Aspera Client User Guide

Windows XP/2003/Vista/2008

Version 2.2.1

1. Introduction

Aspera Client is a file transfer client application supercharged with Aspera's *fasp™* file transport technology. It includes the following features:

Features

***fasp™* transport server**	A transport server that accepts incoming connections.

Aspera Scp	A desktop application for initiating *fasp™* file transfers.
ascp Command	A command-line transfer program
Aspera Sync	A hot-folder synchronization feature in Aspera Scp.

The most up-to-date document can be found at http://asperasoft.com/support/documentation/scp-client. For further assistance, please contact us at http://asperasoft.com/support.

2. Setting Up

2.0 Upgrade from a Previous Version

If the system has a previous Aspera transfer product installed, follow these steps to backup and prepare the system for upgrade:

Step 1 **Backup the configuration files**

Backup the following folders:

32bit

- \Program Files\Aspera\FASP\etc\ *User settings, license info*
- \Program Files\Aspera\Aspera Scp\etc\ *Remote Hosts info, Hot Folders info*

64bit

- \Program Files (x86)\Aspera\FASP\etc\ *Server config, web config, user settings, license info*
- \Program Files (x86)\Aspera\Aspera Scp\etc\ *Remote Hosts info, Hot Folders info*

Step 2 **Remove old Point-to-Point**

XP/2003	Go to `Control Panel` > `Add or Remove Programs`. Select the `Aspera Scp Client` and click `Remove`.
Vista/2008	Go to `Control Panel` > `Programs and Features`. Select `Aspera Scp Client` and click `Uninstall`.

2.1 Installation

Follow these steps to set up the application:

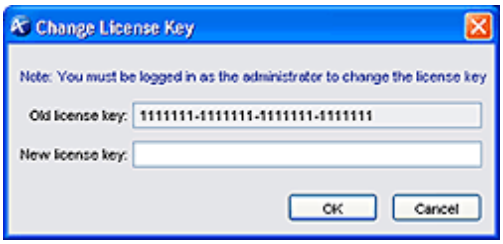
Step 1 **Download the installer**

Download the installer from the link below. Use the credentials provided to your organization by Aspera to access. If needed, contact Aspera Technical Support in determining your firm's access credentials.
http://www.asperasoft.com/downloads/scp-client

Step 2 **Execute the installer**

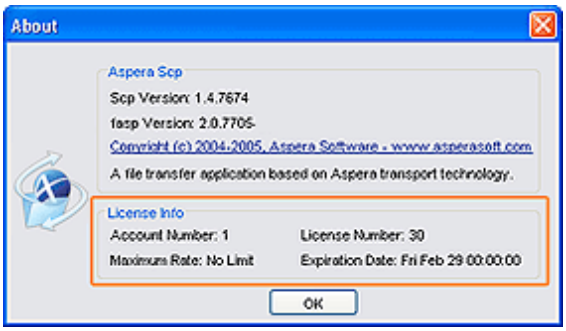
When downloaded, double-click the installer package and start the installation. Click Next to proceed.

2.2 Enter the License Key



To enter your product license key, go to Start Menu > All Programs > Aspera > Aspera Scp Client and click Aspera Scp. It will prompt for a license key upon the first launch. When the license is entered and verified, a *Set Connection Speed* window appear. Enter a default connection speed and proceed to the application.

To change the license key afterwards, in the *Aspera Scp*, go to Menu bar > Tools > Change License Key.



To view the license info, in the *Aspera Scp*, go to Menu bar > Help > About. You can see it under the *License Info* section.

2.3 Configure the Firewall

The following table is a basic guideline and simple instructions to configure your firewall. Please refer to your operating system documentation for specific instructions on configuring your firewall:

Firewall Configuration Instructions

- Allow outbound connection for the SSH. (**TCP/22**)

- Allow outbound connection for the *fasp* transfers. (**UDP/33001**)

2.4 Test Transfer with the Aspera Demo Server

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

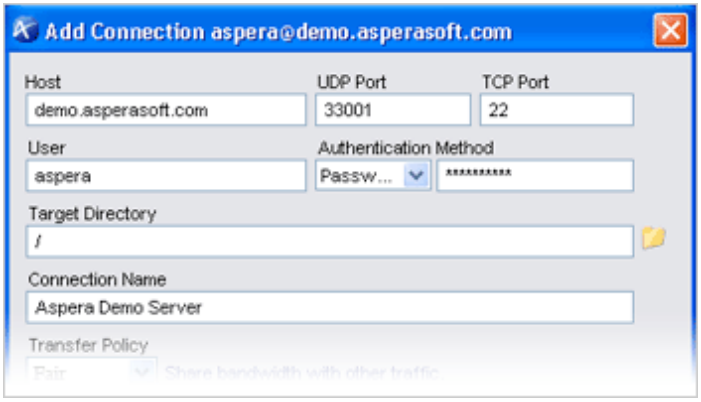
Step 1 **Launch Aspera Scp Client**

Go to Start menu > All Programs > Aspera > Aspera Scp Client and launch Aspera Scp.

Step 2 **Add the Aspera Demo Server as a remote endpoint**

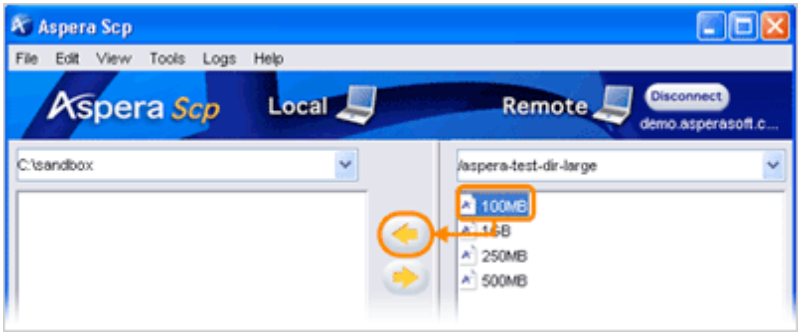
Under Saved Remote panel, click New and enter the following information. Click OK when finished:

- Host: `demo.asperasoft.com`
- User: `aspera`
- Authentication Method: Choose Password and enter `demoaspera`
- For the rest options, keep the default values.



Step 3 **Download from the Aspera Demo Server**

In the main window, select Aspera Demo Server and click Connect. On the "Remote" side, browse to the folder */aspera-test-dir-large*, select the file *100MB* and click "left arrow" (see picture) to download it to your local machine.



Step 4 Upload to the Aspera Demo Server

When the file is downloaded, try uploading the same file back to the Aspera Demo Server. First, on the "Local" side, select the same file (*100MB*). Second, on the "Remote" side, navigate to the folder */Upload*. Click the "right arrow" to upload it to the Aspera Demo Server.

Troubleshooting

Invalid license key	See 2.2 Enter the License Key and verify the key.
Can't browse the Demo Server	See 2.3 Configure the Firewall and review the SSH firewall settings.
Can't transfer files	See 2.3 Configure the Firewall and review the *fasp* firewall settings.

2.5 Optimize Performance

Aspera's *fasp™* transport has no theoretical throughput limit. Other than the network capacity, the transfer speed may be limited by the resources of the computers. To improve the transfer speed, upgrade the related hardware components:

Hardware Upgrade Guide

Hard disk	The I/O throughput, the disk bus architecture (e.g. 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 the encryption is enabled.

To verify that your system's *fasp* transfer can fulfill the maximum bandwidth capacity, follow these steps:

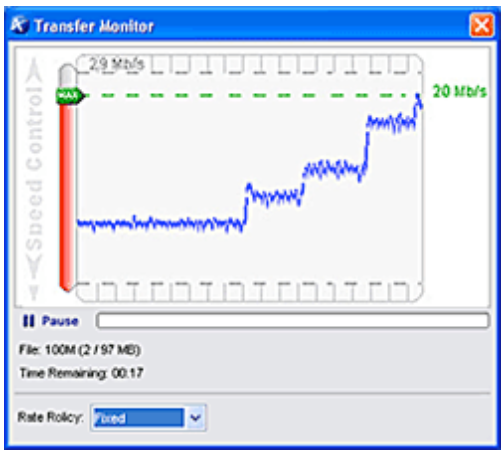
Step 1 Start and monitor the transfer

On this machine, open Aspera Scp and start a transfer. Click  to open the Transfer Monitor.

Step 2 Test the Fair transfer policies

To leave more network resource for other high-priority traffics, use `Fair` policy and adjust the `MAX` and `MIN` rate.

Step 3 Test the maximum bandwidth



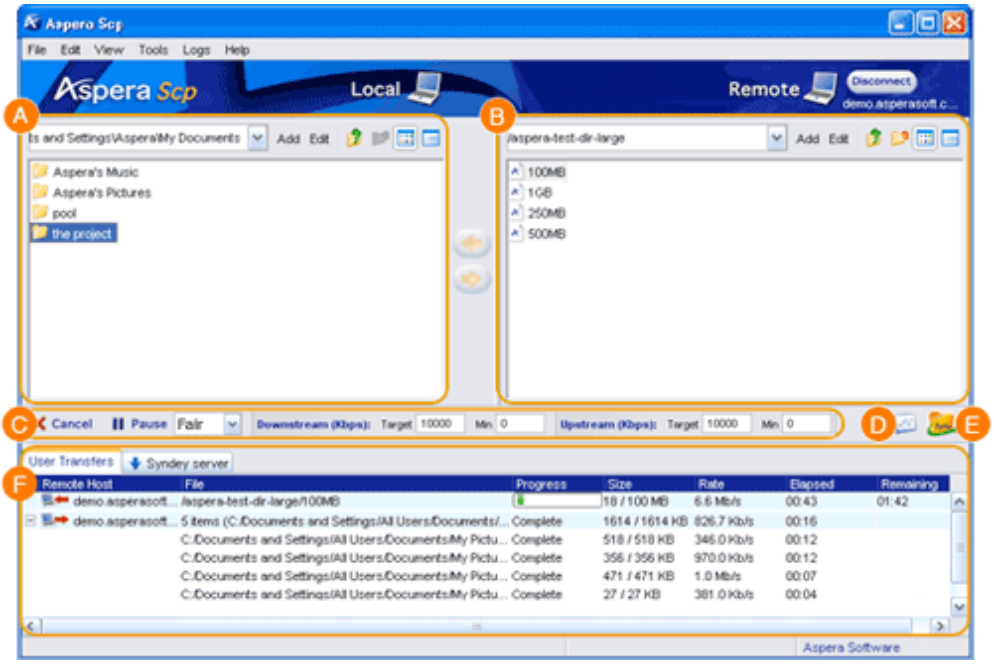
Use "Fixed" rate transfers for the maximum transfer speed. Start with a lower transfer rate and increase gradually toward the network bandwidth.

> **Note:** 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.

3. Using Aspera Scp

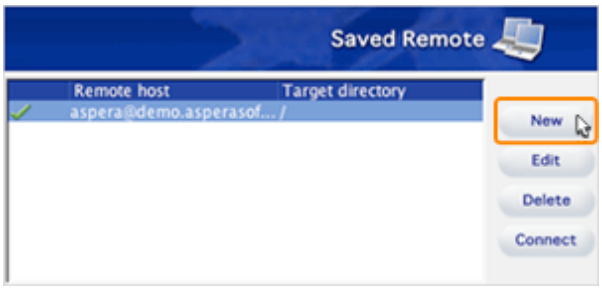
Aspera Scp is a desktop application for initiating *fasp™* file transfers. This chapter covers all features of this application.

3.1 Application Overview



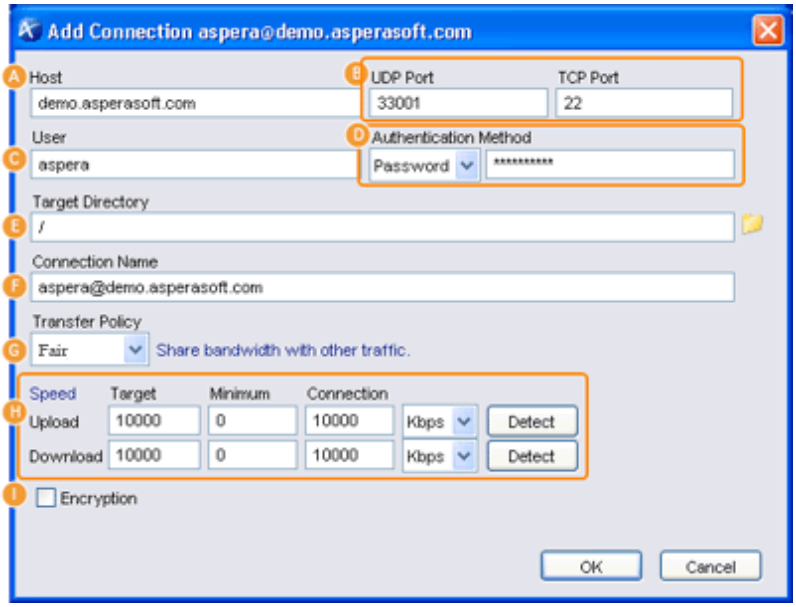
A	Local File Browser	Browse the local file system to find files to transfer.
B	Remote	When not connected, this area lists saved remote hosts and the "Active list" for one-to-many transfers. When connected, it shows the remote file system.
C	Transfer Controls	Set transfer options and control the ongoing transfer.
D	Transfer Monitor	Monitor and control the transfer.
E	Hot Folder Manager	Open the Hot Folder Manager window.
F	Transfer List	Display all previous and ongoing transfers.

3.2 Set Up a Remote Endpoint

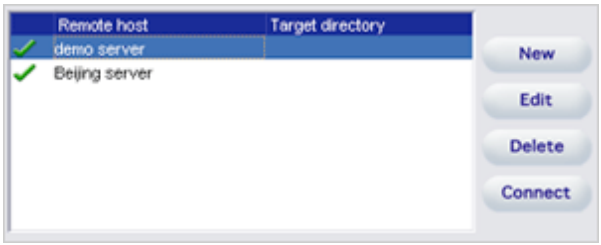


To add a remote enpoint, click `New` under "Saved Remote" panel to open the `Add Remote Endpoint`.

The Add Remote Endpoint window contains the following items:



A	Hosts:	Required The server's address, such as `192.168.1.10` or `companyname.com`.
B	Ports:	Required Network ports. Default: UDP/`33001`, TCP/`22`.
C	User:	The login user for the server.
D	Authentication Method:	Choose either password or public key for authentication. To use the key-based authentication, refer to 3.4 Public Key Authentication.
E	Target Directory:	The default directory.
F	Connection Name:	A name for this remote connection profile.
G	Transfer Policy:	The transfer policy to use. The default policy "Fair" is recommended. Refer to Appendix 1. Transfer Policies and Transfer Rate.
H	Speed:	The transfer rate and connection speed to the server. Click Detect to attempt the bandwidth measurement.
I	Encryption:	When checked, *fasp™* encrypts files while transferring. Encryption may decrease performance, especially at higher transfer speeds and with slower computers.



When finished, click OK to save this configuration, which will appear in the Saved Remote list. To connect, select the server and click Connect.

3.3 Transfer Files

3.3.1 Browse and Manage the Files

All options in the File Browser are listed below:

A		Change path. If a favorite directory is added, the list appears in the drop menu.
B	Add, Edit	Add to or edit the favorite directory list
C		Go to the parent directory.
D		Create a new folder.
E		Choose between the detail or list views.
F	New	Create a new folder.
G	Delete	Delete the selected file.
H	Rename	Change the selected file's name.
I	Refresh	Refresh the current directory.
J	Upload	Open the upload dialog window. The content protection can be enabled here.
K	Cut/Copy/Paste	Cut, copy and paste selected files.
L	Properties	Show selected item's properties, such as file count and size.

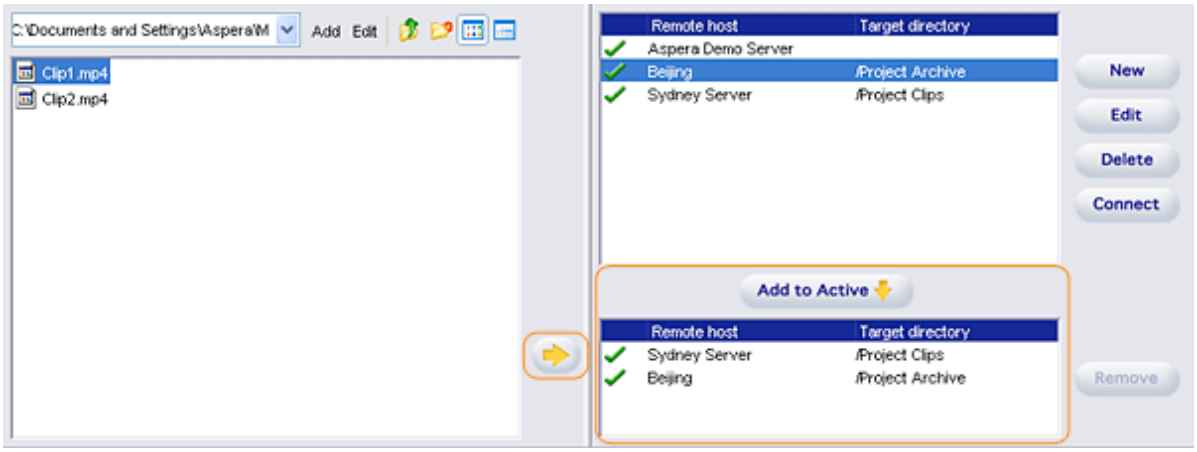
3.3.2 Transfer Controls

The Transfer Control toolbar includes options for you to set the transfer policy and transfer speed before starting a transfer, and the control buttons  to pause or cancel your transfer, respectively. For more information about transfer policies, refer to Appendix 1. Transfer Policies and Transfer Rate.

3.3.3 Initiate Basic Transfers

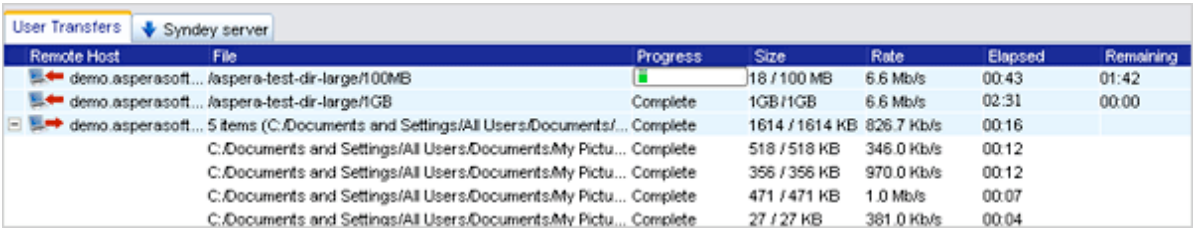
When connected to a server, you can start transfers by selecting the file and clicking  or  to download or upload. To transfer multiple files, hold the Ctrl key on the keyboard while clicking files, or hold the Shift key to select a range of files.

To transfer the same files to multiple endpoints, first select the designated servers from the Remote Endpoint list, click `Add to Active` to add it into the `Active` panel. When all endpoints have been added, select the files on the local file browser and click  to send the files to the active servers consecutively.



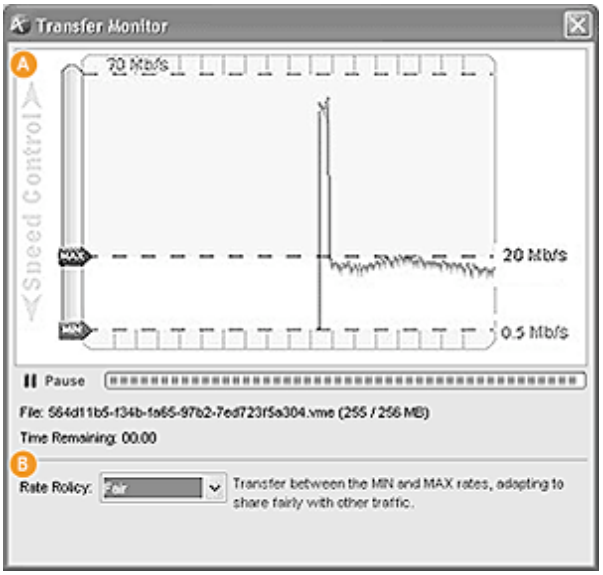
3.3.4 Transfer List

All previous and current transfers are listed in the Transfer List panel. If you have the Hot Folders configured, the `User Transfers` shows all the transfers initiated by you, whereas the other tabs contain activity for Hot Folders.



3.3.5 Transfer Monitor

The transfer monitor gives you additional visibility and control over your transfers. To open it, click  on the main window.



A **Speed Control:**

Set the maximum (target) and minimum transfer rates.

B **Policy:**

Set the transfer policy. For more information refer to Appendix 1. Transfer Policies and Transfer Rate.

3.3.6 Resume Transfers

If a transfer was interrupted, you can re-initiate the same transfer, and it will resume from where it left off.

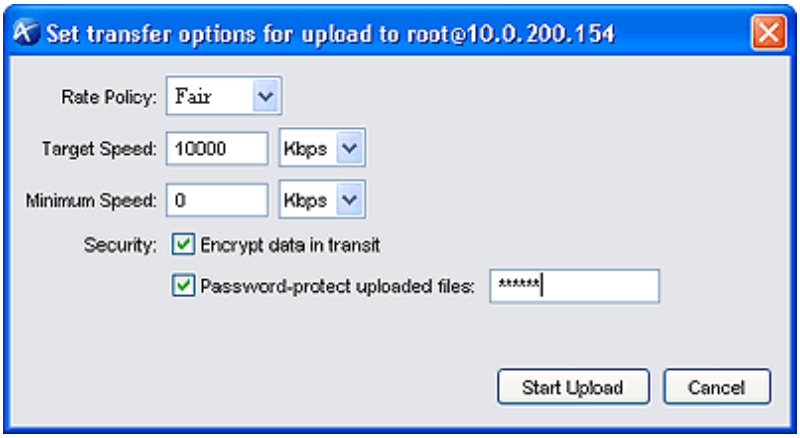
To configure the resume feature, go to `Menu bar` > `Tools` > `Preferences` and select `Transfers`. You can enable or disable the feature, and choose between the three resume options:

- File size check — *Only check if the existing file is the same size.*
- Fast integrity check — *Perform a sparse checksum on the existing file.*
- Full integrity check — *Perform a full checksum on the existing file.*

Note: When changing the resume option, unfinished transfers will be disregarded and cannot be resumed.

3.4 Content Protection

The content protection is a feature that allows the uploaded files be encrypted during a transfer, to protect them while stored on the remote server. The uploader sets a password while uploading the file, and the password is required to decrypt the protected file.

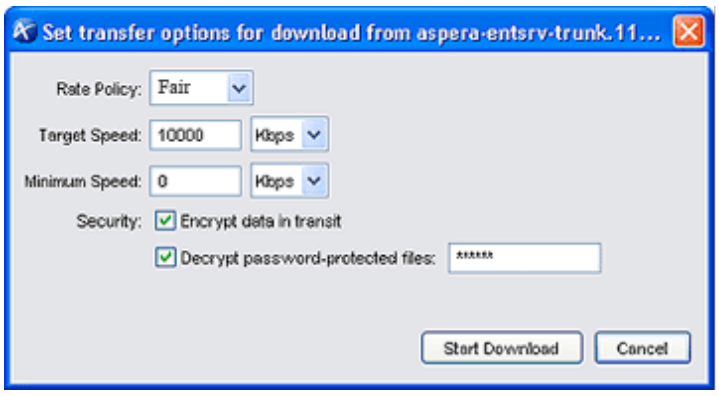


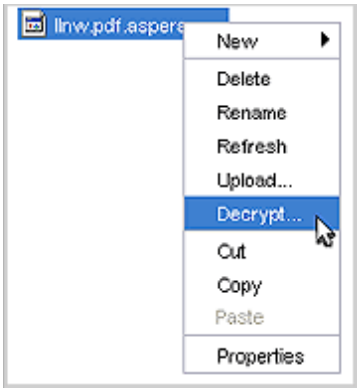
To use this feature, right-click a file and select Upload... from the menu to open the Transfer Options window.

Check the Password-Protect uploaded files and enter a password for the protected file. Click Start Upload to send the file to the server.

The protected file has the extension `.aspera-env` appended to the file name. To download it, right-click the file and select the Download... . Check the Decrypt password-protected files and enter the password.

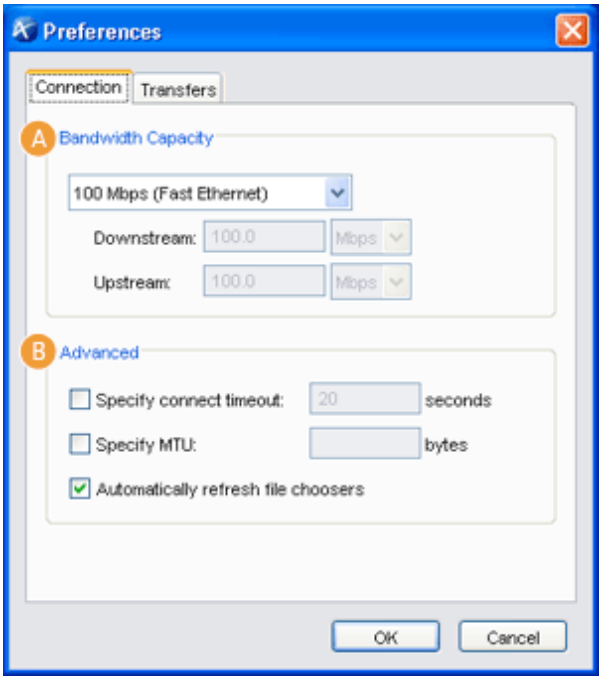
If you have already downloaded a protected file without decrypting it, right-click the file in the local file browser, select the Decrypt... , and enter the password.





3.5 Aspera Scp Preferences

To access the Preferences window, go to Menu bar > Tools > Preferences .



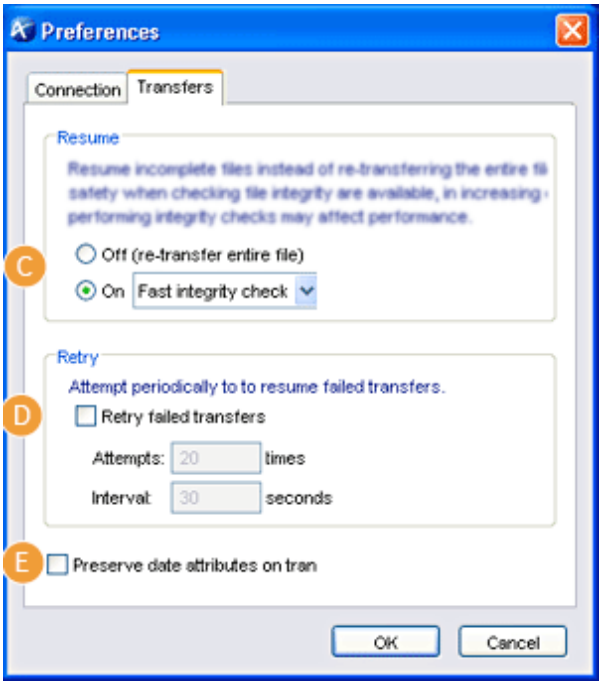
A **Bandwidth Capacity:**
The default connection bandwidth for your computer.

B **Advanced**

Specify the connect timeout How long to try to connect. (Default: 20s)

Specify MTU The datagram size for file transfers (Default: auto detect).

Automatically refresh file choosers Auto-refresh file browsers.



C **Resume:**
What to do when a file already exists. Refer to 3.3.6 Resume Transfer section for more info.

D **Retry:**
Enable or disable automatic retry of failed transfers.

E **Preserve date attributes on transferred files:**
Keep date attributes (i.e. creation time, last modification time, etc.) for transferred files.

3.6 Public Key Authentication

Public key authentication is an alternative to password authentication, allowing users to authenticate without entering or storing a password. Setting up public key authentication involves generating a public and private key-pair, and giving the public key to servers you want to transfer with.

To use the public key authentication to establish the connection, follow these steps:

Step 1 Create a SSH public key-pair

In Aspera Scp, go to Menu bar > Tools > Public Key Manager. Enter the following info. When finished, click Create to generate the key pair, which will appear in the Public Key Manager:

A Identity

Give a name to your key pair, such as your computer's name.

B Passphrase

(Optional) Set a passphrase on your SSH key, which will be prompted for whenever Aspera Scp needs to use the key. If you plan to use Hot Folders (Sync), do not set a passphrase.

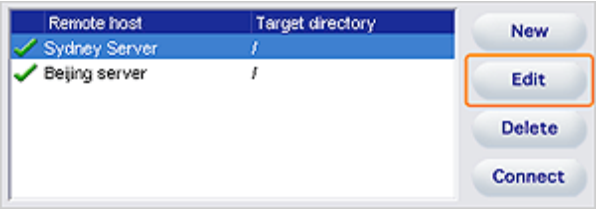
C Key Type

Choose between RSA (default) and DSA keys.

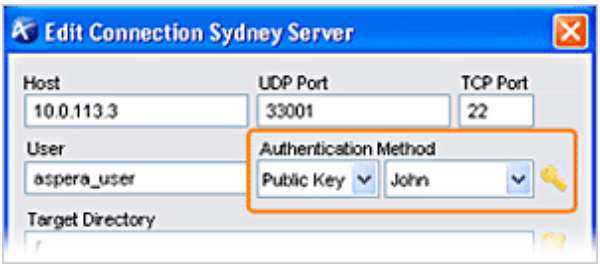
Step 2 Provide the public key

To acquire the key, select the item in the Public Key Manager window and click Copy Public Key to Clipboard. Paste the string into an e-mail and address it to the server administrator.

Step 3 Connect with public key authentication



After the server's administrator installed your public key authentication on the server, highlight the saved connection by clicking once, then choose Edit.



In the Edit Remote Endpoint window, select **Public Key** from the Authentication Method pull-down menu and select the key you want to use for this endpoint. Click **OK** when finish.

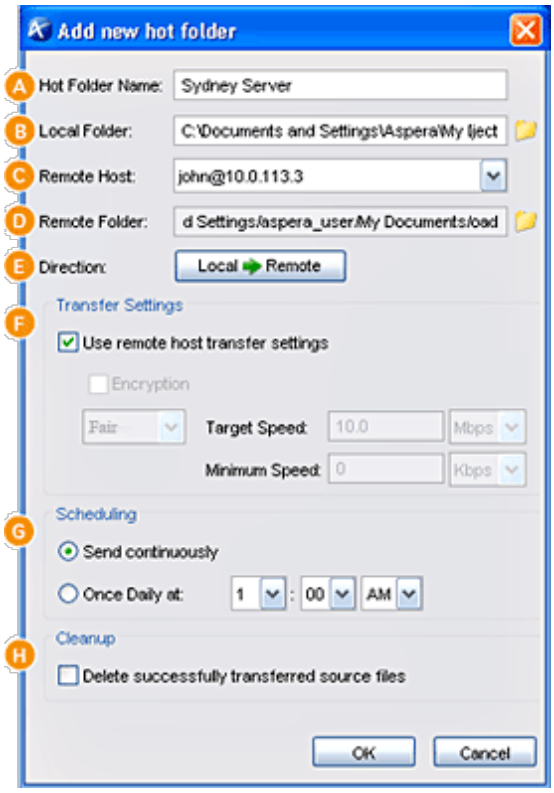
fasp™ uses putty private key for the public key authentication. The key will be generated when you are using Aspera Scp to connect to a host through public key authentication. If you are using the public key authentication in the command-line transfer, make sure the putty private key is available.

3.7 Synchronize Folders with Aspera Sync

Aspera Sync is a feature 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.

Step 1 Set up hot folders

In the Aspera Scp main window, click (Hot Folder Manager) to open the Hot Folder Manager. Click New (New) to create a new hot folder:



A **Hot Folder Name:**
The hot folder's name. Use the default name or enter your own.

B **Local Folder:**
The local folder to use. Click (Folder browser) to choose one.

C **Remote Host:**
The remote endpoint to use.

D **Remote Folder:**
The remote folder to use. Click (Folder browser) to choose one.

E **Direction:**
The direction of synchronization.
Set `Local > Remote` for push, or `Local <- Remote` for pull.

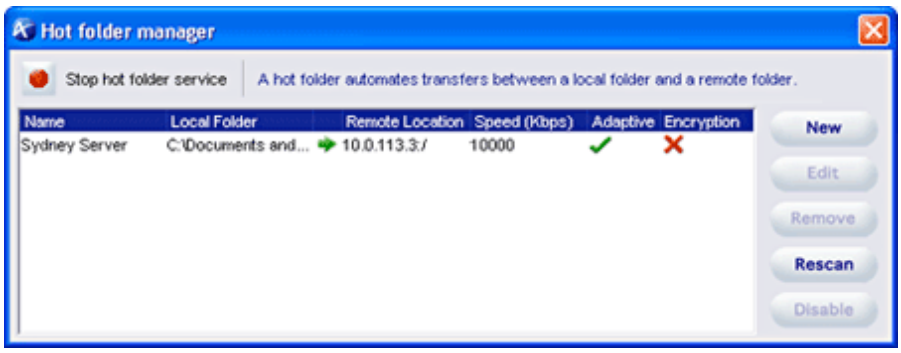
F **Transfer Settings:**
The transfer settings to use. Choose either to use the endpoint's transfer settings, or to override them.

G **Scheduling Policy:**
Select when to synchronize.

H **Cleanup using:**
Check to delete successfully transferred source files.

Step 2 Initiate Aspera Sync

The hot folder should appear in the Hot Folder Manager. Click  (Arrow) to activate Aspera Sync service. To stop, press  (Stop).
You can manage each hot folder individually. To disable a hot folder, select it and click `Disable`. To delete a hot folder, click `Remove`. To force Sync to check if the folder is synchronized, click `Rescan`.



Step 3 Monitor Aspera Sync

When a hot folder is set up, the folder's transfer status is shown in a separate tab at the bottom. To refresh the status, click on the list or the Refresh Stats button at the lower right.

4. ascp Command-line Reference

ascp is a core command-line program for *fasp™* transfers. This section covers the usage and examples.

4.1 ascp Usage

The basic *ascp* syntax guideline:

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

If needed, you can use the command to set the password, token, and cookie in the environment variables:

- Password: `set ASPERA_SCP_PASS=the-password`
- Token: `set ASPERA_SCP_TOKEN=the-token`
- Cookie: `set ASPERA_SCP_COOKIE=the-cookie`

ascp Synopsis

```
ascp   [-{ATdpqv}] [-{Q|QQ}] [-l max-rate] [-m min-rate] [-w{f|r} [-K probe-rate]]
       [-k {0|1|2|3}] [-i pubkey-file.ppk] [-Z dgram-size] [-M mgmt-port]
       [-u user-string] [-X rexmsg-size] [-g read-size] [-G write-size]
       [-S remote-ascp] [-L local-logdir] [-R remote-logdir][-e pre-post]
       [-f config-file] [-C n-id:n-count] [-E pattern1 -E pattern2...]
       [-O fasp-port] [-P ssh-port] [-o Option1=x[,Option2=y..]]
       [-U {1|2}] [-W token-string] [-y {0|1}] [-j {0|1}]
       [-Y key-file] [-I certif-file] [-t port] [-x proxy-server]
       [[user@]host1:]source-file [[user@]host2:]target-path
```

ascp General Options

`-A`	Display version and license information; then exit.

`-T`	Disable encryption for maximum throughput.
`-d`	Create target directory if it doesn't already exist.
`-p`	Preserve file timestamp.
`-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 max-rate`	Set the target transfer rate in kilobits per second. (Default: 10000)
`-m min-rate`	Set the minimum transfer rate in kilobits per second. (Default: 0)
`-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}`	Enable resuming partially transferred files. (Default: always retransfer) `0` Always retransfer the entire file. `1` Check file attributes and resume if they match. `2` Check file attributes and do a sparse file checksum; resume if they match. `3` Check file attributes and do a full file checksum; resume if they match.
`-i pubkey-file.ppk`	Use public key authentication and specify the putty private key file. If not specified, *fasp™* looks for the key file in $HOME/.ssh/id_[algorithm].ppk.
`-Z dgram-size`	Specify the datagram size (MTU) for *fasp™*. By default it uses the detected path MTU.
`-M port`	Set a management port for monitoring and controling the transfer.
`-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 (max 1440).
`-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 pre-post`	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.
`-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: ***** represents zero to many characters in a string, for example "*.tmp" matches ".tmp" and "abcde.tmp". **?** represents one character, for example "t?p" matches "tmp" but not "temp".
`-O fasp-port`	Set the UDP port used by *fasp™* for data transfer. (Default: 33001)
`-P ssh-port`	Set the TCP port used for *fasp™* session initiation. (Default: 22)
`-o`	Advanced ascp options as listed below. Use comma "," to separate: SkipSpecialFiles=yes Skip special files such as devices and pipes. (Default: no) RemoveAfterTransfer=yes Remove source file but folder when finish.(Default: no) RemoveEmptyDirectories=yes Remove empty folder on the source. (Default: no) PreCalculateJobSize={yes|no} Calculate total size before transfer. (Default: no) Overwrite={always | never | diff | older} Overwrite available files. (Default: diff) always Always overwrite the file with same name. never Never overwrite the file with the same name. diff Overwrite if the file with same name is different from the source. older Overwrite if file with same name is older than the source. FileManifest={none | text} Generate a list of all transferred files. FileManifestPath=filepath Specify the path to store the manifested file. FileCrypt={encrypt | decrypt} Encrypt or decrypt files. Passphrase is required. RetryTimeout=secs Specify the (timeout) duration, in seconds, for a retry attempt.
`-U {1|2}` (default:2)	Priority when sharing virtual bandwidth cap. 1 for higher priority, 2 for regular.
`-W token-string`	Specify the token string for the transfer.

ascp HTTP Fallback Options

`-y {0|1}` (default:0)	Enable HTTP Fallback transfer when UDP connection fails. Set **1** to enable.
`-j {0|1}`	Encode all HTTP transfers as JPEG files. Set **1** to enable. (default: 0)
`-Y key-file`	The HTTPS transfer's key file name.
`-I certif-file`	The HTTPS certificate's file name.
`-t port`	Specify the port for HTTP Fallback.
`-x proxy-server`	

Specify the proxy server address used by HTTP Fallback.

4.2 ascp Examples

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

```
> ascp -T -l 100000 /local-dir/files root@10.0.0.2:/remote-dir
```

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

```
> ascp -TQ -l 100000 -m 1000 /local-dir/files root@10.0.0.2:/remote-dir
```

3. To perform a transfer with UDP port *42000*:

```
> ascp -l 100000 -O 42000 /local-dir/files user@10.0.0.2:/remote-dir
```

4. To perform a transfer with the public key authentication, using the key file *(home directory)/.ssh/asp1.ppk*:

```
> ascp -T -l 10000 -i "/Documents and Settings/asp1/.ssh/asp1.ppk" \
  local-dir/files root@10.0.0.2:/remote-dir
```

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

```
> ascp -l 100000 local-dir/files "User Name@10.0.0.2:/remote directory"
```

6. 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. 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. Upload the file *space\files* to the server *10.0.0.2* with password protection (password: *secRet*):

```
> ASPERA_SCP_FILEPASS=secRet ascp -l 10m -o FileCrypt=encrypt local-dir/files \
  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 -o FileCrypt=decrypt \
  root@10.0.0.2:/remote-dir  /local-dir
```

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

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

Appendix 1. Transfer Policies and Transfer Rate

The transfer policy and speed determine how you utilize the network resource for *fasp™* file transfers. Four transfer policies described below:

fasp™ Transfer Policies

Fixed	*fasp™* 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. In this mode, a maximum rate value is required.
Fair / Adaptive	*fasp™* monitors the network and adjusts the transfer rate to fully utilize the available bandwidth up to the maximum rate. When other traffic builds up and congestion occurs, *fasp™* shares the bandwidth with other traffic and transfers at a fair rate. In this mode, both the maximum and the minimum transfer rates are required.
Trickle	Similar to Fair mode, the Trickle policy uses the available bandwidth up to the maximum rate, but much less aggressive than other network traffic. When congested, the transfer rate is reduced down to the minimum rate, until no competition with other flows.
Set Finish Time	This option is only available on Aspera Scp. This policy allows your to set the end time of file transmission by automatically adjusting the minimum transfer rate. This can be useful for file delivery deadlines.

Appendix 2. The Log File

The log file includes detailed transfer information and can be useful for review and support request. The file can be found in the location:

fasp Transfer Log File

32bit	\program files\aspera\fasp\var\log\aspera-scp-transfer.log
64bit	\program files (x86)\aspera\fasp\var\log\aspera-scp-transfer.log

Appendix 3. Uninstall Aspera Client

The un-install can be done in Control Panel, depending on the version of your Windows, choose `Add/Remove Programs` or `Uninstall a program`.
