# **IBM Aspera Connect User Guide 3.9.1**

Windows Revision:338 Generated:04/12/2019 19:33

# Contents

Introduction	
Setting Up Connect	
Installation	
Network Environment	
Basic Configuration	
Security Configuration	
Connect Functionality	
Initiating a Transfer	
The Activity Window	
Monitoring Transfers	
File Encryption	
Maintaining Your Connect Installation	25
Upgrading	
Uninstalling	
File Cleanup	
Appendices	
Log Files	
Troubleshooting	27
Error When Installing with a Non-Admin Account	
Connectivity Issues.	
Connectivity issues	
Technical Support	
Legal Notice	

# Introduction

IBM Aspera Connect is an install-on-demand application that facilitates high-speed uploads and downloads with an Aspera transfer server.

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

Feature	Description	
FASP file transport	High-performance transport technology.	
Browser interface	Uploads and downloads are launched transparently by a Web browser.	
Flexible transfer types	Easily transfer single files, multiple files, or entire directories.	
Transfer retry and resume	utomatically retries and resumes partial and failed transfers.	
Browser-independent transfer	The Web browser can be closed once transfer operations have begun.	
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 in a queue.	

### **Drag-and-Drop Support**

When used with IBM Aspera Faspex and some third-party web applications, Connect supports the drag-and-drop feature for specifying which files and folders to transfer; however, this feature is not available for certain browsers. The following table shows which browsers support the drag-and-drop feature in this release of Connect:

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

\* Drag-and-drop capability is limited with Internet Explorer because of how it records drop events.

# Setting Up Connect

# Installation

There are two ways of installing IBM Aspera Connect on your system:

- Guided Installation: The most common way of installing Connect. If Connect is not installed or needs upgrading when you try to upload or download files from an Aspera web app, such as Aspera Faspex or Aspera Shares, you are prompted to install Connect and guided through the process.
- Manual Installation: A fallback method for users with non-typical web apps. You first install the Connect web extension for your browser. You then install the Connect application by running a desktop installer you download from the Aspera website.

Both methods include adding a Connect web extension.

Note: Internet Explorer is an exception that requires no extension

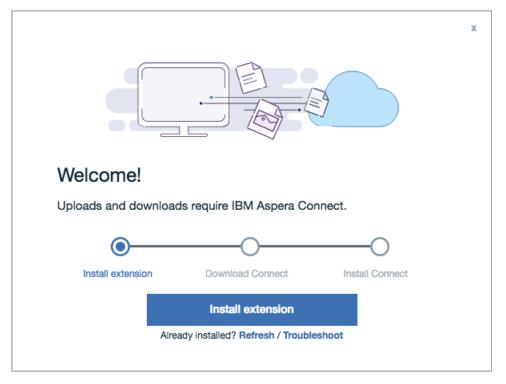
**System Requirements**: For information on supported operating systems and browsers, see the release notes for this release of IBM Aspera Connect.

#### Important:

- You cannot install Connect under the Guest account.
- 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 26.
- Connect requires your browser's local storage to be enabled.

### **Guided Installation**

If you do not have Connect installed and you attempt to transfer packages or files using an Aspera web application (such as Faspex or Shares), the Connect Welcome screen appears and prompts you to install Connect:

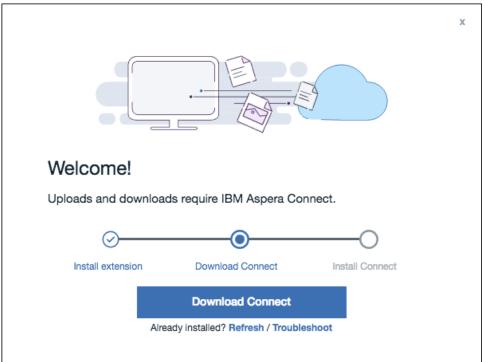


Depending on your browser/platform combination, the screens shown in these instructions may vary. In particular, the screens for Internet Explorer do not prompt you to install the extension, because Connect with Internet Explorer does not use an extension.

1. To begin, click Install extension.

Your browser's page for the Connect extension opens. See the instructions for your browser in Adding the Connect Browser Extension on page 6 to install the Connect extension. If successful, you'll see the message confirming the extension has been added.

2. The welcome screen now prompts you to download the Connect application:



Click **Download Connect**. The installer file (.exe, .dmg, or .rpm depending on your OS) is downloaded to your Downloads folder.

- x Welcome! Please run the Connect installer. Install extension Download Connect Install Connect Refresh Download failed? Download Connect
- 3. The welcome screen now prompts you to install the Connect application:

To install the Connect application, locate the installer file you just downloaded, open it, and follow the instructions to install the Connect application. Once the Connect application has been installed, return to the above screen and click **Refresh** to refresh the browser.

#### Manual Installation

#### Step 1. Install the Connect extension for your browser.

For instructions about obtaining the Connect extension for your browser, see Adding the Connect Browser Extension on page 6.

#### Step 2. Download and run the Connect application installer.

You can download the Connect installer directly from http://downloads.asperasoft.com/connect/. Once downloaded, run the installer and follow the Setup screens. You will need to accept the terms and conditions, and confirm whether to install Connect for you only (Typical) or for all users of this machine (Custom).

### Adding the Connect Browser Extension

For supported web browsers, this section explains how to obtain and add the IBM Aspera Connect extension to the browser you will use. The Connect extensions are specific to the browser; the procedure for adding an extension to a browser is the same regardless of which OS platform that browser is running on. With a guided install, clicking **Install extension** opens the extension link for the browser you are using. With a manual install, be sure to download the extension for the browser you intend to use with Connect.

#### **Chrome**

To obtain and install the Connect extension for Chrome, follow the procedure below:

1. Click Install extension (guided install method), or open the IBM Aspera Connect page on the Chrome Web Store (manual install method). The following page opens:

chrome web store	\$
IBM Aspera Connect Offered by: IBM Aspera ★★★★★ 1   Productivity   ≜ 261 users Overview Reviews Related	Add to Chrome
Activity - IBM Aspera Connect      IGB      C:/Users/dev/Downloads/1GB      Downloading 496.4 / 1,000.0 MB (899.22 Mbps) - 0:04 remaining	□ × ⊙ @ ● 0:11 elapsed

- 2. Click Add to Chrome. The Add "IBM Aspera Connect"? popup appears.
- 3. Click Add extension.

G Add "IBM Aspera Connect"?	×	
It can:		
Read and change all your data on the websites you visit		
Communicate with cooperating native applications		
Add extension Cancel		

If successful, you'll see the message "IBM Aspera Connect has been added to Chrome".

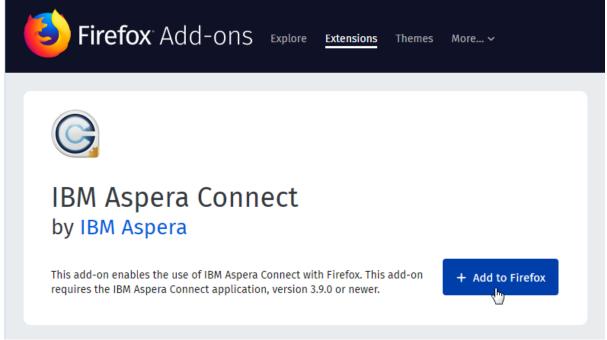
**Note:** By default, the Connect extension is disabled in Chrome's incognito mode. To enable the Connect extension, right-click the small Connect icon in the upper-right corner of your browser page. Then open **Manage extensions** and scroll down to the heading **Allow in incognito**. Then set the switch to ON as shown below. Note that the Connect extension does not record browser history.



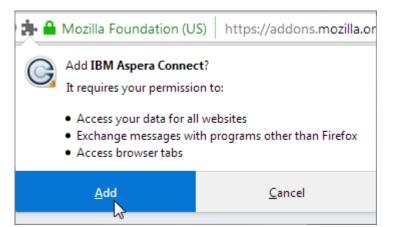
### <u>Firefox</u>

To obtain and install the Connect extension for Firefox follow the procedure below:

1. Click Add extension (guided install method), or open the IBM Aspera Connect page on the Firefox Add-Ons page (manual install method). The following page opens:



2. Click + Add to Firefox. The Add IBM Aspera Connect? popup appears.



3. Click Add.

If successful, you'll see the message "IBM Aspera Connect has been added to Firefox".

### Internet Explorer

Microsoft Internet Explorer does not use a Connect extension; instead it uses ActiveX to provide the same functionality as the extension.

### Microsoft Edge

To obtain and install the Connect extension for Microsoft Edge, follow the procedure below:

1. Click Install extension (guided install method). Or, open the IBM Aspera Connect for Edge page on the Microsoft Store (manual install method). The following page opens:

You own this app.		Install	
œ	IBM Aspera Connect for Edge IBM Corp. • Business > File management	. This add-on requires the IBM	
ESRB EVERYONE	Wish list This contains an extension for Microsoft Edge		

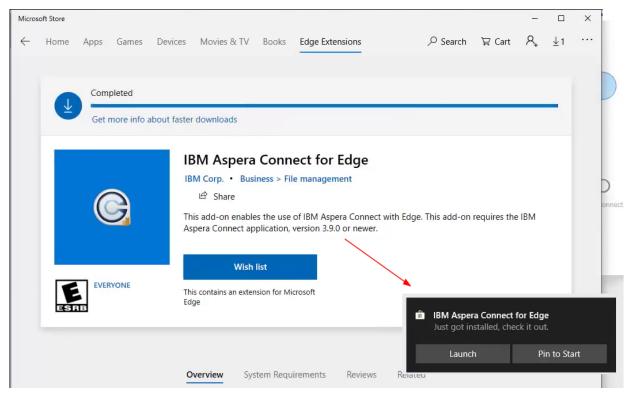
(If you are prompted to sign in, doing so is not required. You can dismiss the Sign in window.)

2. Click Install.

If the message below appears, clicking Refresh the page usually resolves it.

	Try that	again	
Page co	uld not be loaded	l. Please try aga	in later.
	Report this problem	Refresh the page	
		à	

A popup appears indicating the extension is installed.



3. Click Launch. This returns you to the browser, and the following popup appears:



If clicking Launch opens an empty window, return to the browser and the above popup should appear.

4. Click Turn it on.

**Note:** If the Connect extension for Edge is disabled, and you try to use a web app, the launch bar asks you to install the extension. Clicking **Install Extension** opens the Microsoft app store and shows a Launch button—however, the Launch button will *not* enable the extension. Enable the extension in the settings for Edge.

### After Installation

Once Connect is installed, you can launch it from the following location:

Start > All Programs > Aspera > GAspera Connect	
On Windows 10, E> E> Aspera > Aspera Connect	t.

**Tip:** Aspera provides a web-based diagnostic tool that can be helpful in identifying connection issues. You can access the IBM Aspera Connect Diagnostic Tool here:

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

## **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 network practices. Although TCP/33001 is the default setting, consult your IT department for questions related to which SSH ports 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 will need to allow the following:

- Outbound connections for SSH, which is TCP/33001 by default, although the server side may run SSH on another port. Check with your IT department for which SSH ports are open for file transfers.
- 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 which SSH ports are open for FASP transfers.

### Limit Transfer Rates

**Important:** Set values in these fields only if you need to limit the bandwidth that Connect uses. For example, your office may have limited bandwidth to share among its users. **Exception:** For the SaaS products Files and Aspera on Cloud, use this field to set the *default transfer speed*.

Launch Connect as follows:



Open Preferences:

From the system tray: Right-click G > Preferences

Activity	Ctrl+T
Unlock encrypted files	Ctrl+R
Open log folder	Ctrl+L
Preferences	Ctrl+P
Check for updates	Ctrl+U
About	Shift+F1
Quit	Ctrl+Q
^ 🧟 🕫 🖆 🗐 👫	42 PM
- 0	

You can limit Connect transfer rates from the **Bandwidth** tab:

Preferences	- IBM Aspera Cor	nnect			_		×
i General	👫 Transfers	Network	松 Bandwidth	🔒 Security			
Transfer speed transfer rates.		er settings and yo	our network connec	tivity. The setting	gs below allow	you to limit	t
Download							
<mark>∠ L</mark> imit t	100	Mbps 🔻					
Upload							
☑ L <u>i</u> mit t	xo: 100	Mbps ▼ Kbps Mbps					
			-				
			L	OK	Cancel	Apply	

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 setting a maximum speed doesn't guarantee your transfers will ever achieve that speed. Actual performance 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 Proxy**

HTTP fallback serves as a secondary transfer method when the Internet connectivity required for Aspera accelerated transfers (UDP port 33001, by default) is unavailable. If UDP connectivity is lost or cannot be established, if you have configured an HTTP proxy, the transfer continues over the HTTP protocol based on this proxy configuration.

Note: Although the HTTP proxy is used primarily for the HTTP fallback feature, it can be used for all HTTP-related activities performed by Connect. However, it cannot be used for FASP transfers.

To configure and enable an HTTP proxy server, open **Preferences > Network** in Connect and look for the HTTP Proxy section.

Preferences - IBM Aspera Connect	- □ >
🤷 General 👫 Transfers 🙂 Network 🦗 Bandwidth 🔒 Se	
	curity
Configure proxy settings.	
HTTP Proxy	
Obtain proxy configuration from Manual	
Use HTTP Proxy	
Username: alyce	
Password:	
Address: 10.0.0.1	Por <u>t</u> : 3866

To configure the HTTP proxy, select one of the following configuration methods from the drop-down list:

- System to have Connect use the HTTP proxy settings that are configured for your operating system.
- **Manual** to enter your HTTP proxy settings manually. (This may require the assistance of your system administrator.)

These settings include username and password authentication credentials, as well as the host name, IP address, and port number.

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

### **FASP Proxy**

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

To set up a FASP proxy, do the following:

- 1. Go to Preferences > Network in Connect and locate the FASP Proxy section in the lower half of the dialog.
- 2. Select the following checkboxes:
  - Use FASP Proxy (DNAT)
  - Secure (DNATS)
- 3. Enter your proxy server username, password, address, and port number.

FASP Proxy			
Use EASP Pr	oxy (DNAT)		
Secure (DNA	NTS)		
User <u>n</u> ame:	proxy_user		
Pass <u>w</u> ord:	•••••		
Address:	fasp_proxy_server.net	Port:	7777

Note: If you enable FASP proxy, you may need to add local.connectme.us as a proxy exception in order for Connect to function.

## **Basic Configuration**

To change the application's default settings, launch Connect as follows:



**Open Preferences:** 

From the system tray: Right-click **G** > **Preferences** 

Activity	Ctrl+T
Unlock encrypted files	Ctrl+R
Open log folder	Ctrl+L
Preferences	Ctrl+P
Check for updates	Ctrl+U
About	Shift+F1
Quit	Ctrl+Q
^ 🔍 🗤 🗊 🗐 4	:42 PM

### **General Preferences**

Connect's general application behavior can be configured in the General tab.

🕞 Preferences - IBM Aspera Connect	-		×
😰 General 👫 Transfers 💷 Network 🚧 Bandwidth 🔒 Security			
Automatically launch when Windows starts			
Activity Window			
Remove transfer list items: Manually Manually Upon Successful Transfer			
Logging			
Logging Level: Info 🔻			
OK Ca	ncel	Apply	

Under the General tab, you can modify the following settings:

- Specify whether to launch Connect whenever the user logs in to the system.
- Specify how to remove transfer sessions from the Activity window: manually, or automatically on successful transfers.
- Specify the level of detail to be logged for transfers:

- Info Default. Displays general messages about requests, ascp spawn options, and transfer status changes.
- **Debug** Verbose. Displays validation and FASP management messages, and passes D to ascp.
- Trace Extra verbose. Passes -DD to ascp. Used only for diagnosing problems.

G Preferences	- IBM Aspera Cor	nnect			-		×
i General	It Transfers	Network	M Bandwidth	Security			
Automatic	ally launch when W	indows starts					
Activity Wine	dow						
Remove	transfer list items:	Manually	•				
Logging							
Logging	Level: Info Info Debug Trace	*					
				ОК	Cancel	Apply	/

The logging feature is typically used for troubleshooting and when contacting Aspera Support.

### **Transfer Preferences**

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

G Preferences	- IBM Aspera Co	nnect			_		×
🤷 General	It Transfers	Network	Pandwidth	🔒 Security			
Downloads							
Save	e downloaded files	to:					
C:\t	mp					Browse	
⊖ Alwa	ays ask me where t	o save downloade	d files.				
Queue							
✓ Enat	ole queuing						
Max	mum concurrent tra	ansfers: 3					
Retry							
Auto	matically retry faile	ed transfers					
Atte	mpts: 3	time(s)					
Inte	rval: 30	seconds 🔻	•				
The inte	rval specifies an an	nount of time that	will elapse between	each attempt t	to retry a fail	ed transfer.	
				ОК	Cancel	Apply	1

#### Downloads

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 the location where downloaded files should be saved.
- Always ask me where to save downloaded files Choose this option to select a location for each download.

#### Queue

- Enable queuing Enable or disable the queuing of transfers.
- Maximum concurrent transfers This allows a specified number of transfers to run concurrently and places the remainder in a queue.

### Retry

You can set a retry rule if a transfer fails. Set the retry rule as follows:

- Automatically retry failed transfers enable or disable.
- Attempts specify the number of times Connect should attempt to retry a failed transfer.
- Interval specify the amount of time that Connect should wait before retrying a transfer (in seconds, minutes, or hours).

# **Security Configuration**

IBM 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 in the Connect Preferences dialog. To open it, first launch Connect:



Then, from the system tray, right-click  $\bigcirc$  > **Preferences** 

Activity	Ctrl+T
Unlock encrypted files	Ctrl+R
Open log folder	Ctrl+L
Preferences	Ctrl+P
Check for updates	Ctrl+U
About	Shift+F1
Quit	Ctrl+Q
^ दू∿ ঢ় ঢ় 색	42 PM

#### **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.

Preferences - IBM Asp	era Connect				-"	
🙋 General 🛛 👫 Tran	sfers 🌐 N	letwork	* Bandwidth	🔒 Security		
Trusted Hosts Rest	ricted Hosts	Passwords	Content Pro	otection		
Trusted hosts are hosts made to start a transfer						
transfer. Address:						
Address.						Add
Host					Re	emove
https://demo.asperas	oft.com				Ren	nove All
https://faspex.com						

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.

General	🕈 Transfers 🛛 💷	Network 💡	* Bandwidth	Security		
Trusted Hosts	Restricted Hosts	Passwords	Content Pro	tection		
	are hosts for which yo ost that is on this list,					start a
		you will be pre	sented widta w	arning before it can		-
Address:					A	dd
Host					Ren	nove
https://www.u	intrustedhost.com				Remo	ove All

**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 password information for a host, go to **Security > Passwords**. Here, you can remove saved login credentials; however, you cannot add credentials to this list directly. Whenever you attempt a transfer with a server where your credentials are not saved, you are prompted with an authentication dialog and offered a **Remember this password** checkbox. Marking the checkbox causes your login credentials to be saved and appear in this tab.

Preferences	- IBM Asper	a Connect				-		
General	👫 Transf	ers 🕕	Network	松 Bandwidth	Security			
Trusted Hos	ts Restric	ted Hosts	Password	s Content Pro	otection			
Login informa	tion has beer	n saved for	the following	hosts:				
Host	L	lser				Re	emove	
https://10.	0.204.100 a	sp1				Ren	nove All	
https://198	.23.89.123 a	speraweb						

### **Content Protection**

To specify hosts to which you want all uploads to be encrypted, open the **Content Protection** tab under **Security**. In the Address field enter the Aspera server address and click **Add**. The server is then added to the list.

General	It Transfers	Network	松 Bandwidth	🔒 Security		
Trusted Hosts	Restricted Hos	ts Password	ls Content Pro	tection		
	tion allows you to le which you want to			which they have	been uploaded	. Enter a
Address:						Add
						400
Host					Re	move
https://demo	.asperasoft.com				Rem	ove All

When uploading files to a server on the list, or one that is configured as a content-protected host, you are prompted for a passphrase to encrypt the files. You can also choose not to encrypt files if the server allows it.

For details on encryption and decryption, see File Encryption.

# **Connect Functionality**

## **Initiating a Transfer**

The steps below describe how to use Connect to initiate a file transfer, and shows how to perform a download from Aspera's demo server.

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

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

Enter the following credentials when prompted:

- User: asperaweb
- Password: demoaspera

**Note:** Internet Explorer 11 Security Settings: When you open IBM Aspera Connect Server or IBM Aspera Faspex using Internet Explorer 11, an information bar appears and asks whether to run the Connect add-on. Click Allow to proceed.

This webpage wants to run the following add-on: 'Aspera, Inc.' from 'Aspera, Inc.'.	What's the risk?	Allow	•	×
---	------------------	-------	---	---

2. In Connect Server, open the folder aspera-test-dir-large.

To select a file or folder you want to download, click the checkbox next to it. You can also click multiple boxes to select more than one file or folder to download at a time. Once you've made your selections, click the **Download** button.

🕞 a	Welcome asperaweb ( <u>change us</u> aspera connect server									
	demo.asperasoft.com > aspera-test-dir-large aspera-test-dir-large									
Dow	nload 🛛 🕞 Upload 🖉 Upload Folder	Delete	New Folder							
	Name	Size	Last Modified							
t	Parent Directory									
	100MB	100MB	Apr 10, 2014 10:49:29 AM							
	10GB	10GB	Apr 10, 2014 10:49:04 AM							
	1GB	1000MB	Apr 10, 2014 10:49:23 AM							
	200MB	200MB	Apr 10, 2014 10:49:27 AM							

**3.** Confirm the download.

A dialog appears asking you to confirm whether the transfer should proceed. Select **Allow** to begin. To skip this dialog in the future, enable the checkbox **Use my choice for all connections with this host**.

G C	🤤 Confirm - IBM Aspera Connect					
	An attempt is being made to connect with 198,23,89,123. Do you want to allow this?					
	Use my choice for all connections with this host					
	Allow Deny					

4. Enter credentials to authenticate the transfer.

The following dialog appears asking for a username and password. Fill in the server account name and password.

**Note:** If the server OS is Windows and the you are using a domain account, all characters in the domain name must be uppercase.

Authe	nticate - IBM Aspera Connect	<
î	Login to: 198.23.89.123 User Name:	
	Password:	
	Remember this password OK Cancel	

You can also use the Aspera demo server to upload files. When you log in to the server, open the Upload folder. Click the **Upload** button to select files from your system to upload to the demo server. You can use the checkboxes to select multiple files to upload at once. To select folders to upload, click **Upload Folder**. Note: When uploading, do not transfer files whose names contain the following characters:

/ \ " : ' ? > < & \* |

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. To get started, simply point your browser to your server's host name. For example, if the server is running IBM Aspera Connect Server:

http://server\_host\_name/aspera/user

Note that the URL format of the address can be different, depending on your server product.

## **The Activity Window**

In the Activity window, you can view and manage all transfer sessions.

The Activity window contains the following controls:

- Open the Transfer Monitor. For more information on this feature, see Monitoring Transfers.
- C Open the folder on your computer that contains this content.
- • Stop the transfer.
- • • Resume a stopped transfer, or retry a failed transfer.

When the queuing option is enabled, the number of concurrent transfers is limited. The additional transfers are queued in the Activity window and initiated when a transfer is finished. You can manually start a queued transfer by clicking the  $\odot$  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.

G Activity - IBM Asp	yera Connect	_ '		×
IMG_6695.g	if			
Stopped	Resume Remove Show in Transfer Monitor Open containing folder Go to "http://demo.asperasoft.com/aspera/user/?B=%	2Faspera	-test-dir	
	Clear list			

# **Monitoring Transfers**

Connect lets you monitor and adjust file transfer speed from the Transfer Monitor window. To monitor a transfer session shown in the Activity window, click the  $\bigcirc$  icon shown with the session. The Transfer Monitor opens:

Transfer Monitor		_		×
10GB C:/tmp/10GB				
Downloading 2.9 / 1	0.0 GB (58.90 Mbps) - 17:19 remaining		7:57 e	~ ~
	100.00 Mbps			
60.57 Mbps				_
2				
0 bps				
Fair				•

The following controls are available in this window:

- Open the folder on your computer that contains this content.
- • Stop the transfer.
- $\odot$  Resume a stopped transfer, or retry a failed transfer.

If you have sufficient server privileges and your transfer server is configured to allow it, you can adjust or set your desired transfer rate, minimum transfer rate, and rate policy. However, actual performance is subject to the available bandwidth on your network as well as the transfer settings on your server:

•	Target transfer rate – To adjust the transfer rate, locate and select the upper slider $\bigcirc$ on the left side of the graph and move it up or down to change the desired rate. Note that the actual rate depends on several factors.
•	Minimum transfer rate – To set the minimum transfer speed, locate and select the bottom slider $2$ on the left side of the graph and move it up or down to set the desired rate. The actual minimum rate depends on several factors.
•	Transfer policy – Select the transfer policy from the drop-down list at the bottom of the window. Note that your specified rate policy may be subject to external limitations:
Fixed	
	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.
High	
0	The transfer rate is adjusted to use the available bandwidth up to the maximum rate.
Fair	
	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 no less than the minimum rate.
Low	
	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.
•	Additional options – Right-clicking in the area above the graph opens the same menu as doing so in the Activity window, giving options such as stop or remove transfers, and open the transfer's containing folder.

## **File Encryption**

When you upload files to a server configured as a content-protected host, you are prompted for a passphrase to protect the files with Aspera encryption. When you download those files, access to the files' contents requires that you provide the passphrase to decrypt them. Files can be decrypted during the download transfer, or decrypted after the download has completed. Files can be decrypted from within Connect, or by using the utility IBM Aspera Crypt, which is included in the Connect installation.

### **Encrypting Files**

Servers to which you want to upload encrypted files must be enabled for content protection. For more information, see Content Protection.

When uploading files to a content-protected server, you are prompted for a passphrase to encrypt the files. You can either enter the passphrase in the text field, or check **Keep files unencrypted** to proceed without using this feature (if allowed by the server). To start the transfer, click **OK**.

G Pr	otect Content - IBM Aspera Connect	×
1	Enter a passphrase to store files in an encrypted format on th server. A passphrase is required. Passphrase:	e
	Confirm:	
	OK Cancel	

Once Aspera-encrypted files have been uploaded to your server, they can be identified by an additional file extension, .aspera-env (Aspera Security Envelope).

Welcome asperaweb ( <u>change user</u> ) welcome asperaweb ( <u>change user</u> )							
	demo.asperasoft.com Download Jupload Colder Colder						
		Name	Size	Last Modified			
		Name IMG_4333.CR2.aspera-env	Size	Last Modified Apr 3, 2018 9:03:00 PM			
		IMG_4333.CR2.aspera-env	18MB	Apr 3, 2018 9:03:00 PM			

### **Decrypting Files During Download**

When you use Connect to download a content-protected file, a window opens prompting you for a decryption passphrase:

G Protected Content - IBM Aspera Connect X	G Protected Content - IBM Aspera Connect X
Enter a passphrase to decrypt protected files as they are downloaded. Passphrase: ••••••• Keep files encrypted	Enter a passphrase to decrypt protected files as they are downloaded. Passphrase: Keep files encrypted OK Cancel

You have two options:

- Enter the passphrase. In this case, Connect decrypts the files *during* the download. When the files arrive at their destination, they are no longer encrypted, and no further steps are necessary.
- Check the **Keep files encrypted** box. In this case, Connect transfers the files to the destination in the encrypted state. You don't need to enter a passphrase (if you do, it is ignored). With this option, the files retain the .aspera-env extension on your disk. You can decrypt the files any time after the download has completed.

To proceed with the download, click **OK**. The Connect Activity window appears and shows the progress of the transfer. When finished, the progress bar disappears, indicating the files are now at their destination.

#### **Decrypting Files after Download**

To decrypt downloaded files you have chosen to keep encrypted, run the IBM Aspera Crypt utility. You can launch Crypt using any of the following methods:

• From the Connect Activity window: Once the transfer is complete, the Connect Activity window displays the link Unlock encrypted files:

G Activity - IBM Aspera Connect	-		×
asptest_111.gif.aspera-env			
Decryption finished Done		∞ &	•
3697499833.jpg.aspera-env Unlock encrypted files Done		∞ @	۲

To launch Crypt, click **Unlock encrypted files**. This is the most convenient method for unlocking protected files once they've been transferred. Depending on your preferences settings, you can also decrypt your files from here later, as the transfer records remain in the Connect Activity window until you remove them by clicking **Clear List**. However, the files remain only if under the **Preferences > General** you chose to remove transfer list items **Manually** instead of automatically after transfer.

- By opening an Aspera-encrypted file: You can launch Crypt by opening an .aspera-env file from the context menu or by double-clicking the file.
- From the Connect application menu: To open the application menu, right-click the Connect icon in the Windows system tray. To launch Crypt, select **Unlock encrypted files**.

When you l	launch Crypt,	the following	window opens:
------------	---------------	---------------	---------------

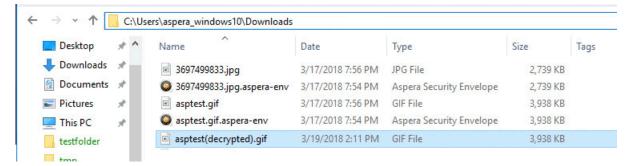
IBM Asperiation IBM Asperiation			_	×
	pen Folder Settings			
Passphrase:	Decrypt Decrypt 0%	Yiew:	Latest	•

If you launched Crypt from the Connect Activity window or by opening an aspera-env file, Crypt decrypts the files that were selected. From the Crypt window, you can also select **Open Files** or **Open Folder** and browse for files or folders to decrypt. 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.

To unlock protected content, fill in the encryption passphrase and click **Decrypt**. The files are unlocked and the results displayed in the window:

IBM Aspera Crypt File Options About						×
Open Files Open Folder Settings						
Passphrase: Show passphrase		Decrypt				
		100%	View:	Lates	t	•
3697499833.jpg.aspera-env	100.0%	Finished -> C:\ \aspera_windo\ \3697499833.jp	ws10\Do	ownloa	ads	

The decrypted files are placed in the same directory as the original encrypted files:



If you choose to decrypt a file and there is already an unencrypted file of the same name in that folder, the newly decrypted version appears in the Crypt window and the folder listing with "(decrypted)" added to the filename, as in the above example. However, note that if you decrypt the file yet again, the "(decrypted)" file is overwritten without notice.

# **Maintaining Your Connect Installation**

# Upgrading

When a new version becomes available, Connect prompts you to confirm whether to upgrade.

If Connect does not prompt you to upgrade (for example, because the system has no Internet access), you can obtain an upgrade from the Aspera download site. To download the latest version of Connect, go to http://downloads.asperasoft.com/connect. Click **Download Now** and follow the on-screen instructions. This downloads the latest installer.

You are also prompted to upgrade if you attempt a download and Connect is not found or otherwise unable to launch:

If Connect is not installed, or is out of date, you can download it from here by clicking **Download latest version**. If Connect s already installed, you can click **Troubleshoot** to open the IBM Aspera Connect Diagnostic Tool. You can also access the tool here:

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

## Uninstalling

Important: You must quit Connect before uninstalling it.

To uninstall Connect, 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

Old Connect files can be safely removed from your system.

### Log Files

Log files are found in the following location. Log files can be removed at any time.

C:\Users\username\AppData\Local\Aspera\Aspera Connect\var\log\

#### http.uri and process.pid Files

You can 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. To remove the database file for all users, you must locate and remove the database file for each user account:

```
C:\Users\username\AppData\Local\Aspera\Aspera Connect\var
\asperaconnect.data
```

Note that when uninstalling earlier versions of Connect, the database file may instead be found in the following location:

```
C:\Users\username\.aspera\connect\connectdb.data
```

### **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

## Log File Location

Log files are located in the following directory:

C:\Users\username\AppData\Local\Aspera\Aspera Connect\var\log\

You can also access the log folder from the Connect system tray: right-click G > Open log folder

Activity	Ctrl+T
Unlock encrypted files	Ctrl+R
Open log folder	Ctrl+L
Preferences	Ctrl+P
Check for updates	Ctrl+U
About	Shift+F1
Quit	Ctrl+Q

For information on removing old log files, see File Cleanup.

# Troubleshooting

## Error When Installing with a Non-Admin Account

You may encounter an error such as the following (or with similar wording) if you are not an Administrator when executing the MSI installer file.

The system administrator has set policies to prevent 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 2016:

1. Launch the Microsoft Management Console (MMC).

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

resource, and Windows will open it for you.	(4) Design (a) and (2) Designed a second (2) (2) → Φ (4) a (2) Design (2) → Φ(2) Design (2) Design (2) Design (2) Design (2) → Φ(2) Design (2)	den en de	T	6 LL	
Open: mmc		Open:	mmc		、 、

- 2. Add the Group Policy Object Editor Snap-in.
  - a. In the MMC, go to the toolbar and select File > Add/Remove Snap-in:

-	File	Action	View	Favorites	Window	Help
		New			Ctrl+N	
C		Open			Ctrl+0	-
		Save			Ctrl+S	
		Save As				
		Add/Rem	ove Sna	p-in	Ctrl+M	
		Options				
		Recent File				
		Exit				

b. In the Add or Remove Snap-ins window, select the Group Policy Object Editor and click Add:

ailable snap-ins:	n		Selected snap-ins:	
nap-in	Vendor	<u>^</u>	Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Remove
Authorization Manager	Microsoft Cor			KENOVE
Certificates	Microsoft Cor		2.22	
Component Services	Microsoft Cor			Move Up
Computer Managem	Microsoft Cor			Move Down
Device Manager	Microsoft Cor	Add	>	PROVE DOWN
Disk Management	Microsoft and			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Internet of the state of the last of the last of the state of the stat				
IP Security Monitor	Microsoft Cor		1	
IP Security Policy M	Microsoft Cor			
Link to Web Address	Microsoft Cor	~		Advanced
cription:				

c. In the Select Group Policy Object window (wizard), under Group Policy Object, click **Browse** and select either **This Computer** or specify another computer. When done, click **OK** to return to the wizard window.

- **d.** In the wizard window, click **Finish**. When you are returned to the **Add/Remove Snap-ins** window, click **OK** to save the changes.
- 3. Grant the Windows installation group policy.
  - a. In the MMC, navigate into Console Root > Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components and locate Windows Installer:

🖀 Console1 - [Console Root\Local Computer Policy\Computer Configuration\Administrative Templates\Windows C 👝 💼 💌					
🔚 File Action View Favorit	es Window Help			_ 8 ×	
🗢 🔿 🖄 🖬 😖 🛛 🗊	7				
Console Root	📋 Windows Components			Actions	
<ul> <li>Local Computer Policy</li> <li>Response Computer Configuration</li> </ul>	Windows Installer	Setting	*	Windows Components 🔺	
Software Settings		📔 Windows Defender		More Actions	
Windows Settings Administrative Tem		Windows Error Reporting Windows Explorer		Windows Installer	
Administrative Ferri Diagonal Control Panel		Windows Installer		More Actions 🔹 🕨	
D Metwork		📔 Windows Logon Options 🛛 🗟			
Printers		🚞 Windows Mail			
System		🚞 Windows Media Center			
Windows Comp		📔 Windows Media Digital Rights N	Ξ		
All Settings		📔 Windows Media Player			
Viser Configuration		📔 Windows Messenger			
		📔 Windows Mobility Center	Ŧ		
	l	4			
۰ III • •	Extended Standard				

- b. Double-click Windows Installer.
- c. In the list that appears, locate Turn off Windows Installer and double-click it.
- d. The Turn Off Windows Installer window opens.
- e. Under the Turn off Windows Installer heading, select **Enabled**. In the Disable Windows Installer box, open the pull-down and select **Never**. When finished, click **OK**:

Turn off Windows Installer	— <b>D</b> X
Turn off Windows Installer	Previous Setting Next Setting
<ul> <li>Not Configured Comment:</li> <li>Enabled</li> <li>Disabled</li> <li>Supported on:</li> </ul>	At least Windows 2000
Options: Disable Windows Installer Never Always For non-managed applications only Never	Help: This policy setting restricts the use of Windows Installer. If you enable this policy setting, you can prevent users from installing software on their systems or permit users to install only those programs offered by a system administrator. You can use the options in the Disable Windows Installer box to establish an installation setting. The "Never" option indicates Windows Installer is fully enabled. Users can install and upgrade software. This is the default behavior for Windows Installer on Windows 2000

- f. To close the MMC, click File > Exit.
- g. When prompted to save console settings, click Yes to save the settings to a file. When prompted for a .msc filename, click Save.
- h. Reboot the computer to apply the changes, or execute the following command at a command prompt:

> gpupdate /force

## **Connectivity Issues**

### SSH Connectivity Errors: "Timeout establishing connection"

If you receive the error "Timeout establishing connection," the TCP connection between the IBM Aspera Connect 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.

### **IBM 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 https://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 https://www.ibm.com/mysupport/ using your IBMid (not your company Aspera credentials), or set up a new account. Search for Aspera and select the product. Click **Follow** to receive notifications when new knowledgebase articles are available.

### **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.

Email	aspera-support@ibm.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

# Legal Notice

© 2008-2016-2017-2018 Aspera, Inc., an IBM Company. All rights reserved.

Licensed Materials - Property of IBM 5737-A72 © Copyright IBM Corp. , 20082016,2017, 2018. 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.