Aspera Connect 2.7.7

Windows XP, 2003 SP2, Vista, 2008, 7

Document Version: 1

Contents

Introduction

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

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

On Windows, Connect supports the following web browsers:

Browser	Version
Internet Explorer	6+ *(32 bit-only)*
Firefox	3+ *(32 bit-only)*
Google Chrome	5+

Setting Up

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

Installation

Perform a fresh installation of Aspera Connect.

> **WARNINGS FOR WINDOWS USERS:** On Windows, you cannot install Connect under the *Guest* account.
> Additionally, if you are installing Connect on a Windows 2003 machine, then your system *must* be upgraded to
> Service Pack 2 (SP2) before proceeding with the installation process.

> **IMPORTANT NOTE:** For the Connect auto-installer to work properly, Java must be installed on your system. If you
> do not have Java installed, or your system doesn't support it, then you can manually download and set up Connect
> per the instructions below. For Connect to function correctly, you must have *cookies enabled* within your browser.
> Please review your browser help for instructions on verifying this setting.

If you are running Internet Explorer 7 or 8 on a Windows system, and plan to use the Connect auto-installer, you
will need to configure several browser settings before proceeding. Please refer to the table below for information on
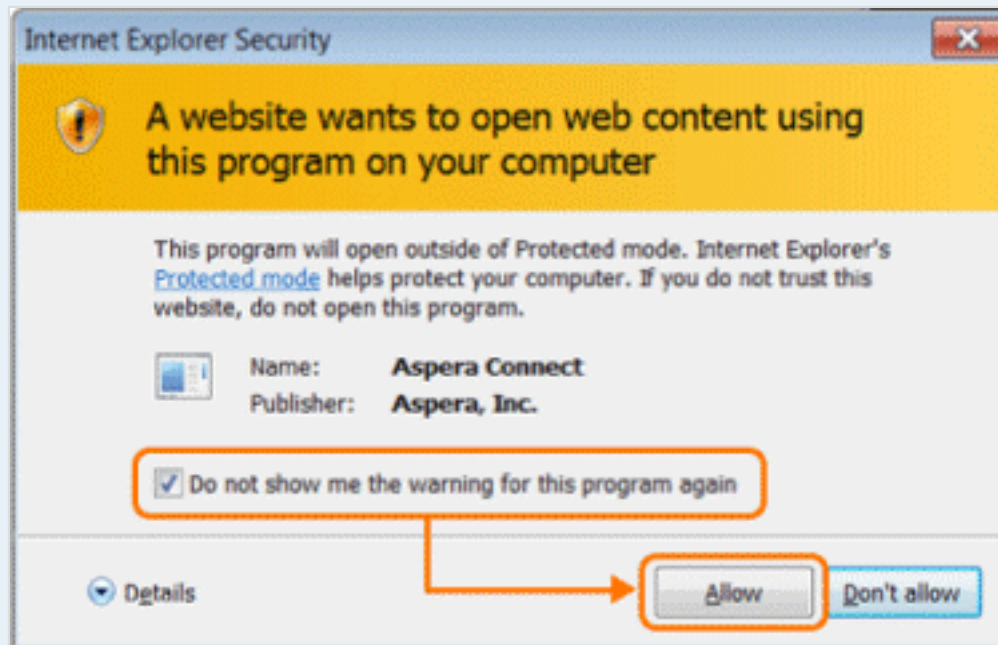allowing Connect to install through your browser.

Browser	Instructions
Internet Explorer 7	Within your IE 7 browser, you will be prompted to run the "Aspera Connect" ActiveX control add-on. Click **Run** to continue.

| Browser	Instructions
	You will then encounter a security warning when Connect Server or Faspex Server attempts to launch the Aspera Connect browser plug-in. Check the option **Do not show me the warning for this program again** and click **Allow**.
Internet Explorer 8	Within your IE 8 browser, go to **Tools** > **Internet Options** > **Security** > **Custom level...**. Under *ActiveX controls and plugin-ins*, perform the following actions: • **Enable** Binary and script behaviors • **Prompt** Download signed ActiveX controls • **Enable** Only allow approved domains to use ActiveX without prompt • **Enable** Run ActiveX controls and plug-ins • **Enable** Script ActiveX controls marked safe for scripting Under *Scripting*, perform the following actions: • **Enable** Active scripting • **Prompt** Scripting of Java applets • **Enable** Only allow approved domains to use ActiveX without prompt • **Enable** Run ActiveX controls and plug-ins • **Enable** Script ActiveX controls marked safe for scripting

Browser	Instructions

	Click **OK**, and then the **Trusted Sites** zone (green check). Click the **Sites** button and **Add** the following:
	
	`http://download.asperasoft.com`
	`https://download.asperasoft.com`
	
	When finished, click **Close** and then **OK**. Your IE 8 browser must be restarted at this time.

Use your browser to navigate to your organization's Connect Server or Faspex Server website (note that you may need to request this information from your IT Department). Once you have reached the server's website, you will see an **Install Now** button. Depending on your Operating System and browser, clicking on the **Install Now** button will either launch the automatic installer or redirect you to the Aspera Connect download page (for manual installation). Follow the on-screen instructions to complete the installation process.
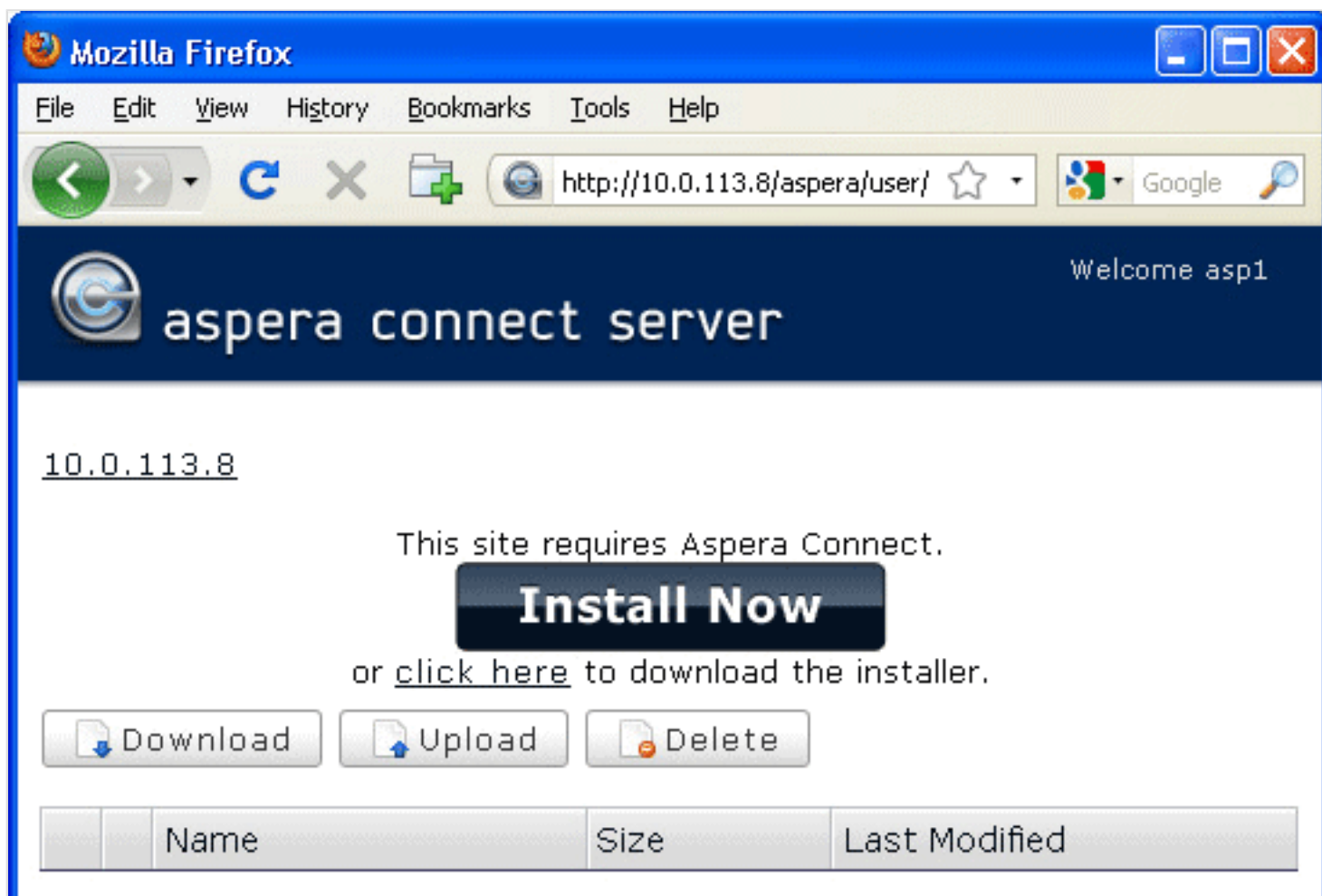
Upgrading from a Previous Version

Upgrade your existing installation of Aspera Connect to the latest version.

Aspera Connect supports auto-upgrading, as well as installer upgrading. To update your existing installation of Aspera Connect to the latest version, go to *http://asperasoft.com/connect*, click the **Update Now** button and follow the on-screen instructions. Clicking the button will either initiate auto-upgrade or download the latest installer.

Set Up Network Environment

Configure your firewall, connection speed, and a proxy server (if applicable).

The following table provides basic information for configuring your firewall to allow Connect 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:

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

You may also want to specify your network's connection speed for improved transfer efficiency, as well as set up Aspera Connect to work with your organization's proxy server. To specify your connection speed and/or configure your proxy server, launch Aspera Connect (**Start Menu** > **All Programs** > **Aspera** > **Aspera Connect**), open **Preferences** (**System Tray** > **Right-click Aspera Connect** > **Preferences**) and navigate to the **Network** preferences option.
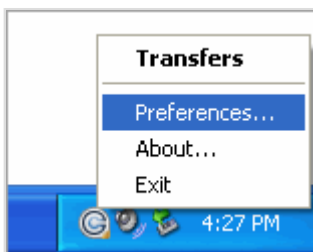

Within the *Connection* section, you may utilize the drop-down list to select a common network connection or specify exact downstream and upstream connection speeds. Please note that Connect's ability to attain these speeds is dependent upon your network bandwidth.
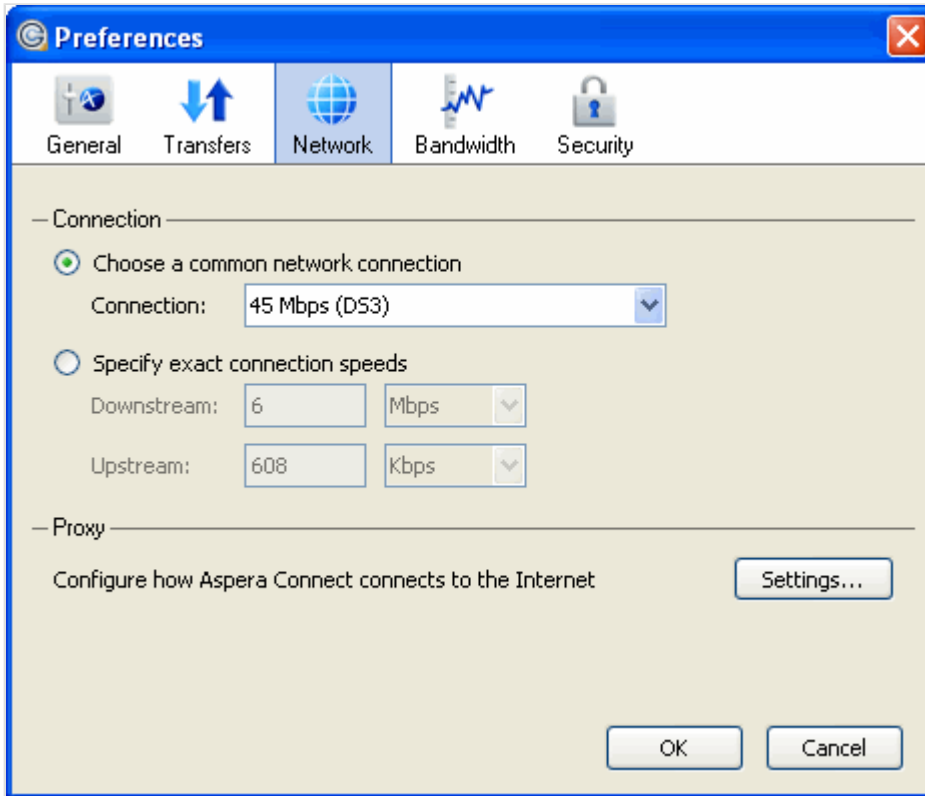
In addition, your organization may require you to use a proxy. The proxy settings dialog box enables you to specify how Aspera Connect should obtain your proxy configuration. To access your Connect proxy settings, click **Settings** under the *Proxy* section.

Within the proxy settings dialog box, you have several configuration options that are available under the drop-down list. Please note that the HTTP checkbox and fields will only be enabled if you select "Manual" from the drop-down list.

- **System:** Choose "System" if you want Aspera Connect to use the proxy settings configured for your Operating System.
- **Firefox:** Choose "Firefox" if you want Aspera Connect to automatically detect the proxy settings from your Firefox Web browser.
- **Manual:** Choose "Manual" if you would like to manually input your proxy hostname and port number (which may require the assistance of your System Administrator).
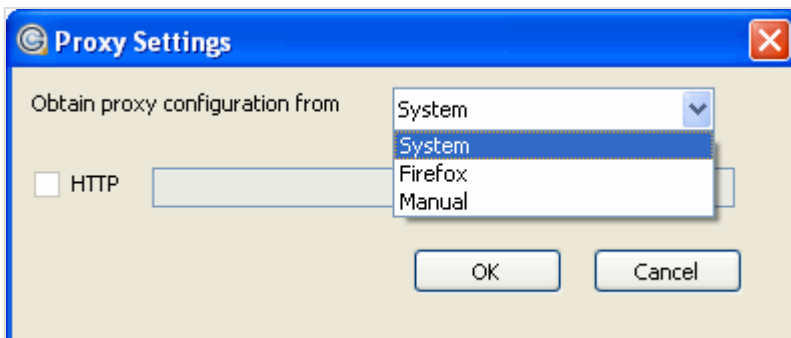
Note that Aspera Connect automatically archives the bandwidth (download and upload) measured between your computer and connected host(s) under the **Bandwidth** preferences option. You may utilize these measurements to optimize your transfer rates, or you can choose to remove the host(s) from the list.

Basic Configuration

Configure Aspera Connect for basic operation, including setting up application behavior, download location and the retry rule.

Before using Aspera Connect, you may want to change the application's basic settings, including where to save downloaded files and how transfer retries should behave. To update these preferences, launch Aspera Connect (**Start Menu** > **All Programs** > **Aspera** > **Aspera Connect**) and open *preferences* (**System Tray** > **Right-click Aspera Connect** > **Preferences**).
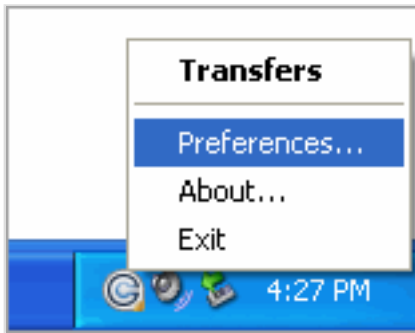

Aspera Connect's general application behavior can be configured under the **General** preference option.
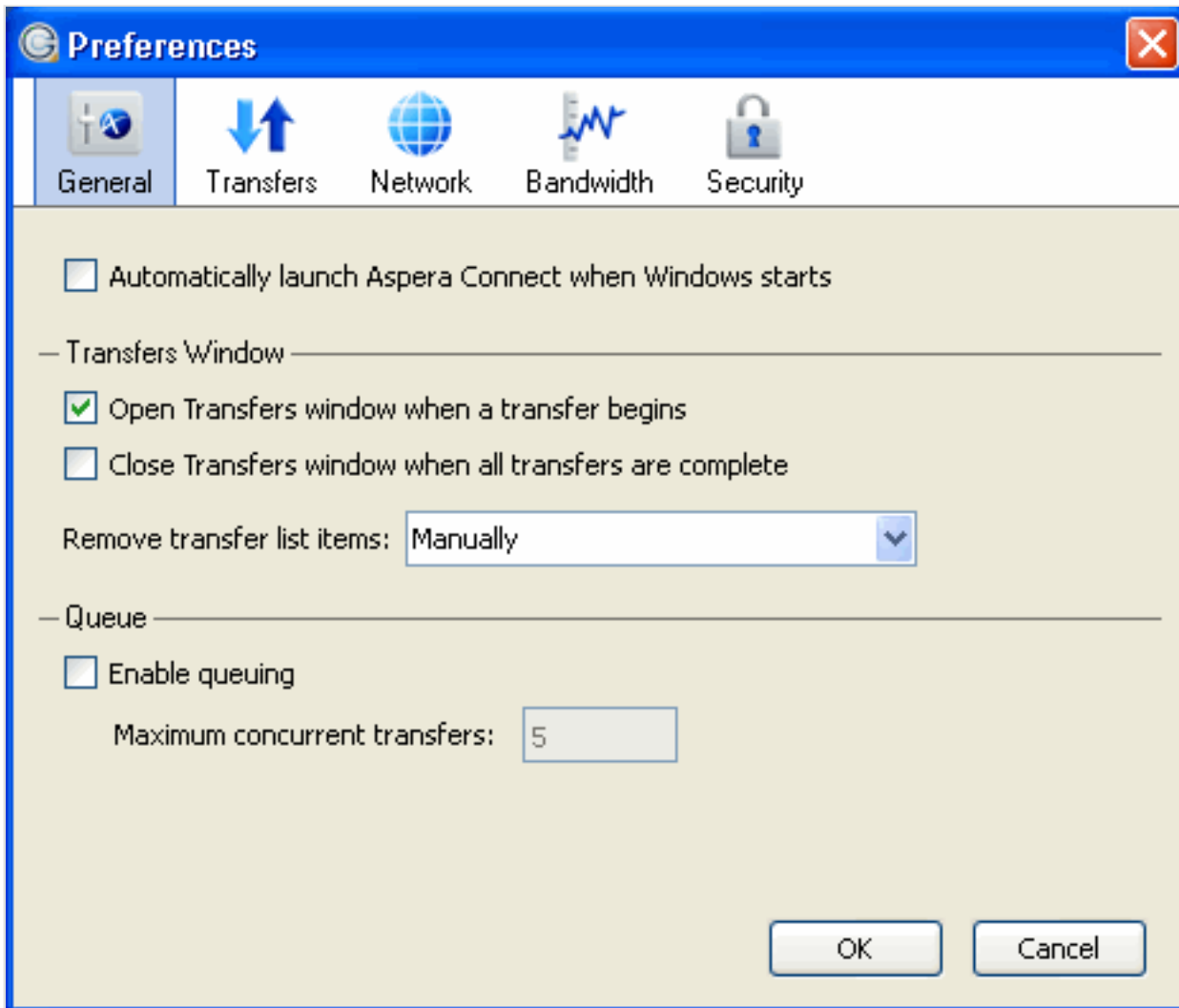
Under the *General* tab, you can modify the following settings:

- Specify whether or not Aspera Connect should launch when your Operating System starts (via the checkbox)
- Specify how the *Transfers* window should behave when a transfer begins and completes (via the checkboxes)
- Specify how transfer list items should be removed from the *Transfers* window (via the drop-down list)
- Enable or disable transfer queuing via the checkbox (which allows a fixed number of concurrent transfers and places the rest in a queue) and identify the maximum number of concurrent transfers via the text box.

Aspera Connect's transfer behavior can be configured under the **Transfers** preference option.
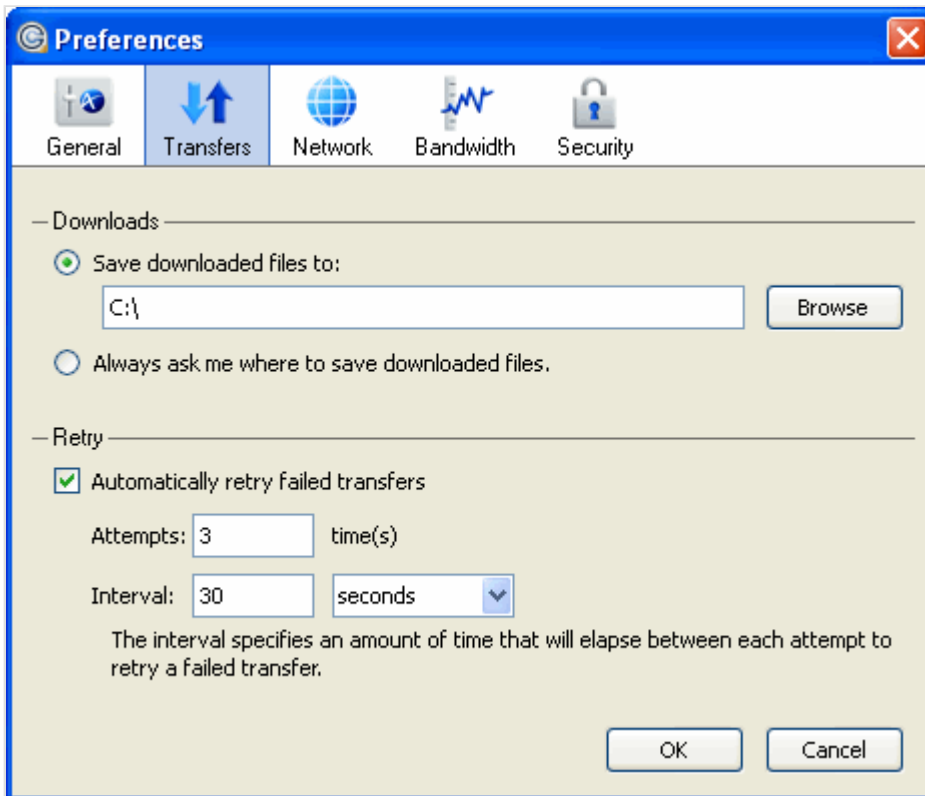
By default, Connect downloads files to the current user's desktop. To change this setting within the **Transfers** preferences option, set the download rule within the *Downloads* section as follows:

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

You can also set a retry rule if a transfer fails. In the **Transfer** option preferences, set the retry rule within the *Retry* section as follows:

- Automatically retry failed transfers *(Check this option to enable the retry feature)*
- Attempt *(Specify how many times Connect should attempt to retry the transfer)*
- Interval *(Specify the amount of time that should elapse between each attempt)*

Using Connect

Transfer files using Aspera Connect.

Starting a Transfer

Initiate file transfer through Aspera Connect

To test whether or not Aspera Connect is configured (and working) properly, follow these steps to test transfers between your system and the Aspera Demo Server.

**1.** Open your web browser and navigate to the following URL (entering in the credentials when prompted)

- http://demo.asperasoft.com/aspera/user
- User: asperaweb
- Password: demoaspera

Internet Explorer 7 Security Settings: When opening a Connect Server or Faspex Server web page using Internet Explorer 7, the Information Bar will appear and ask for the permission to use the Aspera Connect add-on. Click the bar and select **Run ActiveX Control**, and then click **Run** in the *Security Warning* window.
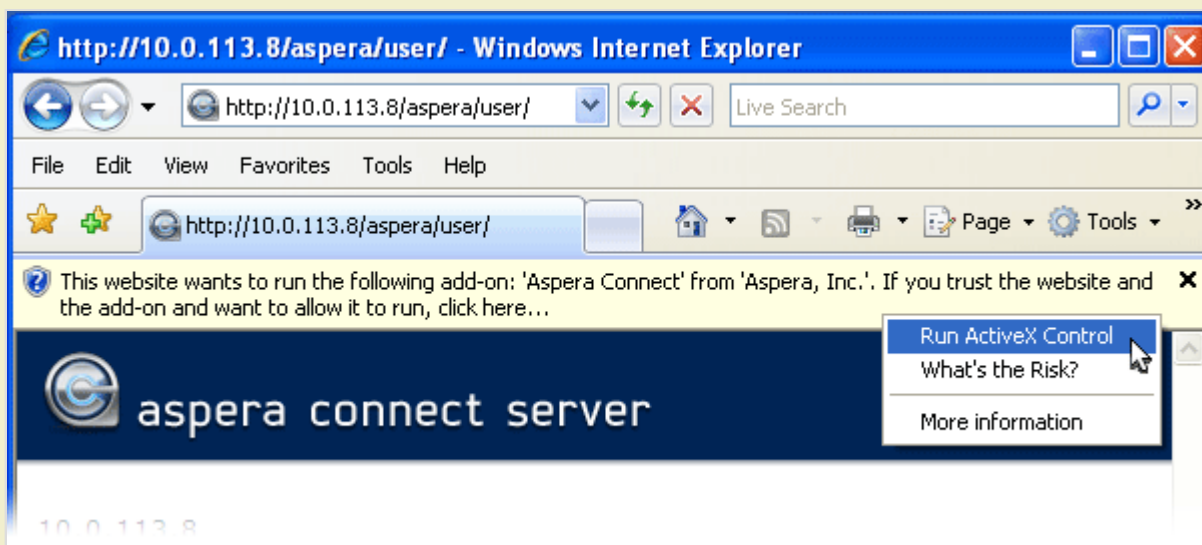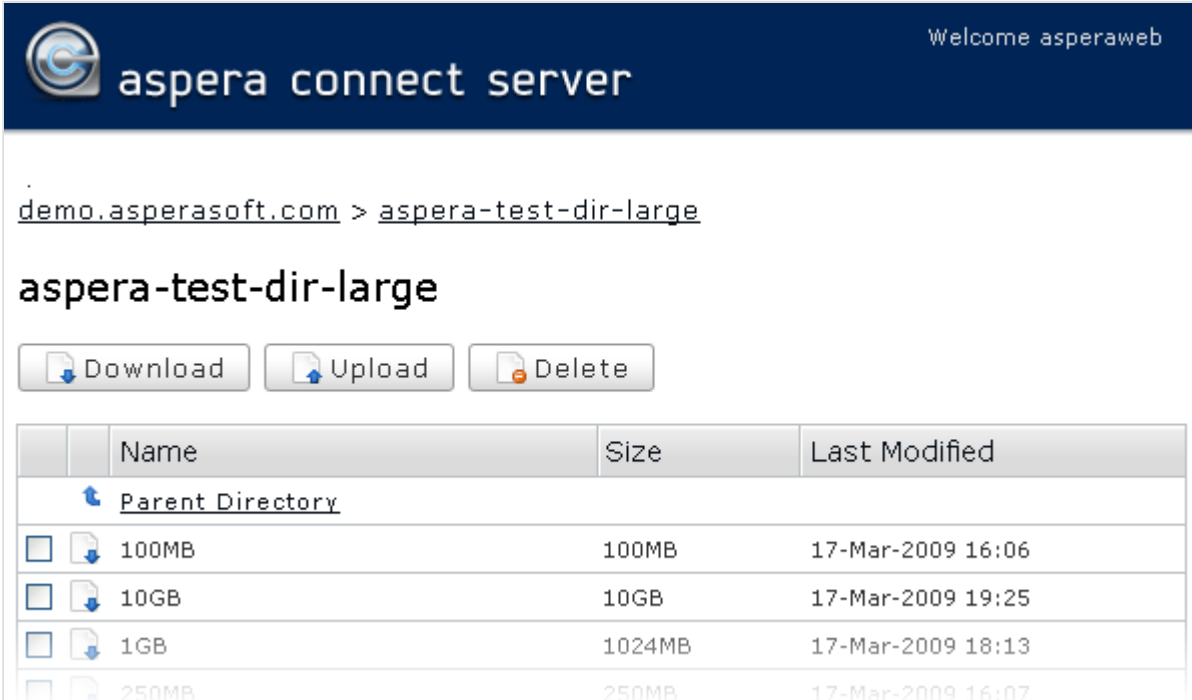
If you accidentally clicked **Don't Run**, then just click the gear icon at the bottom of the Connect Server or Faspex Server web page to bring up the *Manage Add-Ons* window. Select **Aspera Web Control** and set **Enable** under *Settings*.
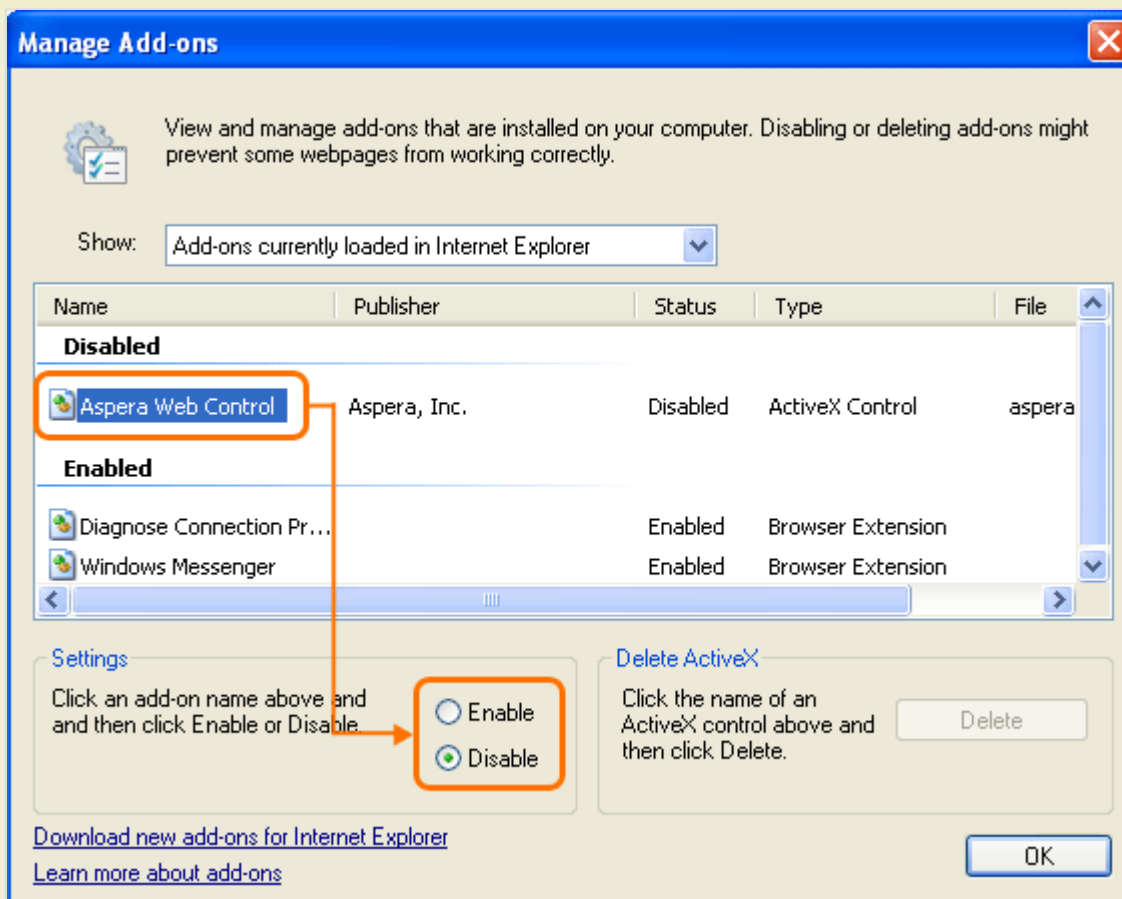
2. On the Connect Server or Faspex Server web page, browse into the folder */aspera-test-dir-large*

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

3. Confirm the transfer.

   Select **Allow** to begin. Check the *"Use my choice for all transfers with this host"* option to skip this dialog in the future.
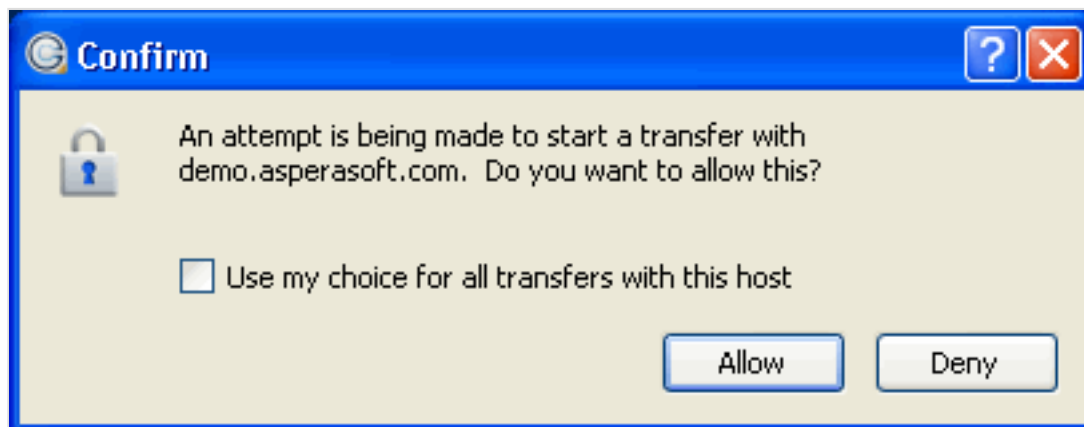
Once you confirm that the configuration settings are correct and that Aspera Connect is working properly, you can begin transferring with your organization's Connect Server or Faspex Server. Simply point your browser to your server's address (e.g., *http://companyname.com/aspera/user*) to get started.
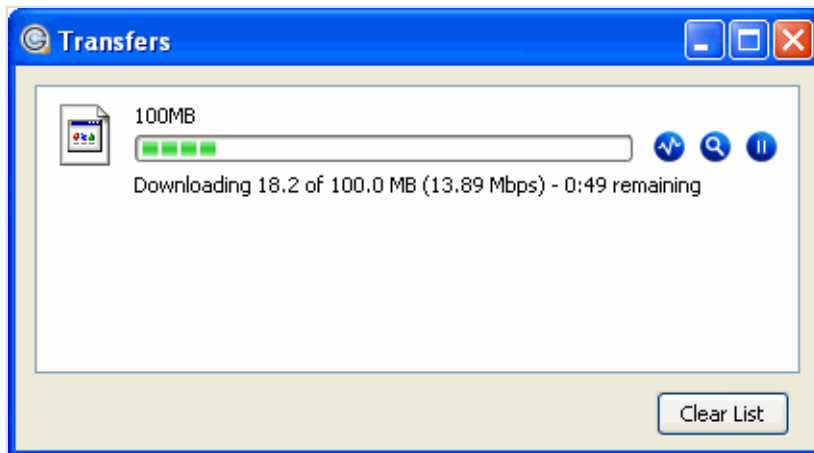
Note that when uploading, you should avoid transferring files with the following characters in the file name:

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

Managing Transfers

View and manage all transfer sessions.

You may view and manage all transfer sessions within the *Transfers window*. Click the Aspera Connect icon in the System Tray's task bar to open it.

The *Transfers window* contains the following items:

- Open the Transfer Monitor.

- Reveal the file on your computer.

- Pause the transfer session (note that this icon appears after the transfer has started).

- Resume transfer.

- Retry a failed transfer.

When the queuing option is enabled, only a certain number of concurrent transfers are allowed. The additional transfers will be queued in the *Transfers window* and initiated when a transfer is finished. You can manually start a queued transfer by clicking the (Resume) button.

Controlling Transfer Speed

Monitor and adjust the transfer speed.

You can monitor and adjust file transfer speed by clicking the (Transfer Monitor icon) to open the *Transfer Monitor*. Here, you may specify the transfer policy and transfer speed if you have sufficient server privileges.
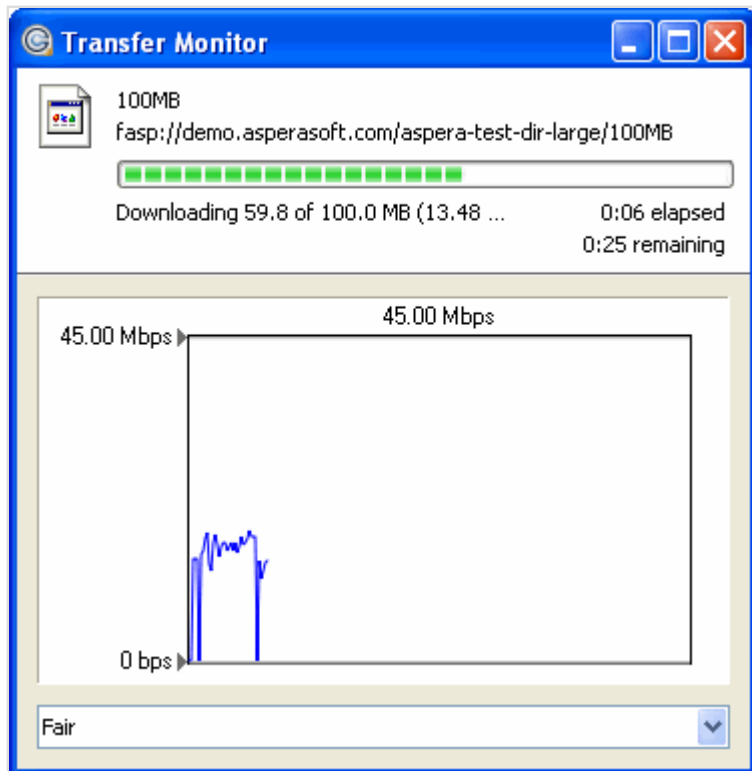
Content Protection

Encrypt files during the transfer or password-protect them while stored on the server.

Content protection is a feature that allows uploaded files be encrypted during a transfer *(if the server is configured as a content-protected host)*, for the purpose of protecting them while stored on a remote server. The uploader sets a password while uploading the file, and the password is required to decrypt the protected file. You may enable this feature within Aspera Connect's preferences window (**System Tray** > **Right-click Aspera Connect** > **Preferences**). Go to the **Security** preferences option and click the **Content Protection** tab. Enter the Connect Server or Faspex Server address in the Address text field and click **Add**. The server will be added to the Host list.
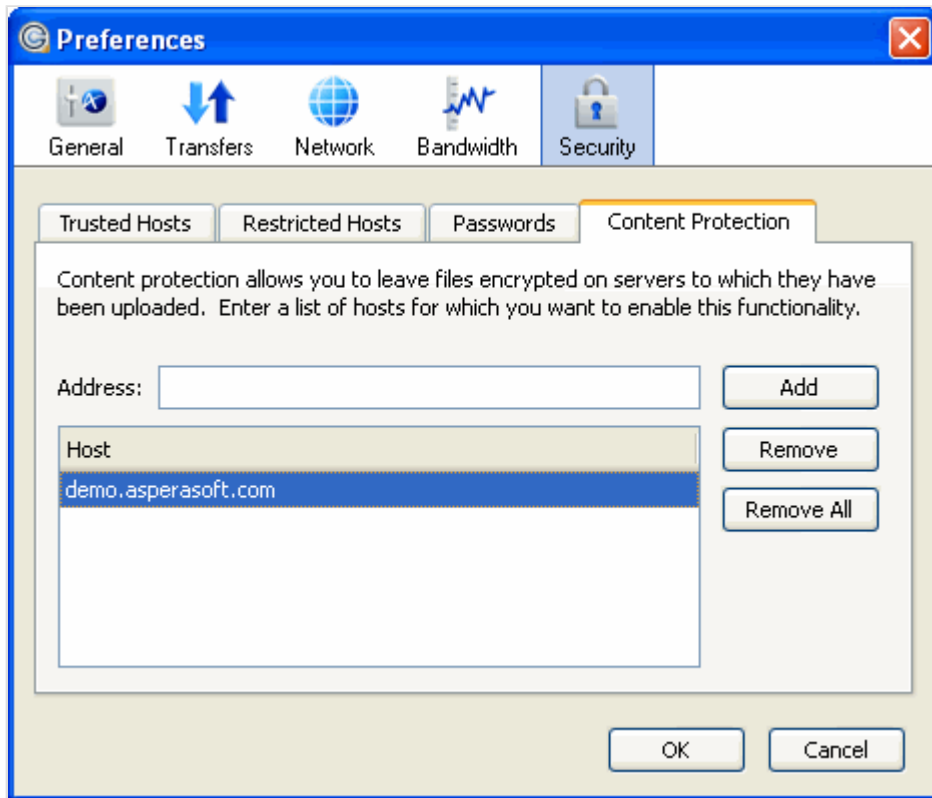
When uploading files to a server that is configured as a content-protected host, a confirmation window will appear and prompt you for a passphrase to encrypt the file. You can enter the passphrase in the text field, or check **Leave uploaded files unencrypted** *(if allowed by your host)* to proceed without using this feature. Click **OK** to start the transfer.

Encypted files will be indicated by an an encrypted file icon.
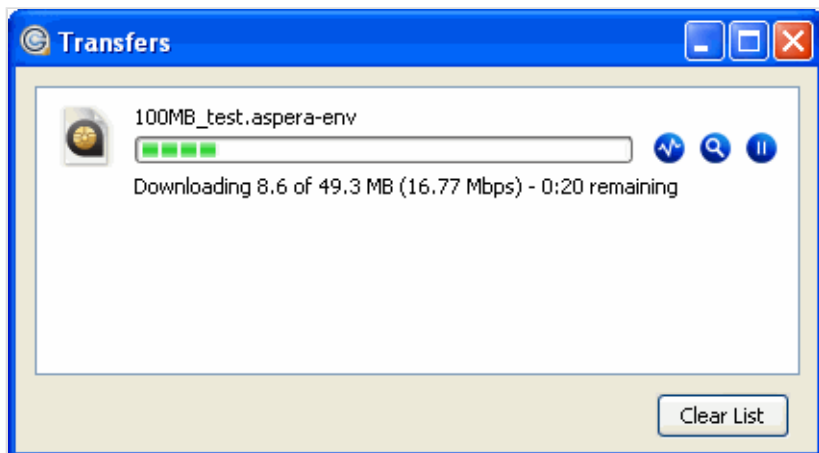
When the encrypted file has been downloaded to your computer, the file will display the extension *aspera-env* (Aspera Security Envelope). Double-click the file to bring up **Aspera Crypt**, enter the passphrase into the specified field, and click **Decrypt**. The decrypted file will appear in the same directory.
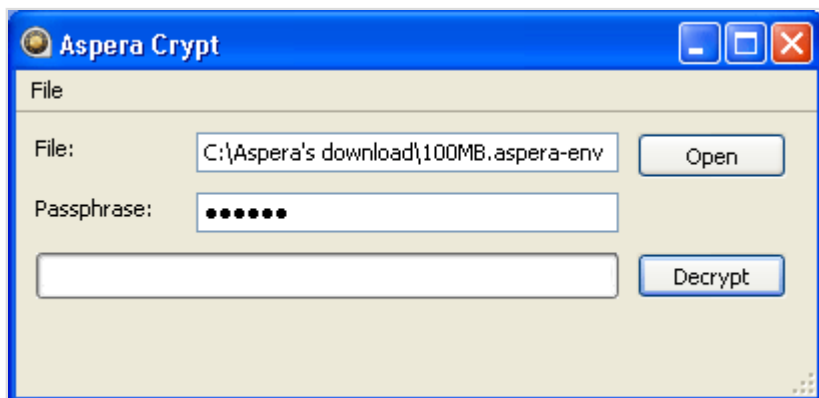

Managing Hosts

Add your Connect Server or Faspex Server as a trusted host to avoid the confirmation dialog box, or add a server to the restricted hosts lists to block it.

You can add your Connect Server or Faspex Server as a trusted host to avoid the confirmation dialog box, or add a server to the restricted hosts lists to block it. To access your trusted and restricted hosts list, open your Connect preferences window (**System Tray** > **Right-click Aspera Connect** > **Preferences**) and go to the **Security** preferences option.

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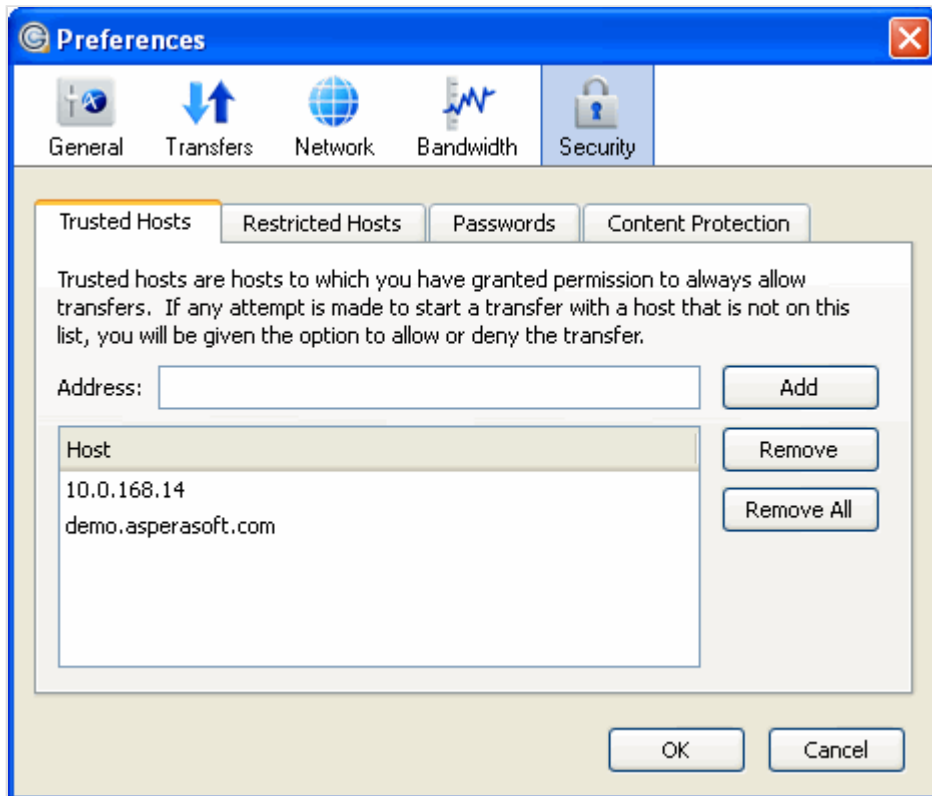
To view, add or remove additional trusted hosts, go to the **Trusted Hosts** tab in the preferences box. Enter the host's address in the specified text field and click **Add**.

To view, add or remove additional restricted hosts, go to the **Restricted Hosts** tab in the preferences box, enter the host's address in the specified text field, and click **Add**. Note that by adding a host to the restricted list, you will be required to provide confirmation every time you attempt to initiate a transfer with that host. If a host is in both the Trusted Hosts and Restricted Hosts list, then the restriction takes precedence.

If you have saved login information for a host, it is stored in the **Passwords** tab. Here, you may remove the saved credentials.
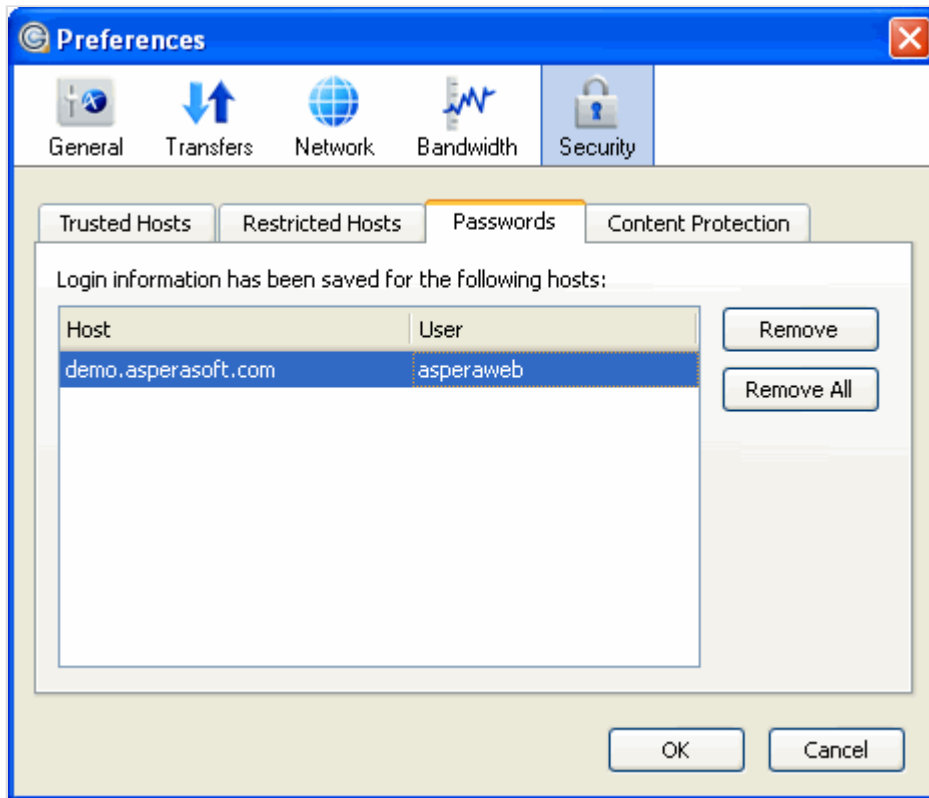
Appendix

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	*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. 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	*fasp* monitors the network and adjusts the transfer rate to fully utilize the available bandwidth up to the maximum rate. When congestion occurs, a *fasp* 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. **Note:** This policy is not available in the Connect browser plug-in.
Fair	*fasp* 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, *fasp* 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.

Uninstalling Aspera Connect

Remove the Aspera Connect from your computer.

To uninstall Aspera Connect, go to the *Control Panel*. Depending on the version of the Windows operating system, choose **Add/Remove Programs** or **Uninstall a program**. Select *Aspera Connect* and remove it.

Troubleshooting

Error when Installing with a Non-admin Account

Problem installing the MSI package when logged in as a non-admin.

You may encounter an error when executing the installer MSI file if you are not an Administrator. For example:

OS Version	Error
Windows 2003	The system administrator has set policies to prevent this installation.
Windows XP	You do not have access to make the required system configuration modifications. Please rerun this installation from an administrators account / Error 1925. You do not have sufficient privileges to complete this installation for all users of the machine. Log on as administrator and retry this installation.

These error messages are due to not having permissions to install an MSI package as a non-admin account. Other than logging in as an administrator to install Aspera Connect, you may also ask that your Administrator grant the group policy access for non-admin users to install applications.

The following example shows you how to grant group policy access for non-admins to install software on Windows 2003:
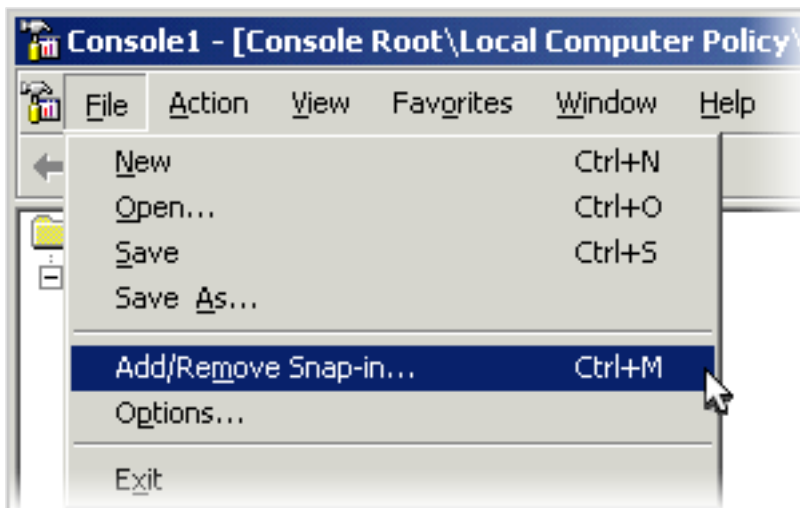
1. Launch the Microsoft Management Console (MMC)

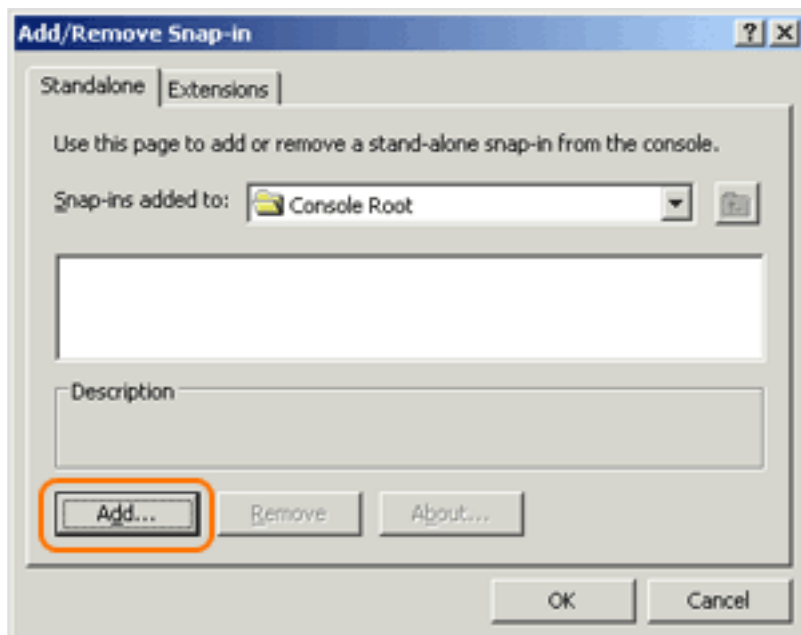   Go to **Start menu** > **Run...** and enter *mmc*, click **OK** to launch it.
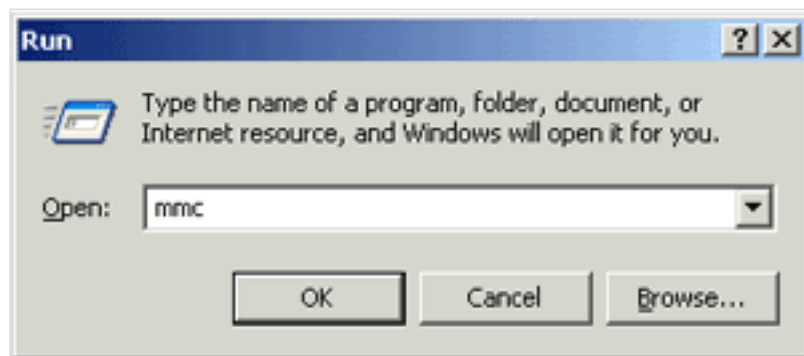
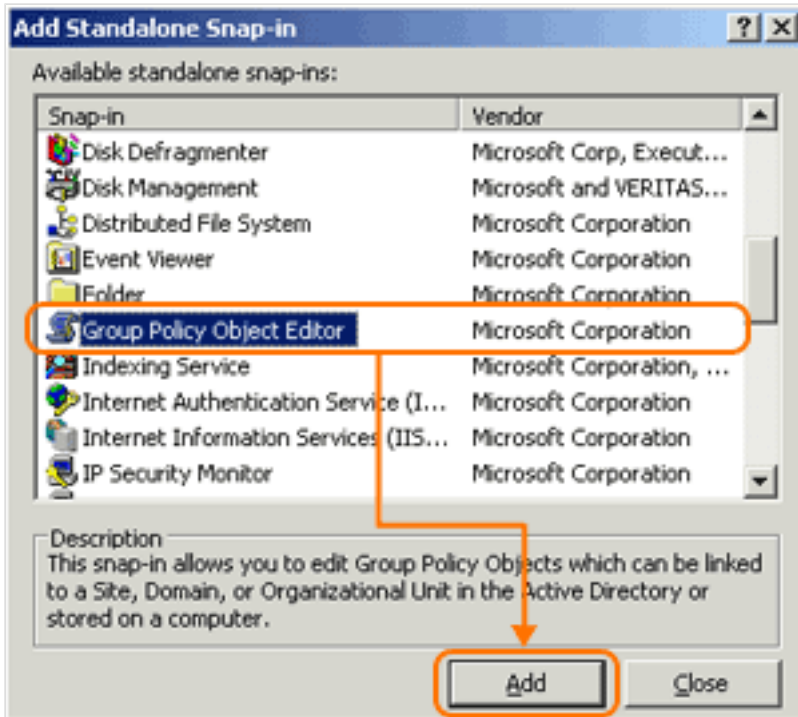2. Add the Group Policy Object Editor Snap-in

   In the MMC, go to **File** in the toolbar and select **Add/Remove Snap-in...**.

In the *Add/Remove Snap-in* window, click **Add...** to bring up the *Add Standalone Snap-in* window.


Select the **Group Policy Object Editor** and click **Add**.

In the *Group Policy Wizard* window, click **Finish**. Close the *Add Standalone Snap-in* window, and click **OK** in the *Add/Remove Snap-in* window to save the changes.

3. Grant the Windows installation group policy

   In the MMC, navigate into **Console Root** > **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Windows Installer**.
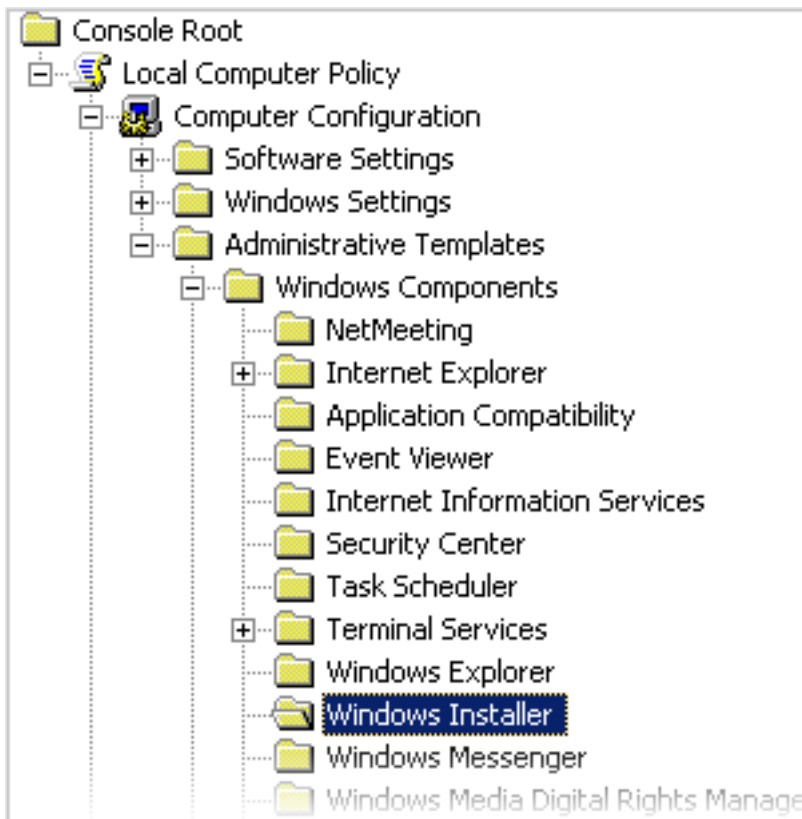
Locate the *Disable Windows Installer*, right-click and select **Properties**.

In the *Properties* window, select **Enabled** from the radio button options, and select **Never** in the *Disable Windows Installer*. Click **OK** when finished.
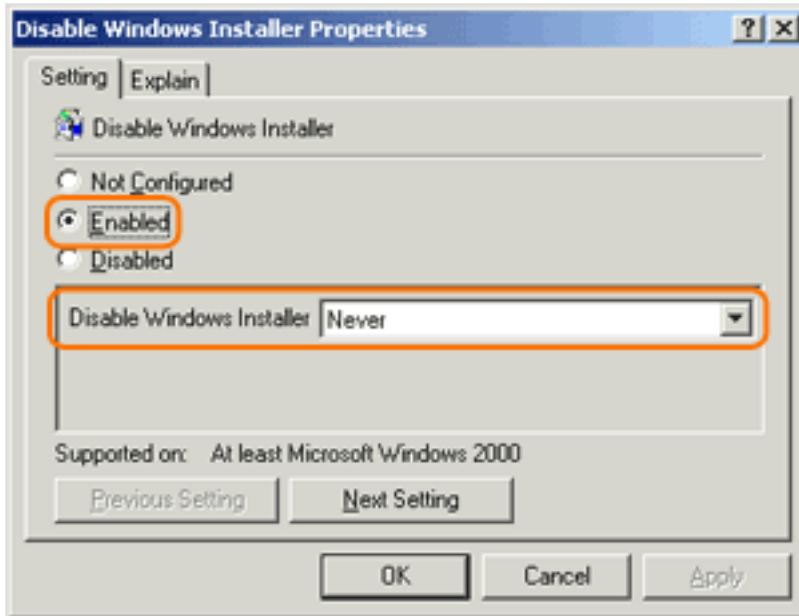
Close the MMC, click **Yes** to save the settings to a file. Reboot the computer to apply the changes, or execute the command in the Command Prompt:

```
> gpupdate /force
```

Missing Install Button on Windows 2003

On Windows 2003, the Connect installation button doesn't appear on the Connect Server or Faspex Server webpage.

On Windows 2003 SP2, Aspera Connect's install button may not appear on the Connect Server or Faspex Server Web UI properly. This problem may be due to additional security restrictions within Internet Explorer (Version 8). To resolve this, follow these steps:
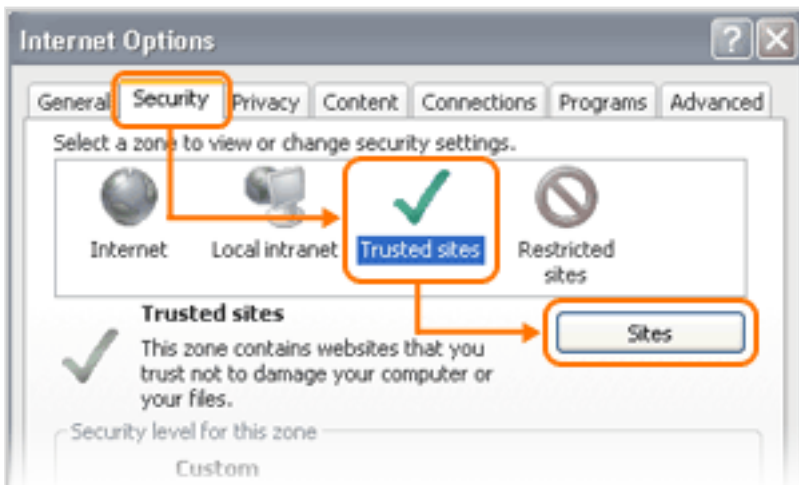
1. Launch Internet Explorer (version 8) and bring up the Internet Options

Launch the Internet Explorer, click **Tools** from the Toolbar, and select **Internet Options**.
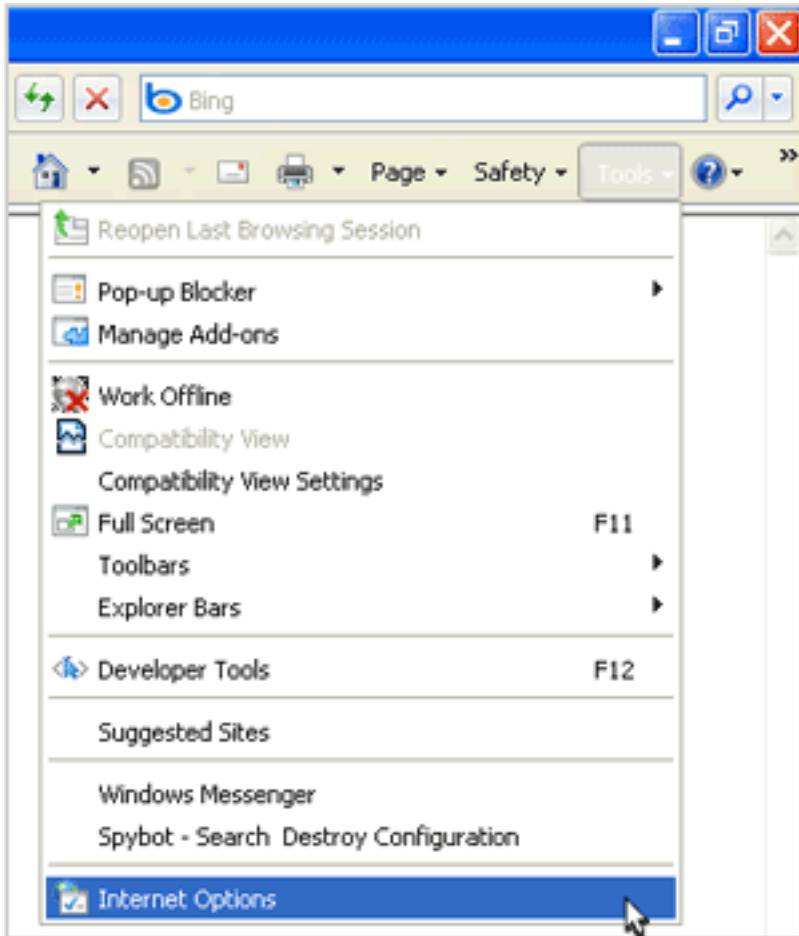

2. Add the Trusted Sites

In the *Internet Options* window, go to **Security** and select **Trusted Sites**. Click **Sites** to bring up the *Trusted sites* window.

In the *Trusted sites* window, first un-check the option **Require server verification (https:) for all sites in this zone**, then add the following websites. Replace the "my.connect.server.address" with the address of the Connect Server or Faspex Server that you are browsing:

- http://*.asperasoft.com
- http://java.com
- http://my.connect.server.address
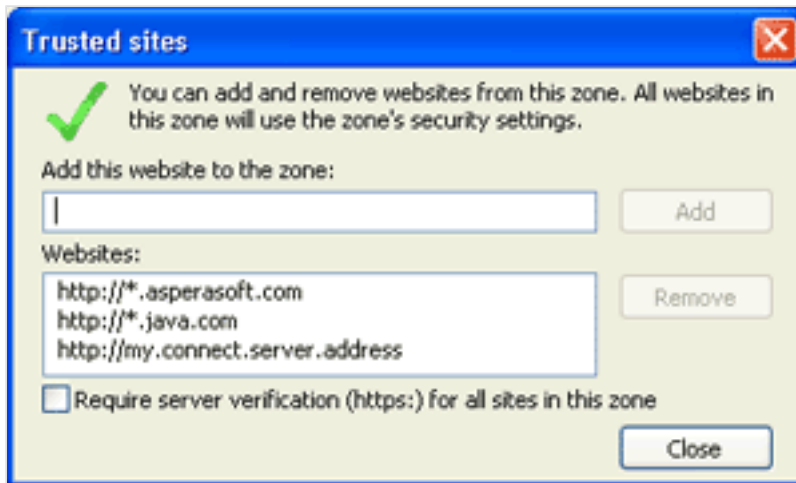
Troubleshooting Connectivity

SSH Connectivity Errors

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

```
> telnet server-ip-address 33001
```

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

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

UDP Connectivity Errors

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

Technical Support

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

Contact Info

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

The technical support service hours:

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

We are closed on the following days:

Support Unavailable Dates

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

Legal Notice