

 **Aspera Connect 3.3.4**

Windows XP SP2, 2003 SP2, Vista, 2008, 7, 8

Document Version: V1

Contents

Introduction.....	3
System Requirements.....	4
Setting up Connect.....	5
Part 1: Installation.....	5
Part 2: Network Environment.....	7
Part 3: Basic Configuration.....	12
Part 4: Security Configuration.....	15
Connect Functionality.....	23
Initiating a File Transfer.....	23
The Transfer Manager.....	26
Monitoring Transfers.....	28
Decrypting Local Files.....	29
Uninstalling.....	33
Appendix.....	34
Log Files.....	34
Plugin Locations.....	34
File Clean-up.....	35
Troubleshooting.....	37
Web Installation is Blocked in IE7.....	37
Error when Installing with a Non-admin Account.....	37
Missing Install Button on Windows Server.....	41
Troubleshooting Connectivity.....	43
Technical Support.....	45
Feedback.....	46
Legal Notice.....	47

Introduction

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

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

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

System Requirements

System requirements for installing/running Connect.

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

- Windows XP SP2, 2003 SP2, Vista, 2008, 7, 8 (see note below)
- IE 7+, Firefox 4+ (*32-bit only*) or Google Chrome 5+

WARNING! Aspera Connect does not support the *64-bit* IE 10 browser on Windows 8.

Setting up Connect

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

Part 1: Installation

Instructions for installing Aspera Connect on your system.

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

WARNINGS:

- You cannot install Connect under the *Guest* account.
- If you are installing Connect on a Windows 2003 or Windows XP machine, then your system *must* be upgraded to Service Pack 2 (SP2) before proceeding with the installation process.
- Before performing a system-wide installation (all users of the machine), uninstall any per-user installations. **Aspera does not support local and system-wide installations of Connect on the same system.** For details, refer to the topic "[Uninstalling Aspera Connect.](#)"
- Quit any open browsers before continuing with the steps below.

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

Aspera Connect Web Installer

Use your browser to navigate to your Aspera Web application (i.e. Faspex Server, Connect Server or Shares). Once you have reached the server's webpage, you will see an **Install Now** button (or **Upgrade Now** button if you have an older version of Connect installed on your system). Depending on your Operating System and browser, clicking on this button will either launch the automatic installer or redirect you to the Aspera Connect download page (for [manual installation](#)). Follow the on-screen instructions to complete the installation process. If your browser displays a security prompt/warning, click **Allow** or **Continue** to proceed.

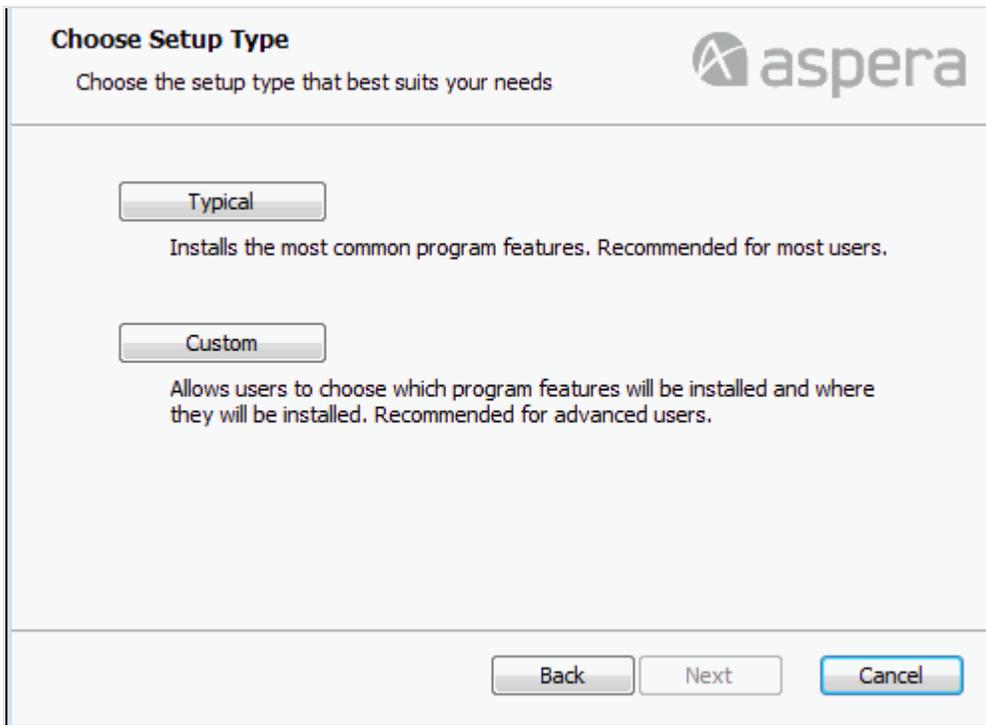
Note that for the following cases, a non-admin cannot perform a Web installation because ActiveX controls are not allowed:

- Non-admin XP IE7, IE8
- Non-admin 2003 IE7, IE8
- Non-admin Vista IE7 with UAC off
- Non-admin 2008 IE7 with UAC off

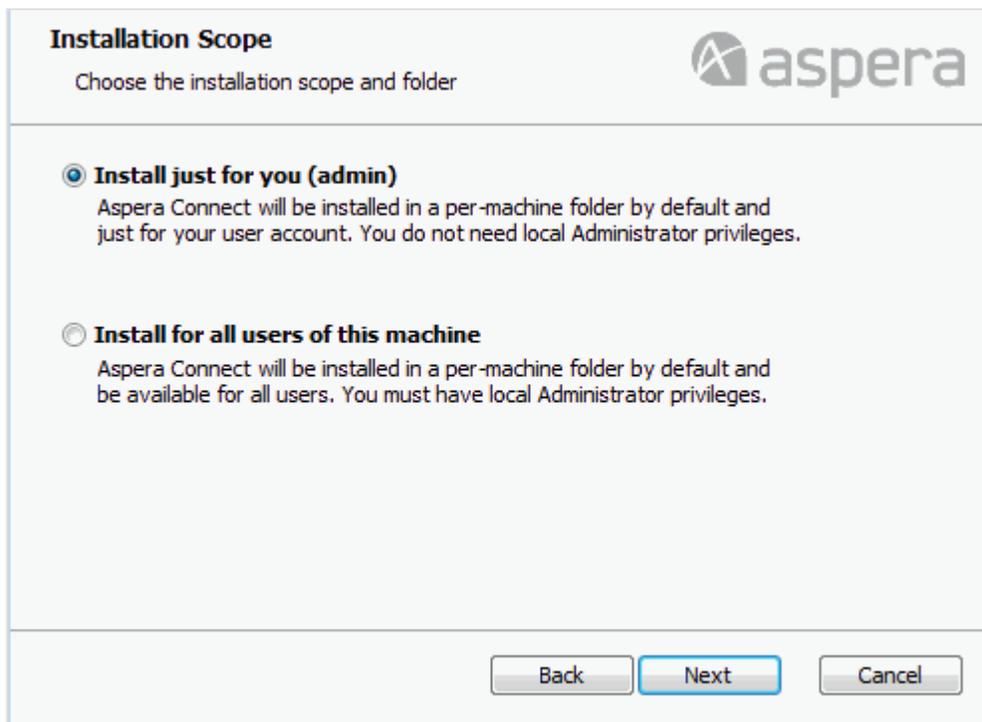
IMPORTANT NOTE: When installing the file `npinstallhelper.cab` (relevant only to the Web installation), ensure that you install it for just the current user and not for all users on the system. Installing `npinstallhelper.cab` system-wide may cause the installation to fail.

Aspera Connect Desktop Installer

You can download the Aspera Connect MSI directly from http://beta-www.asperasoft.com/download_connect/. Once downloaded, run the installer on your machine. You will need to accept the terms and conditions, as well as confirm where Aspera Connect should be installed. You can install the application in the standard location by clicking the **Typical** button.



Or select an alternative location.



Post Installation

Once Aspera Connect has finish installing, you can access it in the following location: **Start Menu > All Programs > Aspera > Aspera Connect**

Part 2: Network Environment

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

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

Network Requirements

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

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

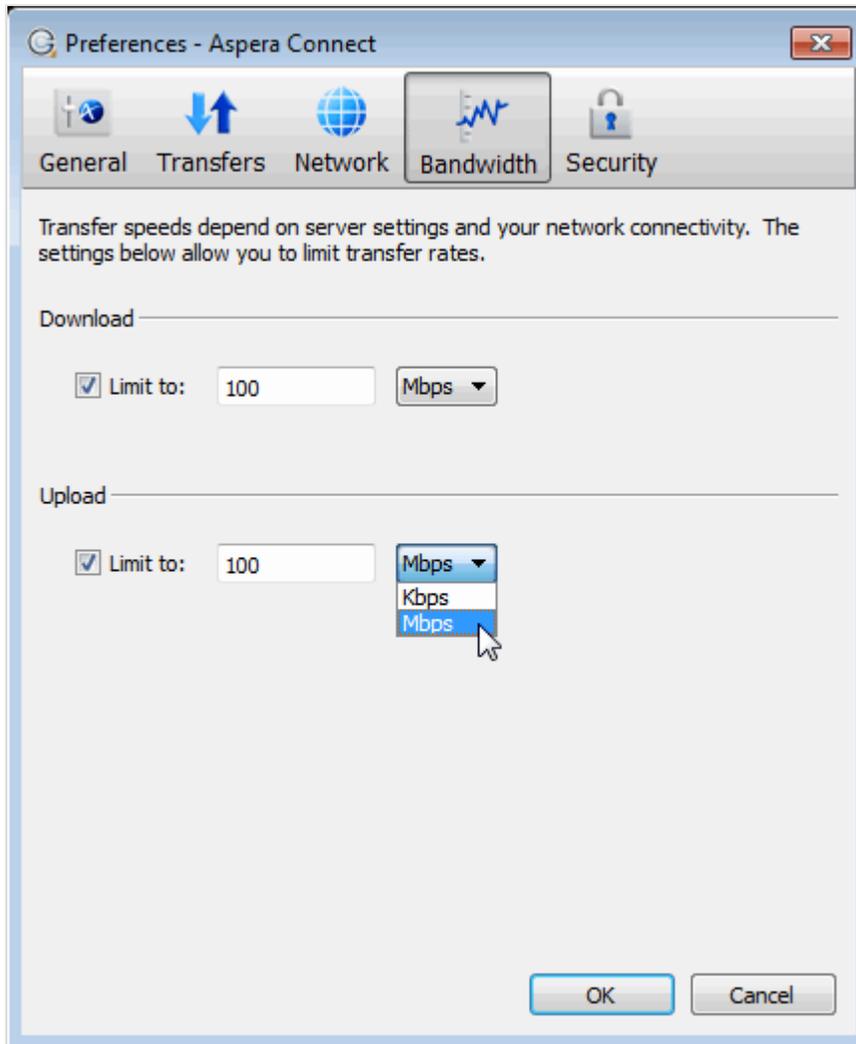
Limit Transfer Rates

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

Launch Aspera Connect (**Start Menu > All Programs > Aspera > Aspera Connect**) and open **Preferences** (**System Tray > Right-click Aspera Connect > Preferences**).

T ransfers	Ctrl+T
U nlock encrypted files	Ctrl+R
O pen log folder...	Ctrl+L
P references...	Ctrl+P
A bout...	Shift+F1
Q uit	

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

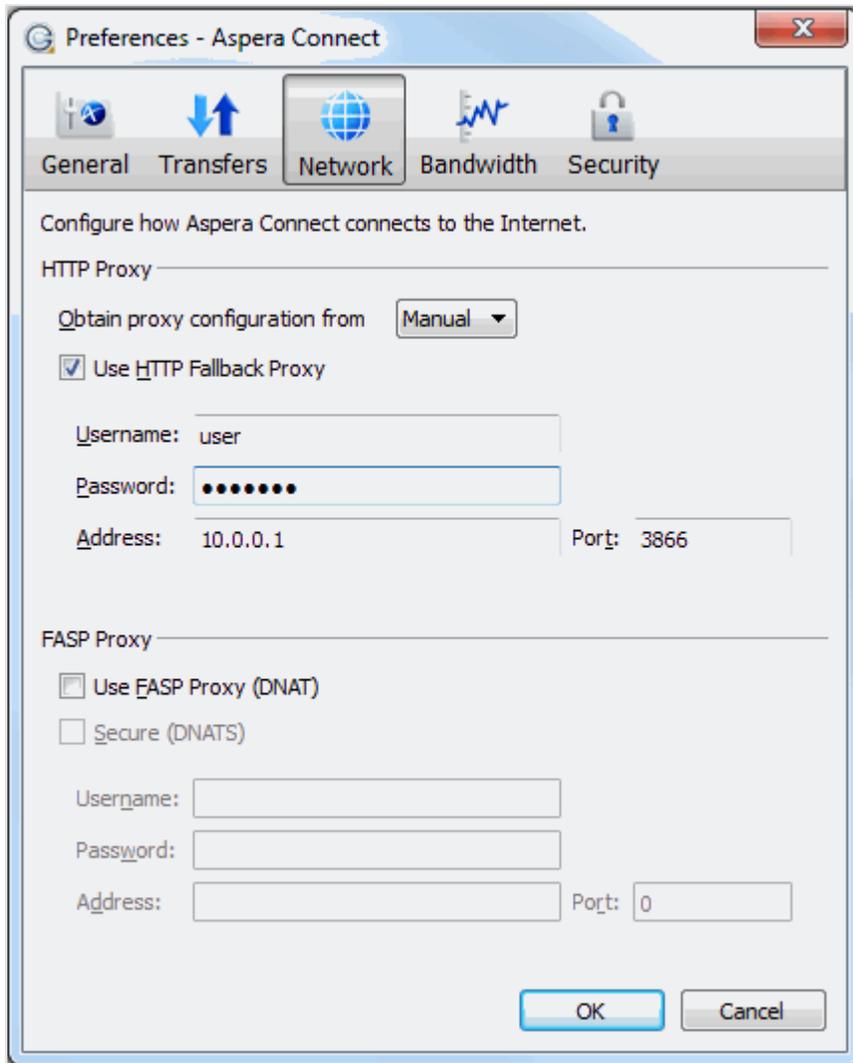


You may limit the download and/or upload transfer rates by enabling the respective checkboxes and inputting a rate in either Mbps or Kbps. Note that your ability to limit these rates depend on the following factors:

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

HTTP Fallback Proxy

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



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

To configure an HTTP fallback proxy, select one of the following configurations from the drop-down list:

- **System:** Choose "System" if you want Aspera Connect to use the HTTP fallback proxy settings configured for your Operating System.
- **Manual:** Choose "Manual" if you would like to manually input your HTTP fallback proxy settings (which may require the assistance of your System Administrator). These settings include NTLM authentication credentials (username and password), as well as the host name/IP address and port number. Please note that the **Use HTTP Fallback Proxy** checkbox and fields will only be enabled if you select "Manual" from the drop-down list.

HTTP Proxy

Obtain proxy configuration from Manual ▾

Use HTTP Fallback Proxy

Username:

Password:

Address: Port:

FASP Proxy

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

Preferences - Aspera Connect

General Transfers **Network** Bandwidth Security

Configure how Aspera Connect connects to the Internet.

HTTP Proxy

Obtain proxy configuration from Manual ▾

Use HTTP Fallback Proxy

Username:

Password:

Address: Port:

FASP Proxy

Use FASP Proxy (DNAT)

Secure (DNATS)

Username:

Password:

Address: Port:

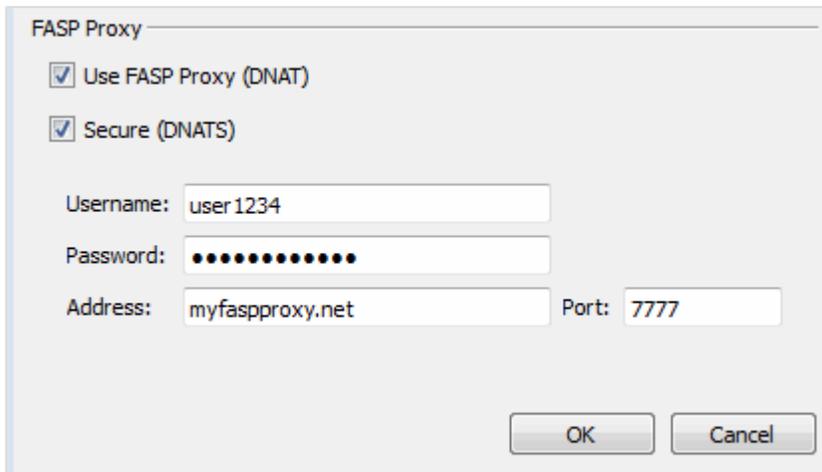
OK Cancel

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

- Use FASP Proxy (DNAT)

- Secure (DNATS)

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



FASP Proxy

Use FASP Proxy (DNAT)

Secure (DNATS)

Username: user 1234

Password: ●●●●●●●●●●

Address: myfaspproxy.net Port: 7777

OK Cancel

Part 3: Basic Configuration

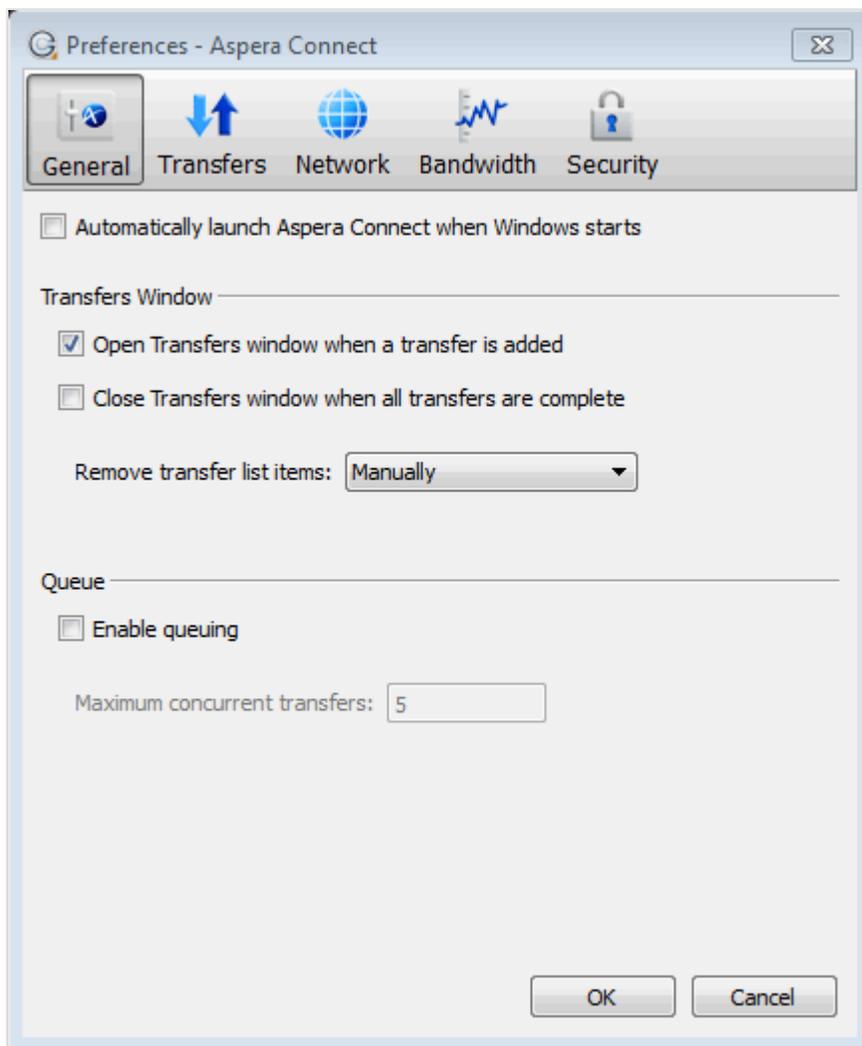
Changing Aspera Connect's default settings via the "Preferences" option.

To change the application's default settings before transferring files, launch Aspera Connect (**Start Menu > All Programs > Aspera > Aspera Connect**) and open **Preferences** (**System Tray > Right-click Aspera Connect > Preferences**).

T ransfers	Ctrl+T
U nlock encrypted files	Ctrl+R
O pen log folder...	Ctrl+L
<hr/>	
P references...	Ctrl+P
A bout...	Shift+F1
Q uit	

General Preferences

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

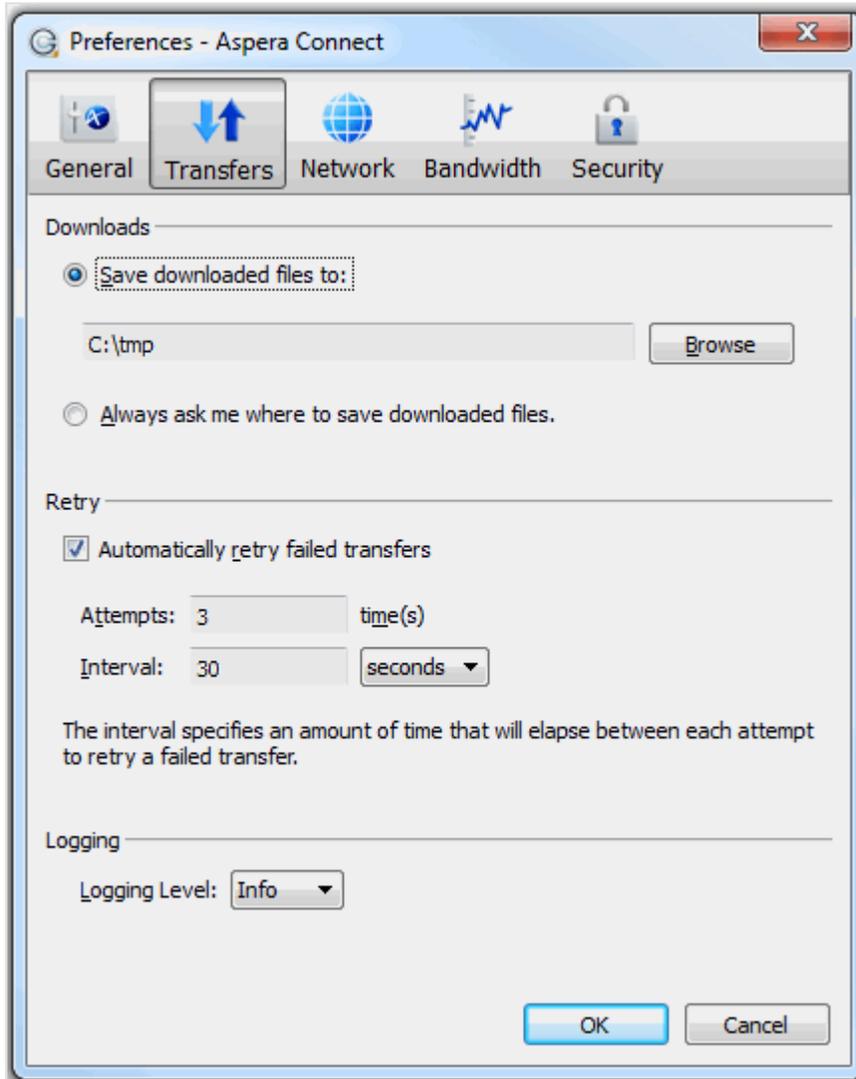


Under the **General** option, you can modify the following settings:

- Specify whether or not Aspera Connect should launch when the user logs into the system (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.

Transfer Preferences

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



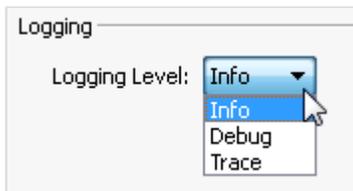
By default, Connect downloads files to the current user's desktop. To change this setting, set the download rule within the *Downloads* section as follows:

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

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

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

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



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

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

Part 4: Security Configuration

Configuring Aspera Connect's security preferences.

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

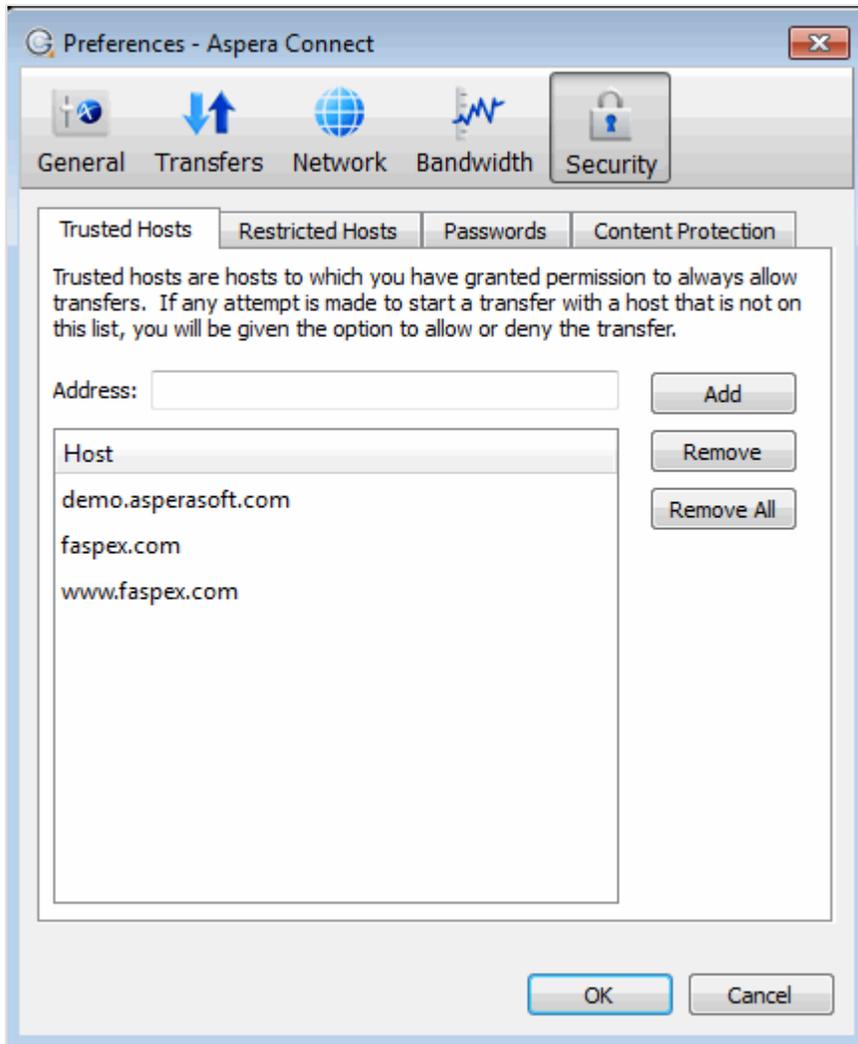
- You can add Aspera servers as **Trusted Hosts** to avoid the recurring security prompt, or add servers to the **Restricted Hosts** list to require confirmation every time you attempt to initiate a transfer with that host.
- You have the option of saving your authentication credentials when you connect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

The settings above can be configured via the the Aspera Connect **Preferences** dialog box. To open Connect's **Preferences** dialog box, launch Aspera Connect (**Start Menu > All Programs > Aspera > Aspera Connect**) and open **Preferences** (**System Tray > Right-click Aspera Connect > Preferences**).

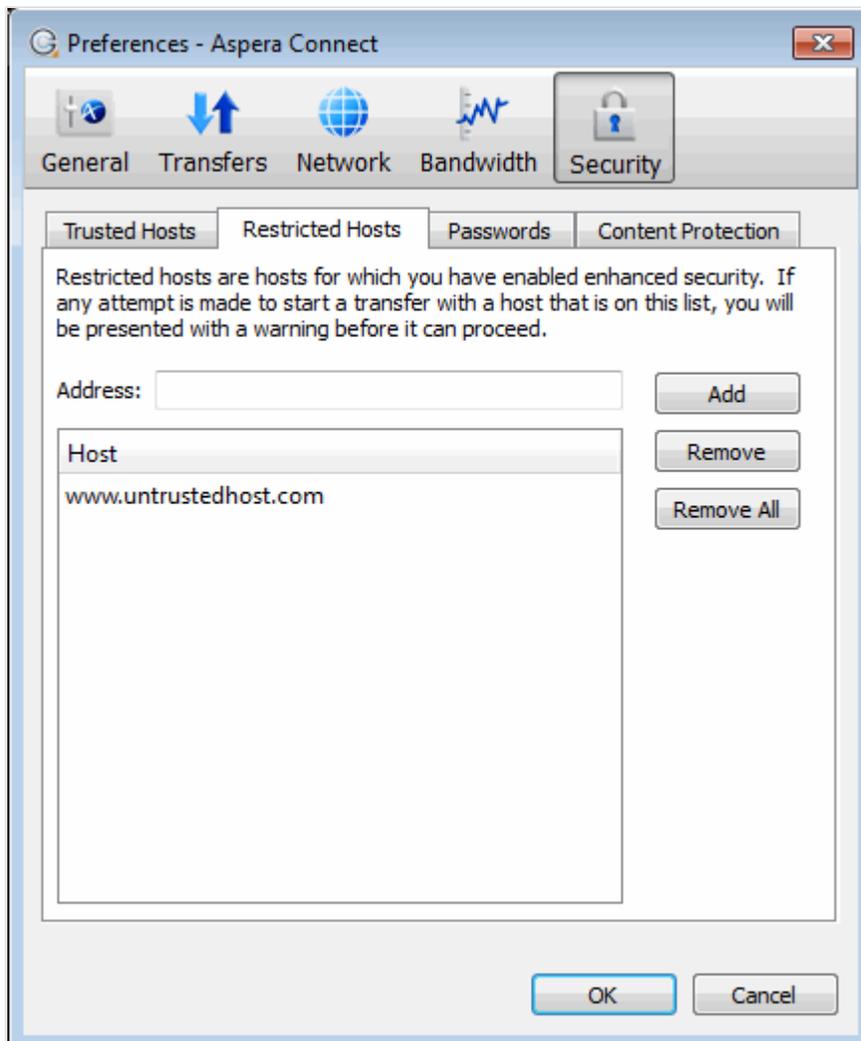
T ransfers	Ctrl+T
U nlock encrypted files	Ctrl+R
O pen log folder...	Ctrl+L
P references...	Ctrl+P
A bout...	Shift+F1
Q uit	

Managing Hosts

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

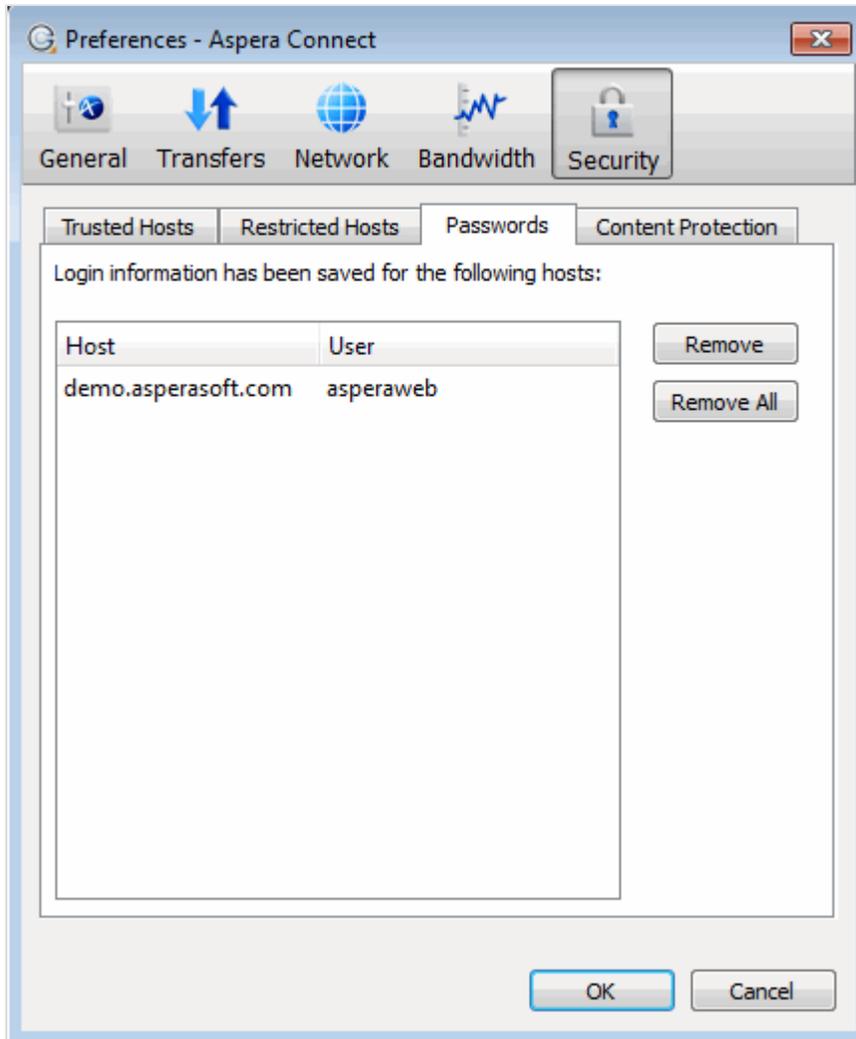


To view, add or remove restricted hosts, go to **Security > Restricted Hosts** . Here, enter the host's address in the specified text field and click **Add**.



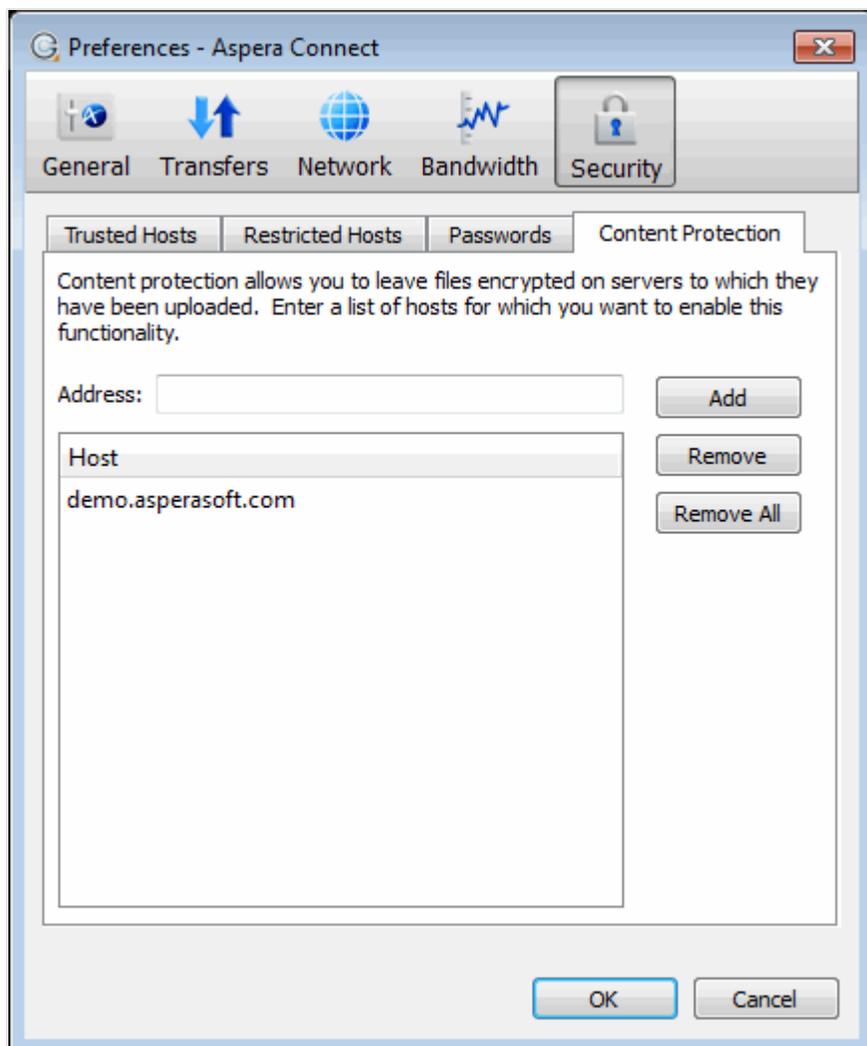
IMPORTANT NOTE: By adding a host to the restricted list, you will be required to provide confirmation every time you attempt to initiate a transfer with that host.

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



Content Protection

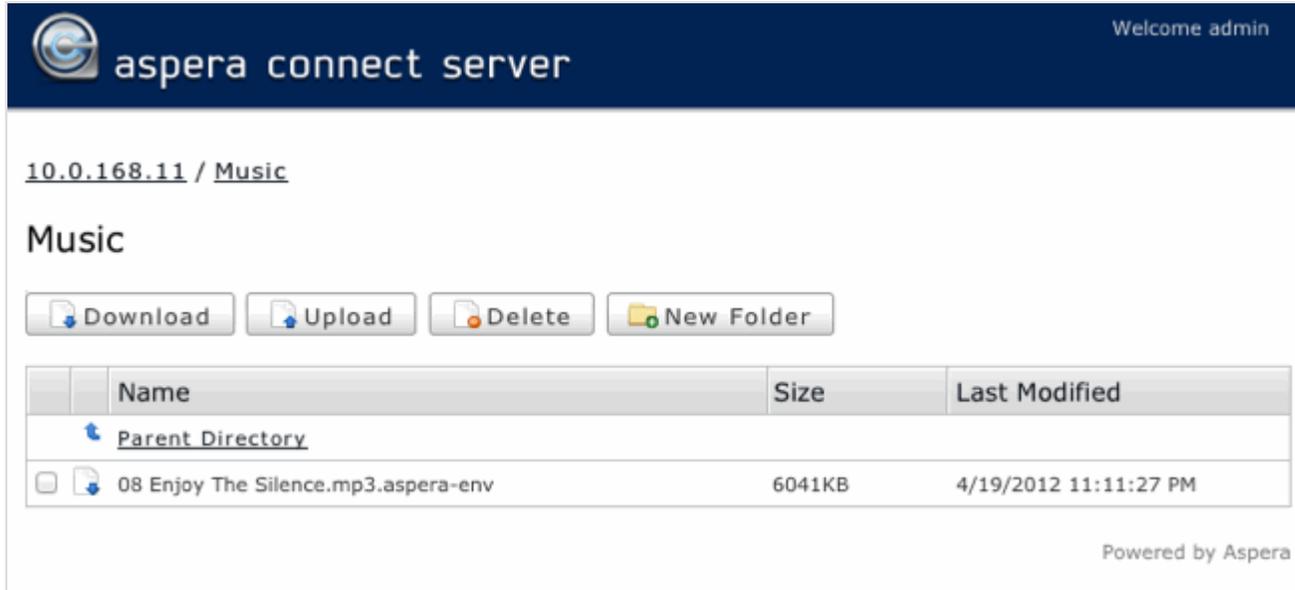
To add hosts that require uploaded files to be encrypted during a transfer, click the **Content Protection** tab under the **Security** option. Enter your Aspera server address in the Address text field and click **Add**. The server will be added to the host list.



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



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

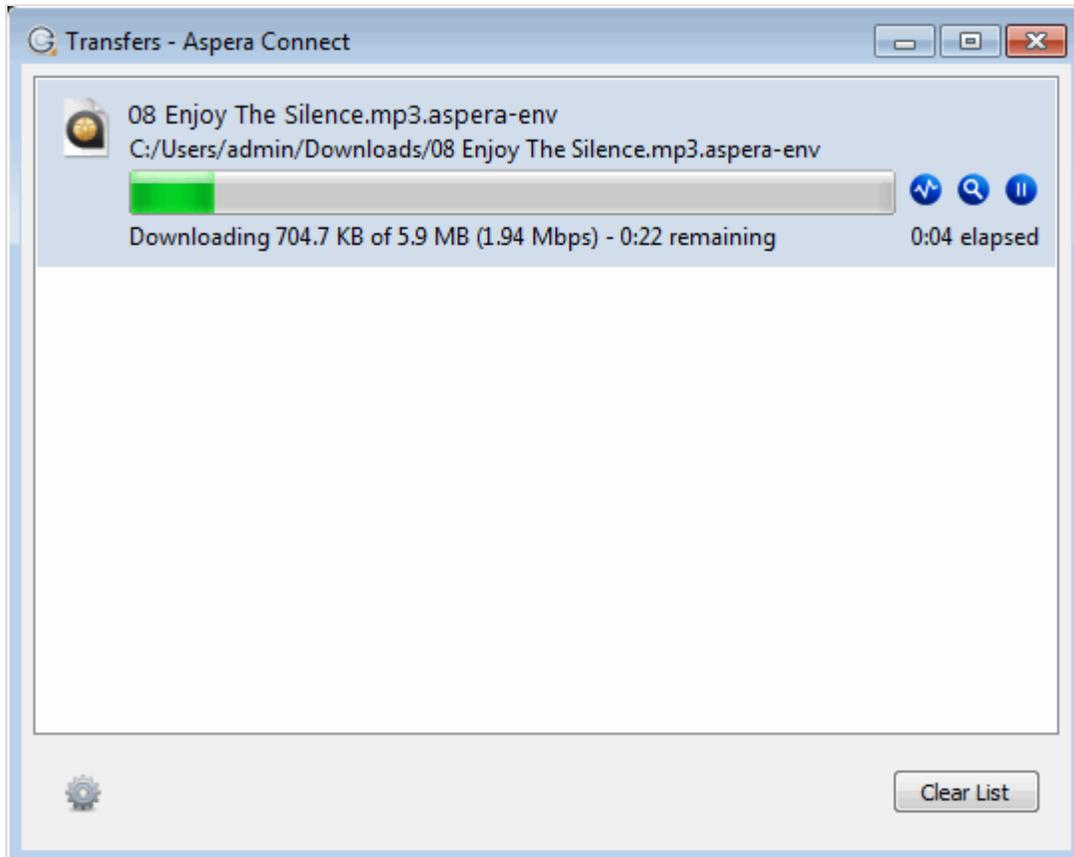


When using Aspera Connect to download a content-protected file, you have two decryption options.

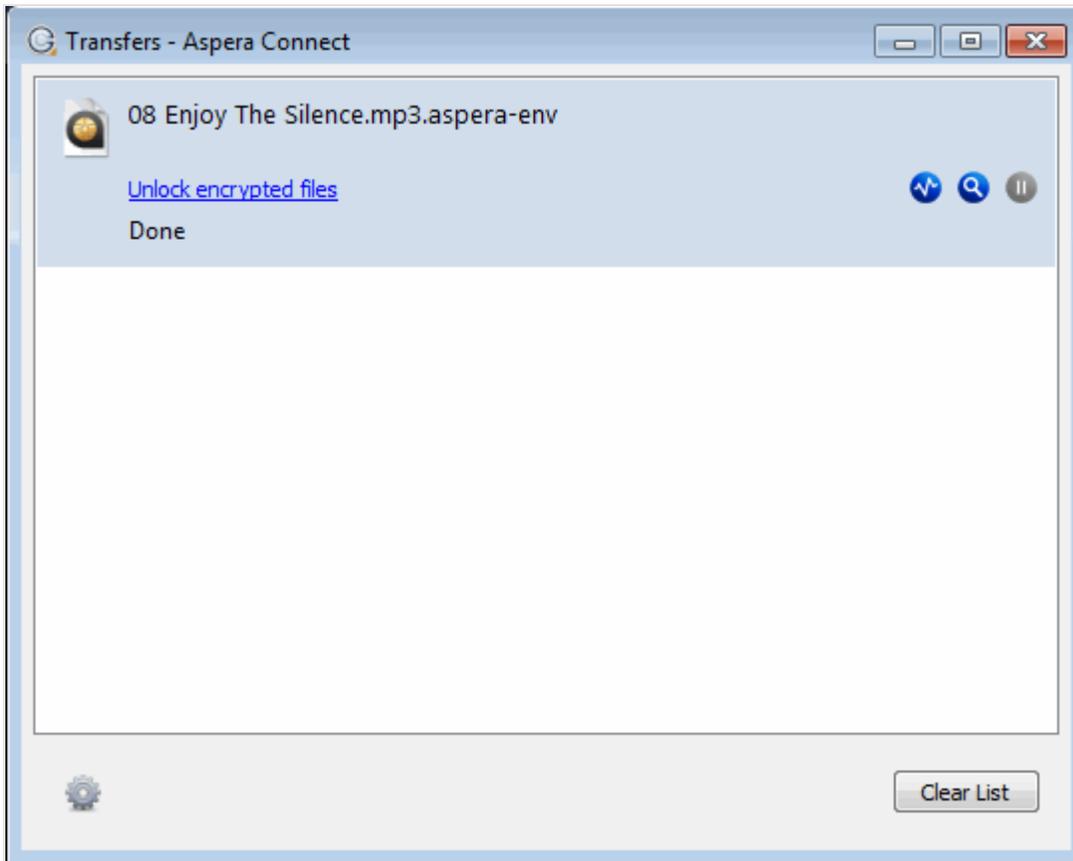
1. You can input and confirm your passphrase to decrypt the files *during* the download.
2. OR, you can enable the Keep downloaded file encrypted checkbox to download the content-protected files, and decrypt the files *after* the download has completed. When you select this option, you don't need to input your passphrase into the dialog box; however, you will need to take additional steps to decrypt the files on your local computer. Please refer to the topic "[Decrypting Local Files](#)" for details.



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



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



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

T ransfers	Ctrl+T
<u>U</u> nlock encrypted files	Ctrl+R
<u>O</u> pen log folder...	Ctrl+L
<u>P</u> references...	Ctrl+P
<u>A</u> bout...	Shift+F1
<u>Q</u> uit	

For instructions on using the decryption utility, refer to the topic "[Decrypting Local Files](#)."

Connect Functionality

Transfer files using Aspera Connect.

Initiating a File Transfer

Testing and initiating file transfers with Aspera Connect.

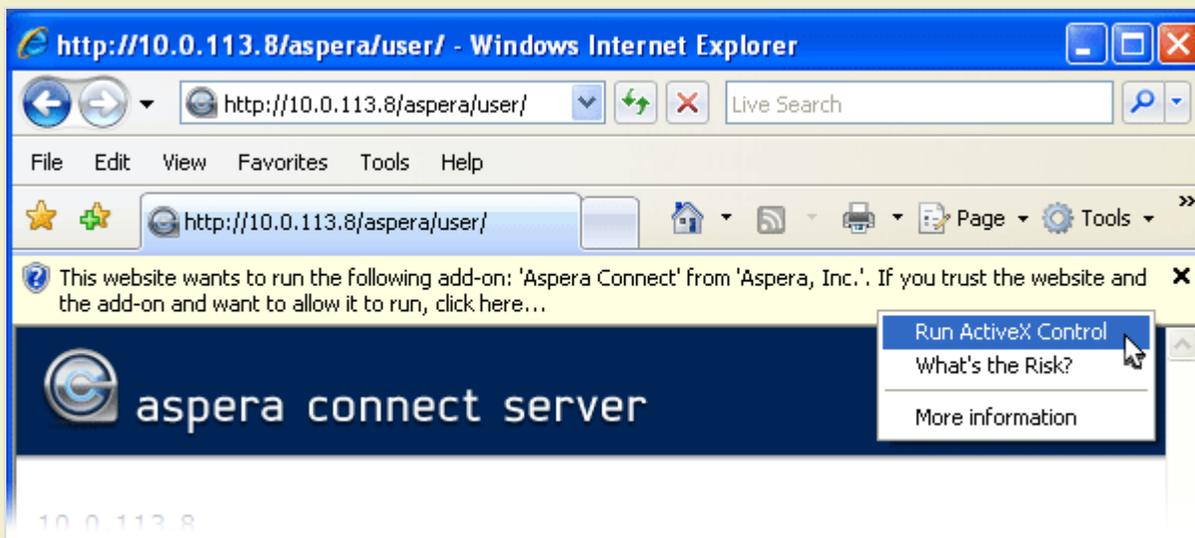
The following steps describe (1) how to perform a download test using Aspera's test server and (2) how to initiate a common file transfer using Aspera Connect.

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

Enter the following credentials when prompted:

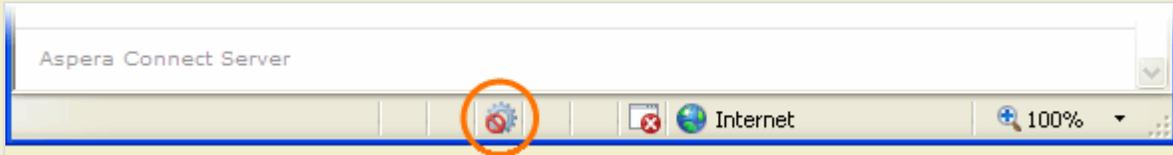
- **User:** asperaweb
- **Password:** demoaspera

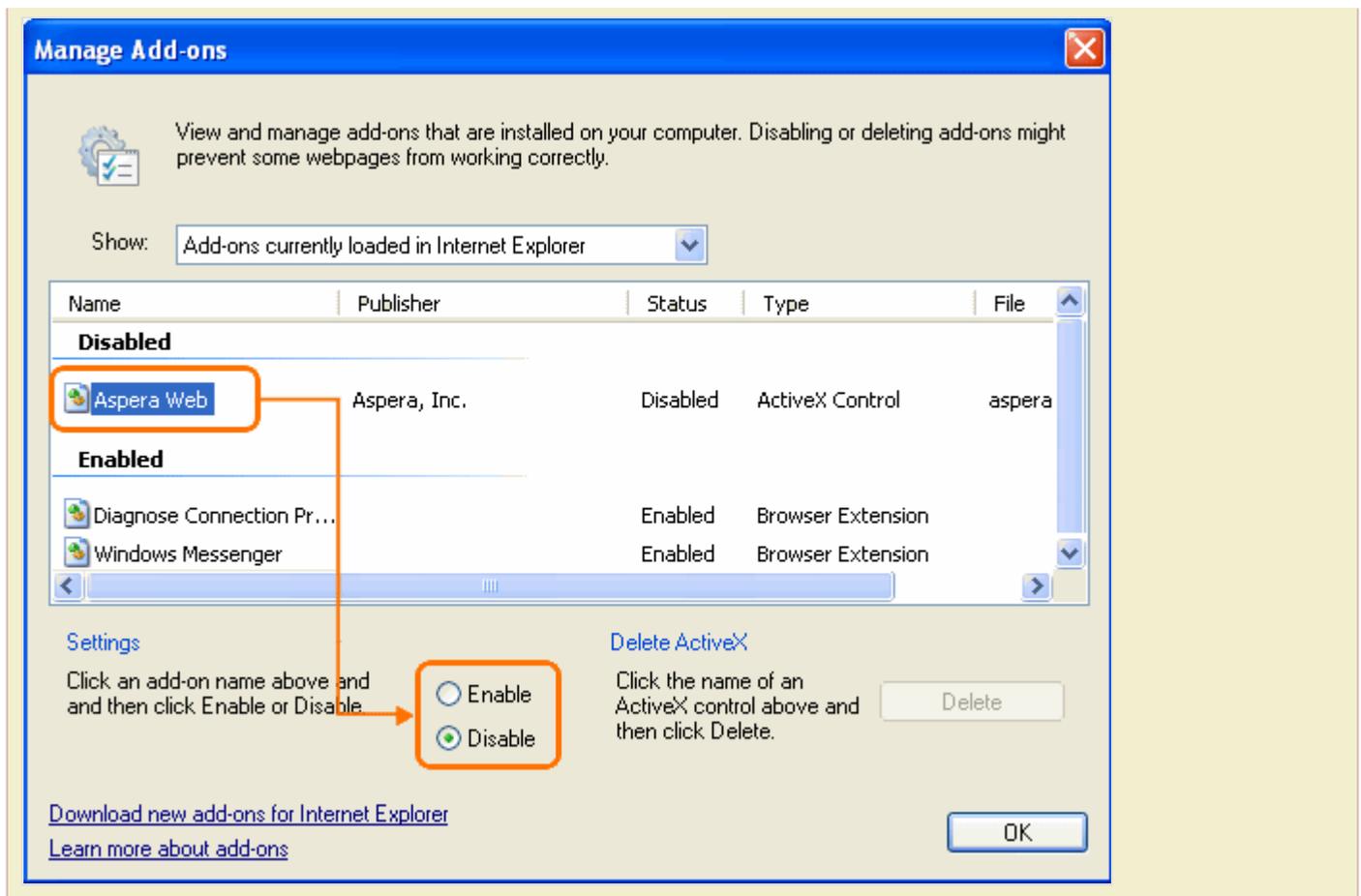
Internet Explorer 7 Security Settings: When opening a Connect Server or Faspex Server web page using Internet Explorer 7, the Information Bar will appear and ask for the permission to use the Aspera Connect add-on. Click the bar and select **Run ActiveX Control**, and then click **Run** in the *Security Warning* window.





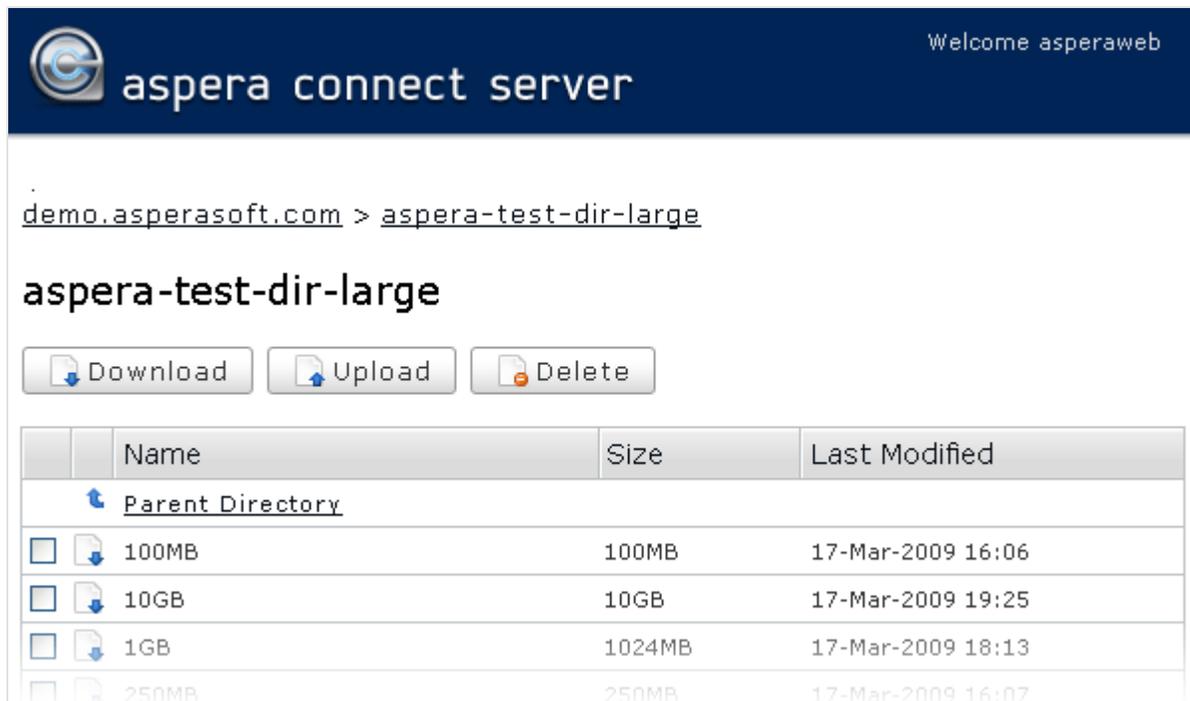
If you accidentally clicked **Don't Run**, then just click the gear icon at the bottom of the Aspera server web page to bring up the *Manage Add-Ons* window. Select **Aspera Web** and set **Enable** under *Settings*.





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

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



demo.asperasoft.com > aspera-test-dir-large

aspera-test-dir-large

Download Upload Delete

	Name	Size	Last Modified
	Parent Directory		
<input type="checkbox"/>	100MB	100MB	17-Mar-2009 16:06
<input type="checkbox"/>	10GB	10GB	17-Mar-2009 19:25
<input type="checkbox"/>	1GB	1024MB	17-Mar-2009 18:13
<input type="checkbox"/>	250MB	250MB	17-Mar-2009 16:07

3. Confirm the transfer.

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



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

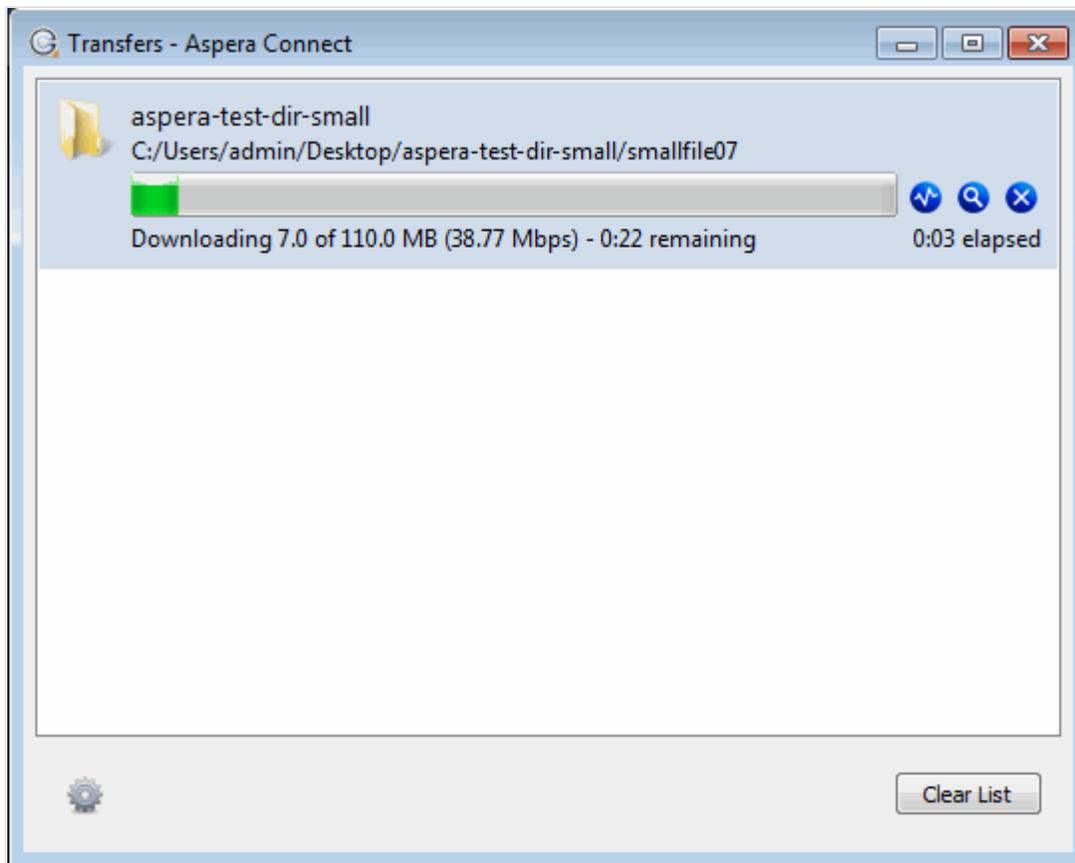
Note that when uploading, you should **avoid transferring files with the following characters** in the file name:

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

The Transfer Manager

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

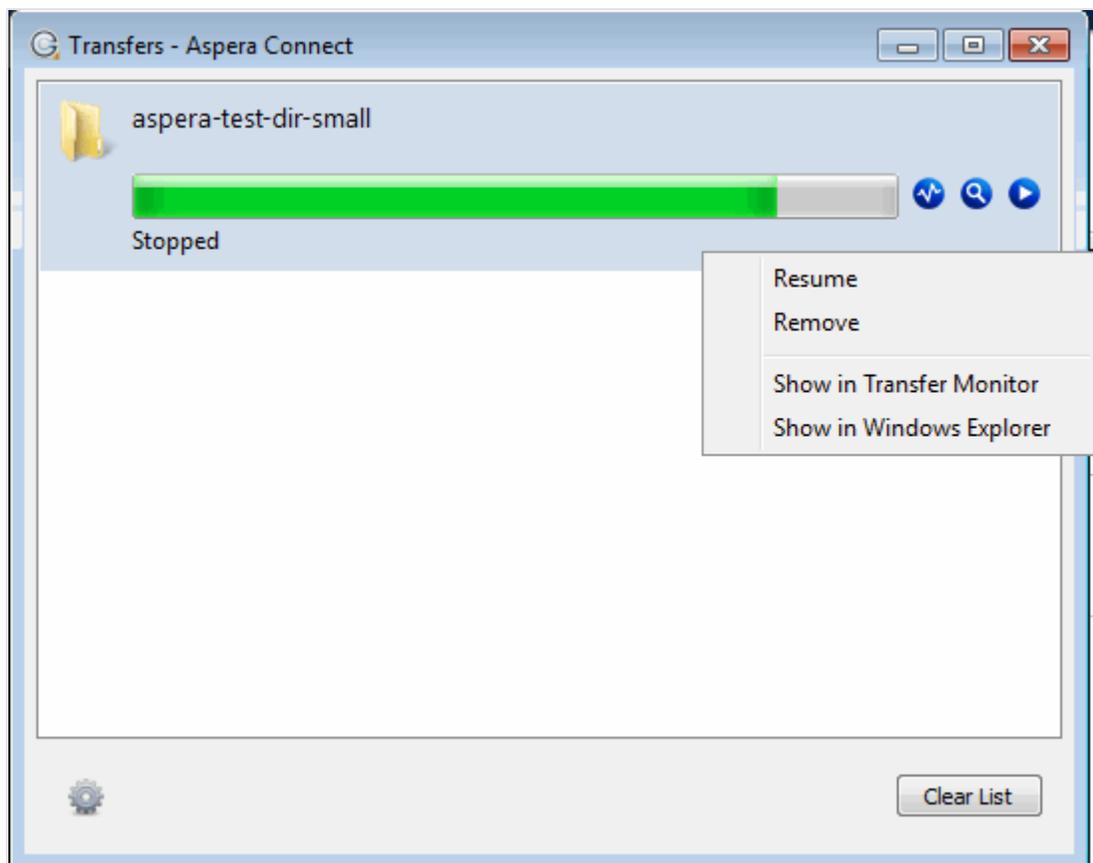
You may view and manage all transfer sessions within the Aspera Connect **Transfers** window.



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

-  Open the Transfer Monitor. For more information on using this feature, please refer to the topic "[Transfer Monitor](#)."
-  Reveal the file on your computer.
-  Stop the transfer session.
-  Resume transfer.
-  Retry a failed transfer.

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



Monitoring Transfers

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

Field	Value
Transfer progress bar	Adjust the file transfer speed by clicking and sliding the transfer progress bar.
	Click to view the destination folder of the transferred files.
	Click to stop the transfer session.
Transfer policy:	Select the transfer policy from the drop-down list: <ul style="list-style-type: none"> • Fixed • High • Fair • Low

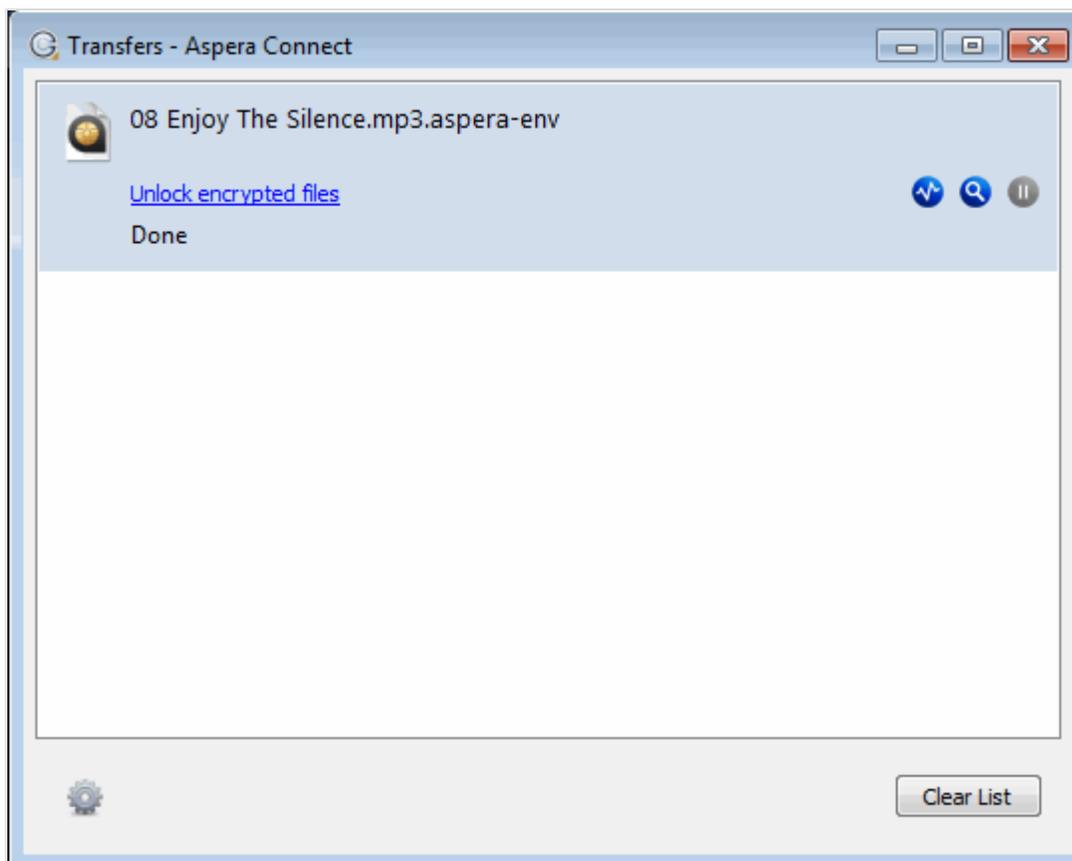
Field	Value
	<ul style="list-style-type: none"> • The transfer attempts to transmit data at a rate equal to the target rate. If network conditions do not permit that, it transfers at a rate lower than the target rate, but not less than the minimum rate. • The transfer rate is less aggressive than Fair when sharing bandwidth with other network traffic. When congestion occurs, the transfer rate is decreased to the minimum rate, until other traffic retreats.

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

Decrypting Local Files

Decrypt content-protected files on your local system.

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



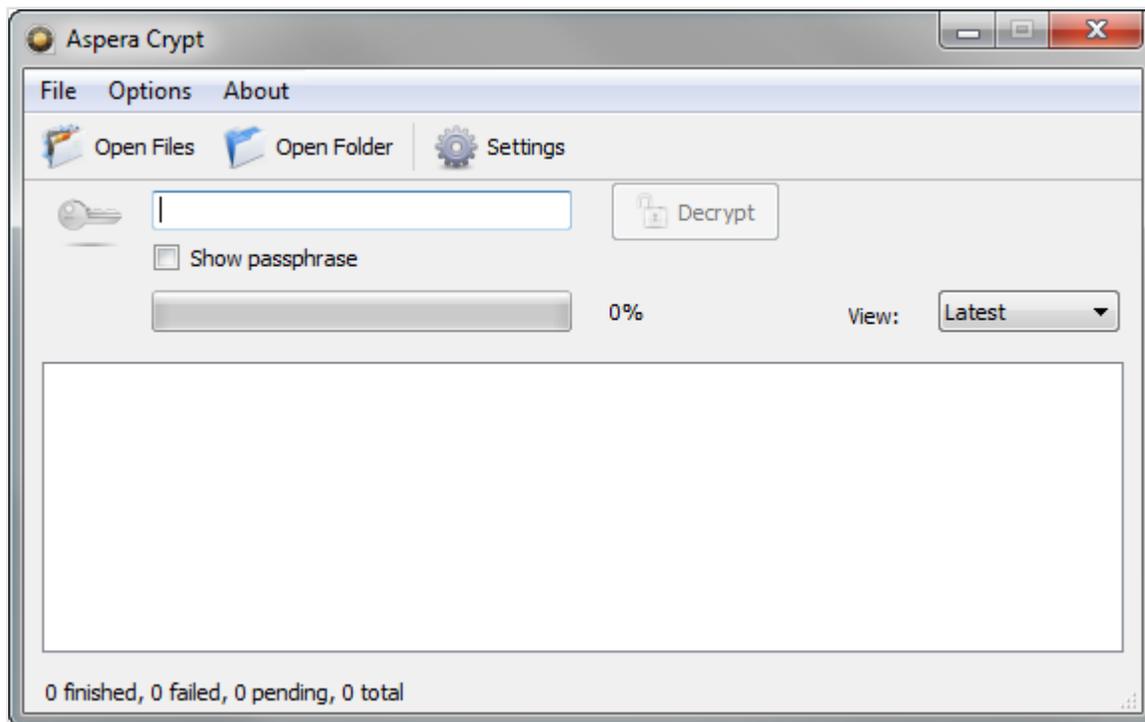
Note that when encrypted items have been downloaded to your computer, they will display the extension *aspera-env* (Aspera Security Envelope). You may also access this utility by going to **System Tray > Right-click Aspera Connect > Unlock encrypted files** .

T ransfers	Ctrl+T
<u>U</u> nlock encrypted files	Ctrl+R
<u>O</u> pen log folder...	Ctrl+L
<u>P</u> references...	Ctrl+P
<u>A</u> bout...	Shift+F1
<u>Q</u> uit	

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

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

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



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

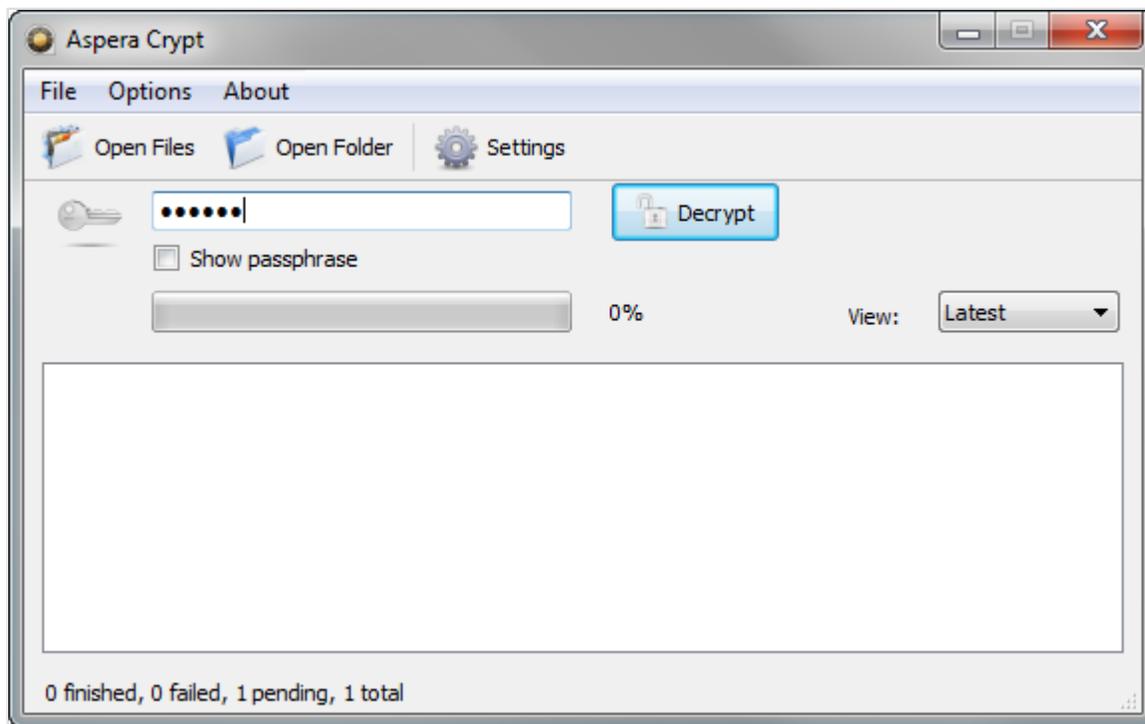
2. Adjust settings, if needed.

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

- **Delete encrypted files when finished (checkbox):** When enabled (i.e., checked), Aspera Crypt will remove the encrypted files from your system after the destination (decrypted) content has been created.
- **Number of concurrent threads for decryption (drop-down list):** Select from 1 (default), 2, 4 and 8, which determines the number of threads that are being decrypted at any given time (i.e., queuing).

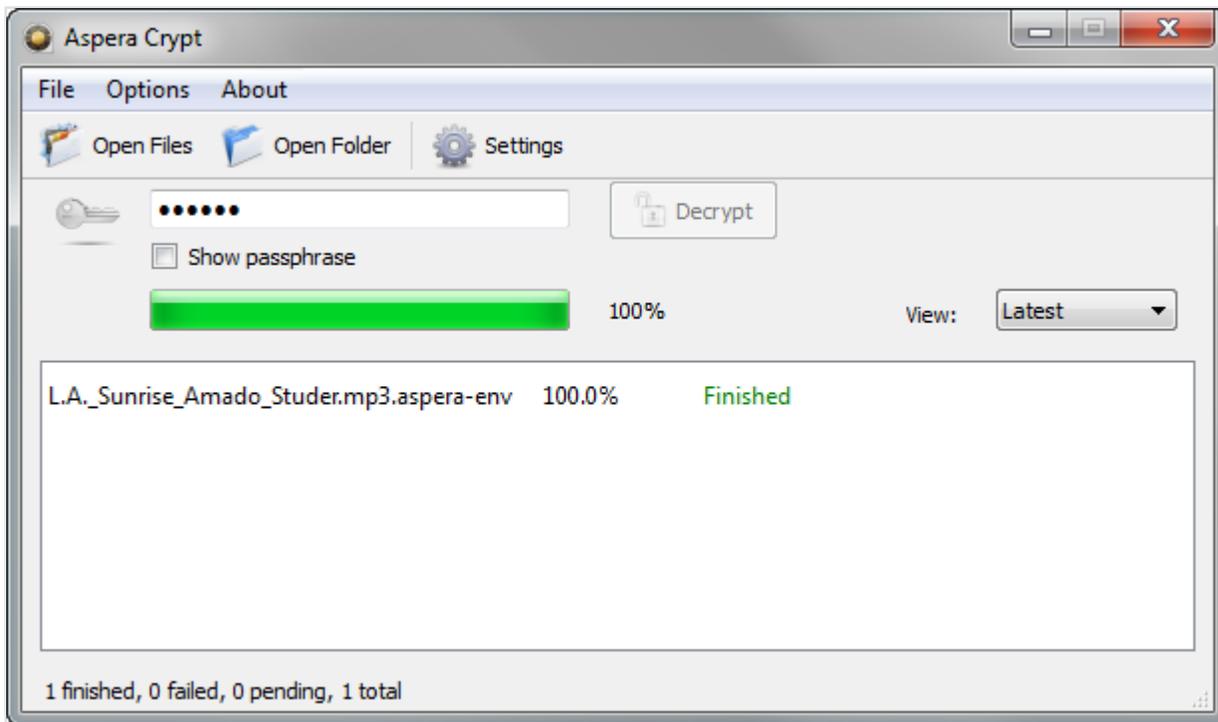
3. Input your passphrase and click the **Decrypt** button

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

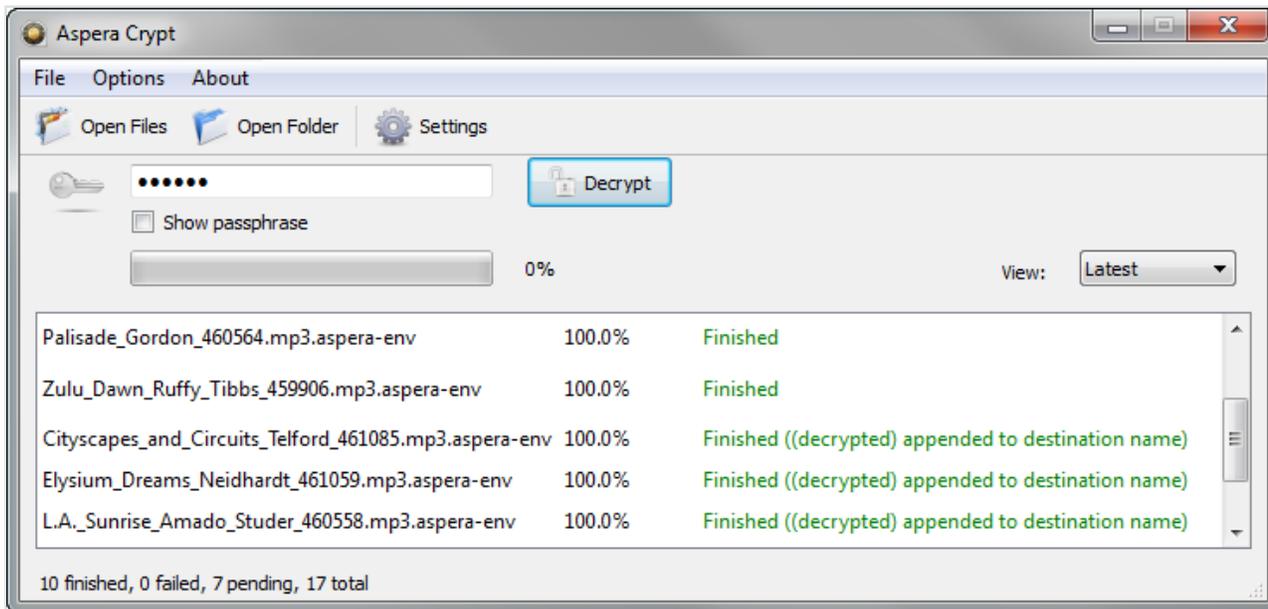


4. View output and confirm decryption

Once your file(s) have been successfully decrypted, you can view the output in the Aspera Crypt viewing window.



The decrypted contents will appear in the same directory as the original encrypted contents. Note that “(decrypted)” is added to the file name any time the decrypted file (without the *.aspera-env* extension) already exists in the same folder.



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

Uninstalling

Remove Aspera Connect from your computer.

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

To uninstall Aspera Connect, quit both the Aspera Connect application and any open web browsers. Additionally, ensure that no other users are logged into this machine. Then, go to the Windows **Control Panel** and--depending on the version of your Windows operating system--choose **Add/Remove Programs** or **Programs and Features**. Select **Aspera Connect** and remove it.

Appendix

Log Files

Locate Aspera Connect's log files.

Log Files

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

Log File Location

Log files are located in the following directory:

Operating System	Log File Location
Windows XP and 2003	C:\Documents and Settings\ <username>\Local Settings\Application Data\Aspera\Aspera Connect\var\log\</username>
Windows Vista, 2008 and 7	C:\Users\ <username>\AppData\Local\Aspera\Aspera Connect\var\log\</username>

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

T ransfers	Ctrl+T
U nlock encrypted files	Ctrl+R
O pen log folder...	Ctrl+L
P references...	Ctrl+P
A bout...	Shift+F1
Q uit	

For information on removing old log files, please refer to the topic "[File Clean-up](#)."

Plugin Locations

System locations for the Connect and Web Installer plugins.

Connect Plugin Location

Installation Type	Connect Plugin Location
User	%LOCALAPPDATA%\Programs\Aspera\Aspera Connect\lib
System	%PROGRAMFILES%\Aspera\Aspera Connect\lib

Web Installer Plugin Locations

Browser	Web Installer Plugin Location
Chrome	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions \aljbeaimggdioicepilc jnkphjobddok
Firefox	%APPDATA%\Mozilla\Firefox\Profiles*.default\extensions \awi@asperasoft.com
Internet Explorer	Depending on your version of Windows and UAC settings, the plugin will be located in one of the following directories: <ul style="list-style-type: none"> • C:\Windows\Downloaded Program Files • %LOCALAPPDATA%\Microsoft\Internet Explorer\Downloaded Program Files

File Clean-up

Manually remove old Aspera Connect folders and files.

After upgrading to or uninstalling this version of Aspera Connect, old Connect files can be safely removed from your system.

Log Files

Pre-Connect v2.8 Log Folders

Operating System	Pre-Connect v2.8 Log Folders
Windows XP and 2003	C:\Documents and Settings \<username>\Application Data\Aspera\Aspera Connect\var\log
Windows Vista, 2008 and 7	C:\Users\<username>\AppData\Local\Programs \Aspera\Aspera Connect\var\log\
All 32-bit Windows versions	C:\Program Files\Aspera\Aspera Connect\var \log\
All 64-bit Windows versions	C:\Program Files (x86)\Aspera\Aspera Connect\var\log\

Connect v2.8 Log Folders (only remove after uninstalling Connect v2.8!)

Operating System	Log File Location
Windows XP and 2003	C:\Documents and Settings\ <username>\Local Settings\Application Data\Aspera\Aspera Connect\var\log\</username>
Windows Vista, 2008 and 7	C:\Users\ <username>\AppData\Local\Aspera\Aspera Connect\var\log\</username>

http.uri and process.pid Files

You may remove the `http.uri` and `process.pid` files in the following folder:

```
C:\Users\\AppData\Roaming\Aspera\Aspera Connect\var\run\
```

Database File

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

```
C:\Users\\.aspera\connect\
```

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

Miscellaneous Files and Folders

```
C:\Users\\AppData\Local\Aspera\connect-cleanup.log
C:\Users\\AppData\Roaming\Aspera\
```

Troubleshooting

Web Installation is Blocked in IE7

You receive an error that Windows has blocked the Web installation because the browser can't verify the publisher.

If you have received an error during a Web installation of Aspera Connect that states "Windows has blocked this software because it can't verify the publisher," it may be the result of a partially downloaded `npinstallhelper.cab` file. To address this issue, you need to clear your browser's cache. Follow the instructions below.

1. From the **Tools** menu in the upper right, select **Internet Options**.
2. Under "**Browsing history**", click **Delete....**
3. To delete your cache, click **Delete files....**
4. Click **Close**, and then click **OK** to exit.
5. Refresh your browser.

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:

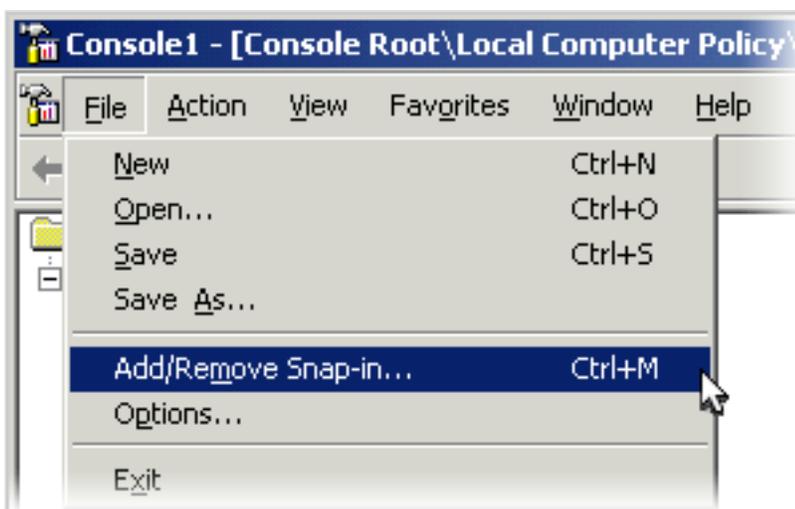
1. Launch the Microsoft Management Console (MMC)

Go to **Start menu > Run...** and enter `mmc`, click **OK** to launch it.

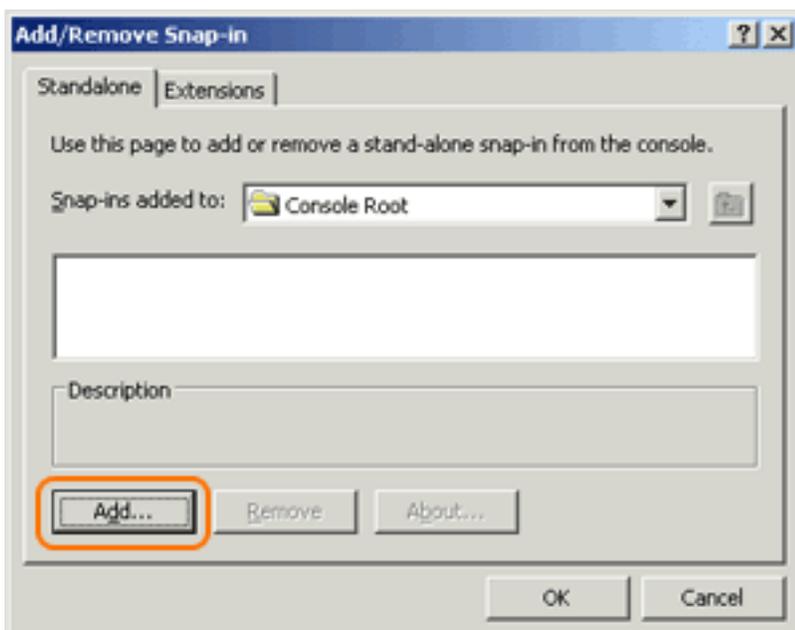


2. Add the Group Policy Object Editor Snap-in

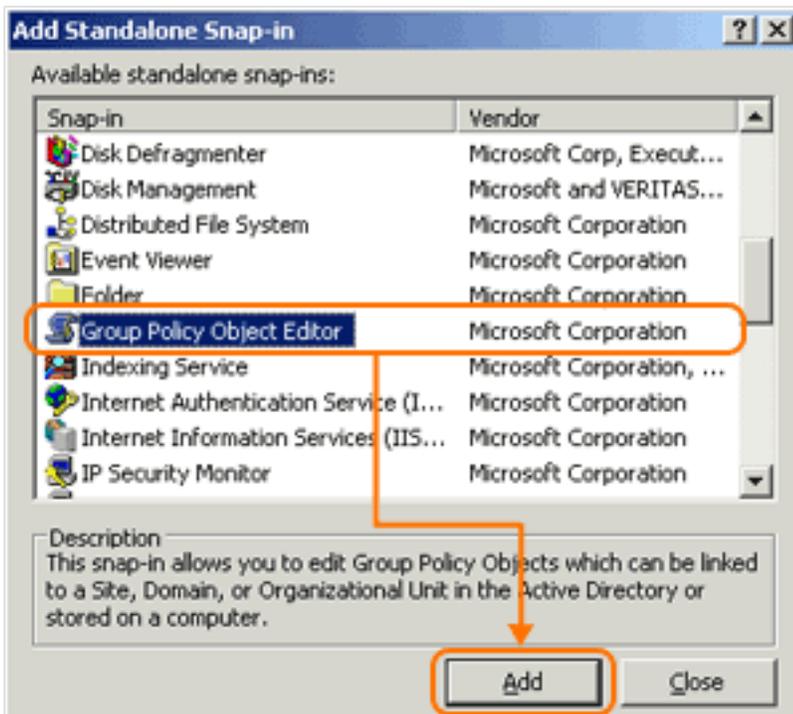
In the MMC, go to **File** in the toolbar and select **Add/Remove Snap-in...**



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



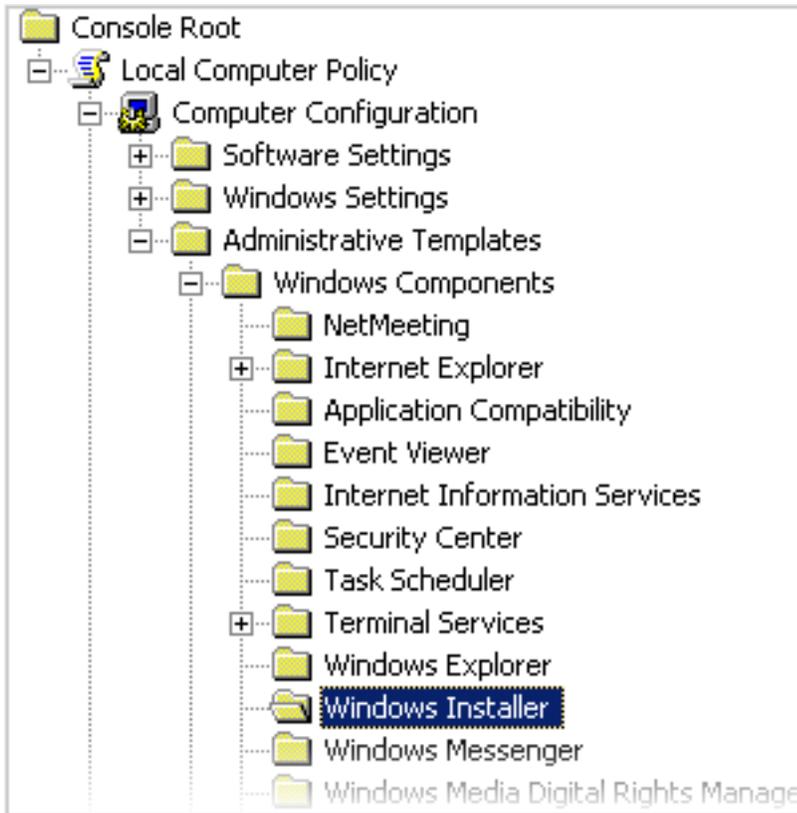
Select the **Group Policy Object Editor** and click **Add**.



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

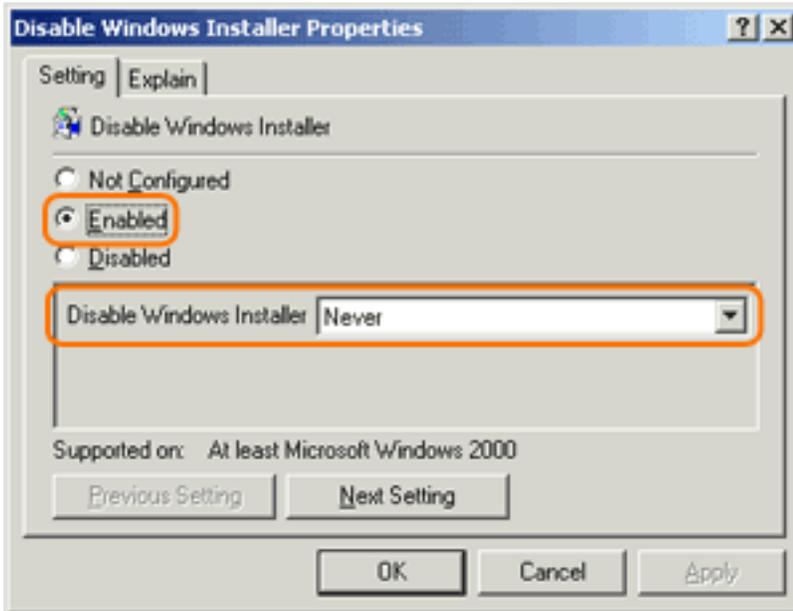
In the MMC, navigate into **Console Root > Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Installer**.



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
```

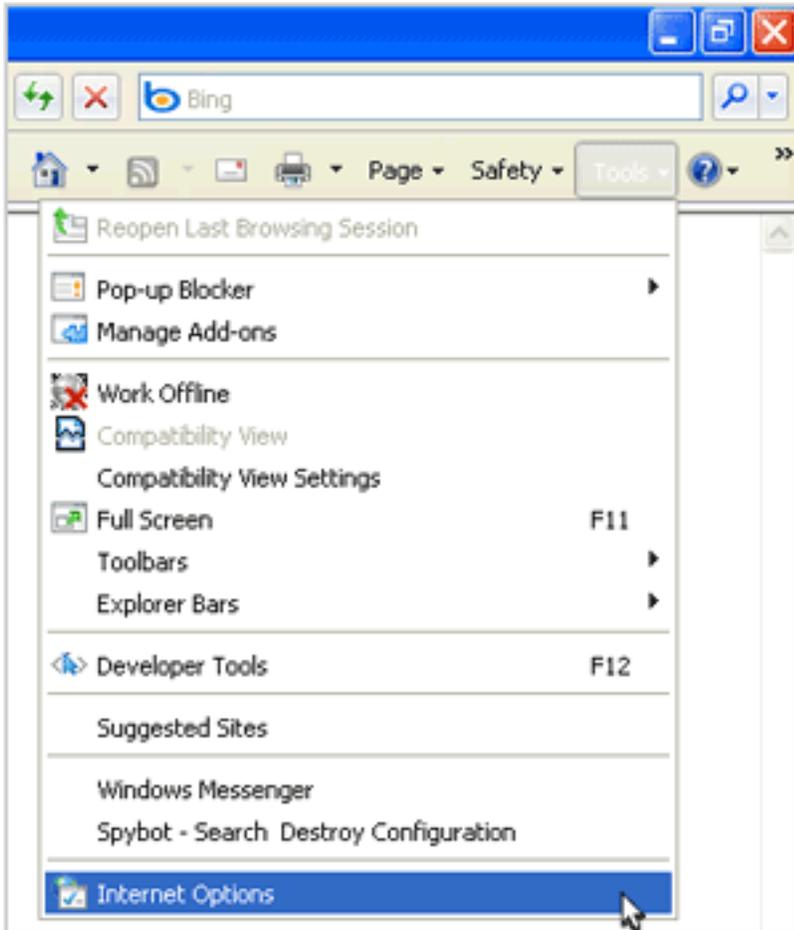
Missing Install Button on Windows Server

Aspera Connect's "Install" button doesn't appear correctly.

On Windows Server 2003 SP2 and Windows Server 2008, Aspera Connect's install button *may not* appear on your host's web interface. This problem may be due to additional Internet Explorer (Version 8) security restrictions. To resolve this, follow the steps below.

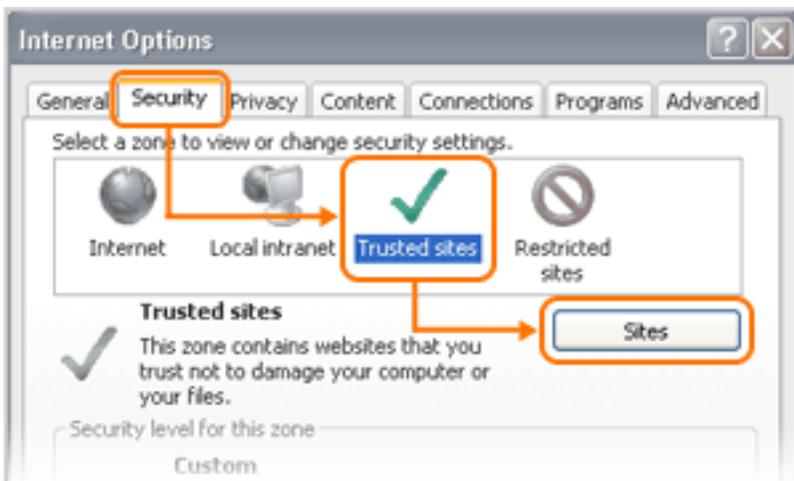
1. Launch Internet Explorer (version 8) and open **Internet Options**.

Launch Internet Explorer and go to **Tools > Internet Options** .



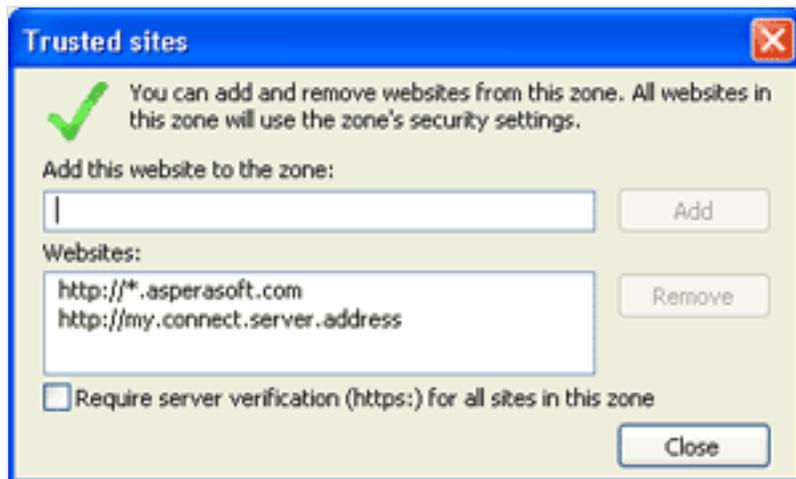
2. Add trusted sites.

In the *Internet Options* window, go to **Security > Trusted Sites** . Click **Sites** to open the *Trusted sites* window.



In the *Trusted sites* window, disable the option **Require server verification (https:)** for all sites in this zone and then add the websites below. Replace the `my.connect.server.address` with the address of the Aspera server that you are browsing:

- `http://*.asperasoft.com`
- `http://my.connect.server.address`



Troubleshooting Connectivity

Connectivity errors and potential solutions.

SSH Connectivity Errors

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

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

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

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

UDP Connectivity Errors

This section applies when Aspera Connect appears to successfully connect to the server; however, the transfer progress reads 0% and eventually the error "Data transfer timeout" is received (error codes 14, 15 or 18). Although the files to be transferred appear at the destination, they are 0 bytes in size. This is 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 Aspera 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	Refer to our Website .

Feedback

The Aspera Technical Publications department wants to hear from you on how Aspera can improve customer documentaion. To submit feedback about this guide, or any other Aspera product document, visit the [Aspera Product Documentation Feedback Forum](#).

Through this forum, you can let us know if you find content that is not clear or appears incorrect. Aspera also invites you to submit ideas for new topics, and what we can do to improve the documentation for easier reading and implementation. When visiting the Aspera Product Documentation Feedback Forum, 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

© 2014 Aspera, Inc., an IBM Company. All rights reserved.

Aspera, the Aspera logo, and *fasp* transfer technology, are trademarks of Aspera Inc., registered in the United States. Aspera Connect Server, Aspera Drive, Aspera Enterprise Server, Aspera Point-to-Point, Aspera Client, Aspera Connect, Aspera Cargo, Aspera Console, Aspera Orchestrator, Aspera Crypt, Aspera Shares, the Aspera Add-in for Microsoft Outlook, and Aspera *aspex* 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.