



Aspera Connect User Guide trunk

Windows

Revision: 149670 Generated: 10/24/2017 12:43

Contents

Introduction.....	3
System Requirements.....	4
Setting Up Connect.....	5
Part 1: Installation.....	5
Part 2: Network Environment.....	6
Part 3: Basic Configuration.....	11
Part 4: Security Configuration.....	14
Connect Functionality.....	22
Initiating a File Transfer.....	22
The Transfers Window.....	24
Monitoring Transfers.....	26
Decrypting Encrypted Files.....	27
Maintaining Your Connect Installation.....	31
Upgrading.....	31
Uninstalling.....	31
File Cleanup.....	31
Appendices.....	33
Log Files.....	33
Plug-In Locations.....	33
Troubleshooting.....	35
Web Installation is Blocked in IE7.....	35
Error When Installing with a Non-Admin Account.....	35
Missing Install Button on Windows Server.....	38
Connectivity Issues.....	40
Technical Support.....	41
Legal Notice.....	42

Introduction

Connect is an install-on-demand Web browser plug-in that facilitates high-speed uploads and downloads with an Aspera transfer server.

Depending on your operating system, Connect is compatible with most standard browsers. It integrates all of Aspera's high-performance transport technology in a small, easy-to-use package that provides unequalled control over transfer parameters. Connect includes the following features:

Feature	Description
FASP file transport	High-performance transport technology.
Browser plugin	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	The Web browser can be closed during transfer operations.
Transfer monitor	A built-in transfer monitor for visual rate control and monitoring.
HTTP fallback	HTTP fallback mode for highly restrictive network environments.
Proxy support	HTTP fallback and FASP proxy settings.
Content protection	Password-protect files that are being transferred and stored on the remote server.
Queueing	Allow a fixed number of concurrent transfers and place the rest into a queue.

System Requirements

To install and run Connect, you must have the following software in place:

- Windows 7, 8 (see note below), or 10. Windows Server 2008r2 or 2012.
- Firefox 27-50, Google Chrome 32-55, Microsoft Edge (EdgeHTML versions 12.10240 and 13.10586), or Internet Explorer 8-11.



Warning: Connect does not support the 64-bit Internet Explorer 10 browser on Windows 8.

Drag-and-Drop Support

-->

When used with Faspex and some third-party web applications, Connect supports the dragging and dropping of files and folders for transfer; but this support varies by platform and browser. See the table below for details on how this release of Connect supports drag-and-drop in your environment:

Browser	Drag-and-Drop of Files	Drag-and-Drop of Folders
Firefox	Supported	Supported
Chrome	Supported	Supported
Internet Explorer*	Supported	Not supported
Edge*	Not supported	Not supported

* Internet Explorer is limited in support for drag-and-drop because of how it records drop events. Edge does not support drag-and-drop from the system into the browser. For further information, see

<https://social.technet.microsoft.com/Forums/en-US/ec3c0be0-0834-4873-8e94-700e9df9c822/edge-browser-drag-and-drop-files-not-working?forum=ieitprocurrentver>

https://wpdev.uservoice.com/forums/257854-microsoft-edge-developer/suggestions/8964523-support-html5-drag-and-drop-of-files-from-explorer?page=1&per_page=20

Setting Up Connect

Part 1: Installation

This section explains the installation process for the IBM Aspera Connect Browser Plug-in on your system. Connect can be installed on your system through the Web installer or downloadable MSI. See the corresponding sections below.



Caution:

- You cannot install Connect under the **Guest** account.
- If you are installing Connect on a Windows 2003 or Windows XP machine, you *must* upgrade your system 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 uninstallation instructions, see [Uninstalling](#) on page 31.



Important: In order for Connect to function correctly, *you must have cookies enabled* within your browser. For instructions on verifying this setting, see the Help documentation for your browser.

The Connect Web Installer

1. Use your browser to navigate to your Aspera Web application (IBM Aspera Faspex, IBM Aspera Connect Server or IBM Aspera Shares).
2. Once you have reached the server's Web page, you 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 this button either launches the automatic installer or redirects you to the Connect download page (for [manual installation](#)).

3. Follow the on-screen instructions to complete the installation process.
4. If your browser displays a security prompt or warning, click **Allow** or **Continue** to proceed.

Note that for the following cases, a non-administrator 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: When installing the file **npinstallhelper.cab** (relevant only to the Web installation), ensure that you install it for the current user only, and not for all users on the system. Installing **npinstallhelper.cab** system-wide may cause the installation to fail.

The Connect Desktop Installer

You can download the Connect MSI directly from http://www.asperasoft.com/download_connect/. Once downloaded, close your Web browser and run the installer on your machine. You will need to accept the terms and conditions, as well as confirm where Connect should be installed. You can install the application in the standard location by clicking **Typical**, or you can select an alternative location.

After Installation

Once Connect has finished installing, you can open it from the following location:

Start Menu > All Programs > Aspera > Aspera Connect

Part 2: Network Environment

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

Network Requirements

Your SSH outbound connection may differ based on your organization's unique network settings. Although **TCP/22** is the default setting, consult your IT department for questions related to which SSH port(s) are open for file transfer. Also see the Help documentation for your particular operating system, for specific instructions on configuring your firewall. If your client host is behind a firewall that does not allow outbound connections, you must allow the following:

- Outbound connections for SSH, which is **TCP/22** by default, although the server side may run SSH on another port (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 (check with your IT department for questions related to which port(s) are open for FASP transfers).

Limit Transfer Rates

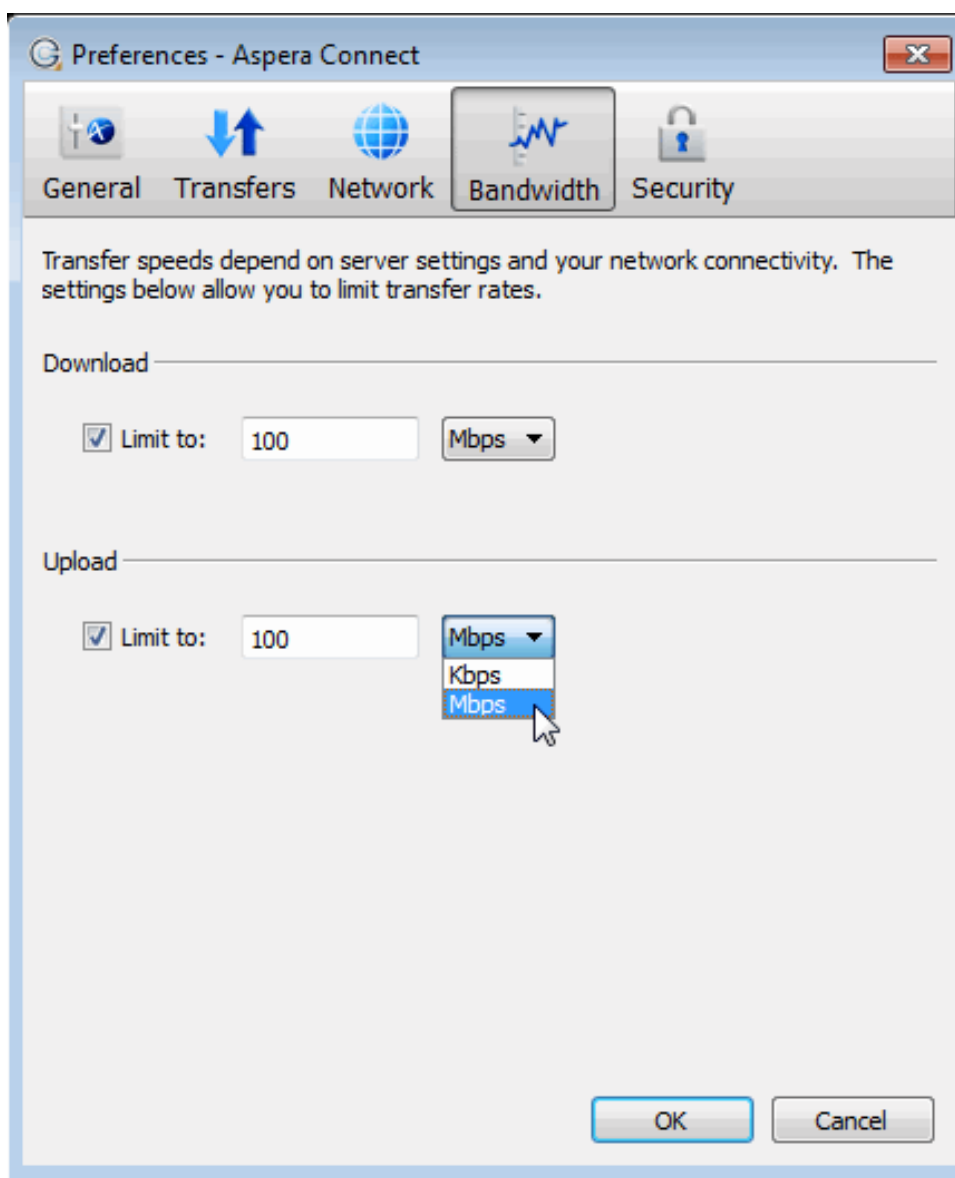


Important: Do not set any values in these fields unless you need to limit the bandwidth that Connect uses.

Launch Connect (**Start Menu > All Programs > Aspera > Aspera Connect** *home_directory* > **Applications > 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 Connect's transfer rates via the **Bandwidth** option.



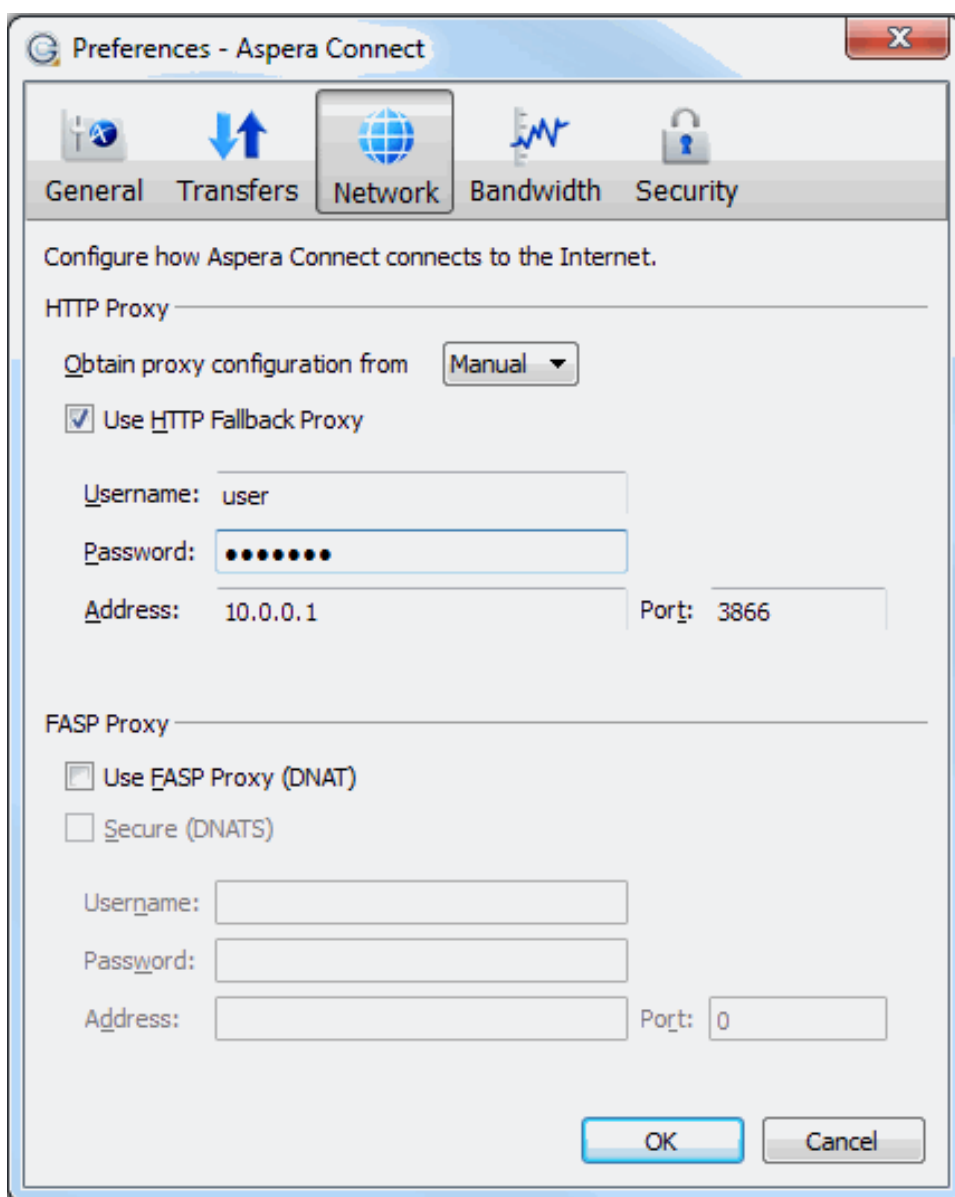
You can limit the download and upload transfer rates by enabling the respective checkboxes and entering a rate in either Mbps or Kbps. Note that your ability to limit these rates depends on the following factors:

- Your network's bandwidth: Available bandwidth on your network may limit your transfer rate, even if you enter larger numbers into these fields.
- Your Aspera server transfer settings: Settings on your server may limit your transfer rate even if your network bandwidth and the numbers you enter are larger.

HTTP Fallback Proxy

The HTTP fallback proxy should be used for fallback transfers only, *not* for FASP transfers.

To set up an HTTP fallback proxy, go to **Preferences > Network** in Connect.



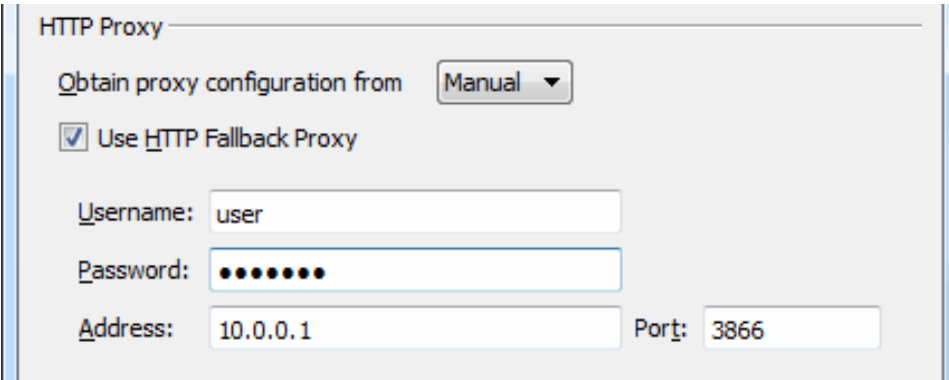
Under the **HTTP Proxy** section, you can modify the proxy configuration for the server handling HTTP fallback. HTTP fallback serves as a secondary transfer method when the Internet connectivity required for Aspera accelerated transfers (that is, UDP port 33001, by default) is unavailable. If UDP connectivity is lost or cannot be established, if you have configured an HTTP fallback proxy, 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** to have Connect use the HTTP fallback proxy settings that are configured for your operating system.
- **Manual** if you want to enter your HTTP fallback proxy settings manually (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.

Note that the **Use HTTP Fallback Proxy** checkbox and fields are enabled only if you select **Manual**.



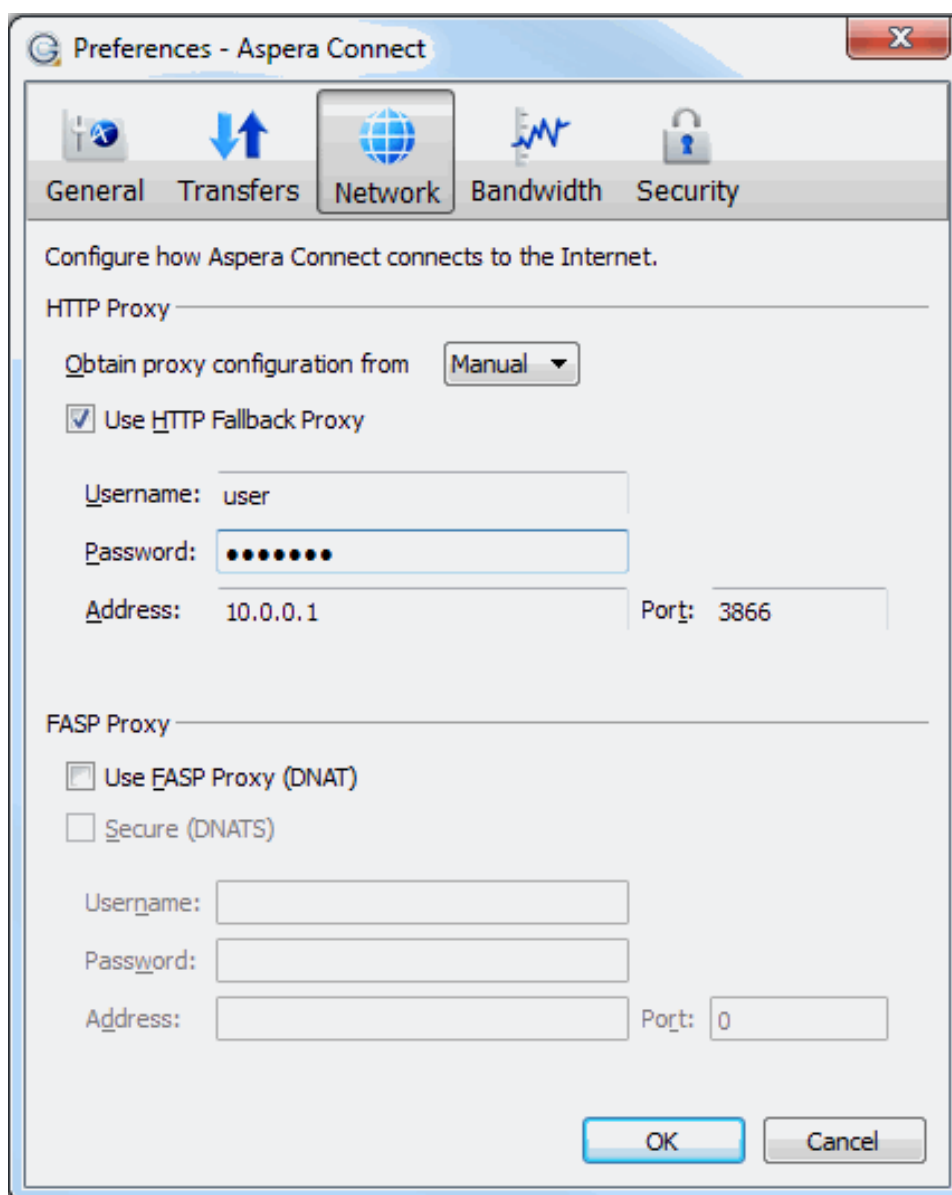
The screenshot shows the 'HTTP Proxy' configuration window. It has a title bar 'HTTP Proxy'. Below the title bar, there is a label 'Obtain proxy configuration from' followed by a dropdown menu set to 'Manual'. Below that is a checkbox labeled 'Use HTTP Fallback Proxy' which is checked. Further down are four input fields: 'Username:' with the text 'user', 'Password:' with masked characters (dots), 'Address:' with the text '10.0.0.1', and 'Port:' with the text '3866'.

FASP Proxy

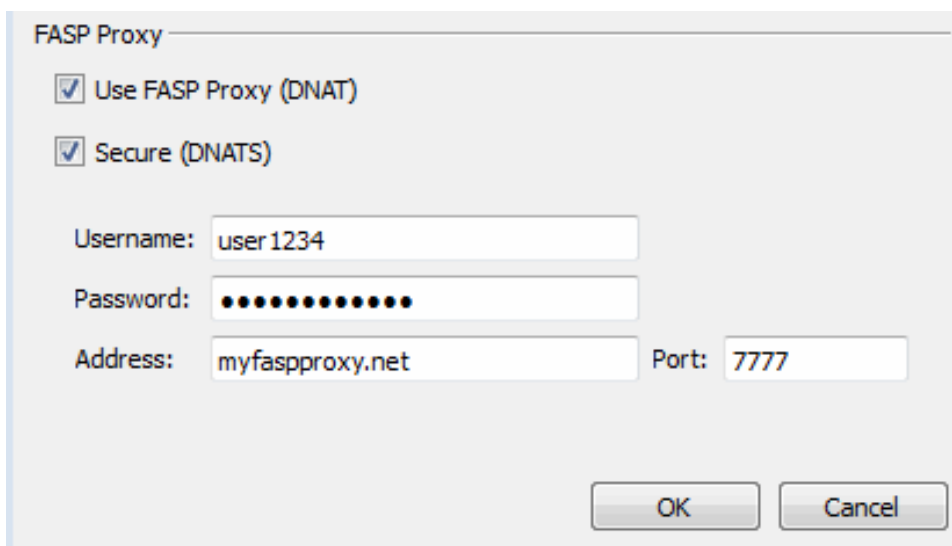
When FASP proxy is enabled, Aspera will pass the DNAT or DNATS (secure) username, server address, and port to **ascp**.

To set up a FASP proxy, do the following:

1. go to **Preferences > Network** in Connect.



2. Enable the following checkbox(es):
 - **Use FASP Proxy (DNAT)**
 - **Secure (DNATS)**
3. Enter your proxy server username, password, address and port number.



The image shows a 'FASP Proxy' configuration window. It has two checked checkboxes: 'Use FASP Proxy (DNAT)' and 'Secure (DNATS)'. Below these are four input fields: 'Username' with the text 'user1234', 'Password' with masked characters, 'Address' with 'myfaspproxy.net', and 'Port' with '7777'. At the bottom right are 'OK' and 'Cancel' buttons.

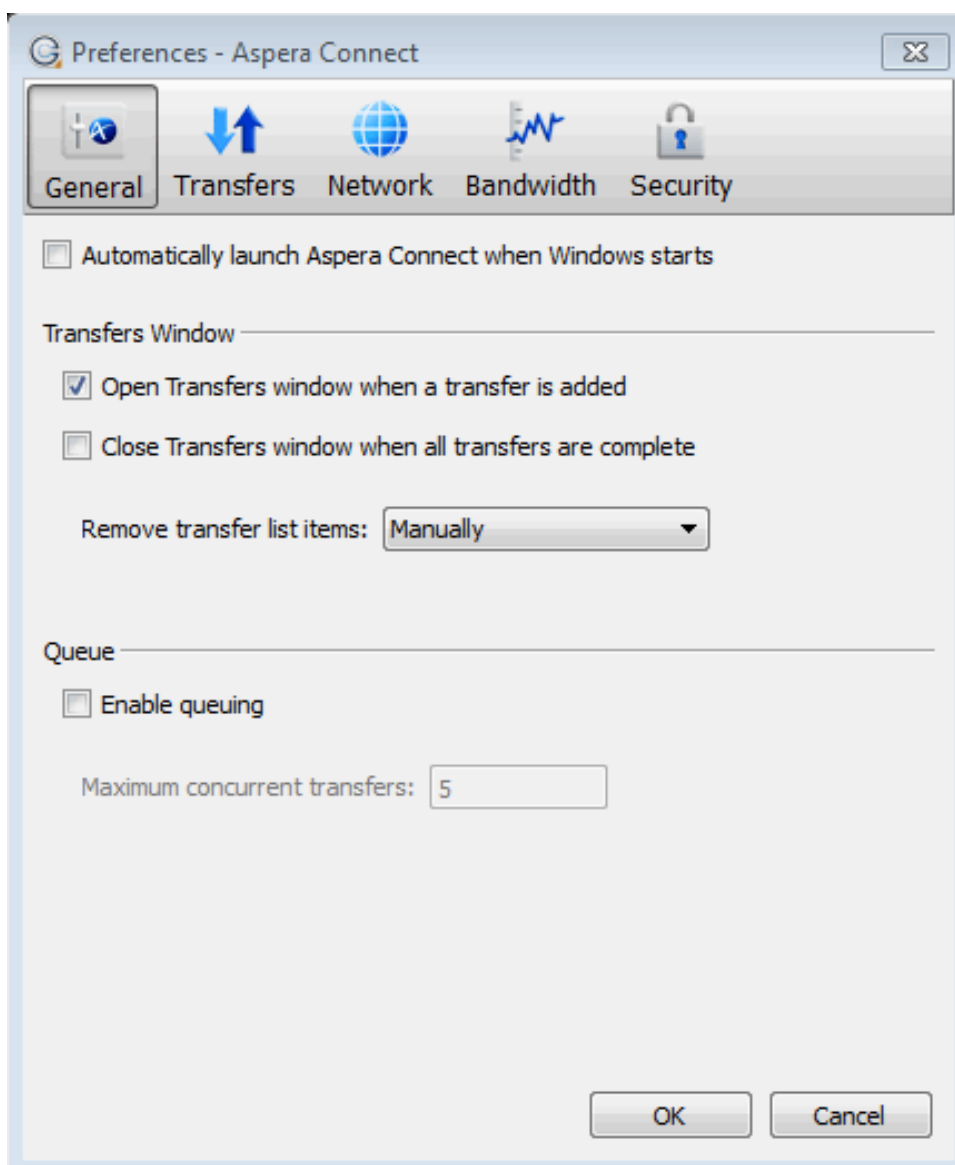
Part 3: Basic Configuration

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

<u>T</u>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	

General Preferences

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

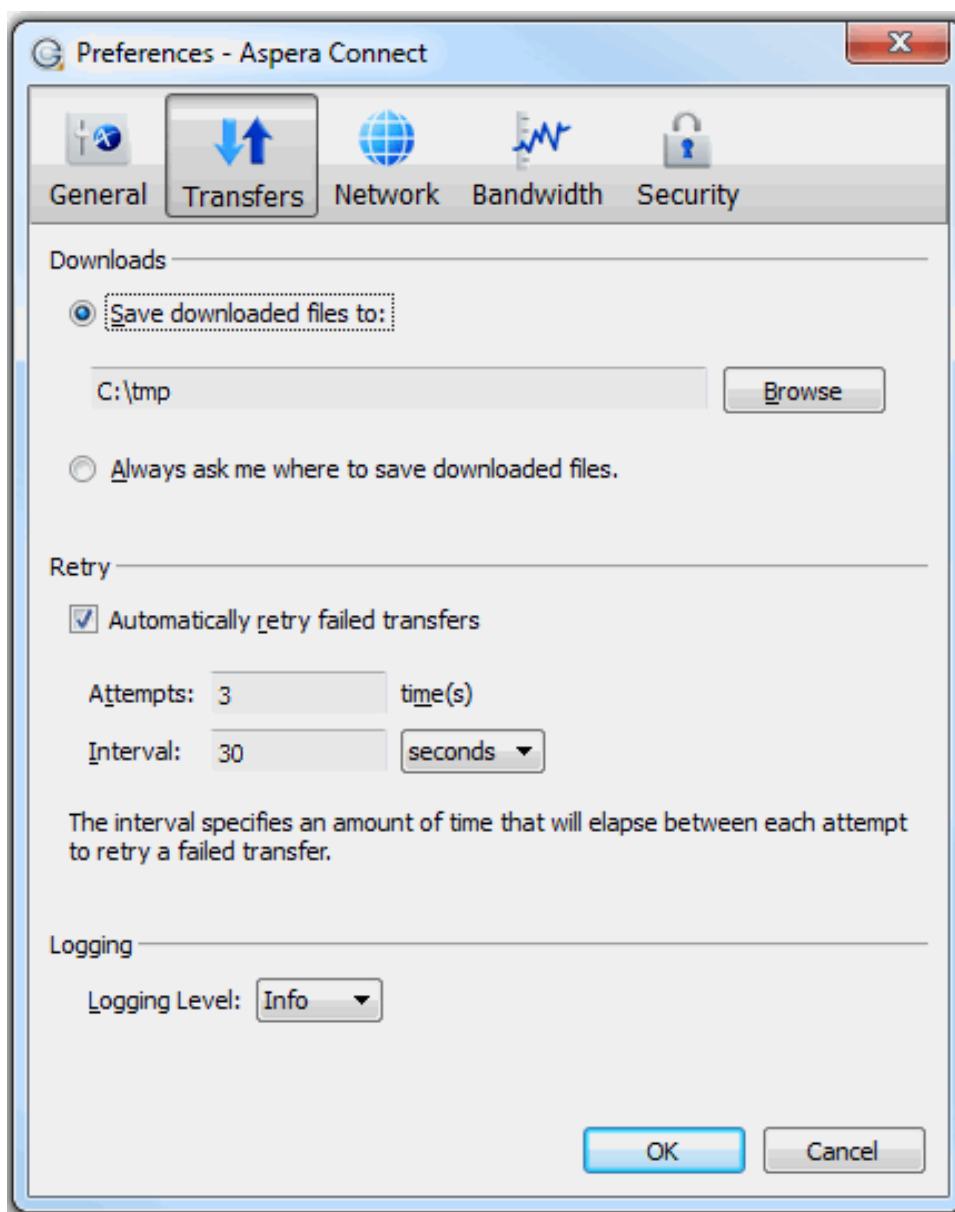


Under the **General** option, you can modify the following settings:

- Specify whether or not 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

Connect's transfer behavior can be configured under **Preferences > Transfers**.



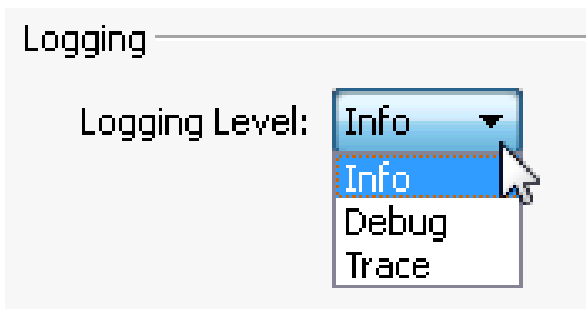
By default, Connect downloads files to the current user's **Downloads** folder. To change this setting, adjust the following settings:

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

IBM Aspera Connect Browser Plug-in features the following capabilities for minimizing security risks when uploading or downloading files:

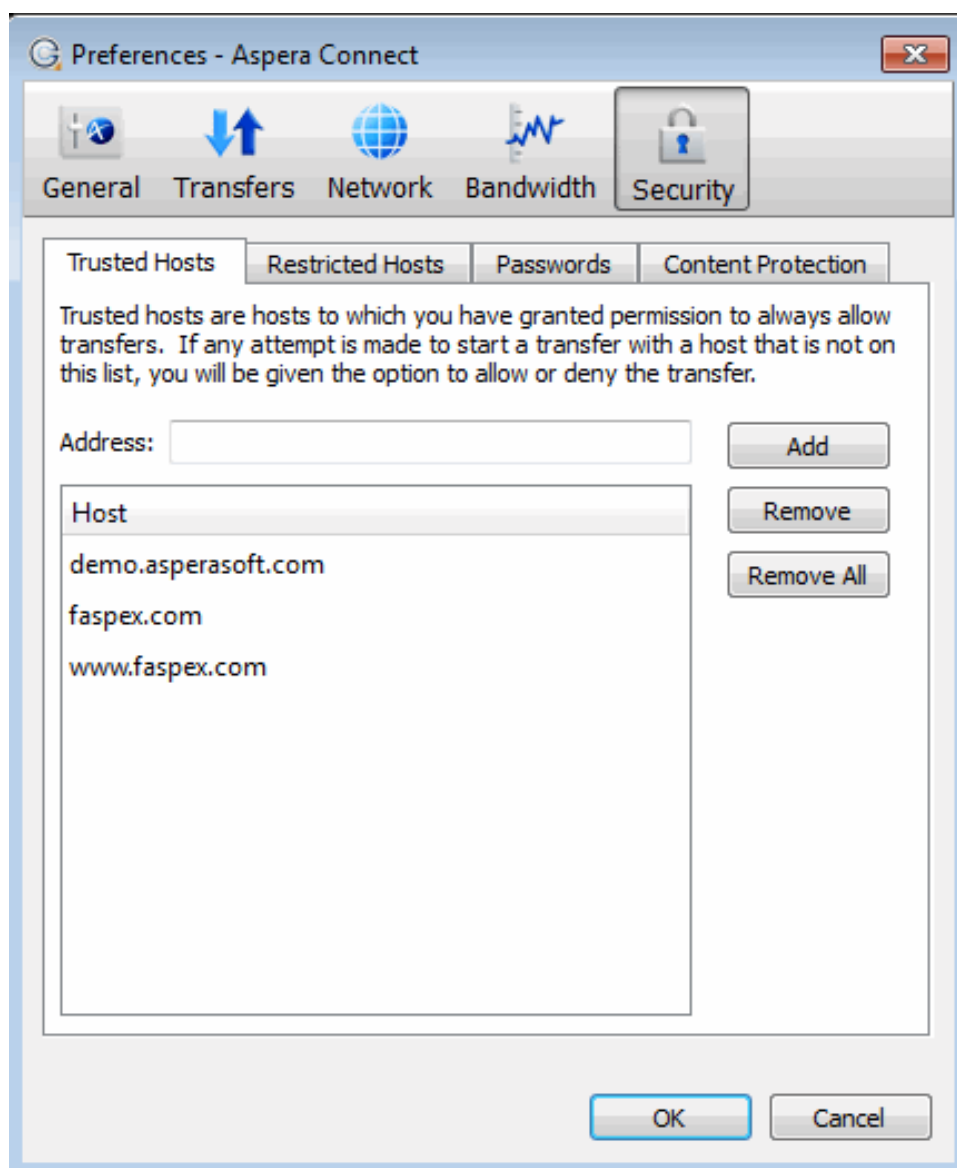
- You can add Aspera servers as **Trusted Hosts** to avoid the recurring security prompt, or add servers to the **Restricted Hosts** list to require confirmation every time you attempt to initiate a transfer with that host.
- You have the option of saving your authentication credentials when you connect 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 in the Connect **Preferences** dialog. To open the Connect **Preferences** dialog, launch Connect (**Start Menu > All Programs > Aspera > Aspera Connect**) and open **Preferences** (**System Tray > Right-click Aspera Connect > Preferences**).

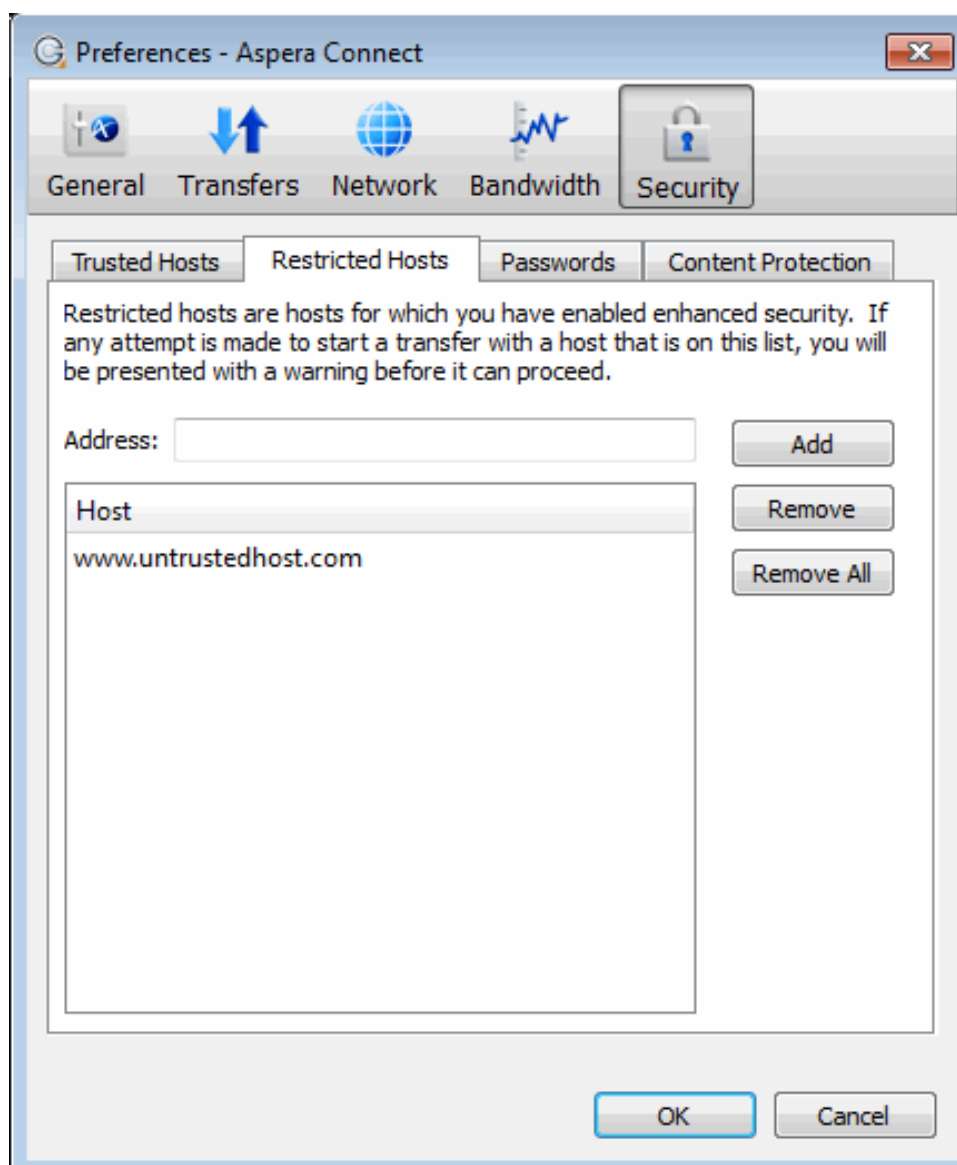
T ransfers	Ctrl+T
U nlock encrypted files	Ctrl+R
O pen log folder...	Ctrl+L
P references...	Ctrl+P
A bout...	Shift+F1
Q uit	


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**.

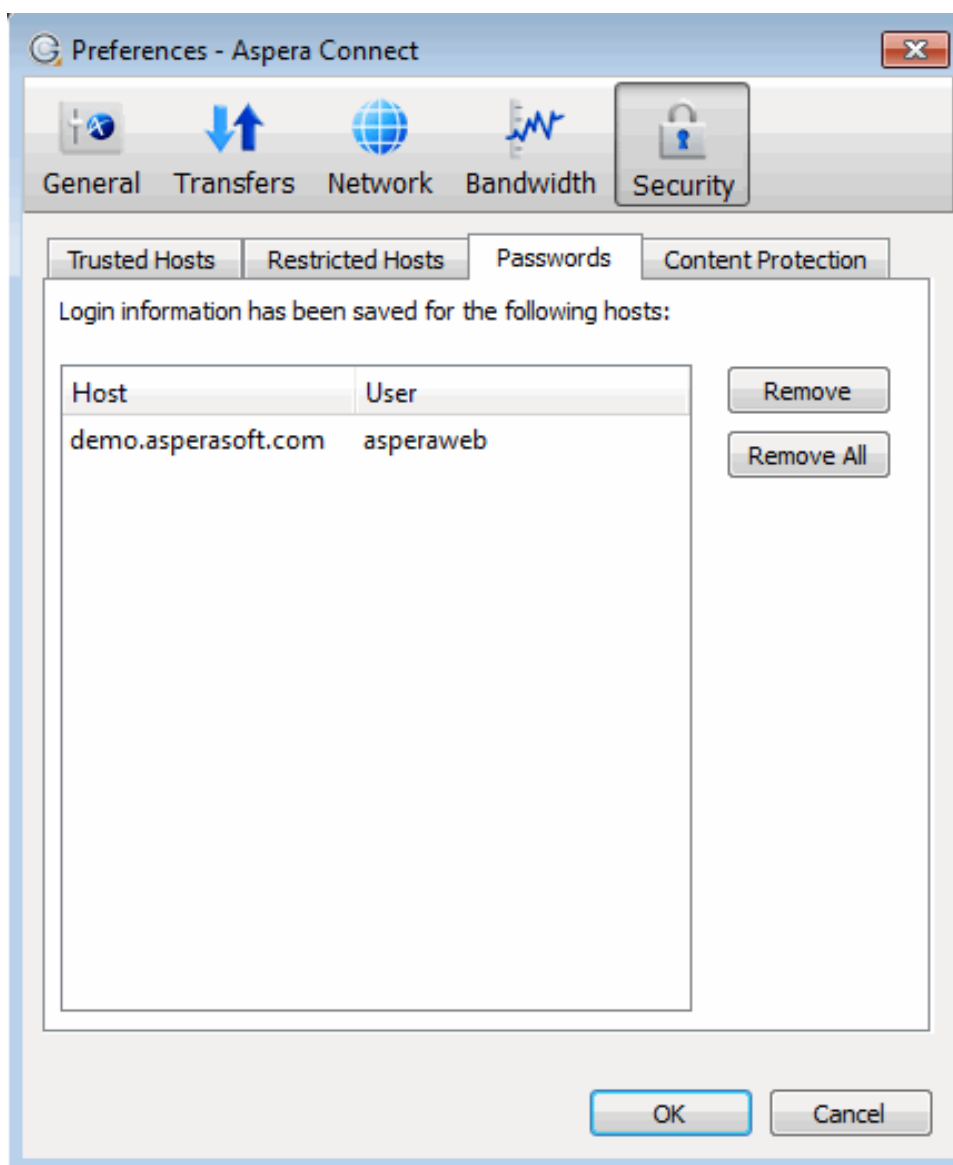


To view, add or remove restricted hosts, go to **Security > Restricted Hosts**. Here, enter the host's address in the specified text field and click **Add**.



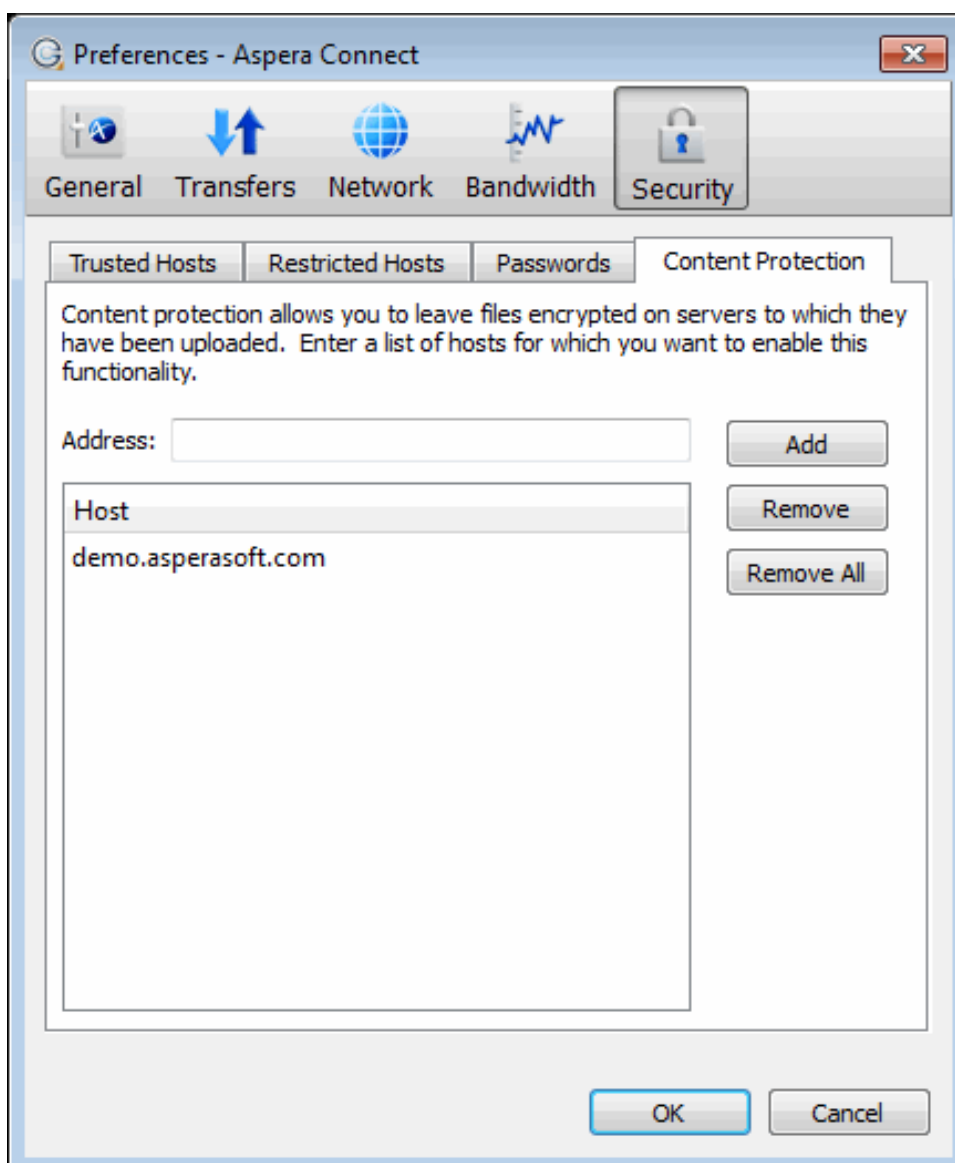
 **Important:** By adding a host to the restricted list, you will be required to provide confirmation every time you attempt to initiate a transfer with that host.

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

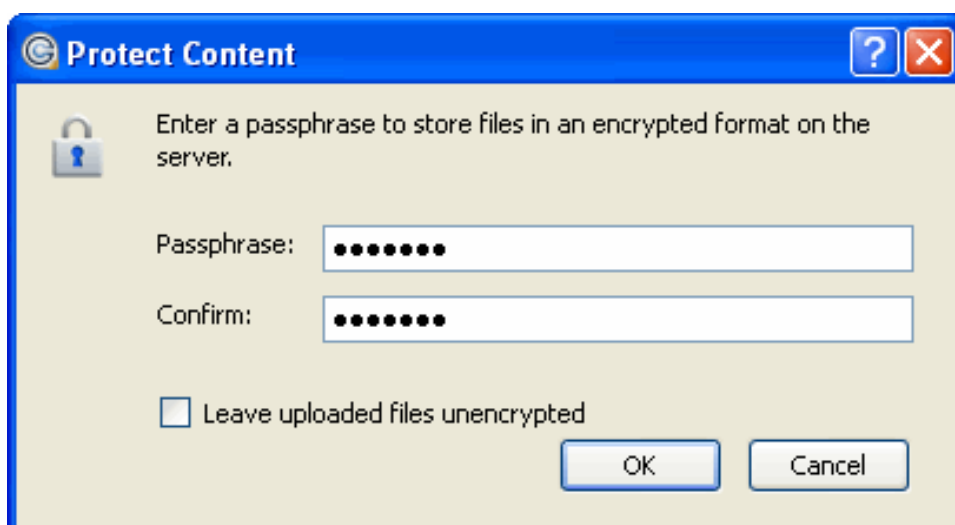


Content Protection

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).

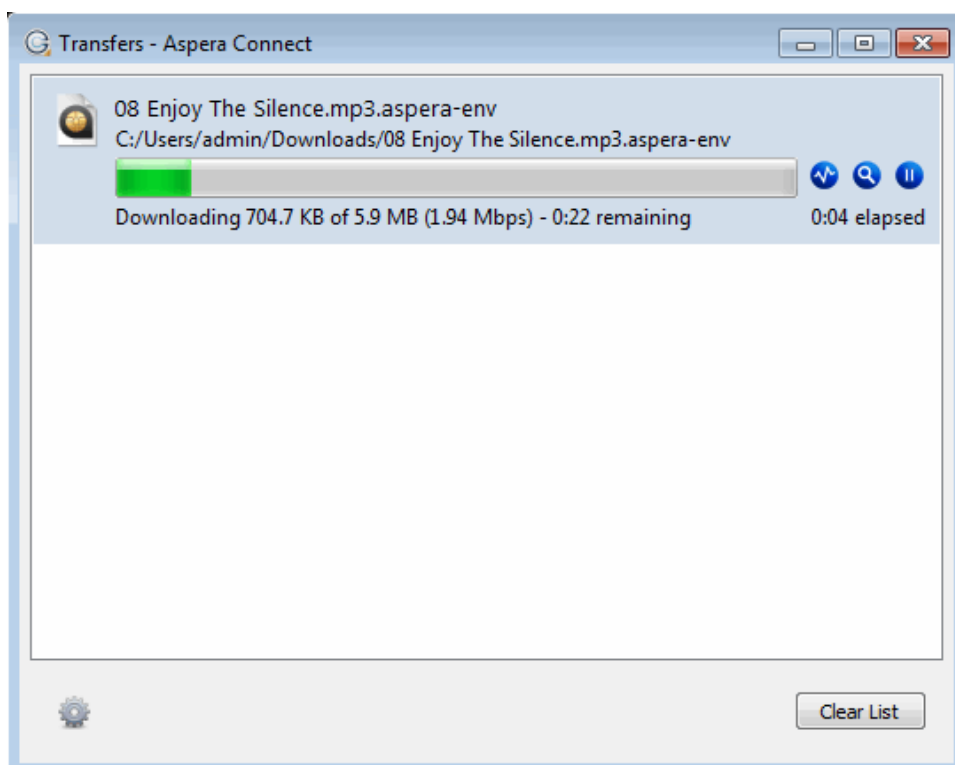


When you use Connect to download a content-protected file, you have two decryption options.

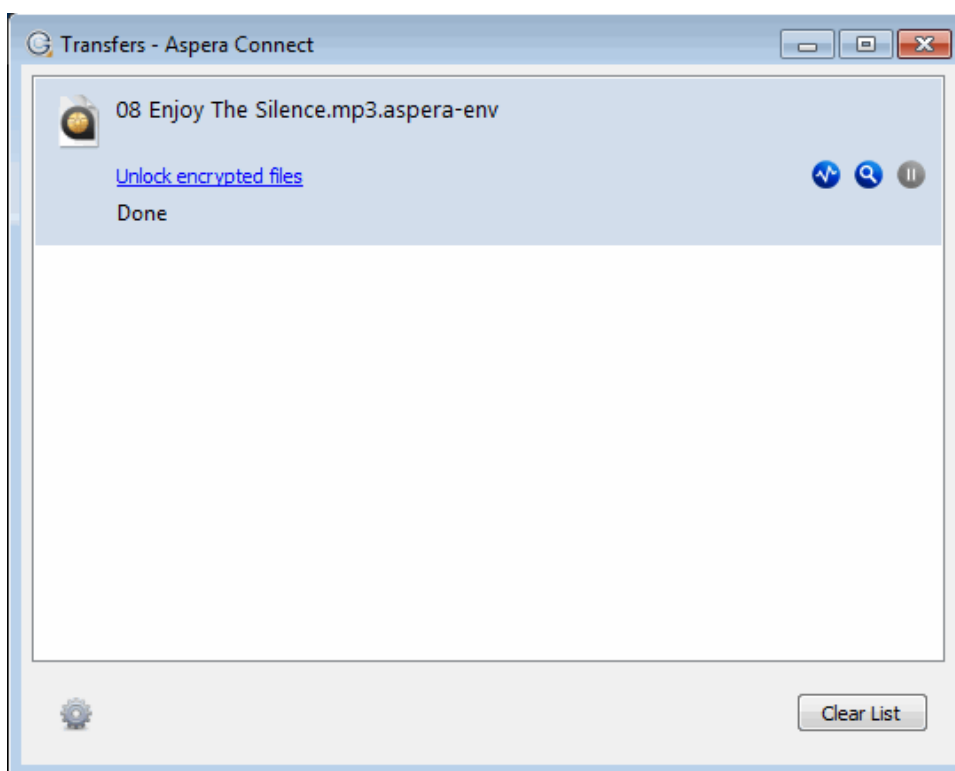
1. You can input and confirm your passphrase to decrypt the files *during* the download.
2. **OR**, you can enable the **Keep downloaded file encrypted** checkbox to download the content-protected files, and decrypt the files *after* the download has completed. When you select this option, you don't 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. See [Decryption](#) 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 Connect **Transfers** window.



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

<u>T</u>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, see [Decryption](#).

Connect Functionality


Initiating a File Transfer

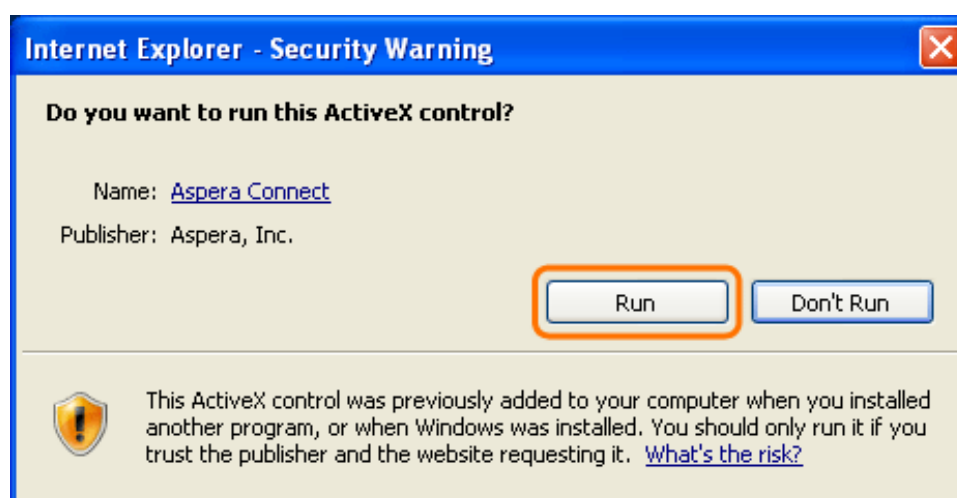
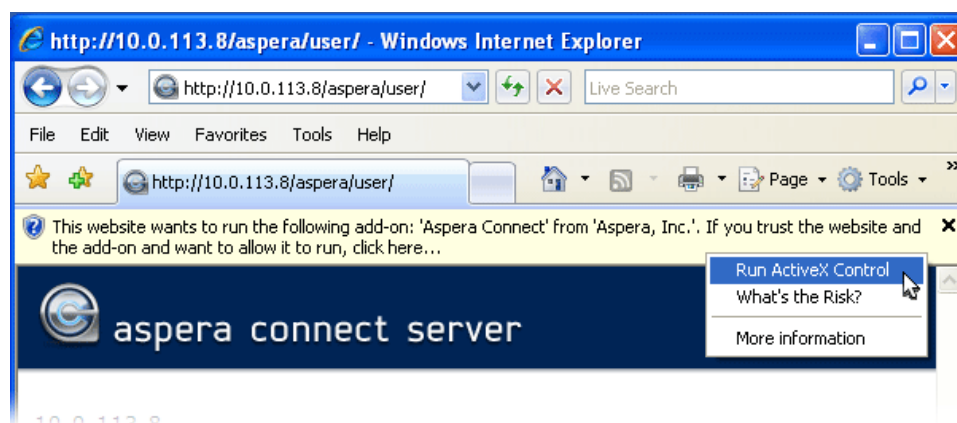
The following steps describe (1) how to perform a download test using Aspera's test server and (2) how to initiate a common file transfer using IBM Aspera Connect Browser Plug-in.

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

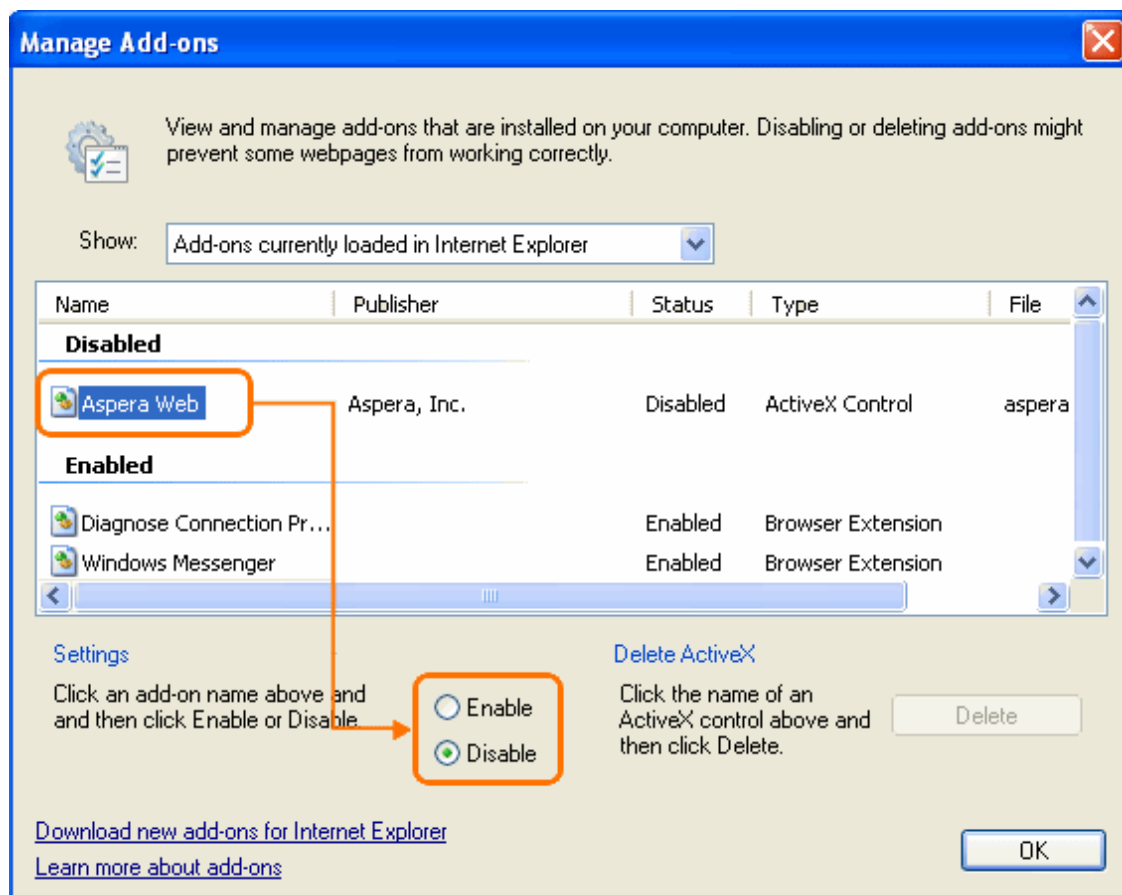
Enter the following credentials when prompted:

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

 **Note: Internet Explorer 7 Security Settings:** When you open an IBM Aspera Connect Server or IBM Aspera Faspex using Internet Explorer 7, the Information Bar appears and asks for permission to use the Connect Browser Plug-in. 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*.



2. On the IBM Aspera Connect Server, 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](#)

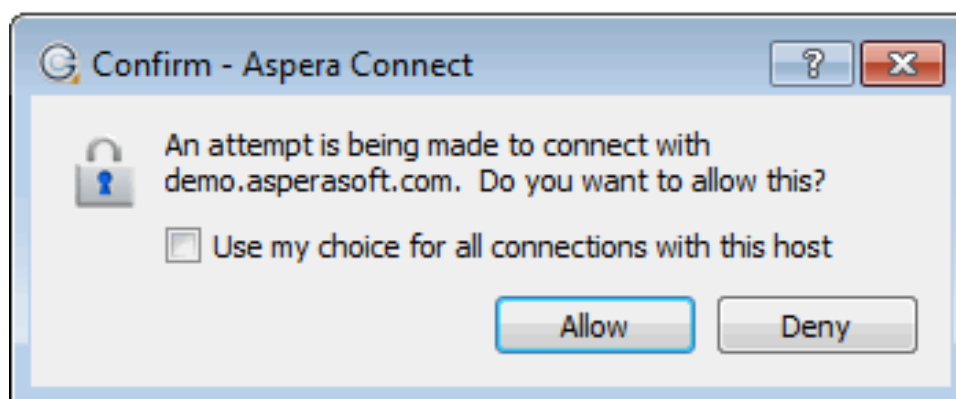
aspera-test-dir-large



	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.



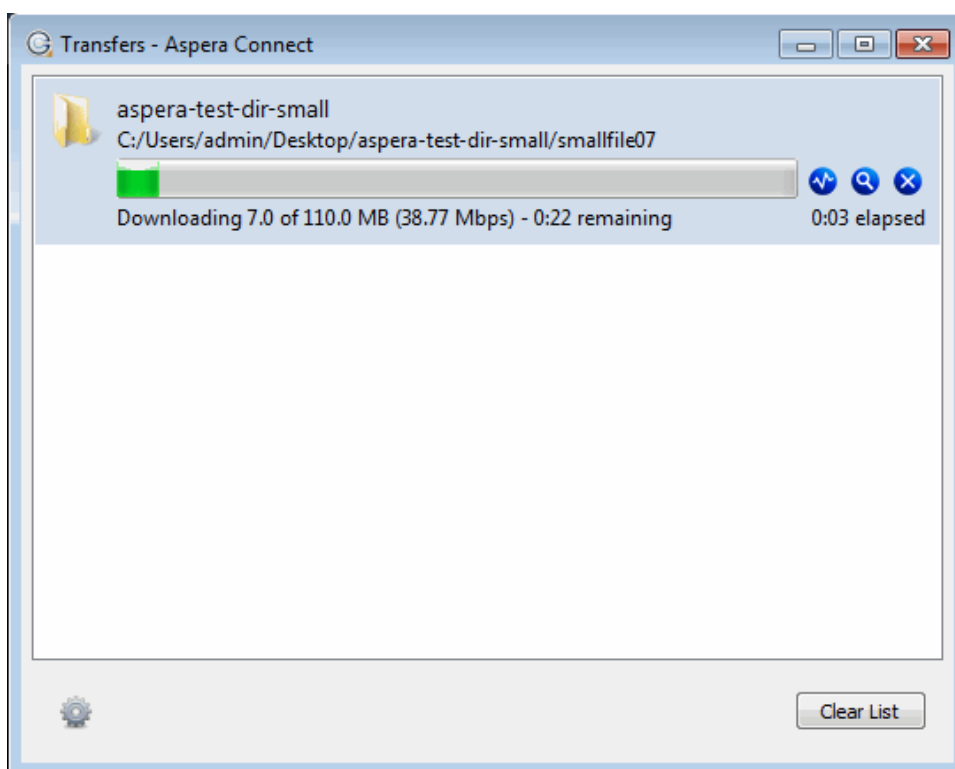
Once you confirm that the configuration settings are correct and that Connect is working properly, you can begin transferring with your organization's Aspera server. Simply point your browser to your server's address (e.g., <http://companyname.com/aspera/user>) to get started.

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






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

The Transfers Window


You can view and manage all transfer sessions within the **Transfers** window.

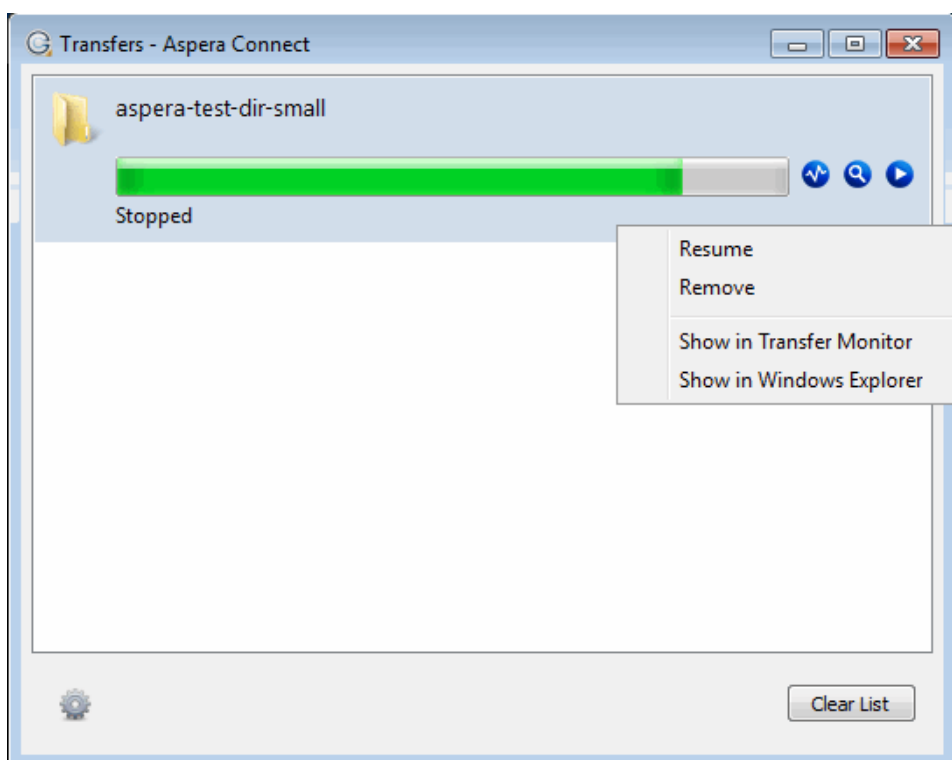


The **Transfers** window contains the following controls:

-  Open the Transfer Monitor. For more information on using this feature, see [Monitoring Transfers](#).
-  Open the folder on your computer that contains this content.
-  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 IBM Aspera Connect Browser Plug-in **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: <ul style="list-style-type: none"> Fixed High Fair Low 	Select the transfer policy from the drop-down list: <ul style="list-style-type: none"> The transfer transmits data at a rate equal to the target rate, although this may impact the performance of other traffic present on the network. The transfer rate is adjusted to use the available bandwidth up to the maximum rate. 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 IBM Aspera Enterprise Server version 3.0 or later.

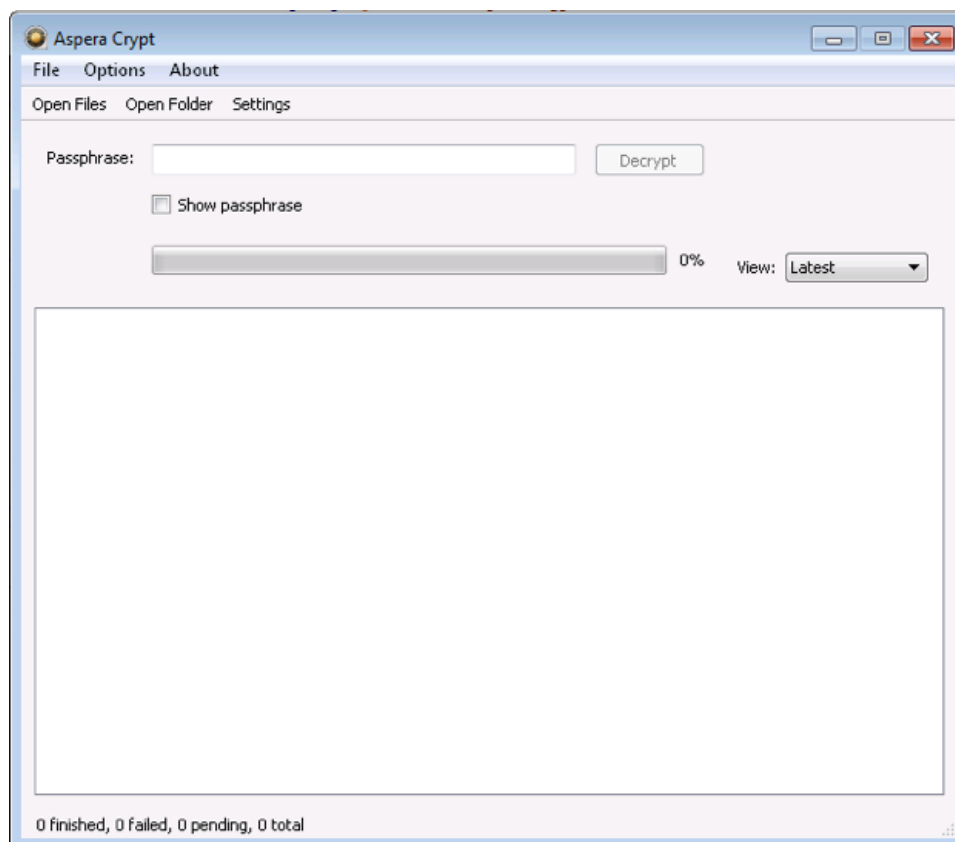
Decrypting Encrypted Files

Once you have downloaded an encrypted package, file or directory, Aspera Crypt makes it simple to browse for it in your file system, enter your passphrase and decrypt the contents.

 **Note:** When an encrypted item has been downloaded to your computer, it will have the extension **.aspera-env** (Aspera Security Envelope).

1. Launch Aspera Crypt and browse for your package, file or directory.

To launch Aspera Crypt, go to **Start > All Programs > Aspera > Crypt > Crypt**.



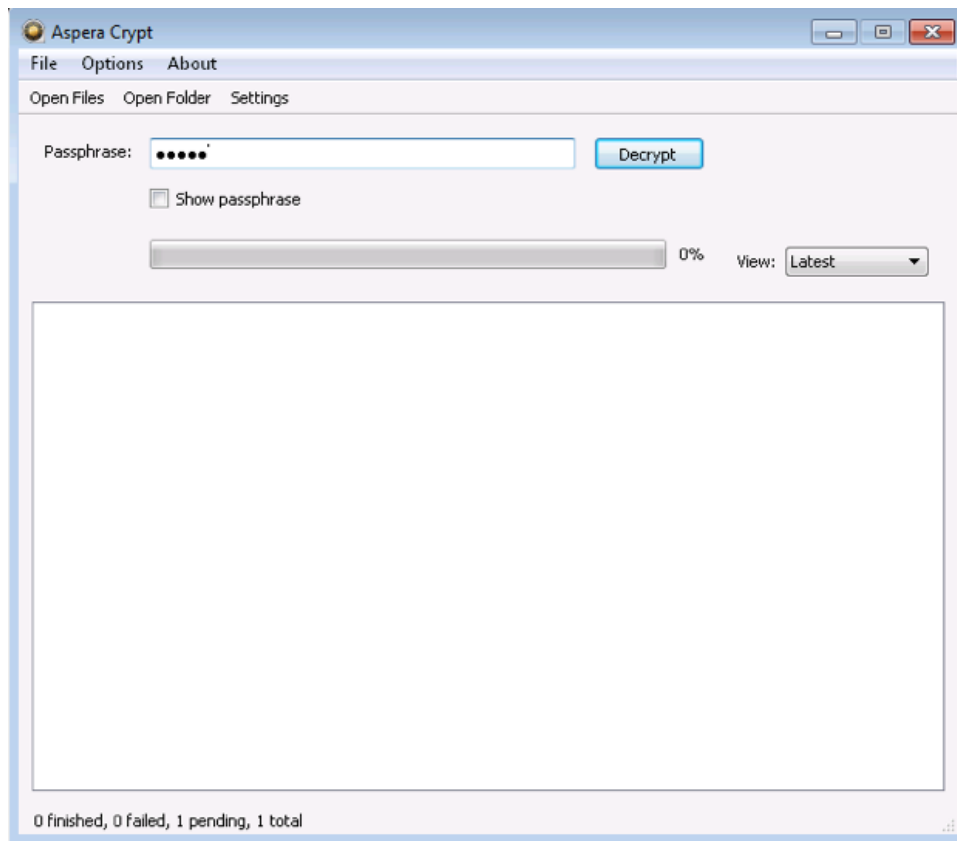
2. Browse for your package, file, or folder:

- Click **Open Files** to locate an Aspera Faspex package or an Enterprise/Connect server file.
- Click **Open Folder** to locate an Enterprise/Connect server folder.

When your encrypted contents are loaded into Crypt, a status message appears at the bottom of the application, displaying the number of items ready for decryption.

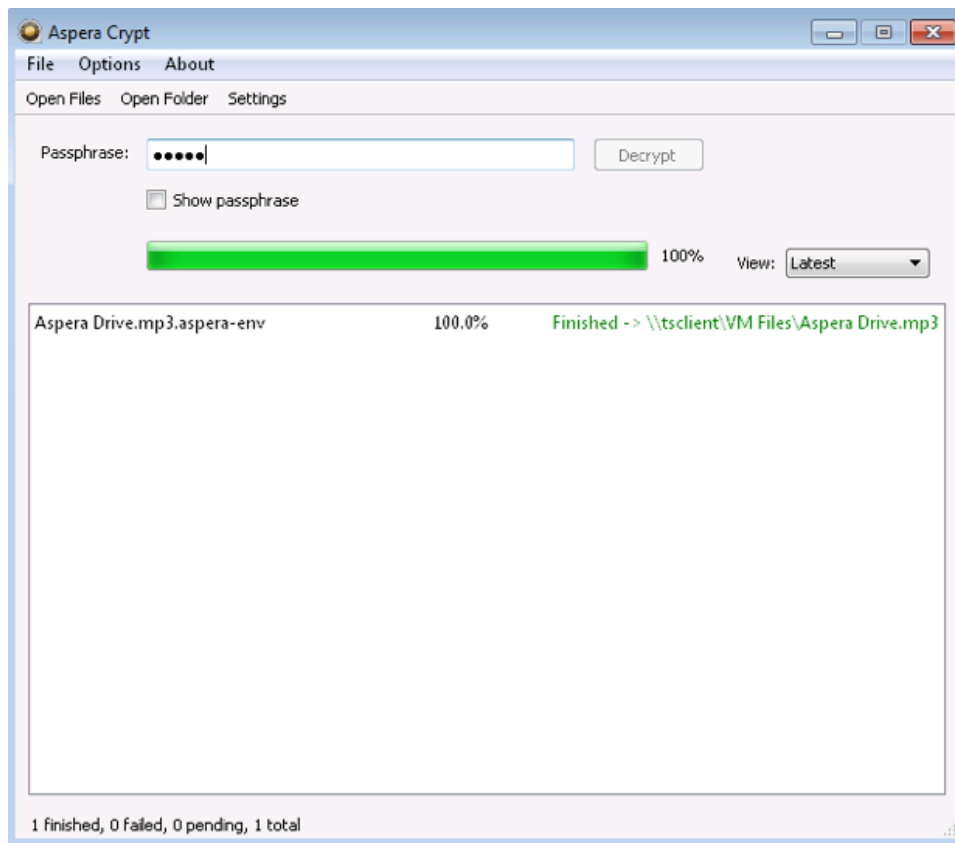
3. Input your passphrase and click the **Decrypt** button.

After browsing for your contents, enter your passphrase in the text field. Your passphrase will be masked, unless you enable the **Show Passphrase** checkbox. Note that you must input the correct passphrase in order to activate the **Decrypt** button. Once the **Decrypt** button is activated, click it to decrypt your package, file or folder.

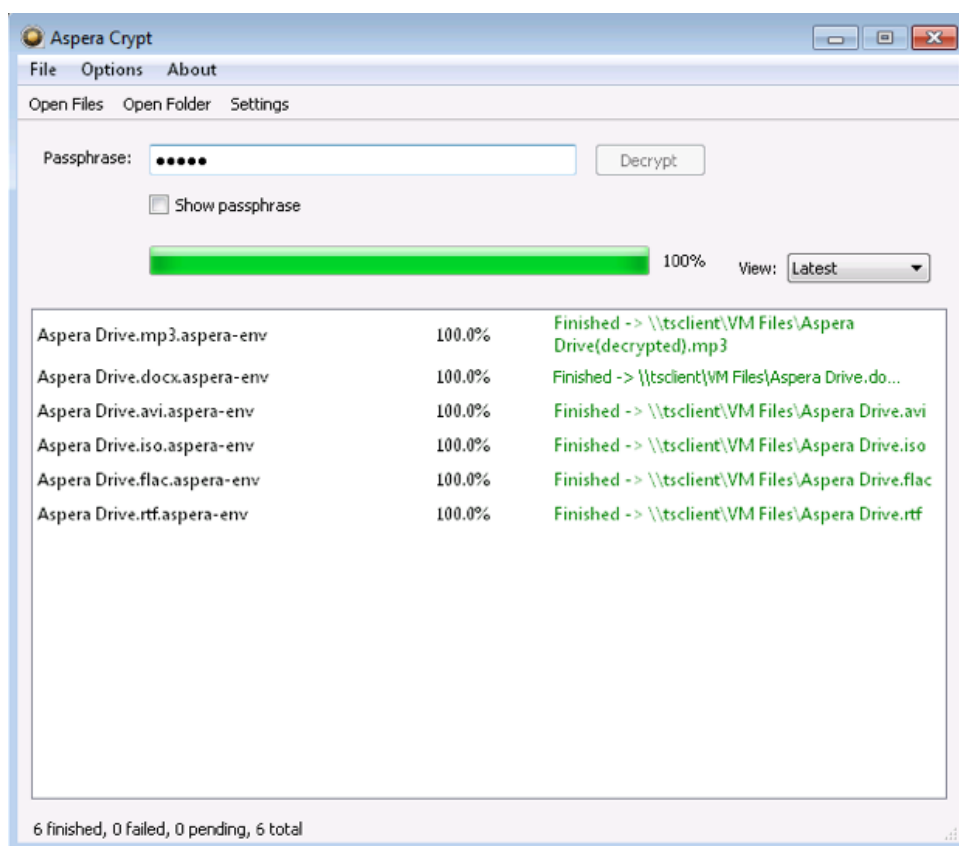


4. View output and confirm decryption.

Once your package, file or folder contents 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. *For decrypted folders, destination files will be displayed with the extension "(decrypted)."*



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**.

Maintaining Your Connect Installation

Upgrading

When a new version becomes available, Connect upgrades itself automatically.

If Connect does not upgrade automatically (for example, because the system does not have Internet access), you can fetch the latest version explicitly. To do so, go to <http://asperasoft.com/connect>. Click **Upgrade Now** and follow the on-screen instructions. This process will either initiate auto-upgrade or download the latest installer.

Download Location

If you are upgrading an existing installation for which you changed the default download location, that custom location is preserved after you upgrade. Connect will continue to save your downloaded content to the location you specified.

Uninstalling



Important: Before proceeding with uninstalling Connect, you must quit any open browsers.

To uninstall the Connect Browser Plug-in, quit both the 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.

File Cleanup

After upgrading or uninstalling IBM Aspera Connect Browser Plug-in, old Connect files can be safely removed from your system.

Log Files

Pre-Connect-2.8 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 2.8+ Log Folders (remove only after uninstalling Connect 2.8!)

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

http.uri and process.pid Files

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

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

Database File

If you previously installed Connect for all users (that is, 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\username\.aspera\connect\
```

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

Miscellaneous Files and Folders

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


Appendices

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\ <i>username</i> \Local Settings\Application Data\Aspera\Aspera Connect\var\log\
Windows Vista, 2008, and 7	C:\Users\ <i>username</i> \AppData\Local\Aspera\Aspera Connect\var\log\

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

<u>T</u>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 information on removing old log files, see [File Cleanup](#).

Plug-In Locations

Plug-In Location

Installation Type	Connect Browser Plug-In Location
User	%LOCALAPPDATA%\Programs\Aspera\Aspera Connect\lib

Installation Type	Connect Browser Plug-In Location
System	%PROGRAMFILES%\Aspera\Aspera Connect\lib

Web Installer Plug-In Locations

Browser	Web Installer Plug-In Location
Chrome	%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions \aljbeaimggdioicepilejnkphjobddok
Firefox	%APPDATA%\Mozilla\Firefox\Profiles*.default\extensions\awi@asperasoft.com
Internet Explorer	Depending on your version of Windows and UAC settings, the plug-in is 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

Troubleshooting

Web Installation is Blocked in IE7

If you have received an error during a Web installation of IBM Aspera Connect Browser Plug-in 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

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

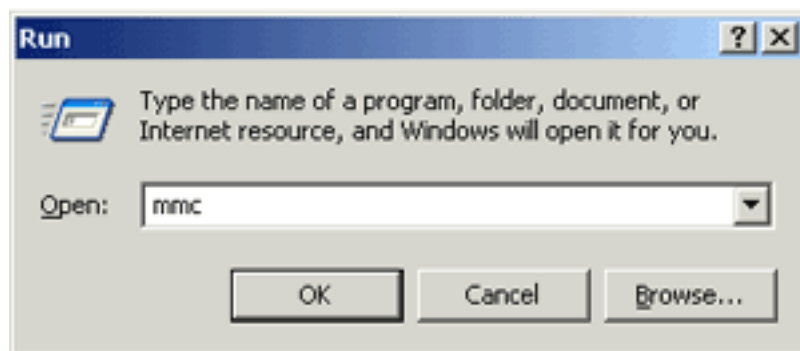
OS Version	Error
Windows 2003	The system administrator has set policies to prevent this installation.
Windows XP	You do not have access to make the required system configuration modifications. Please rerun this installation from an administrators account / Error 1925. You do not have sufficient privileges 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 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:

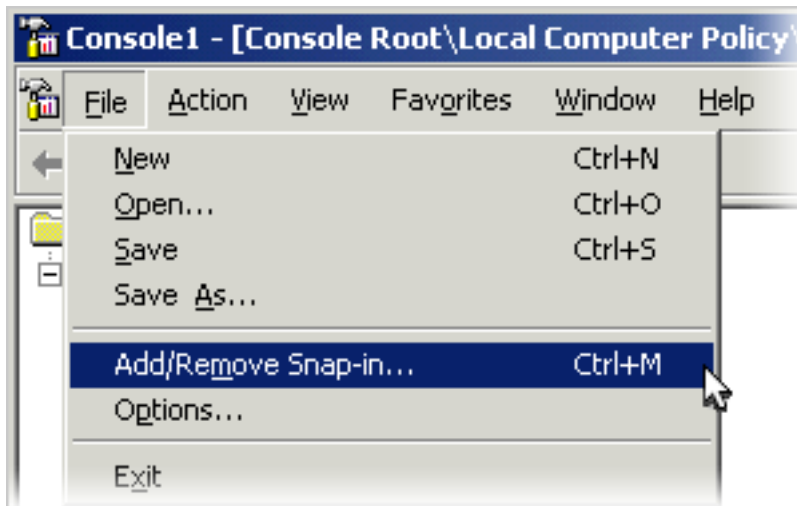
1. Launch the Microsoft Management Console (MMC).

Go to **Start menu > Run**. Enter **mmc** and click **OK** to launch it.

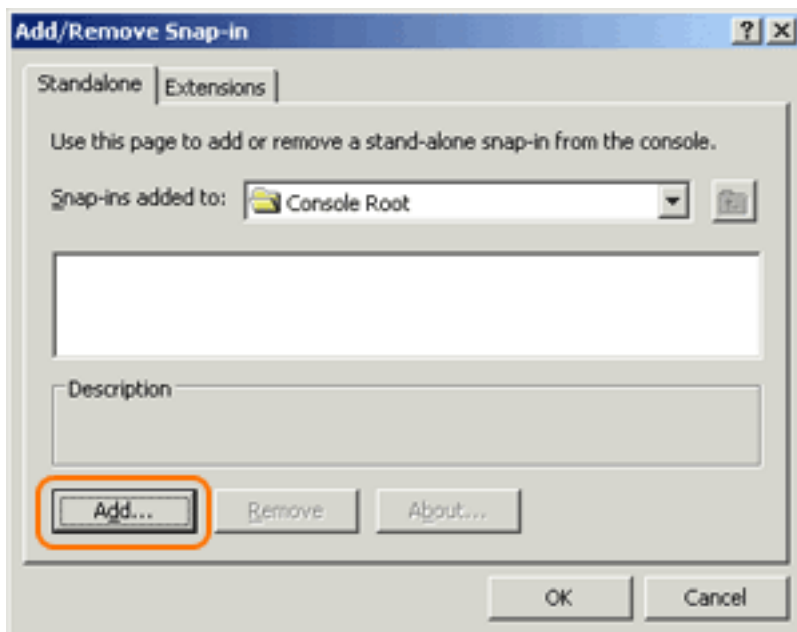


2. Add the Group Policy Object Editor Snap-in.

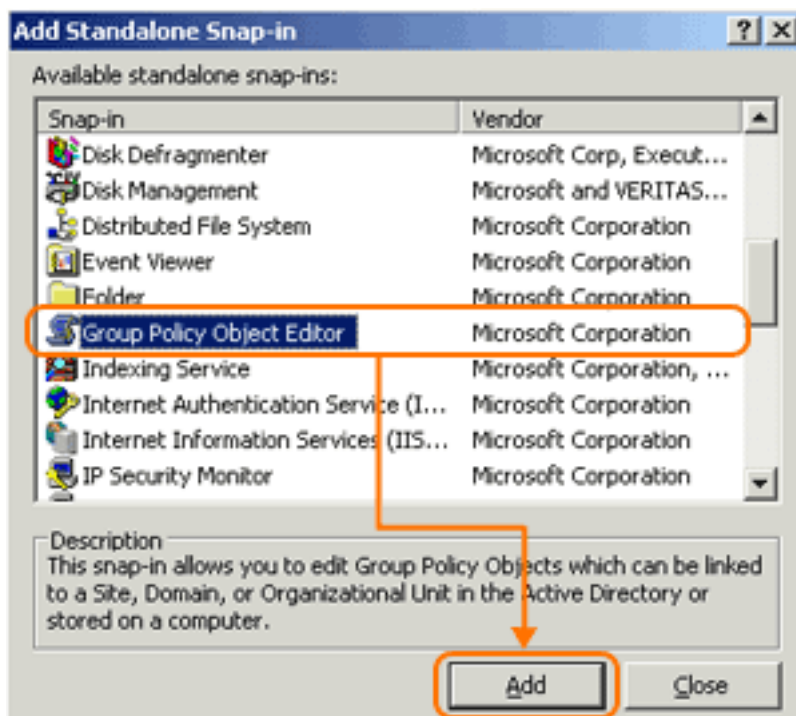
In the MMC, go to the toolbar and select **File > Add/Remove Snap-in**.



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



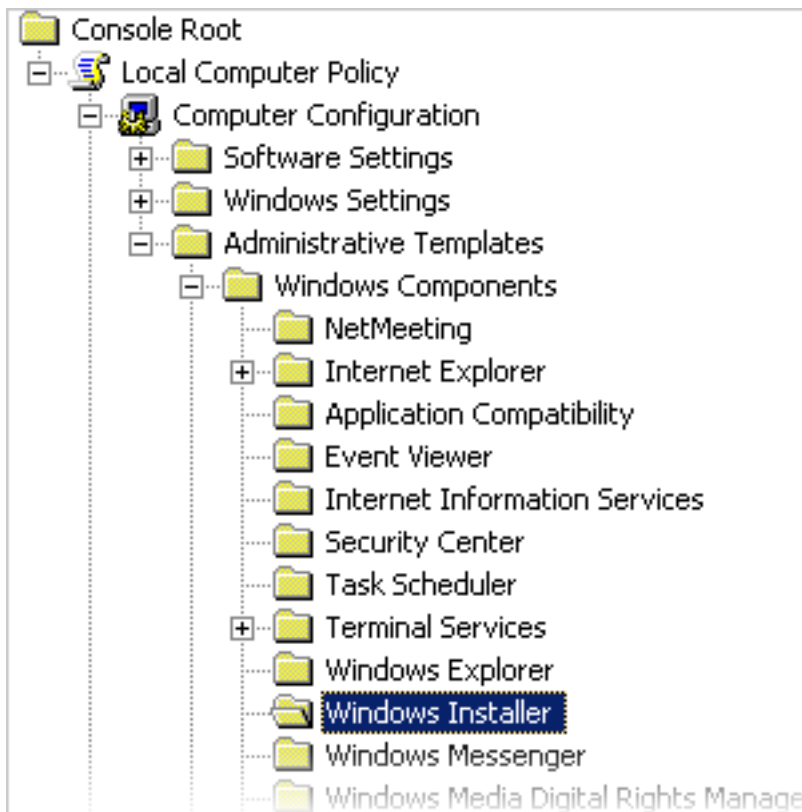
Select the **Group Policy Object Editor** and click **Add**.



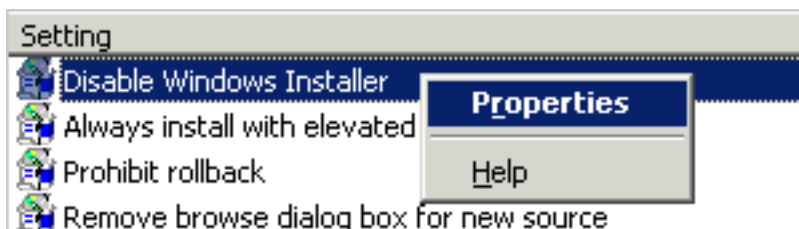
In the **Group Policy Wizard** window, click **Finish**. Close the **Add Standalone Snap-in** window, and click **OK** in the **Add/Remove Snap-in** window to save the changes.

3. Grant the Windows installation group policy.

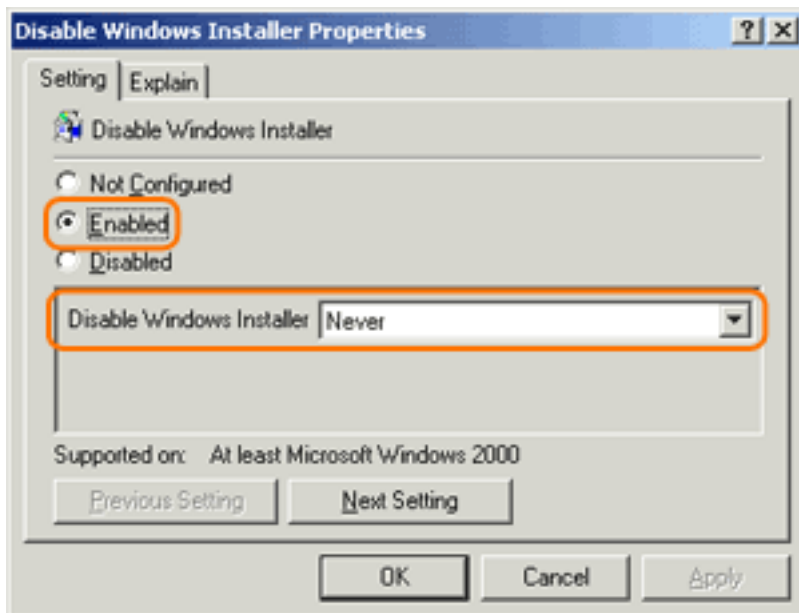
In the MMC, navigate into **Console Root > Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Windows Installer**.



Locate **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**. When finished, click **OK**.



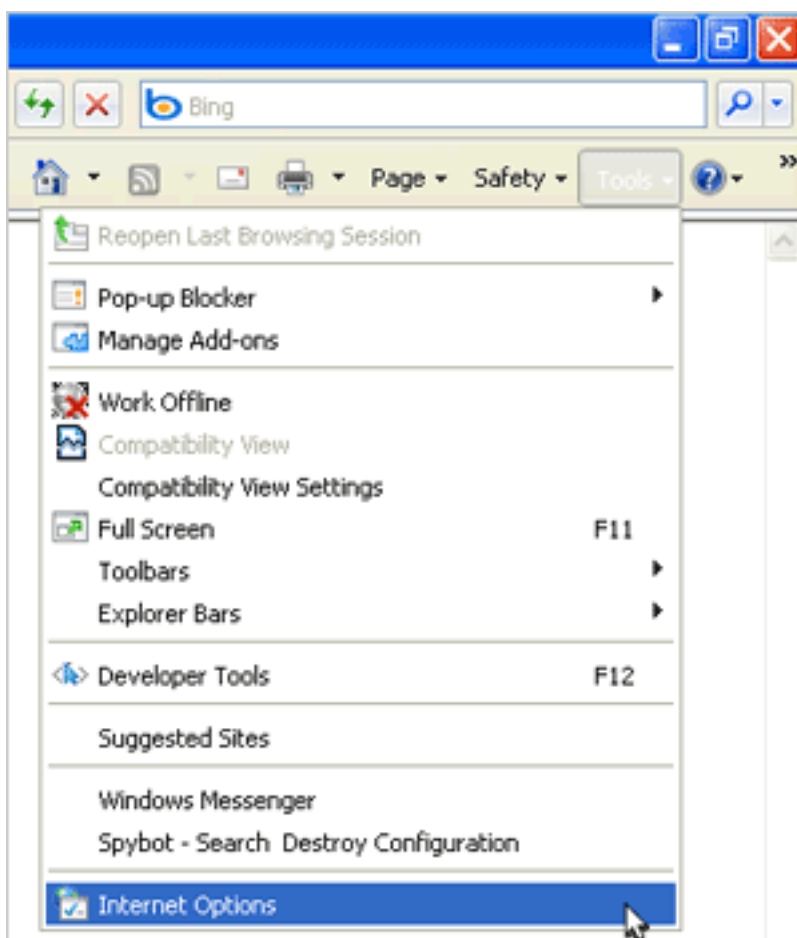
Close the MMC, click **Yes** to save the settings to a file. Reboot the computer to apply the changes, or execute the following command at a command prompt:

```
> gpupdate /force
```

Missing Install Button on Windows Server

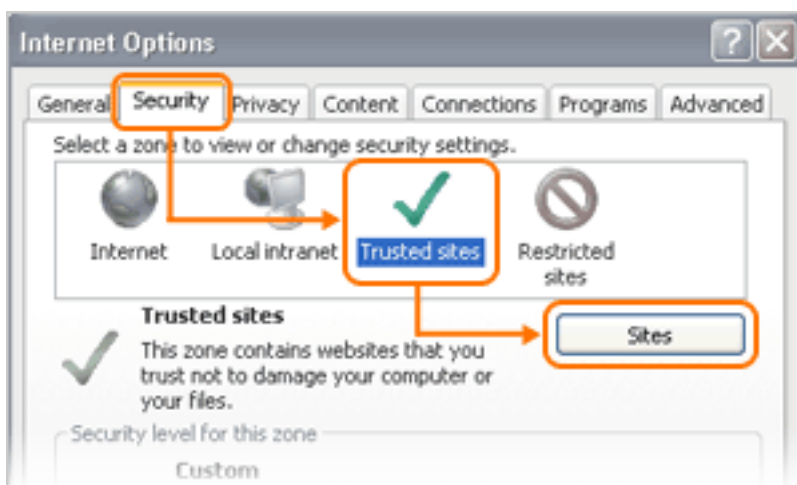
On Windows Server 2003 SP2 and Windows Server 2008, IBM Aspera Connect Browser Plug-in's **Install** button might not appear on your host's Web interface. This problem may be due to additional Internet Explorer (Version 8) security restrictions. To resolve this, follow the steps below.

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



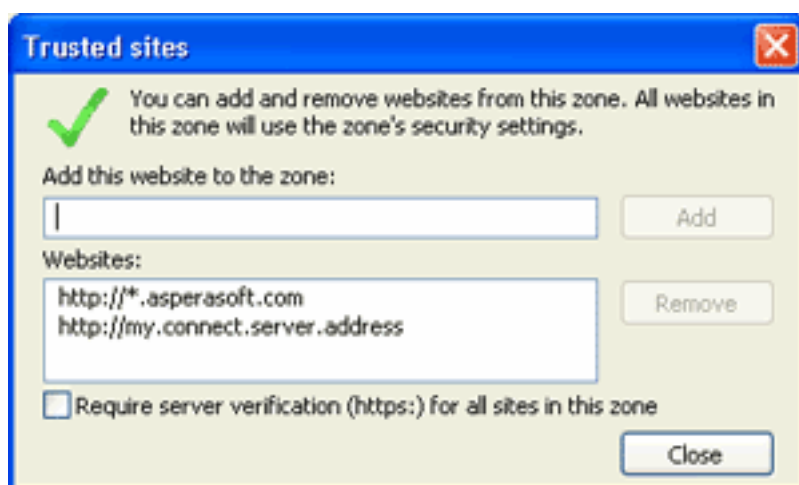
2. Add trusted sites.

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 Web sites below. Replace **my.connect.server.address** with the address of the Aspera server that you are browsing:

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



Connectivity Issues

SSH Connectivity Errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between the IBM Aspera Connect Browser Plug-in and the server is blocked (error codes 13, 15, or 40 in the log files). To determine the cause, open a Terminal or a Command prompt on the client machine (the machine that Connect is installed on). Use `telnet` to test the connection to the server:

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

where *server-ip-address* is the IP address of the Aspera server (ex. 10.0.1.1) on TCP port 33001 (or the configured TCP port, if other than 33001).

You will receive one of the following errors and can take the appropriate action:

- **"Connection refused":** The Aspera server is not running the SSHD service. Have your server administrator review the server's SSH service status.
- **"Timeout":** The client-side firewall is disallowing outbound TCP traffic. Ensure that the client-side firewall allows outbound TCP traffic on port 33001 (or the configured TCP port).

UDP Connectivity Errors: "Data transfer timeout"

If Connect appears to successfully connect to the server but:

- The transfer progress reads 0%.
- Files appear to be transferred to the destination but are 0 bytes.
- You eventually receive the error "Data transfer timeout."

UDP connectivity is blocked, likely by the firewall configuration (error codes 14, 15, and 18 in the log files). Ensure that the client-side firewall allows outbound traffic on the FASP UDP port (33001, by default) and the server firewall allows inbound traffic on UDP port 33001.

Aspera Connect Diagnostic Tool

Aspera provides a web-based diagnostic tool that can be useful for identifying connection issues. You can access the tool here:

```
https://test-connect.asperasoft.com/
```


Technical Support

Support Websites

For an overview of IBM Aspera Support services, go to <http://asperasoft.com/company/support/>.

To view product announcements, webinars, and knowledgebase articles, as well as access the Aspera Support Community Forum, sign into the IBM Aspera Support site at support.asperasoft.com using your email address (not your company Aspera credentials), or set up a new account. You can click on a heading then click **Follow** to receive notifications when new knowledgebase articles are available; if you follow **RELEASE NOTES** under a specific product, you will be automatically notified of new releases.

Personalized Support

You may contact an Aspera support technician 24 hours a day, 7 days a week, through the following methods, with a guaranteed 4-hour response time.

If you have an emergency, create a ticket using the **Support Request Form** with as many details as you have available and then **call**. If you are asked to leave a voice message, include the ticket number.

Email	support@asperasoft.com
Phone (North America)	+1 (510) 849-2386, option 2
Phone (Europe)	+44 (0) 207-993-6653 option 2
Phone (Singapore)	+81 (0) 3-4578-9357 option 2
Support Request Form	https://support.asperasoft.com/anonymous_requests/new/

Legal Notice

© 2008-2016-2017 Aspera, Inc., an IBM Company. All rights reserved.

Licensed Materials - Property of IBM
5737-A72

© Copyright IBM Corp. 2016, 2017. Used under license.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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, Aspera FASPStream and Aspera Faspex 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.