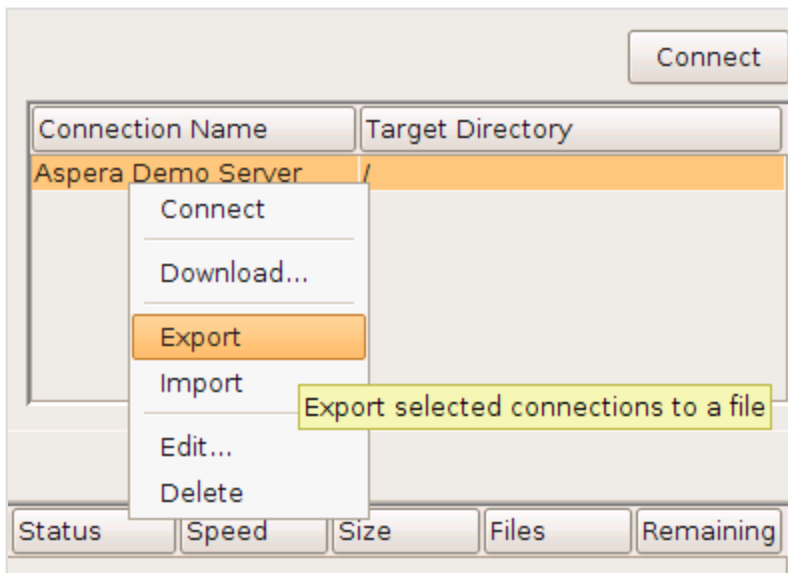
File Handling

Option	Description
Resume	Check <i>Resume incomplete files</i> to enable the resume feature. In the <i>When checking files for differences</i> options: Compare file attributes only checks if the existing file is the same size; Compare sparse file checksums performs a sparse checksum on the existing file. Compare full file checksums perform a full checksum on the existing file. In the <i>When a complete file already exists at the destination</i> , select an overwrite rule when the same file exists at the destination.
File Attributes	<ul style="list-style-type: none"> • Enable the <i>Preserve Timestamps</i> checkbox to save the transferred files' timestamps. • Enable the <i>Preserve Owner and Group</i> checkbox to preserve the transferred files' user ID and group ID.
Source Deletion	Check Automatically delete source files after transfer to delete the successfully-transferred files from the source. Check Delete source directories to also remove the folder.

When finished, click **OK** to save this connection. To connect to this remote host, double-click the connection from the *Connection* panel, or select it and click **Connect**.



You may also *import* your connection list *to* and *export* your connection list *from* a text file. To export your connection list, right-click the remote server panel and select **Export**. To import your connection list, right-click the remote server panel and select **Import**. Both options are shown below (with "export" selected).



Important Note:

- If you are exporting a connection that uses keys, then you will need to manually back up those keys and import separately.
- Email templates are not exported with the connection.

Creating SSH Keys

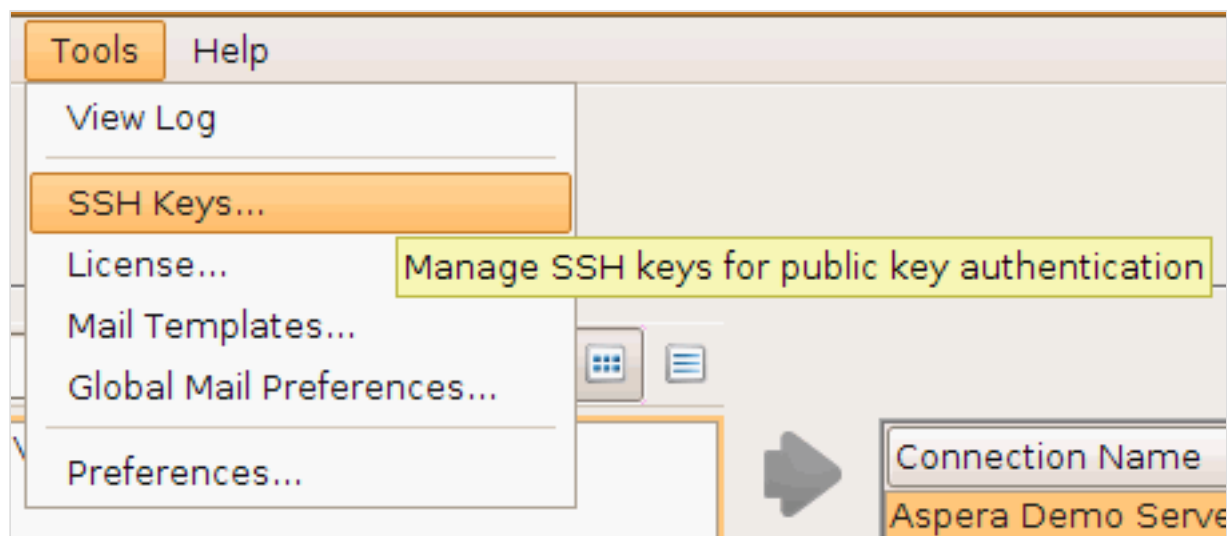
Create a key pair for your computer.


Public key authentication (SSH Key) is a more secure alternative to password authentication that allows users to avoid entering or storing a password, or sending it over the network. Public key authentication uses the client computer to generate the key-pair (a public key and a private key). The public key is then provided to the remote computer's administrator to be installed on that machine. If you wish to use your transfer client functionality with public key authentication, follow the steps below.

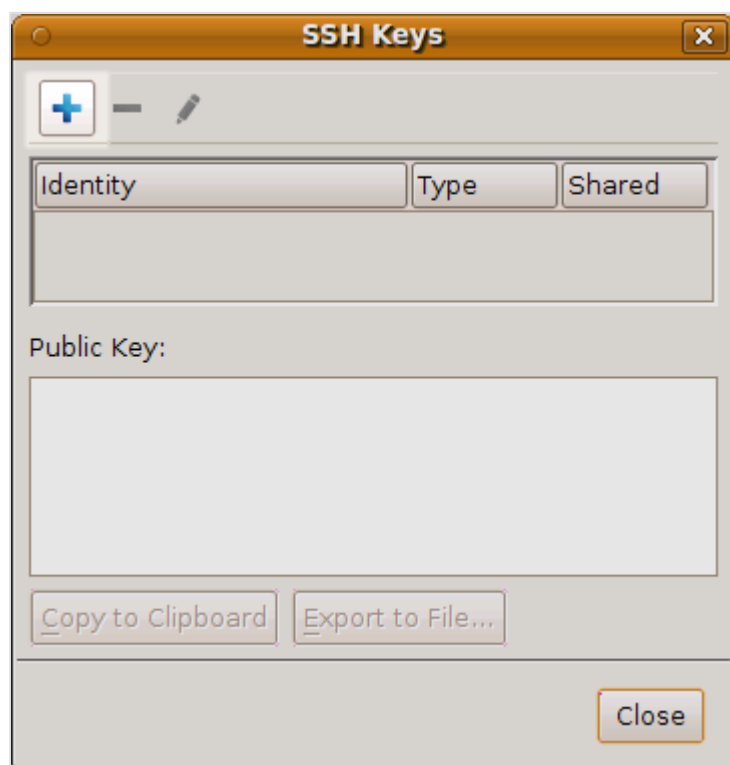
NOTE: You can also generate a key-pair using the command-line. Please refer to [Creating SSH Keys \(Terminal\)](#) on page 56 for instructions.

1. Create a key pair using the GUI

Start the application by launching **asperascp** and selecting **Menu bar > Tools > SSH Keys...**



In the *SSH Keys* window, click  to bring up the *New SSH Key Pair* window.

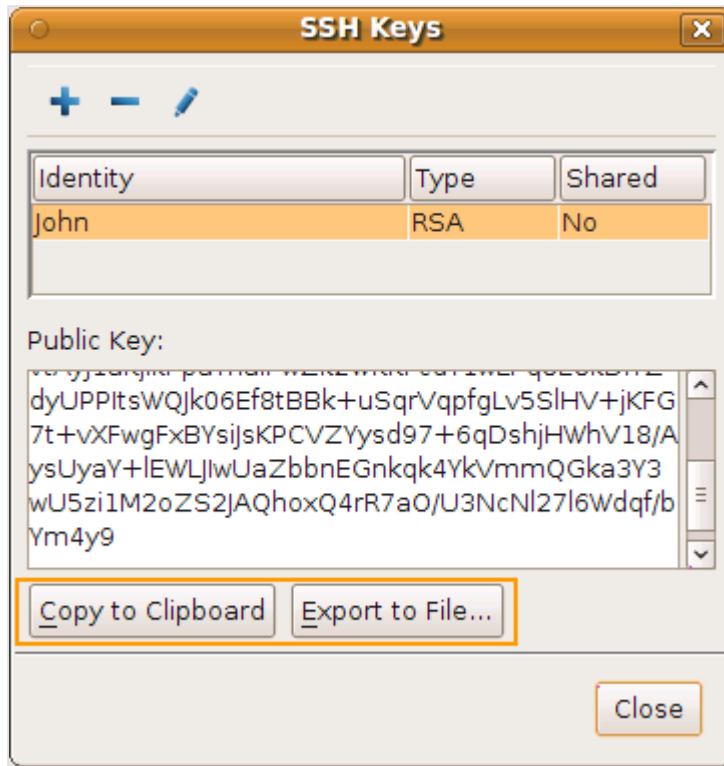


In the *New SSH Key Pair* window, enter the requested information. When finished, click **OK**:

Field	Description
Identity	Give a name to your key pair, such as your user name.
Passphrase	(Optional) Set a passphrase on your SSH key, which will be prompted for whenever it needs to use the key. If you don't want the user to be prompted for passphrase when logging in, leave this field blank.
Type	Choose between RSA (default) and DSA keys.
Access	When sharing a connection with a public key authentication, or a connection that is used with a Hot Folder, that key should have this option checked.

2. Distribute the public key

Then, you will need to provide the public key file (e.g. `id_rsa.pub`) to your server administrator, so that it can be set up for your server connection. To copy or export the public key, select the key in the *Public Key Manager* window, click **Copy Public Key to Clipboard**, and paste the string into an email and address it to the server administrator, or click **Export to File** and save the public key as a file. The instructions for installing the public key on the server can be found in the [Setting Up a User's Public Key](#); however, the server may be installed on an Operating System that is different from the one that your client has been installed on.



You can find the public key in this path:

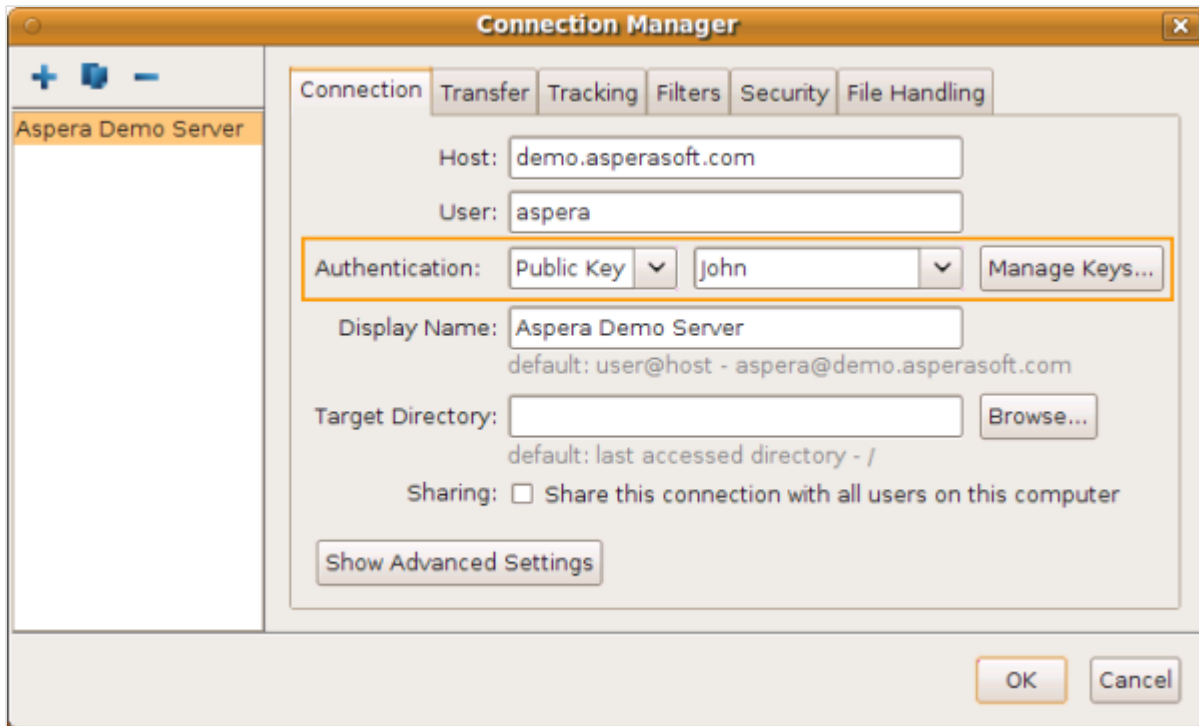
```
/(home directory)/.ssh/
```

3. Set up connections using public key authentication

When your public key has been installed on the remote host by its server administrator, click the **Connections** to bring up *Connection Manager*.



Under the *Connection* tab, select Public Key from the Authentication pull-down menu and select the key that is installed on this host.



Transferring Files

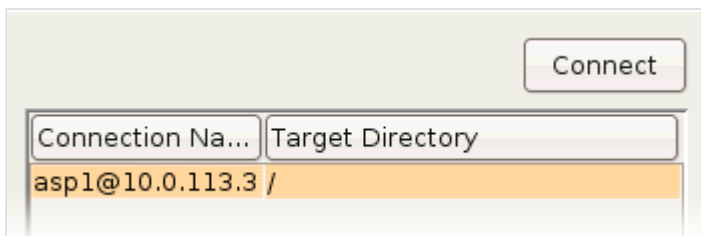
Initiate and manage file transfers.

This topic demonstrates how to start a basic file transfer using the application.

IMPORTANT NOTE: Do not use the following characters in the file name: / \ " : ' ? > < & * |

1. Connect to the remote host

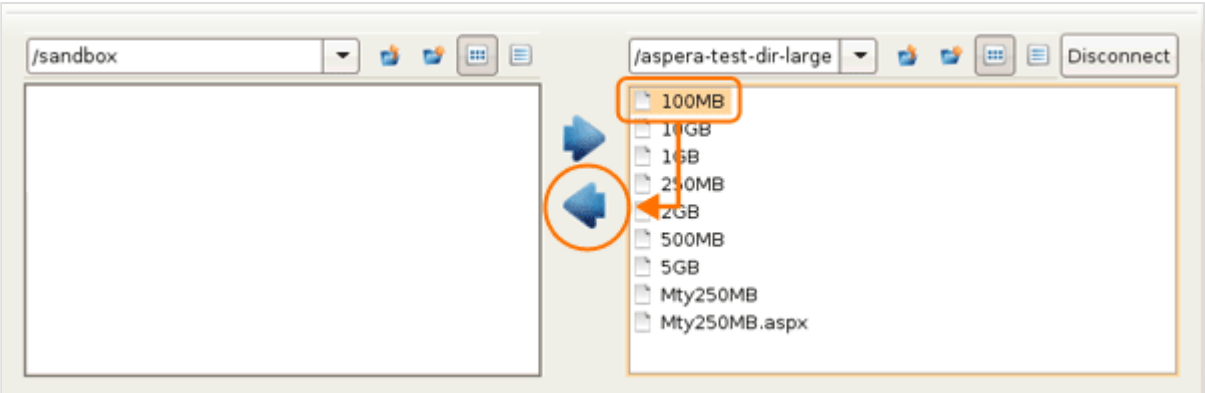
Start the application by launching **asperascp**, and double-click the connection within the *Connection* panel, or select it and click **Connect**.





In the *Connections* panel, the **Target Directory** shows either a specific path when the target directory is set, or the last-visited folder when left blank. Refer to [Managing Connections](#) on page 13 for setting up the target directory.

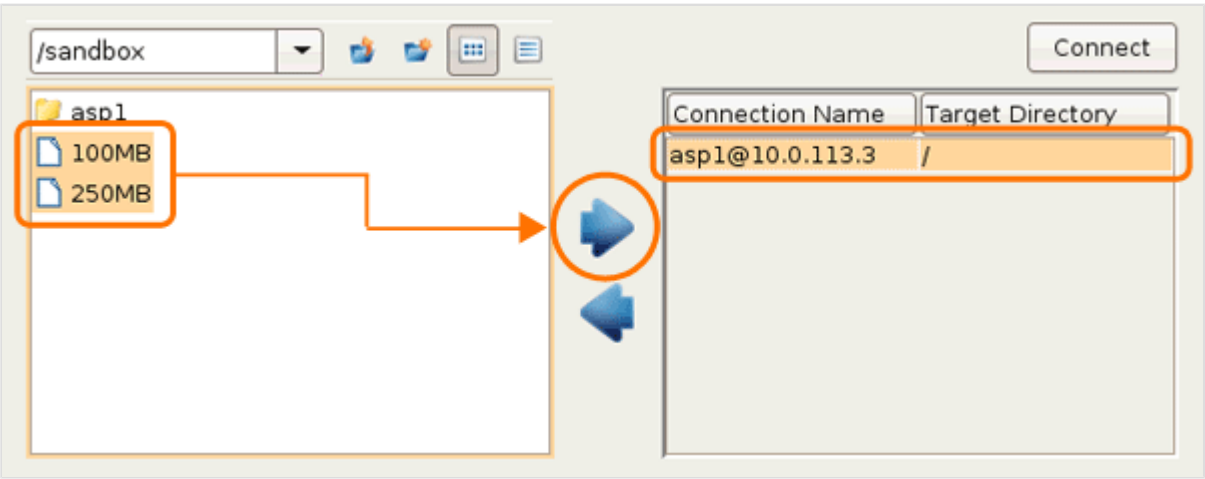
2. Initiate the transfer

To transfer a file to or from the remote computer, select the file that you would like to transfer and then click the upload or download arrow.








3. Transfer files without browsing the remote host

If you have entered the target directory for this connection (See [Managing Connections](#) on page 13), you can also transfer files without browsing the remote computer. To do so, select the files from the left panel (local), select the connection name from the right panel (remote) and click  to push files to the remote computer's target directory (as shown in the screenshot), or  to pull files from it.

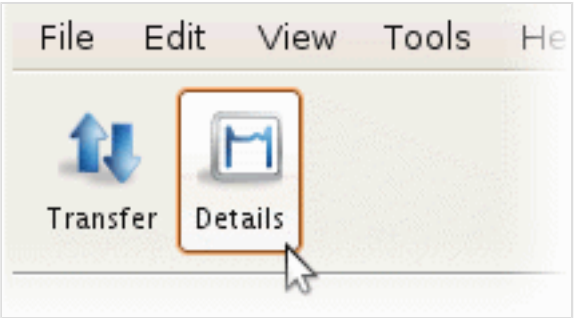


4. Manage the transfer sessions in the Transfers panel

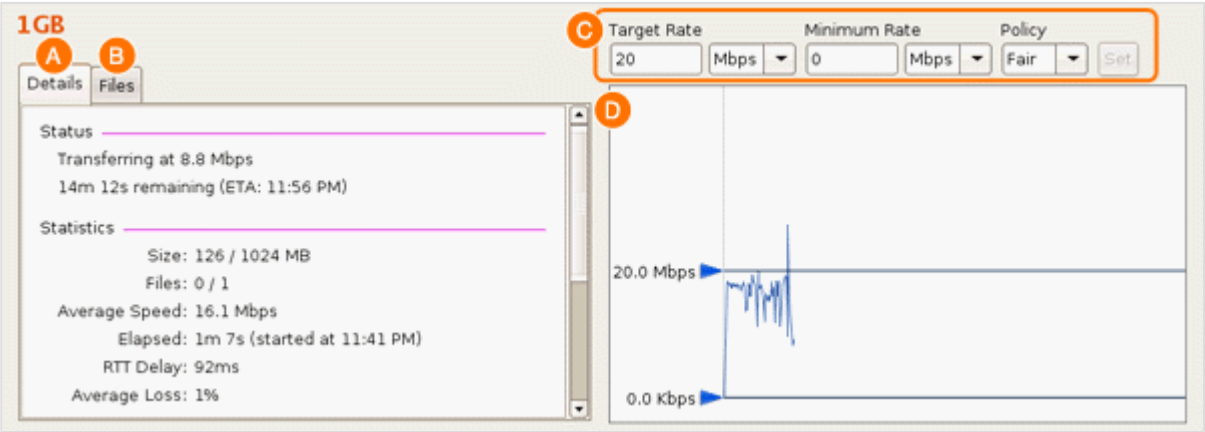
Once the transfer has been successfully initiated, a progress bar will appear in the Transfers panel. If you have multiple ongoing transfers, use the  and  to change the selected transfer's priority. The # field indicates the transfer's order in the queue. Also the , , and  can be used to control the selected transfer session.

5. (Optional) Make adjustments to a transfer session's target rate, minimum rate and/or policy (if allowed)

The **Details** button provides additional visibility and control (if granted the proper permissions) over transfers. Select a transfer session from the *Transfers panel* and click **Details** to view details and/or adjust settings.



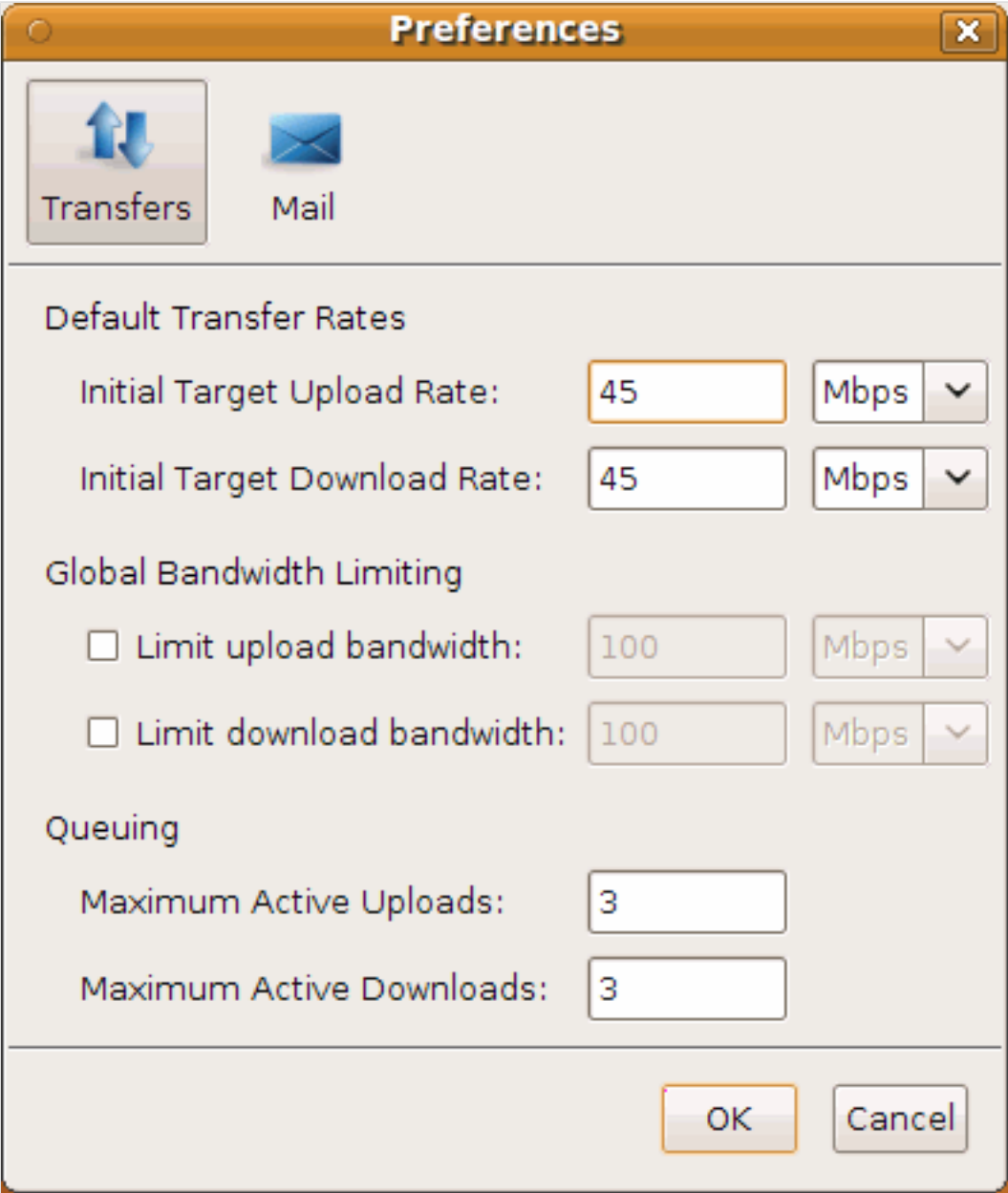
The following is a list of items that can be found on the Details page:



Item	Name	Description
A	Details (tab)	Transfer details, including status (rate and ETA) and statistics (session size, files transferred vs. total files to be transferred, average speed, time elapsed, RTT delay and average loss in percent).
B	Files (tab)	All files being transferred in this session, along with each files' size and transfer progress.
C	Transfer controls	Set the transfer policy and transfer rate, if allowed. Please refer to fasp Transfer Policies on page 58 for additional information.
D	Transfer Monitor	The transfer graph. Note that you may use the sliders to adjust the transfer rate up or down (if allowed).

6. Update the default transfer rate and maximum concurrent active transfers within the Preferences window

To update these settings, click the **Preferences** button from the application's main window.



The following options are available under the *Transfers* tab:

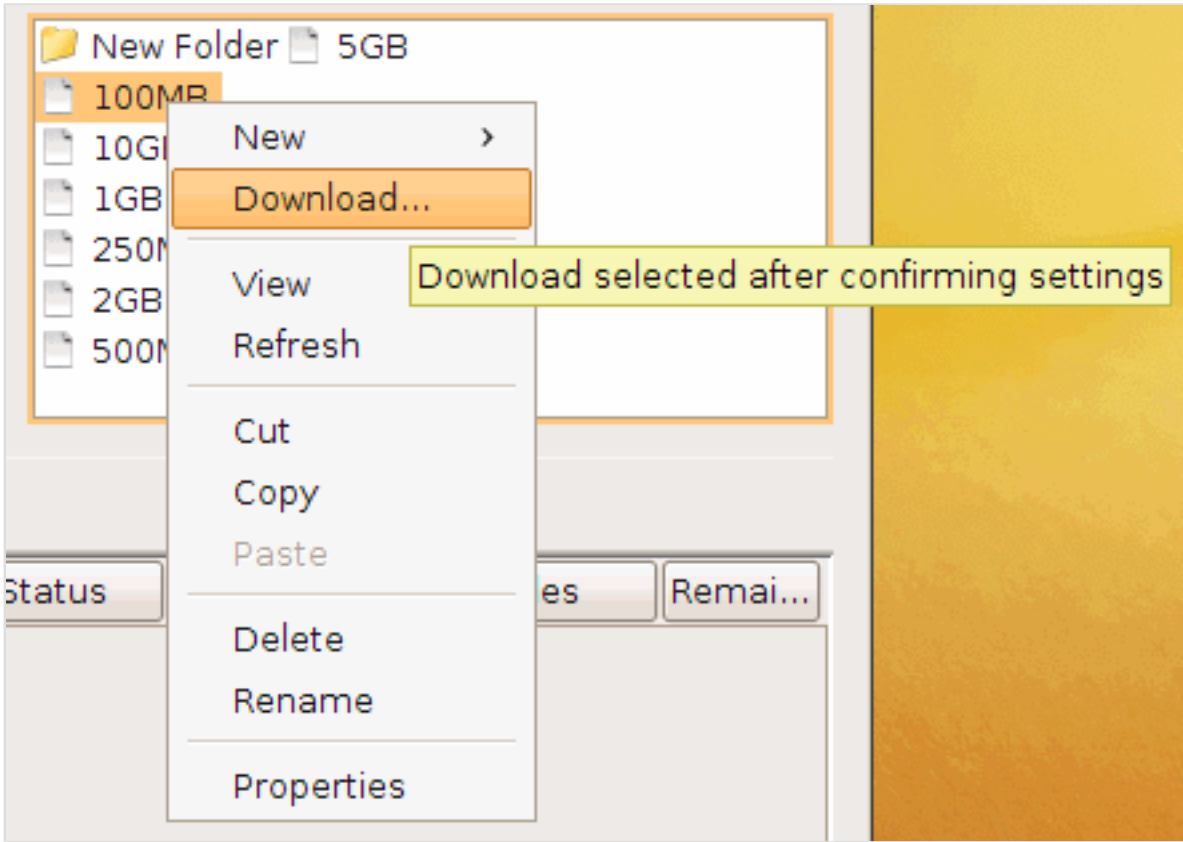
Item	Description
Default Transfer Rates	The initial download and upload rates for all transfers.
Global Bandwidth Limiting	Adjust the aggregated bandwidth cap for all <i>fasp</i> transfers on this computer. For more advanced bandwidth settings, please refer to Bandwidth .
Queuing	Set the maximum number of concurrent upload and download transfers.

To view information about settings located under the *Email* tab, please refer to the topic [Configuring Transfer Notifications](#) on page 27.

Advanced Transfer Mode

Reveal more options when initiating transfers, such as filters, security, and scheduling.

You can start a transfer in advanced mode to reveal per-session transfer setting options, which overwrite the default transfer settings. To initiate the advanced transfer mode when establishing a connection, right-click a file and select **Upload...** or **Download...**



The advanced transfer mode includes the following configuration tabs:

Tab	Description
Transfer	The transfer session-related options, such as the transfer speed and retry rules.
Tracking	Options for tracking the transfer session, including the confirmation receipt and the email notifications.
Filters	Create filters to skip files that match certain patterns.
Security	Enable the transfer encryption and the content protection.
File Handling	Set up resume rule, preserve transferred file attributes, and remove source files.
Scheduling	Schedule this transfer.

IMPORTANT NOTE: All configuration tabs, except **Scheduling**, are identical to those in the *Connection Manager* configuration screen. Please refer to [Managing Connections](#) on page 13 for additional details on the *Connection Manager*. The following table explains only the *Scheduling* tab.

Scheduling

Check **Schedule this transfer** to enable transfer scheduling. Click **Transfer** when finished. The following scheduling options are available:

Start Download from demo.asperasoft.com

Transfer

Tracking

Filters

Security

File Handling

Scheduling

☒ Schedule this transfer

Time: 7:00 PM

Transfer repeats: Monday - Friday


End repeat: ☒ Never

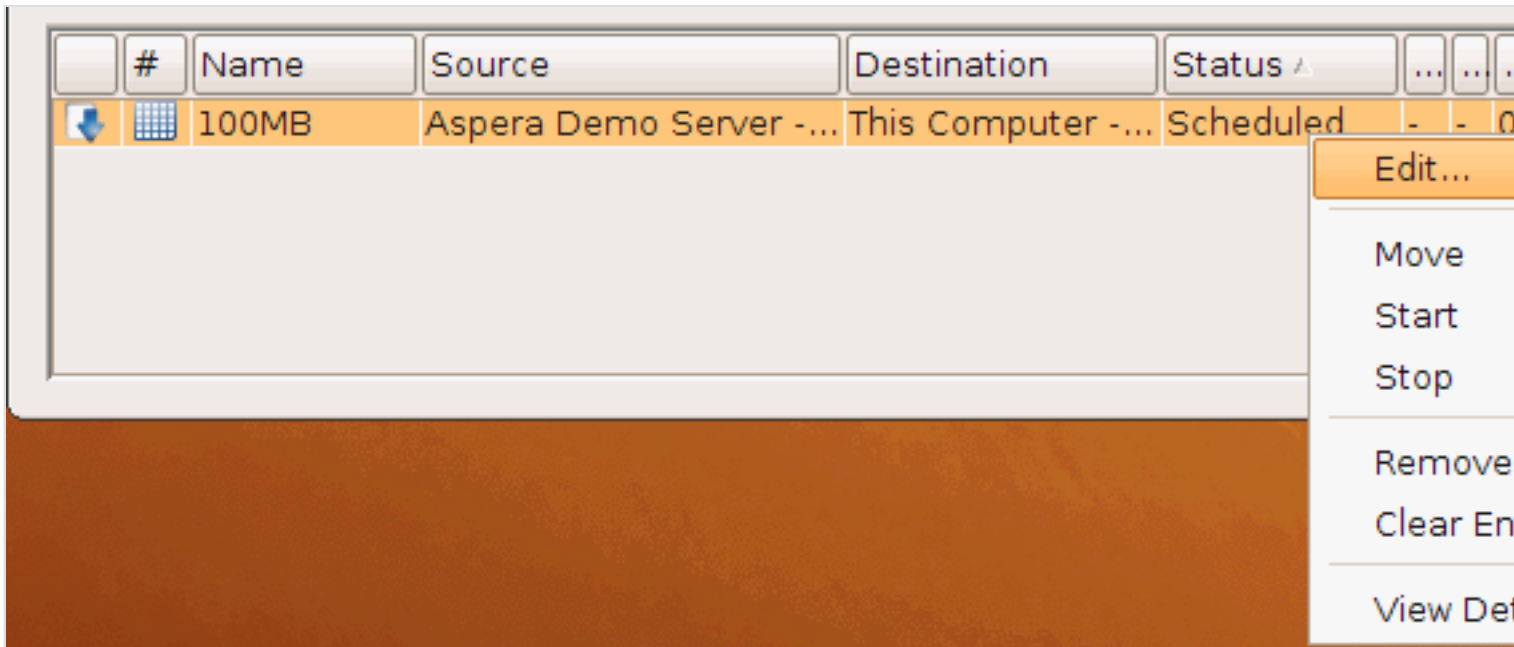
☐ On: 6:28 PM Feb 23, 2011

Transfer

Cancel

Option	Description
Time	Specify the transfer time.
Transfer repeats	Select a repeat mode. When <i>repeat</i> is enable, the Date field appears, which allows a date or repeat-rule setting to be selected.

When submitting a scheduled transfer, you will see it listed under the Transfers tab, along with an icon () under the # column. To modify the transfer, right-click it and select **Edit** to reveal the transfer settings.



IMPORTANT NOTE: When scheduling transfers, ensure that the application is running. Scheduled transfers will not run when the application is closed.

Configuring Transfer Notifications

Set up transfer notifications and modify the templates.

Transfer notification emails (which are based on default or customized mail templates) are triggered by three transfer session events: *start*, *completion* and *error*. Follow the instructions below to configure the SMTP server and/or to create/modify your email templates.

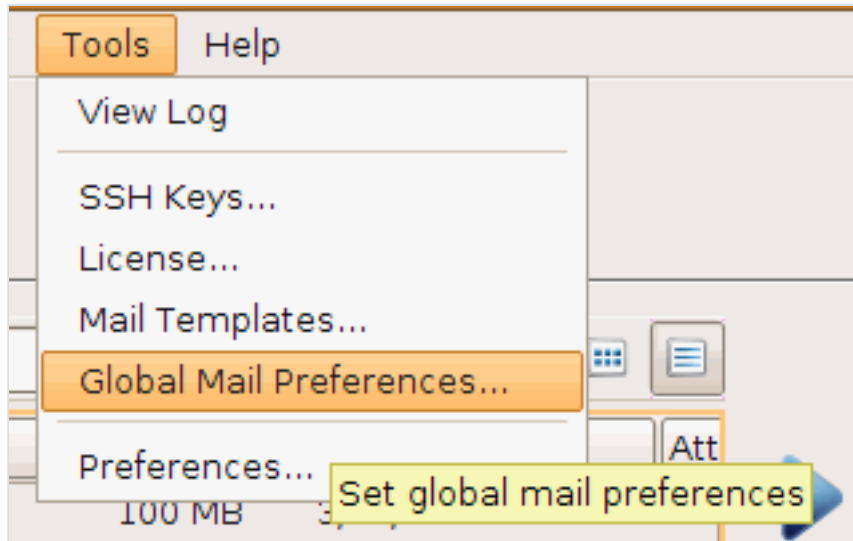
1. Launch with *root* permissions

Configuring transfer notifications requires root access. Run **asperascp** in a Terminal as root to launch the application.

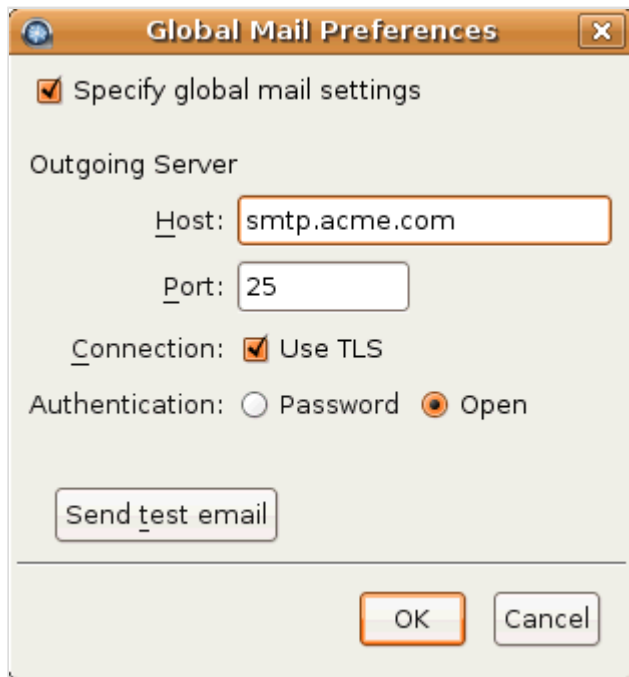
2. Configure global mail preferences

IMPORTANT NOTE: To configure global mail preferences, you must have *root* permissions.

To set up global mail preferences, launch the application with permissions, and select **Tools > Global Mail Preferences....**

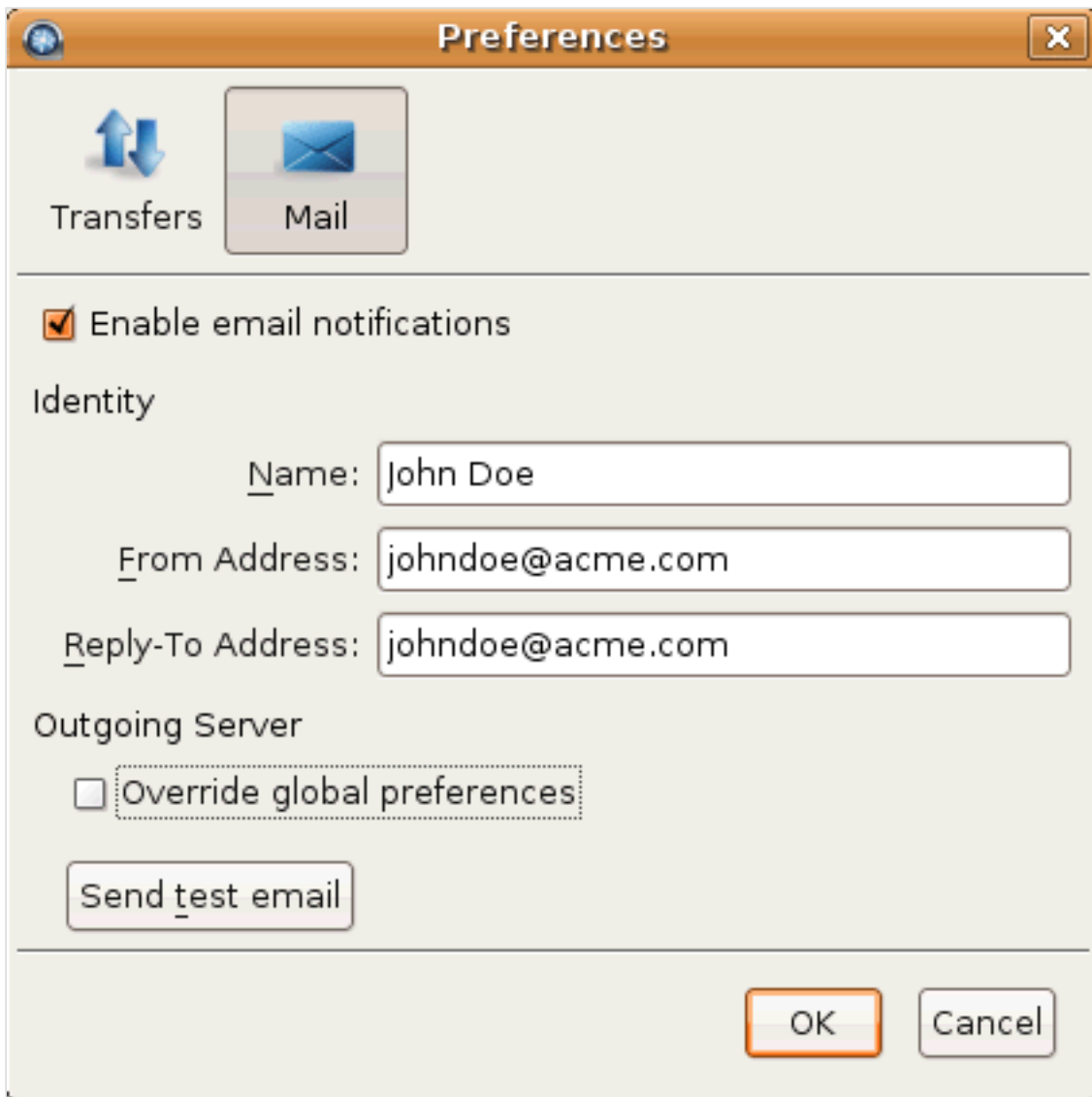


Check the option **specify global mail settings** and enter outgoing email server information. To ensure that the mail server information is correct, click **Send test email** and enter an email address to send to.



3. Enable mail notifications

Go to **Preferences > Mail**.

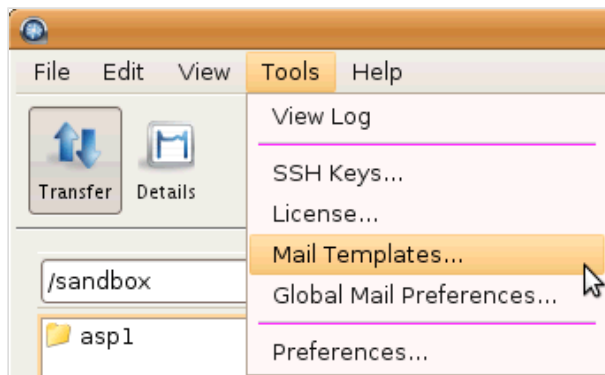



Check the option **Enable email notifications** and enter your email in *Identity* section. To overwrite the global outgoing email server settings, or if the global settings isn't available, check **Override global preferences** and enter an outgoing email server's address. Click **Send test email** to send a test email to the address entered in the *Identity* section.

4. Bring up the Mail Templates window

Templates are used to generate the content of notification emails. You can associate them with connections, hot folders, and individual transfers. We provide a default template. They can be changed to customize notification emails.

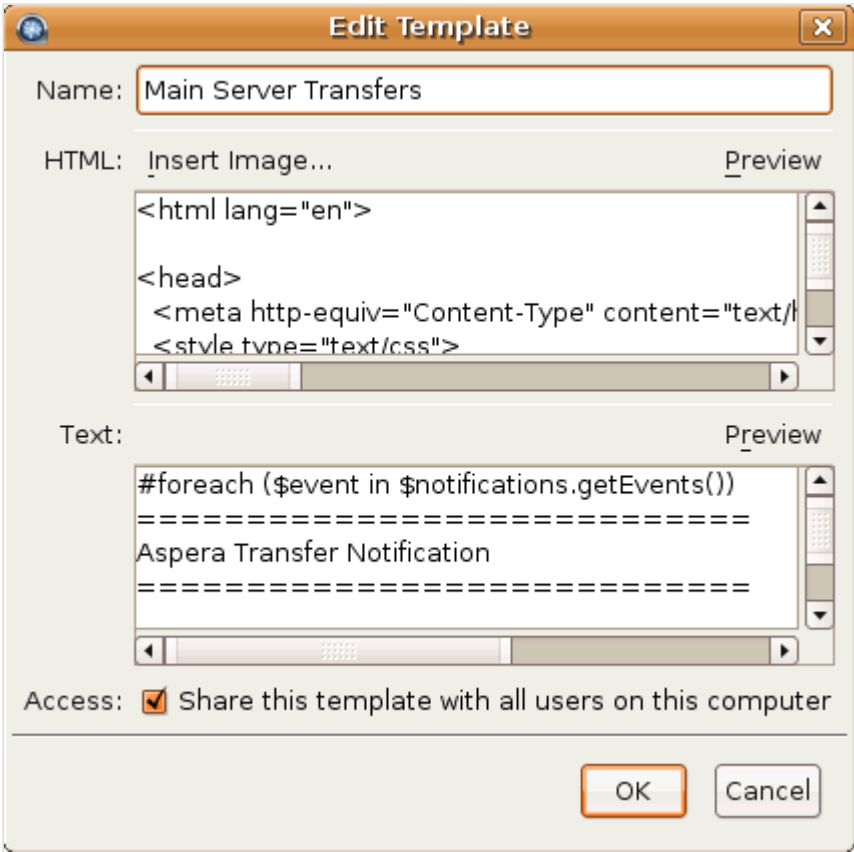
Go to **Tools > Mail Templates...** to bring up the mail template window.



In the *Mail Templates* window, click  to create a template based on existing ones, or select an existing template and click  to edit it.



The mail template supports MIME (Multipurpose Internet Mail Extensions) multipart messages that includes both the HTML and plain text versions of the mail body. In the *Edit Template* window, Enter the template in the specified field:

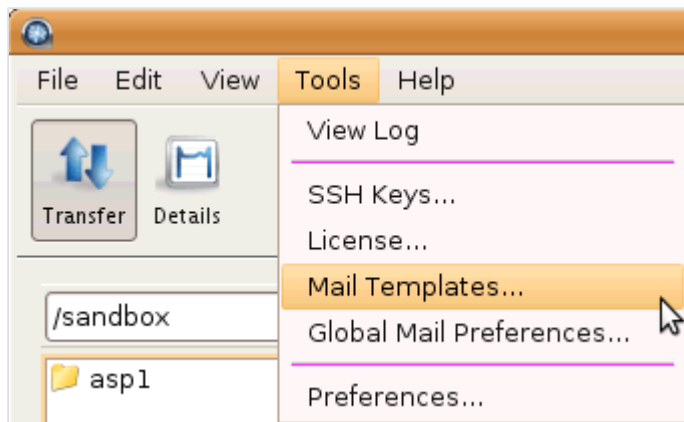


Item	Description
Name	The template name.
HTML	The HTML mail body. Click Insert Image... to insert an image into the template. The selected image will be copied to the template directory. You may preview the template by clicking Preview .
Text	The plain text mail body. You may preview the template by clicking Preview .
Access	Check the option Share this template with all users on this computer to allow other system users to access this template.

5. Modify mail templates

Mail templates serve as models for the email that will be sent.

To modify mail templates, go to **Tools > Mail Templates...** to bring up the template management window.



The templates are rendered using Apache Velocity ([Apache Velocity User Guide](#)). Content is generated for an email according to its template. A conditional statement only generates content if the condition matches. A foreach loop generates content for each iteration of the loop. Within a template, there are two predefined variables:

- **\$formatter** - Contains some utility methods
- **\$notifications** - Holds the transfer notifications

To iterate over notifications, use a foreach loop:

```
#foreach ($event in $notifications.getEvents())
...
#end
```

This declares a local *\$event* variable that can be used within the for-each loop.

The following conditional statements can be used in the templates:

```
#if
...
#else
...
#end
```

All statements are categorized in four parts: conditional, session information, time, and statistics.

Conditional

Use these tests in an **if** statement. For example:

```
#if ($event.isFailed())
...
#end
```


Statement	Description
<code>\$event.isStarted()</code>	If the transfer session is started.
<code>\$event.isCompleted()</code>	If the transfer session is completed.
<code>\$event.isEnded()</code>	If the transfer session is ended.
<code>\$event.isFailed()</code>	If the transfer session is failed.

Session Information

Statement	Description
<code>\$event.getSourceHost()</code>	The source host address.
<code>\$event.getSourcePaths()</code>	The source file path.
<code>\$event.getDestinationHost()</code>	The destination host address.
<code>\$event.getDestinationPath()</code>	The destination file path.
<code>\$event.getInitiatingHost()</code>	The session-initiating host address.
<code>\$event.getId()</code>	The session ID.
<code>\$event.getName()</code>	The session name.
<code>\$event.getType().getDescription()</code>	The session state. Three outputs: "STARTED", "FAILED", and "COMPLETED".
<code>\$event.getUser()</code>	The transfer login.
<code>\$event.GetFiles()</code>	<p>The files that are being transferred. Use this statement in a foreach loop: (Any text after <code>##</code> is a comment)</p> <pre>#foreach (\$file in \$event.GetFiles()) ## \$file is a new variable visible in this foreach loop. ## \$file holds the complete file path and file name. ## \$formatter.decodePath() is used to ensure a correct string decoding. \$formatter.decodePath(\$file) #end</pre> <p>And use the counter <code>\$velocityCount</code> in an if statement to limit the output file count. For example, to list only the first ten files:</p> <pre>#foreach (\$file in \$event.GetFiles()) #if (\$velocityCount > 10) #break</pre>

Statement	Description
	<pre>#end \$file #end</pre>
<code>\$event.getMessage()</code>	The message entered in the notification's "Message" field.
<code>\$event.getError()</code>	The error message.

Time

Statement	Description
<code>\$formatter.date(VAR, "LANG", "FORMAT")</code>	<p>Formatting the date and time output. Enter three values in the parenthesis:</p> <ul style="list-style-type: none"> • Replace <i>VAR</i> with the following two statements. E.g. <code>\$event.getStartTime()</code> • Replace the <i>LANG</i> with an abbreviate language name. E.g. <i>en</i> for English. • The <i>FORMAT</i> is the display format. Use these symbols: <ul style="list-style-type: none"> • yyyy The year. E.g. 2010 • MM Month of the year. E.g. 03 • dd Day of the month. E.g. 28 • HH Hour of the day. • mm Minute. • ss Second. • z Time zone. • EEE The abbreviated weekday name. <p>For example, "<i>EEE, yyyy-MM-dd HH:mm:ss z</i>" shows <i>Fri, 2010-03-26 16:19:01 PST</i>.</p>
<code>\$event.getStartTime()</code>	The session start time.
<code>\$event.getEndTime()</code>	The session end time.

Statistics

Statement	Description
<code>\$event.getSourceFileCount()</code>	The number of source files.
<code>\$event.getCompletedFileCount()</code>	The number of files that successfully transferred.
<code>\$event.getFailedFileCount()</code>	The number of files that failed to transferred.

Statement	Description
<code>\$event.getAverageRatePercentage()</code>	The average transfer rate in bps. Enclose this statement with <code>\$formatter.formatRate()</code> to simplify the output.
<code>\$event.getAverageLossPercentage()</code>	The average packet loss percentage.
<code>\$event.getSourceSizeB()</code>	The source file size. Enclose this statement with <code>\$formatter.toBestUnit()</code> to simplify the output.
<code>\$event.getTransferredB()</code>	The transferred file size. Enclose this statement with <code>\$formatter.toBestUnit()</code> to simplify the output.
<code>\$event.getWrittenB()</code>	The destination file size. Enclose this statement with <code>\$formatter.toBestUnit()</code> to simplify the output.

When configured, you can apply the notifications to a connection host, or a transfer session. Refer to [Using Transfer Notifications](#) on page 35.

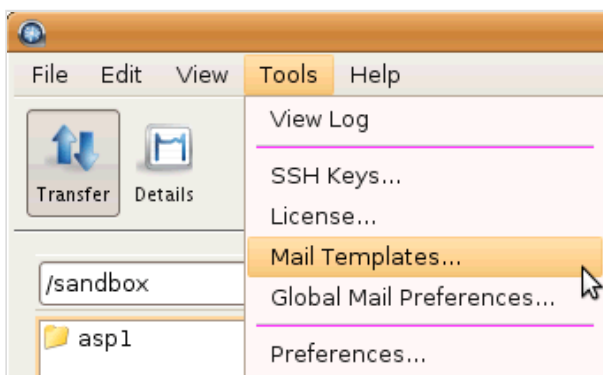
Using Transfer Notifications


Use transfer notifications to send emails based on transfer events.

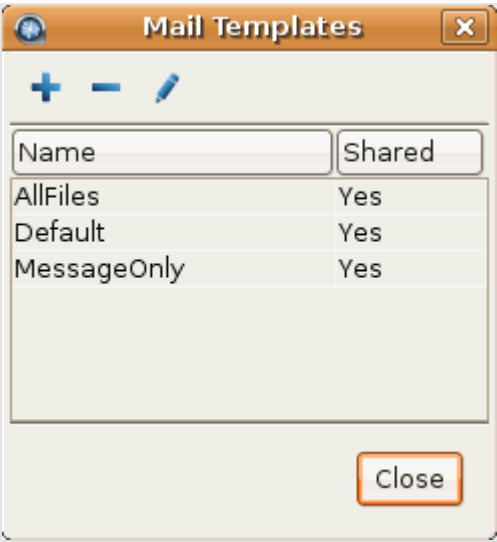
Transfer notifications can be sent for three transfer events: start, complete, and error. Follow these instructions to select and apply them to your transfer sessions:

1. Preview mail templates

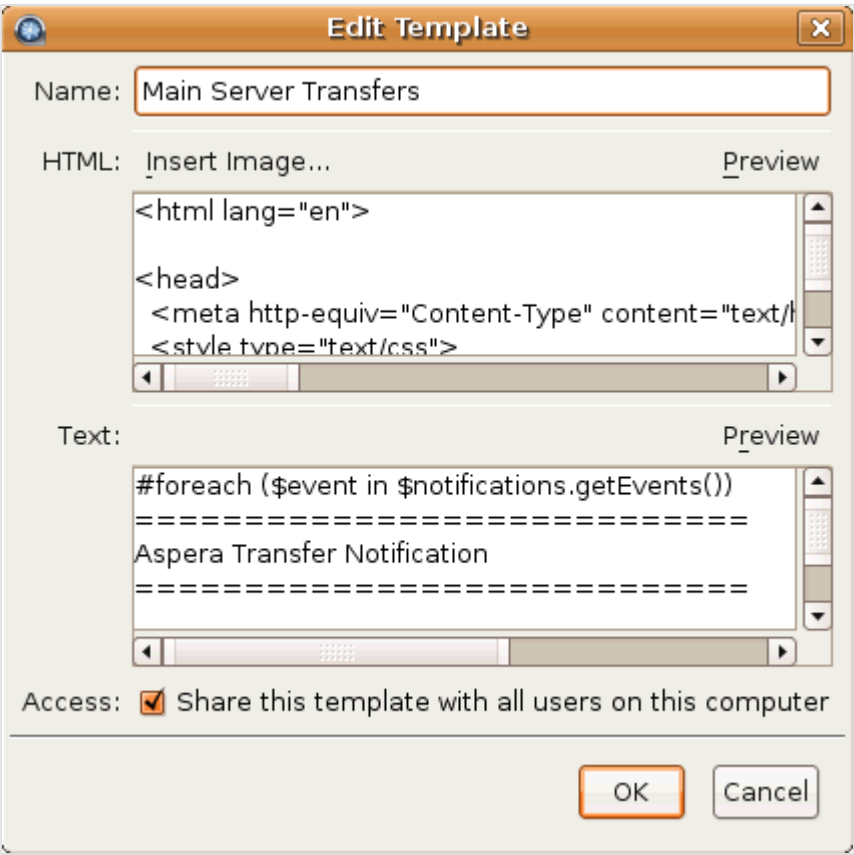
You can preview existing templates to decide which one to use. In the application (**asperascp**), go to **Tools > Mail Templates...** to bring up the *Mail Template* window.



In the *Mail Templates* window, select an existing template and click  to open the edit screen.



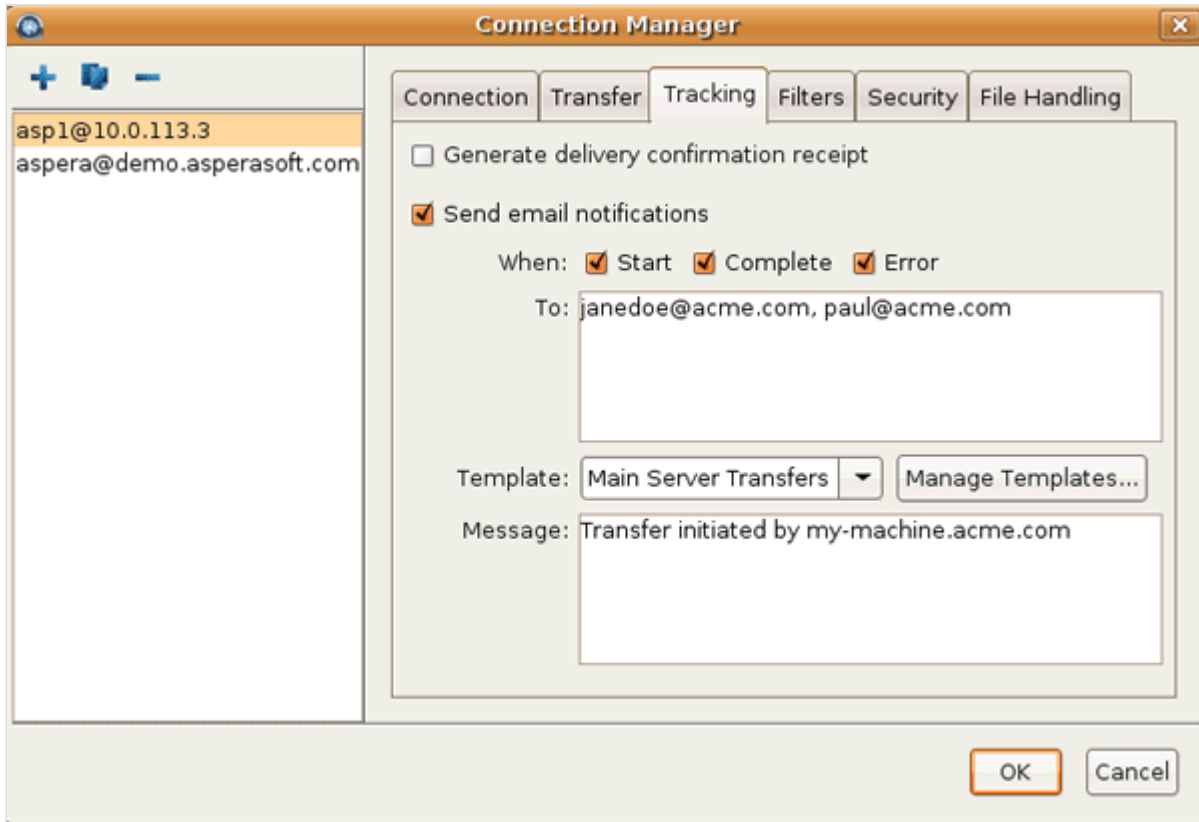
Mail templates supports MIME multipart messages, which include both HTML and plain text versions. In the *Edit Template* window, click **Preview** to view the template's output example.



2. Set up notifications for a connection

You can set up notifications for connections. When transferring with the host, emails will be sent to specified recipients on selected events.

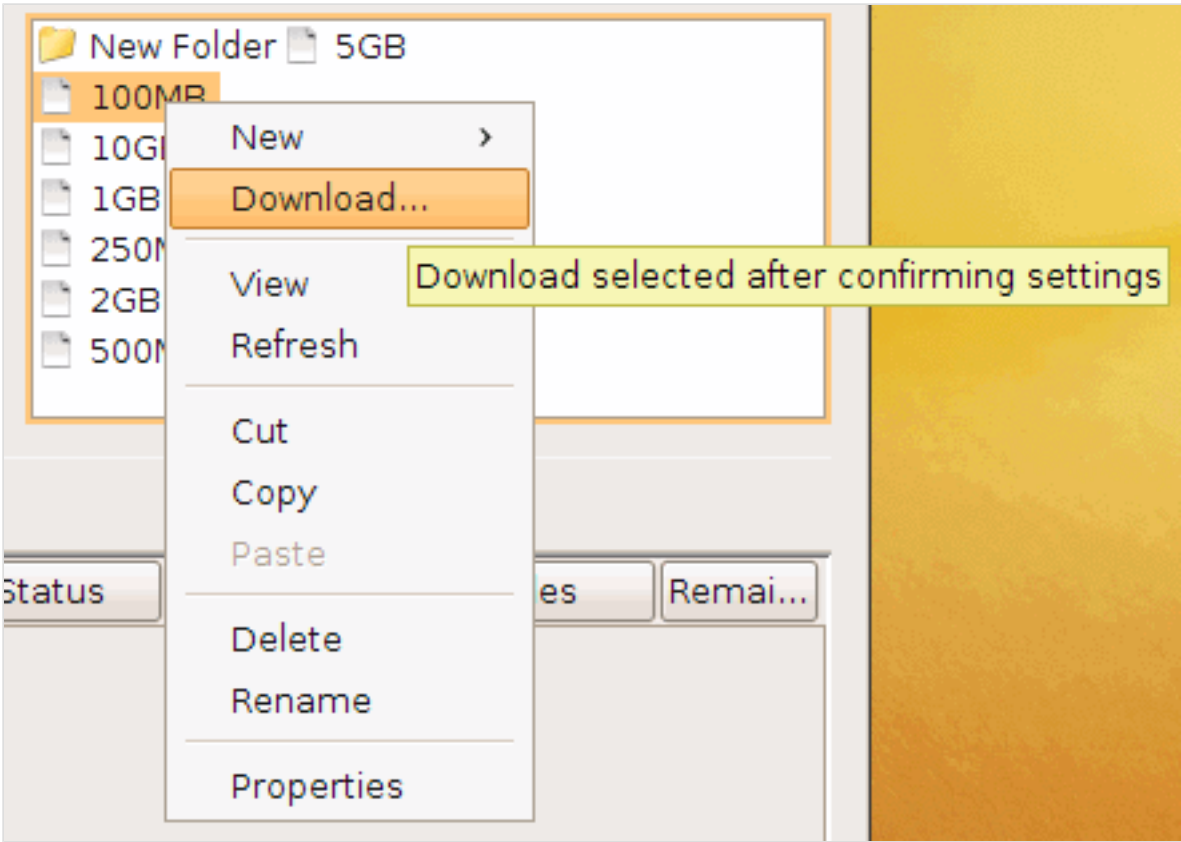
To do so, click **Connections**, choose the connection, and select the **Tracking** tab. Check **Send email notifications** to enable this feature. Enter the following information, and then click **OK**:



Item	Description
When	Check the events to send notifications for.
To	Enter the recipients, comma separated.
Template	Select a mail template.
Message	Optionally enter a message to include in the notifications.

3. Set up notifications for a transfer

Email notifications can also be applied to transfer sessions. Right click the file browser and select **Upload...** or **Download...** to open the advanced transfer window, select the **Tracking** tab, and check **Send email notifications** to enable this feature. Refer to the previous section for help on setting the options.



Global Transfer Settings

The system-wide and default *fasp* transfer settings for your computer.

Setting Global Bandwidth

Allocate the global bandwidth for *fasp* file transfer.

Aspera's *fasp* transport has no theoretical throughput limit. Other than the network capacity, the transfer speed may be limited by rate settings and resources of the computers. This topic shows you how to optimize the transfer rate by setting up the global rate settings.

To set global *fasp* bandwidth, bring up the application (**asperascp**) and click **Preferences**. Enter the global bandwidth value in the Global Bandwidth Limiting field.

Preferences

↑↓

Transfers

✉

Mail

Default Transfer Rates

Initial Target Upload Rate:

45

Mbps

▼

Initial Target Download Rate:

45

Mbps

▼

Global Bandwidth Limiting

☐ Limit upload bandwidth:

100

Mbps

▼

☐ Limit download bandwidth:

100

Mbps

▼

Queuing

Maximum Active Uploads:

3

Maximum Active Downloads:

3

OK

Cancel

Item	Description
Default Transfer Rates	The initial download and upload rates for all transfers.
Global Bandwidth Limiting	Adjust the aggregated bandwidth cap for all fasp transfers on this computer. For more advanced bandwidth settings, refer to Bandwidth .
Queuing	Set the maximum number of concurrent upload and download transfers.

To create global bandwidth using the command line, open the aspera.conf (**/opt/aspera/etc/aspera.conf**) with a text editor. The following example sets the global bandwidth with these value:

Item	Value
Upload bandwidth limit (Outgoing):	88 Mbps (88000 Kbps)
Download bandwidth limit (Incoming):	99 Mbps (99000 Kbps)

```
<?xml version='1.0' encoding='UTF-8'?>
<CONF version="2">
  ...
  <trunks>
    <trunk>      <!-- Create a Vlink with 88000 Kbps bandwidth cap. -->
      <id>108</id>  <!-- ID: 108 -->
      <capacity><value>88000</value></capacity>
      <on>true</on>
    </trunk>
    <trunk>      <!-- Create a Vlink with 99000 Kbps bandwidth cap. -->
      <id>109</id>  <!-- ID: 109 -->
      <capacity><value>99000</value></capacity>
      <on>true</on>
    </trunk>
  </trunks>

  <default>  <!-- Global settings.-->
    <transfer>
      <out>    <!-- Use Vlink ID: 108 for global outgoing bandwidth. -->
        <bandwidth><aggregate><trunk_id>108</trunk_id></aggregate></bandwidth>
      </out>
      <in>     <!-- Use Vlink ID: 109 for global incoming bandwidth. -->
        <bandwidth><aggregate><trunk_id>109</trunk_id></aggregate></bandwidth>
      </in>
    </transfer>
  </default>
</CONF>
```

Aspera Sync

The asperasync file synchronization command.

asperasync Syntax

Configure the asperasync to perform file synchronization.

Aspera Sync is a command-line tool that can be used to monitor configured "hot folders" for changes, automatically transferring any new or modified files. It can be used for one-way replication between two locations or simply as a way of forwarding files in your work-flow. Sync runs as a service in the background.

The following shell script is used to execute Aspera Sync:

```
/opt/aspera/bin/asperasync.sh
```

You can modify the Aspera Sync transfer settings directly in this file. For example, the Aspera Sync is initiated every 10 seconds with target rate 100Mbps (100000Kbps), you can change them by modifying the values of INTERVAL and TARGETRATE in this file, respectively:

```
...
INTERVAL=10           # Interval for directory sync is in seconds
TARGETRATE=100000     # The highest rate the sync will try to achieve.
...
```

To execute the Aspera Sync, use the command asperasync.sh with the following syntax (The environment variable ASPERA_SCP_PASS=pswd can be set in a separate line with export ASPERA_SCP_PASS=pswd):

```
$ ASPERA_SCP_PASS=pswd /opt/aspera/bin/asperasync.sh src-dir des-dir arg
```

Parameter	Description
pswd	The password for remote login. Use the environment variable ASPERA_SCP_PASS to set it.
src-dir	The source folder.
des-dir	The destination folder. Either the source or the destination folder has to be a local directory on your computer. The parameter on the remote-side takes the form user@remote-address.
arg	The ascp command options for this synchronization. See ascp Usage on page 45.

asperasync Examples

Examples of the asperasync settings.

This topic demonstrates the asperasync configuration settings with the following examples:

1. Start a regular synchronization

Item	Value
Remote Login	asp1 / 1234
Source	(Local)
Source folder	/local-src
Destination	10.0.0.5 (Remote)
Destination Folder	/remote-desc

```
$ export ASPERA_SCP_PASS=1234
$ /opt/aspera/bin/asperasync.sh /local-src asp1@10.0.0.5:/remote-dest
```

2. Start the same synchronize with additional ascp command options

Item	Value
ascp Options	Target rate 10Mbps (-l 10000), resume with a full file checksum(-k3)

```
$ export ASPERA_SCP_PASS=1234
$ /opt/aspera/bin/asperasync.sh /local-src asp1@10.0.0.5:/remote-dest -l 10000 -k3
```

3. Keep the script running when the Terminal session is closed

To keep the script running when the Terminal session is closed, start the command with *nohup*, and add a **&** at the end:

```
$ export ASPERA_SCP_PASS=1234
$ nohup /opt/aspera/bin/asperasync.sh /local-src asp1@10.0.0.5:/remote-dest &
```

4. Synchronize from a network shares location

To synchronize from a network shares location, through a remote host, to a local directory:

Item	Value
Remote Login	asp1 / 1234
Source	10.0.0.10 (Remote)
Source folder	\\1.2.3.4\nw-share-src (Network Shares drive)
Destination	(Local)
Destination Folder	/inbox

```
$ export ASPERA_SCP_PASS=1234
```

```
$ /opt/aspera/bin/asperasync.sh aspl@10.0.0.10:"//1.2.3.4/nw-share-src" /inbox
```

Transferring in Command-line

Initiate transfers in Command-line.

ascp Usage

The ascp command reference.

ascp is a command-line *fasp* transfer program. This topic covers the complete command usage, including the general syntax guideline, supported environment variables, synopsis, and the options.

General Syntax Guideline

Item	Description
symbols used in the paths	Use single-quote (' ') and forward-slashes (/) on all platforms.
Characters to avoid	/ \ " : ' ? > < & *

Environment Variables

If needed, you can use the command to set the password, token, and cookie in the environment variables. Replace the highlighted text with your own values:

Item	Initiation Command
Password	export ASPERA_SCP_PASS=the-password
Token	export ASPERA_SCP_TOKEN=the-token
Cookie	export ASPERA_SCP_COOKIE=the-cookie
Content Protection Password	export ASPERA_SCP_FILEPASS=content-protect-password

ascp Usage

```
ascp <options> [[user@]srcHost:]source-file1[,source-file2,...]
[[user@]destHost:]target-path
```

ascp Options

Option	Description
-A	Display version and license information; then exit.
-T	Disable encryption for maximum throughput.
-d	Create target directory if it doesn't already exist.

Option	Description
-p	Preserve source modification time (mtime) and last access time (atime).
-q	Quiet flag, to disable progress display.
-v	Verbose mode, print connection and authentication debug messages in the log file.
-{Q QQ}	Enable fair (-Q) or trickle (-QQ) transfer policy. Use the -l and -m to set the target and minimum rates.
-l target_rate	Set the target transfer rate in Kbps. <i>Default: 10000</i>
-m min-rate	Set the minimum transfer rate in Kbps. <i>Default: 0</i>
-w{r f}	Test bandwidth from server to client (r) or client to server (f). Currently a beta option.
-K probe-rate	Set probing rate (Kbps) when measuring bottleneck bandwidth.
-k {0 1 2 3}	<p>Enable resuming partially transferred files. (<i>Default: 0</i>). Please note that this must be specified for your first transfer; otherwise, it will not work for subsequent transfers.</p> <ul style="list-style-type: none"> • 0 Always retransfer the entire file. • 1 Check file attributes and resume if the current and original attributes match. • 2 Check file attributes and do a sparse file checksum; resume if the current and original attributes/checksums match. • 3 Check file attributes and do a full file checksum; resume if the current and original attributes/checksums match.
-i private-key-file	Use public key authentication and specify the private key file. Typically, the private key file is in the directory <i>\$HOME/.ssh/id_[algorithm]</i> .
-Z dgram-size	Specify the datagram size (MTU) for <i>fasp</i> . By default it uses the detected path MTU.
-u user-string	Apply user string, such as variables for Pre- and Post-Processing, in the transfer.
-X rexmsg-size	Adjust the size in bytes of a retransmission request. (<i>Max: 1440</i>).
-g read-size	Set the read block size (in bytes). E.g. 1M for 1 megabyte.
-G write-size	Set the write block size (in bytes), E.g. 1M for 1 megabyte.
-S remote-ascp	Specify the name of the remote ascp binary if different.
-L local-log-dir	Specify a logging directory in the local host, instead of using the default directory.
-R remote-log-dir	Specify a logging directory in the remote host, instead of using the default directory.
-e prepost	Specify an alternate pre-post command. Use complete path and file name.
-f config-file	Specify an alternate Aspera configuration file other than aspera.conf.

Option	Description
-C n-id:n-count	Use parallel transfer on a multi-node/core system. Specify the node id (nid) and count(ncount) in the format 1:2, 2:2. Assign each participant an independent UDP port.
-E pattern	Exclude files or directories with the specified pattern in the transfer. This option can be used multiple times to exclude many patterns. Up to 16 patterns can be used by using -E. Two symbols can be used in the pattern: <ul style="list-style-type: none"> • * (asterisk) represents zero to many characters in a string, for example "*.tmp" matches ".tmp" and "abcde.tmp". • ? (question mark) represents one character, for example "t?p" matches "tmp" but not "temp".
-O fasp-port	Set the UDP port used by <i>fasp</i> for data transfer. (Default: 33001)
-P ssh-port	Set the TCP port used for <i>fasp</i> session initiation. (Default: 22)
-U {1 2}	Priority when sharing physical or virtual bandwidth cap. 1 for higher priority, 2 for regular. (Default: 2)
-W token-string	Specify the token string for the transfer.
-@[range-low:range-high]	Transfer only part of a file. This option only works for downloading a single file, and does not support resuming. The argument to "-@" may omit either or both numbers, and the ":" delimiter. For example, -@3000:6000 transfers bytes between positions 3000 to 6000; -@1000: transfers from 1000 to the end of the file; and -@:1000 transfers from beginning to 1000.
-6	Enable IPv6 address support. When using IPv6, numeric host can be written inside brackets. For example, [2001:0:4137:9e50:201b:63d3:ba92:da] or [fe80::21b:21ff:fe1c:5072%eth1]
-D -DD -DDD	Specify the debug level. each D is one additional level of debugging.
--mode=MODE	Specify the transfer direction. Replace <i>MODE</i> with send or recv .
--user=USERNAME	The user name that you use for authentication.
--host=HOSTNAME	The server's address.
--args-list=FILENAME	The command file's name. If you are storing command options in a file, use this option to call the file. Refer to Creating Command Files on page 54 for more detail.
--file-list=FILENAME	The file list. If you list all files to transfer in a file, use this option to call the list.
--symbolic-links=METHOD	Specify rule to handle symbolic links. This option takes following values: (Default: follow) <ul style="list-style-type: none"> • follow Follow symbolic links and transfer the linked files.

Option	Description
	<ul style="list-style-type: none"> • copy Copy only the alias file. If a file with the same name exists on the destination, the symbolic link will not be copied. • copy+force Copy only the alias file. If a file with the same name exists on the destination, the symbolic link will replace the file. If the file of the same name on the destination is a symbolic link to a directory, it will not be replaced. • skip Skip the symbolic links.
--remove-after-transfer	Add this option to remove source file except folder when finish.
--remove-empty-directories	Add this option to remove empty folder on the source.
--skip-special-files	Add this option to skip special files such as devices and pipes.
--file-manifest=OUTPUT	Generate a list of all transferred files information. Replace <i>OUTPUT</i> with none or text (Default: none)
--file-manifest-path=DIRECTORY	Specify the path to store the manifested file.
--file-manifest-inprogress-suffix=SUFFIX	Specify the file manifest's temporary file's suffix.
--precalculate-job-size	Add this option to calculate total size before transfer. Please note that the server side conf file setting overrides the ascp command line option.
--overwrite=METHOD	<p>Overwrite files with the same name. This option takes following values (Default: diff):</p> <ul style="list-style-type: none"> • always - Always overwrite the file. • never - Never overwrite the file. • diff - Overwrite if file is different from the source (i.e., if a complete file exists at the destination (no .aspx file) and is the same as the source file, then leave it unmodified (no change on timestamp/attributes either); otherwise re-transfer the whole source file). Note this policy interacts with the <i>resume</i> policy. • older - Overwrite if file is older than the source.
--file-crypt=CRYPT	Encrypt or decrypt files. Replace <i>CRYPT</i> with encrypt or decrypt . Passphrase is required.
--retry-timeout=SECS	Specify the timeout duration in seconds, for a retry attempt.
--keepalive	This options enables a persistent session that doesn't require a predefined source file set and a destination at execution. Instead of reading source/destination paths from command-line, a persistent session reads source and destination paths through mgmt commands. In addition, persistent session supports canceling of individual files and directories.

Option	Description
	In a persistent session, you can also specify the transfer mode with the <code>--mode=MODE</code> option.
<code>--partial-file-suffix=SUFFIX</code>	<p>Filename extension on the destination computer while the file is being transferred. Once the file has been completely transferred, this filename extension will be removed. (Default: blank)</p> <p>NOTE: This option only takes effect when it is set on the receiver side.</p>
<code>--src-base=NAME</code>	<p>If this option is utilized, ascp will strip the srcbase path, while preserving the rest of the directory structure.</p> <p>NOTE: If the target directory does not exist, the "-d" option is required when specifying the "--src-base" option.</p> <p>For example, the "clips" directory on the remote computer contains the following folders and files:</p> <pre>/clips/outgoing/file1 /clips/outgoing/folderA/file2 /clips/outgoing/folderB/file3</pre> <p>In this case, we want to transfer all folders and files within the "outgoing" folder (but not the "outgoing" folder, itself). Upon executing the following command (where -d creates the target directory if it doesn't already exist):</p> <pre>\$ ascp -d --src-base=/clips/outgoing/ root@10.0.0.1:/clips/ outgoing/ /incoming</pre> <p>The following folders and files will appear in the "incoming" directory on the destination computer:</p> <pre>(docroot)/incoming/file1 (docroot)/incoming/folderA/file2 (docroot)/incoming/folderB/file3</pre> <p>Note that files outside of the source base (e.g. /temp/file4 and /temp/file5) are skipped from transmission and warnings will be generated.</p>

Option	Description
	<p>Alternatively, if the --src-base option is not specified (as shown in the following command):</p> <pre>\$ ascp -d root@10.0.0.1:/clips/outgoing/ /incoming</pre> <p>Then the contents of the "outgoing" folder will be transferred, along with the "outgoing" folder itself:</p> <pre>(docroot)/incoming/outgoing/file1 (docroot)/incoming/outgoing/folderA/file2 (docroot)/incoming/outgoing/folderB/file3</pre>
--preserve-file-owner-uid	<p>Preserve transferred files' owner information (uid).</p> <p>NOTE: This option requires that the transfer user be authenticated as a superuser.</p>
--preserve-file-owner-gid	<p>Preserve transferred files' group information (gid).</p> <p>NOTE: This option requires that the transfer user be authenticated as a superuser.</p>
--ignore-host-key	<p>With this option specified, when connecting to a remote host and you are prompted to accept a host key, ascp ignores the request.</p>

ascp HTTP Fallback Options

Option	Description
-y {0 1}	Enable HTTP Fallback transfer server when UDP connection fails. Set 1 to enable.
-j {0 1}	Encode all HTTP transfers as JPEG files. Set 1 to enable. 0 / 1. (Default: 0)
-Y <i>key-file</i>	The HTTPS transfer's key file name.
-I <i>certif-file</i>	The HTTPS certificate's file name.
-t <i>port</i>	Specify the port for HTTP Fallback Server.
-x <i>proxy-server</i>	Specify the proxy server address used by HTTP Fallback.

ascp General Examples

Examples of initiating *fasp* file transfers using the ascp command.

This topic demonstrates the ascp command with the following examples:

1. Fair-policy transfer, without encryption

Transfer with fair rate policy, with maximum rate 100 Mbps and minimum at 1 Mbps:

```
$ ascp -TQ -l 100m -m 1m /local-dir/files root@10.0.0.2:/remote-dir
```

2. Fixed-policy transfer, without encryption

Transfer all files in \local-dir\files to 10.0.0.2 with target rate 100 Mbps and encryption OFF:

```
$ ascp -T -l 100m /local-dir/files root@10.0.0.2:/remote-dir
```

3. Specify an UDP port

To perform a transfer with UDP port 42000:

```
$ ascp -l 100m -O 42000 /local-dir/files user@10.0.0.2:/remote-dir
```

4. Authenticate with public key

To perform a transfer with public key authentication with key file *<home dir>/.ssh/asp1-key* local-dir/files:

```
$ ascp -T -l 10m -i ~/.ssh/asp1-key local-dir/files root@10.0.0.2:/remote-dir
```

5. Authenticate with a login that contains space

Enclose the target in double-quotes when spaces are present in the username and remote path:

```
$ ascp -l 100m local-dir/files "User Name@10.0.0.2:/remote directory"
```

6. Transfer with a network shared location

Send files to a network shares location \\1.2.3.4\\nw-share-dir, through the computer 10.0.0.2:

```
$ ascp local-dir/files root@10.0.0.2:"//1.2.3.4/nw-share-dir/"
```

7. Parallel transfer on a multi-core system

Use parallel transfer on a dual-core system, together transferring at the rate 200Mbps, using UDP ports 33001 and 33002. Two commands are executed in different Terminal windows:

```
$ ascp -C 1:2 -O 33001 -l 100m /file root@10.0.0.2:/remote-dir &
$ ascp -C 2:2 -O 33002 -l 100m /file root@10.0.0.2:/remote-dir
```

8. Use content protection

Upload the file *spacefile* to the server *10.0.0.2* with password protection (password: *secRet*):

```
$ ASPERA_SCP_FILEPASS=secRet ascp -l 10m --file-crypt=encrypt local-dir/file
root@10.0.0.2:/remote-dir/
```

Download from the server *10.0.0.2* and decrypt while transferring:

```
$ ASPERA_SCP_FILEPASS=secRet ascp -l 10m --file-crypt=decrypt root@10.0.0.2:/remote-
dir /local-dir
```

If the password-protected file is downloaded without decrypting (*file1.aspera-env*, with *aspera-env* appended), on the local computer, decrypt the file as *file1*:

```
$ ASPERA_SCP_FILEPASS=secRet asunprotect -o file1 file1.aspera-env
```

ascp File Manipulation Examples

Examples of manipulating files using the *ascp* command.

This topic demonstrates file manipulation using the *ascp* command with the following examples:

1. Upload directory contents to remote computer

Upload the *"/content/"* directory to the remote server.

```
$ ascp /data/content/ root@10.0.0.1:/storage/
```

Result => */storage/content/**

Upload the *"/content/"* directory to the remote server, but strip the *srcbase* path and preserve the rest of the file structure.

```
$ ascp --src-base=/data/content /data/content/ root@10.0.0.1:/storage
```

Result => */storage/**

2. Upload directory contents to remote computer and create the destination folder if it does not already exist

Upload the *"/content/"* directory to the remote server and create the *"/storage2"* folder since it does not exist.

```
$ ascp -d /data/content/ root@10.0.0.1:/storage2/
```

Result => */storage2/content/**

3. Download directory contents from remote computer

Download the "/content/" directory to the remote server, but strip the srcbase path and preserve the rest of the file structure.

```
$ ascp --src-base=/storage/content root@10.0.0.1:/storage/content/ /data
```

Result => /data/*

4. Upload selected files and directories to a remote computer and preserve directory structure

Upload the selected file and directory to the remote server, but strip the srcbase path and preserve the rest of the file structure.

```
$ ascp --src-base=/data/content /data/content/monday/file1 /data/content/tuesday/
root@10.0.0.1:/storage
```

Results => /storage/monday/file1 **AND** /storage/tuesday/*

5. Download selected files and directories from a remote computer and preserve directory structure

Download the selected file and directory from the remote server, but strip the srcbase path and preserve the rest of the file structure.

```
$ ascp --src-base=/storage/content root@10.0.0.1:/storage/content/monday/file1
root@10.0.0.1:/storage/content/tuesday/ /data
```

Results => /data/monday/file1 **AND** /data/tuesday/*

6. Remove source files from the local computer after transferring them to the remote computer

Remove the "/content/" directory of the local computer after the contents (excluding partial files) have been transferred to the remote computer.

```
$ ascp -k2 -E "*.partial" --remove-after-transfer --remove-empty-directories /data/
content root@10.0.0.1:/storage
```

Result => /storage/content/*

Remove the "/content/" directory of the local computer after the contents (excluding partial files) have been transferred to the remote computer. Strip the srcbase path and preserve the rest of the file structure

```
$ ascp -k2 -E "*.partial" --src-base=/data/content --remove-after-transfer --remove-
empty-directories /data/content root@10.0.0.1:/storage
```

Result => /storage/*

IMPORTANT NOTE: For version 2.7.1, the "-d" option is required when specifying the "--src-base" option if the target directory does not exist. As of version 2.7.3+, this constraint has been removed.

Creating Command Files

Create and use ascp command files that stores ascp command options.

The command file feature is useful for specifying the entire command-line parameters inside a single file. To execute ascp command with command file, use the following syntax:

```
ascp --args-list=cmdfile
```

Note that when `--args-list` is present, it shall be the only option.

To make a command file, create a text file with an editor. You may save the file as unicode (UTF-8 and UTF-16, BE and LE). The format must be explicitly specified file extensions: ".utf8" for UTF-8 files and ".unicode" for UTF-16 files.

Separate command flag and value in different lines. For example, to specify target rate of 3000, and set local log directory as /tmp, use the following format:

```
-l
3000
-L
/tmp
```

To support source list file, the ascp long option `--file-list` is introduced . In addition, a second long option `--src-base` is introduced for the purpose of preserving source directory structure. The following shows an example.

When using long options with value, for example, `--symbolic-links=follow`, enter the flag and value in two separate lines, without the equal symbol:

```
--symbolic-links
follow
```

For ascp command options, refer to [ascp Usage](#) on page 45.

When the command file is created, you may execute ascp command with this file through the **--args-list** option. For example, to execute options stored in a command file named `ascp_command_file`:

```
$ ascp --args-list=ascp_command_file
```

Frequently-Asked Questions

This topic lists frequently-asked questions regarding ascp command:

1. How do I control the transfer speed?

You can specify a transfer policy that determines how *fasp* transfer utilize the network resource, as well as maximum and minimum transfer rates where applicable. In *ascp* command, use the following flags to specify fixed, fair and trickle transfer policies:

Policy	Command template
Fixed	<code>-l <u>target_rate</u></code>
Fair	<code>-Q -l <u>target_rate</u> -m <u>min_rate</u></code>
Trickle	<code>-QQ -l <u>target_rate</u> -m <u>min_rate</u></code>

2. What should I expect in terms of transfer speed? How do I know if something is "wrong" with the speed?

Aspera's *fasp* transport has no theoretical throughput limit. Other than the network capacity, the transfer speed may be limited by rate settings and resources of the computers. To verify that your system's *fasp* transfer can fulfill the maximum bandwidth capacity, prepare a client machine to connect to this computer, and test the maximum bandwidth.

NOTE: This test will typically occupy the majority of a network's bandwidth. It is recommended that this test be performed on a dedicated file transfer line or during a time of very low network activity.

On the client machine, start a transfer with fixed policy. Start with a lower transfer rate and increase gradually toward the network bandwidth (e.g. 1m, 5m, 10m...). Monitor the transfer rate and make sure that it fulfills your bandwidth:

```
$ ascp -l 1m source-file destination
```

To improve the transfer speed, you may also upgrade the following hardware components:

Component	Description
Hard disk	The I/O throughput, the disk bus architecture (e.g. RAID, IDE, SCSI, ATA, and Fiber Channel).
Network I/O	The interface card, the internal bus of the computer.
CPU	Overall CPU performance affects the transfer, especially when encryption is enabled.

3. How do I ensure that if the transfer is interrupted / fails to finish, it will resume the transfer without re-transferring the files?

Use the **-k** flag to enable resume, and specify a resume rule:

- **-k 0** Always retransfer the entire file.
- **-k 1** Check file attributes and resume if they match.
- **-k 2** Check file attributes and do a sparse file checksum; resume if they match.
- **-k 3** Check file attributes and do a full file checksum; resume if they match.

4. How does Aspera handle symbolic links?

`ascp` command follows symbolic links by default. There is a **-o SymbolicLink** flag that offers handling options:

- **--symbolic-links=follow**: Follow symbolic links and transfer the linked files.
- **--symbolic-links=copy**: Copy only the alias file.
- **--symbolic-links=skip**: Skip the symbolic links.

5. What are my choices regarding file overwrites on the destination computer?

In `ascp`, you can specify the overwriting rule with the following flags:

- **--overwrite=always**: Always overwrite the file.
- **--overwrite=never**: Never overwrite the file.
- **--overwrite=diff**: Overwrite if file is different from the source.
- **--overwrite=older**: Overwrite if file is older than the source.

NOTE: For **--overwrite=diff**, if a complete file exists on the destination computer (i.e., no `.aspx` file) and is the same as the source file, then the destination file will remain unmodified (no change on timestamp/attributes either). Otherwise the entire source file will be retransferred. Note this policy interacts with the *resume* policy.

Creating SSH Keys (Terminal)

Create a key pair for your computer.

To log in into other Aspera servers with public key authentication, you can also create key-pairs in command line. Follow these instructions:

1. Create `.ssh` folder in home directory

Create a `".ssh"` folder in your user account's home directory if it doesn't exist:

```
$ mkdir /home/<user name>/.ssh
```


Navigate into the .ssh folder and continue:

```
$ cd <path-to-user-home-dir>/ .ssh
```

2. Use ssh-keygen to generate SSH key

Execute the following command in the ".ssh" folder. The program will prompt you the key-pair's file name, hit enter to use the default name **id_rsa**. For a passphrase, you can either enter a password, or press return twice to leave it blank:

```
$ ssh-keygen -t rsa
```

3. Retrieve the public key file

When created, the key-pair can be found in your home directory's ".ssh" folder (Assuming you generated the key with default name **id_rsa**):

```
(user's home directory)/id_rsa.pub
```

Provide the public key file (e.g. id_rsa.pub) to your server administrator, so that it can be set up for your server connection. The instructions for installing the public key on the server can be found in the [Setting Up a User's Public Key](#); however, the server may be installed on an Operating System that is different from the one that your client has been installed on.

4. Start a transfer using public key authentication with ascp command

To transfer files using public key authentication in command line, use the option *-i private-key-file*. For example:

```
$ ascp -T -l 10M -m 1M -i ~/.ssh/id_rsa my/files jane@10.0.0.2:space
```

In this example, you are connecting to the server (10.0.0.2, directory /space) with the user account *jane* and the private key *~/.ssh/id_rsa*.

Appendix

fasp Transfer Policies

The character of the *fasp* transfer policies.

The transfer policy and speed determine how you utilize the network resource for *fasp* file transfers. Here is the description of all transfer policies:

Policy	Description
Fixed	<i>fasp</i> attempts to transfer at the specified target rate, regardless of the actual network capacity. This policy transfers at a constant rate and finishes in a guaranteed time. This policy will typically occupy a majority of the network's bandwidth, and is not recommended in most file transfer scenarios. In this mode, a maximum (target) rate value is required.
High	<i>fasp</i> monitors the network and adjusts the transfer rate to fully utilize the available bandwidth up to the maximum rate. When congestion occurs, a <i>fasp</i> session with high policy transfers at a rate twice of a session with fair policy. In this mode, both the maximum (target) and the minimum transfer rates are required. <div>Note: This policy is not available in the Connect browser plug-in.</div>
Fair	<i>fasp</i> monitors the network and adjusts the transfer rate to fully utilize the available bandwidth up to the maximum rate. When other types of traffic builds up and congestion occurs, <i>fasp</i> shares bandwidth with other traffic fairly by transferring at an even rate. In this mode, both the maximum (target) and the minimum transfer rates are required.
Low (or Trickle)	Similar to Fair mode, the Low (or Trickle) policy uses the available bandwidth up to the maximum rate, but much less aggressive 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.

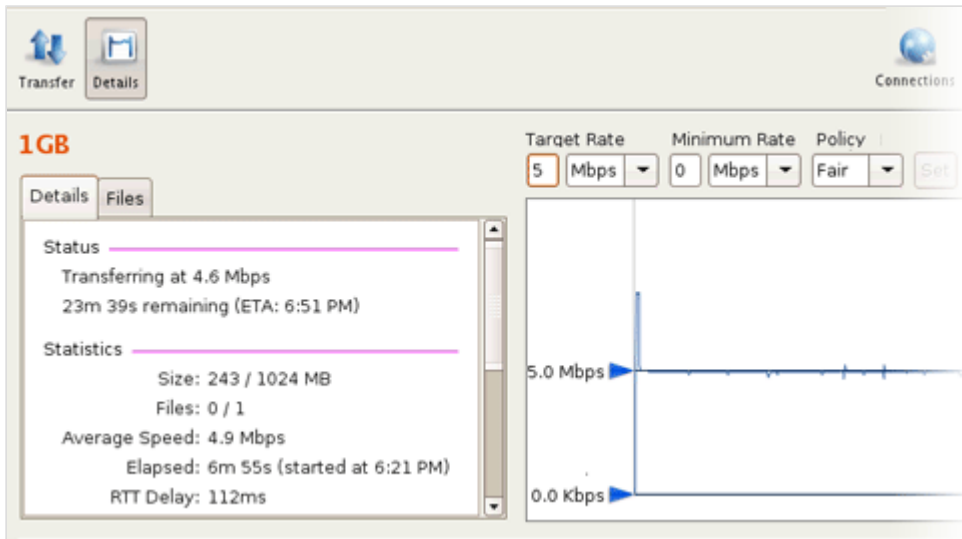
Optimizing Transfer Performance

Tips about testing and improving your computer's transfer performance.

To verify that your system's *fasp* transfer can fulfill the maximum bandwidth capacity, prepare a client machine to connect to this computer, and do the following tests:

1. Start a transfer with Fair transfer policy

On the client machine, open the user interface and start a transfer. Go to the **Details** to open the Transfer Monitor.



To leave more network resource for other high-priority traffics, use **Fair** policy and adjust the Target Rate and Minimum Rate rate by sliding the arrows or enter the values.

2. Test the maximum bandwidth

This test will typically occupy a majority of the network's bandwidth. It is recommended that this test be performed on a dedicated file transfer line or during a time of very low network activity.

Use **Fixed** policy for the maximum transfer speed. Start with a lower transfer rate and increase gradually toward the network bandwidth.



To improve the transfer speed, you may also upgrade the related hardware components:

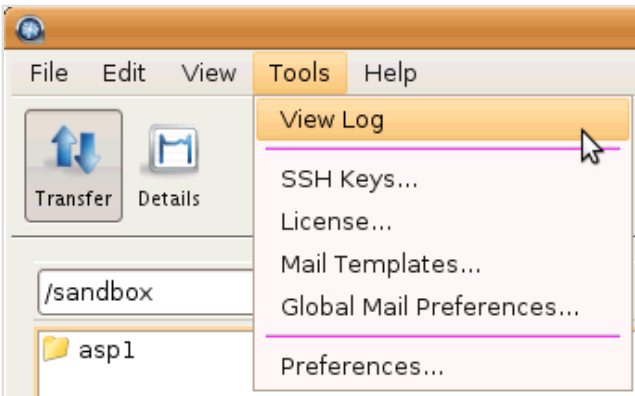
Component	Description
Hard disk	The I/O throughput, the disk bus architecture (e.g. RAID, IDE, SCSI, ATA, and Fiber Channel).
Network I/O	The interface card, the internal bus of the computer.
CPU	Overall CPU performance affects the transfer, especially when encryption is enabled.

Log Files

Locate the log files related to the Aspera product.

The log file includes detailed transfer information and can be useful for review and support request.

To view the application log, go to **Tools > View Log**.



The transfer logs are recorded into the system log file:

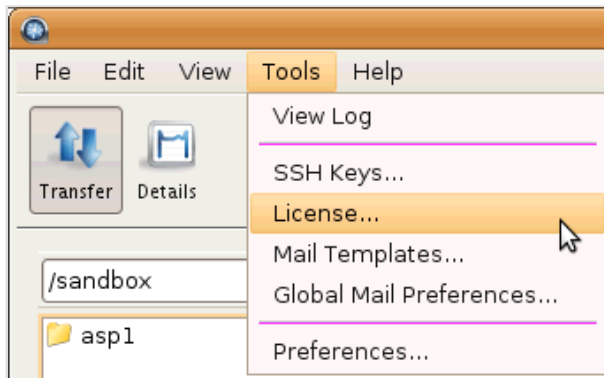
Platform	Path
RedHat	/var/log/messages
Debian	/var/log/syslog

Updating Product License

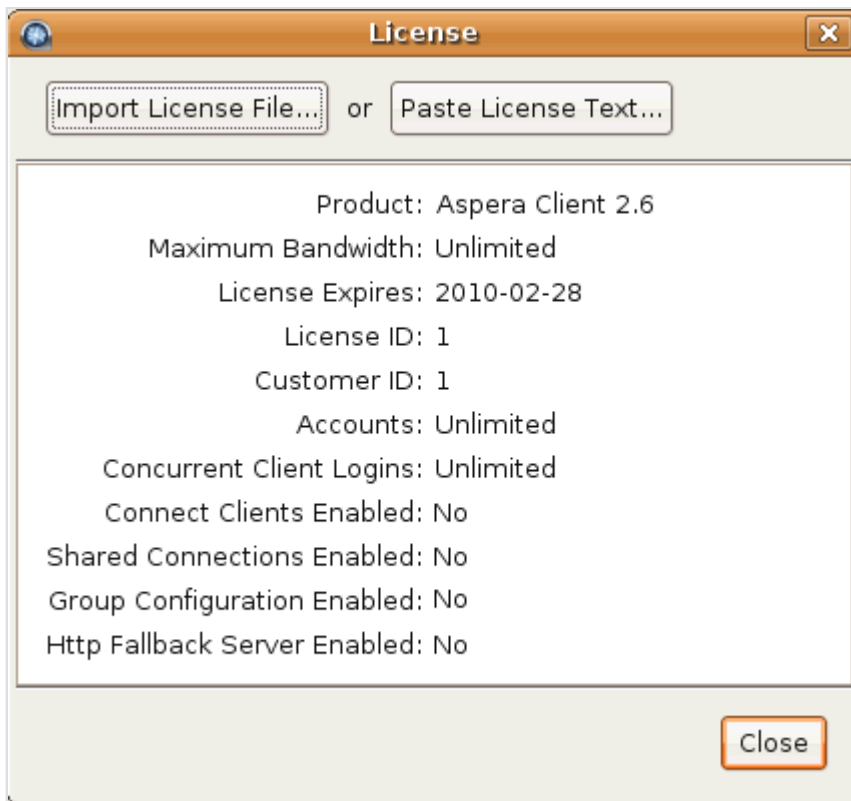
Update your product license.

There are two ways to update the license: Through the GUI, or through the command line.

To update the license in the GUI mode, execute **asperascp** (as a root user) in a Terminal and go to **Menu bar > Tools > License** to bring up the *License* window.



You may click the **Import License File...** and select the license file, or **Paste License Text...** to copy-and-paste the license file's content. When finished, the license information will appear in the window. Verify that it is correct and click **Close**.



To update the license through the command line, open the following file with write permission, replace the existing license key string with the new one:

```
/opt/aspera/etc/aspera-license
```

When finished, save and close the file. Use this command to verify the new license info:

```
$ ascp -A
```

Uninstall

How to uninstall the Aspera product from your computer.

To uninstall the product, use the following commands. For RedHat and Debian, replace the Package-name with the printed name from the first command:

Platform	Command
RedHat	<pre>\$ rpm -qa grep aspera \$ rpm -e Package-name</pre>
Debian	<pre>\$ dpkg -l "aspera*" \$ dpkg -r Package-name</pre>

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

© 2011 Aspera Inc. All rights reserved.

Aspera, the Aspera logo, and *fast* transfer technology, are trademarks of Aspera Inc., registered in the United States. Aspera Connect Server, Aspera Enterprise Server, Aspera Point-to-Point, Aspera Client, Aspera Connect, Aspera Cargo, Aspera Console, Aspera Orchestrator, Aspera Crypt and Aspera *fastpex* are trademarks of Aspera, Inc. All other trademarks mentioned in this document are the property of their respective owners. Mention of third-party products in this document is for informational purposes only. All understandings, agreements or warranties, if any, take place directly between the vendors and the prospective users.