IBM Aspera Connect 4.2 User Guide

IBM

Contents

IBM Aspera Connect User Guide for Linux

Welcome to the Connect documentation, where you can find information about how to install, maintain, and use Connect.

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 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	A web browser starts uploads and downloads transparently.
File syncing	Background synchronization of files.
Flexible transfer types	Easily transfer single files, multiple files, or entire directories.
Transfer retry and resume	Automatically retries and resumes partial and failed transfers.
Browser-independent transfer	The web browser can be closed once transfer operations started.
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.
Queuing	Allow a fixed number of concurrent transfers, and place the rest in a queue.

When you give Connect access to the IBM Aspera on Cloud SaaS platform, you can do the following tasks:

- Transfer files and packages from within the same browser view.
- Synchronize local folders with folders on the transfer server, in both directions.

When you give Connect access to an IBM Aspera Faspex transfer server, you can do the following tasks:

- Send packages to Faspex users and workgroups.
- Automatically download packages as they are received.

When you give Connect access to an IBM Aspera Shares transfer server, you can do the following tasks:

- Transfer files and folders to and from the transfer server.
- Synchronize local folders with folders on the transfer server, in both directions.

Drag-and-drop support

The drag-and-drop feature is not supported on Linux systems in this release of Connect.

Setting up Connect

Installation

The procedure for installing IBM Aspera Connect requires enabling a browser extension for Connect in addition to installing the Connect application itself.

There are two ways to install 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: For system-wide (multi-user) installations, and a fallback method for users with nontypical web apps. You first install the Connect web extension for your browser. You then install the Connect application by running a desktop installer that you download from the Aspera website.

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

Before you begin

Verify that your Linux environment includes the following libraries:

- OpenSSL version 1.0.2g or higher. See the following details.
  - Mesa EGL (If you get a launch error about libel. See the following details.
- glib2 version 2.28 or higher.

The absence of up-to-date versions of these libraries might prevent Connect from starting.

Note: Connect does not support the Wayland compositor in this release. Some new distributions of Linux are switching to Wayland. If so, you can work around it by switching to Xorg mode.

OpenSSL

Depending on your Linux distribution and version, you might need to update your OpenSSL installation to allow Connect to start. The required minimum version of OpenSSL is **1.0.2g**. To determine which version of OpenSSL is installed on your machine, run:

```
$ openssl version
```

For information on how to download and install the latest version of OpenSSL, see the KB article Upgrading OpenSSL on Linux for Connect 3.7.x.

Mesa EGL

Connect requires Mesa EGL to be installed on your machine. If you are unable to start Connect, and you encounter an error about libEGL, it generally means that the Mesa EGL package is not installed. To confirm this, run the following:

```
$ ldd ~/.aspera/connect/plugins/platforms/libqxcb.so
```

If you then see the following, you need to install the Mesa EGL library on your machine:

```
libEGL.so.1 => not found
```

To install the Mesa EGL libraries on Debian (for example), run:

```
$ sudo apt-get install libegl1-mesa
```

Then restart your machine.

For other Linux OSs, run the equivalent command.

Guided installation

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

Required Steps

To enable Aspera uploads and downloads, you need to install
or upgrade to IBM Aspera Connect 4.2.7.

New
Step 1   Install Extension

Step 2   Install Connect

Already installed? Refresh / Troubleshoot

Depending on your browser/platform combination, the screens that are shown in these instructions might vary.

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 7 to install the Connect extension. If successful, you'll see the message confirming the extension was added.

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

When you click **Install Connect** the installer image is downloaded to your `Downloads` directory. Once downloaded, close your web browser and run the following commands in the installer's directory, replacing *version+platform* with the equivalent from the file name of the installer you downloaded:

```
$ tar -zxvf ibm-aspera-connect-version+platform.tar.gz
$ ./ibm-aspera-connect-version+platform.sh
```

Note: Do not run the Connect installation script as the **root** user. Connect on Linux might only be installed per user, as opposed to system wide. To avoid errors, install Connect per user, excluding user **root**.

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 7.

Step 2 - Download and run the Connect application installer.

You can download the `tar.gz` file that contains the Connect installer for your Linux platform directly from https://www.ibm.com/aspera/connect/. Once downloaded, close your web browser and run the following commands in the installer's directory, replacing *version+platform* with the equivalent from the file name of the installer you downloaded:

```
$ tar -zxvf ibm-aspera-connect-version+platform.tar.gz
$ ./ibm-aspera-connect-version+platform.sh
```

Note: The Connect installation script must *not* be run by user **root**. Connect on Linux might only be installed per user, as opposed to system wide. To avoid errors, install Connect per user, excluding user **root**.

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 that you are going to 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 following procedure:

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:
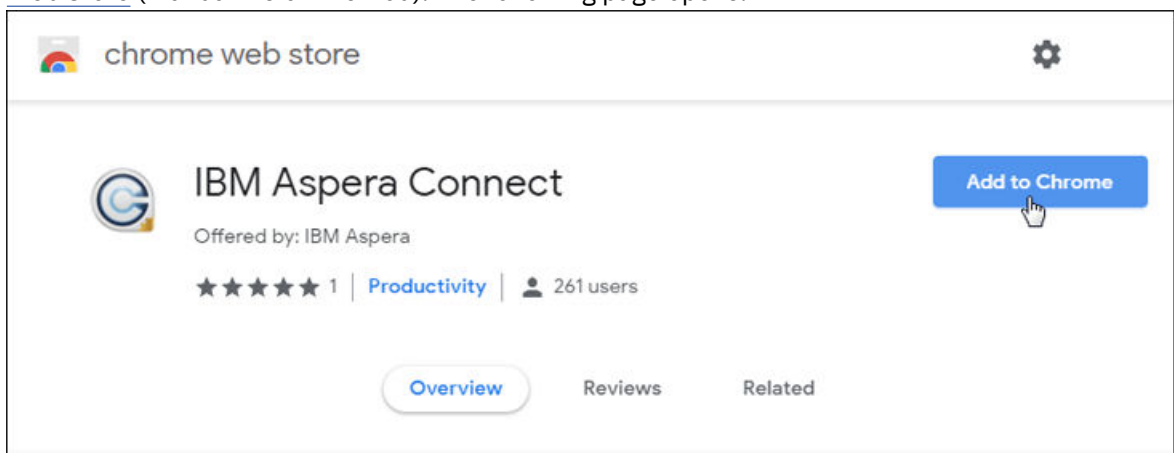
2. Click **Add to Chrome**. The **Add "IBM Aspera Connect"?** window appears.
3. Click **Add extension**.

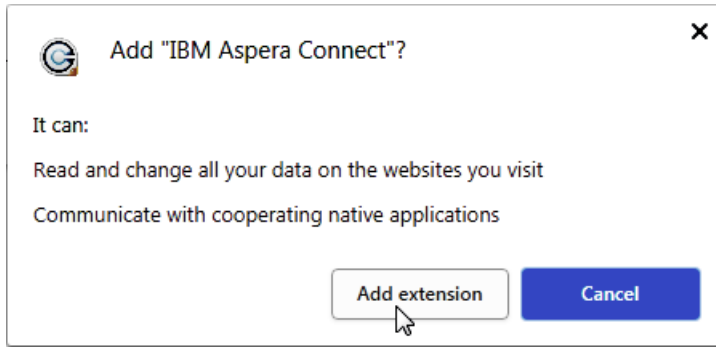If successful, you'll see the message *"IBM Aspera Connect has been added to Chrome"*.

Note: The extension is activated only by websites that have integrated IBM Aspera for file transfers. The extension never reads or stores any personal information or history.

Incognito Mode: By default, the Connect extension is disabled in Chrome's incognito mode. To enable the Connect extension, right-click the Connect icon that is in the extensions bar of your browser. Then open **Manage extensions** and scroll down to the heading **Allow in incognito**. Then set the switch to ON as shown in the following image.

Firefox

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

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:
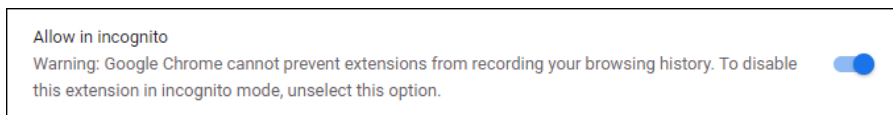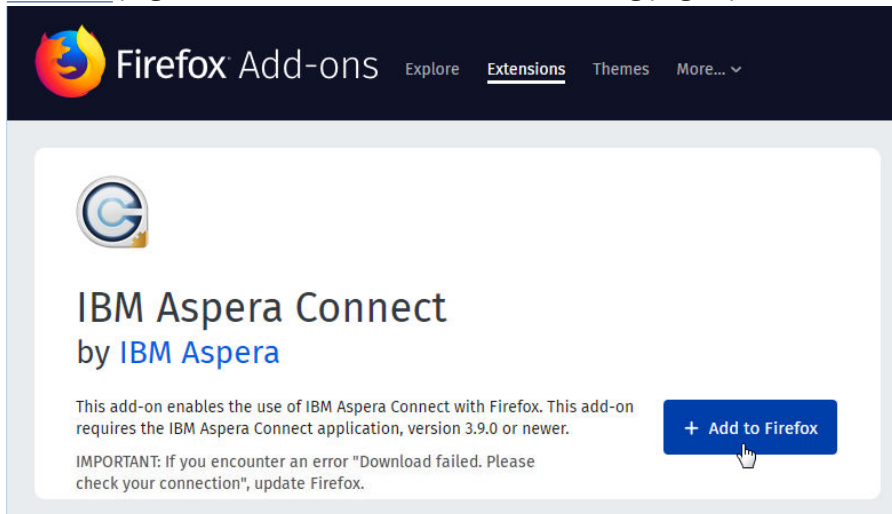

2. Click **+ Add to Firefox**. The **Add IBM Aspera Connect?** pop-up window appears.
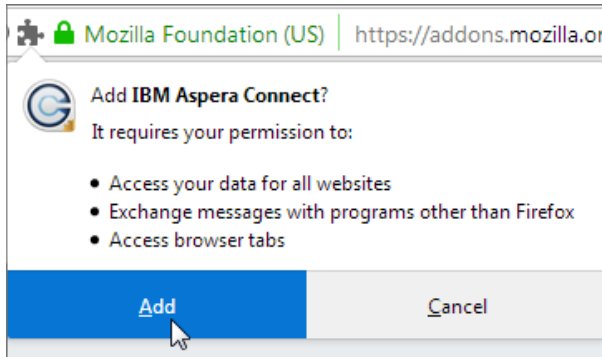
3. Click **Add**.

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

After Installation

Once Connect finished installing, it runs automatically when you access a Connect, Faspex, or IBM Aspera Shares web page. Look for the Connect icon in your menu bar to confirm that it's running.

If Connect does not start automatically (or if you need to restart it), you can run the application manually with the following command:

```
$ ~/.aspera/connect/bin/asperaconnect
```

> **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:
>
> IBM Aspera Connect Diagnostic Tool

Network environment

Connect typically requires some configuration steps to function in your network environment. Configuration settings also allow you to limit transfer rates and use an HTTP proxy.

Network requirements

Your SSH outbound connection might differ based on your organization's network practices. Although TCP/33001 is the default setting, consult your IT department for questions that are 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 need to allow the following connections:

• Outbound connections for SSH, which is TCP/33001 by default, although the server side might 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 might run FASP transfers on one or more other ports. Check with your IT department for which SSH ports are open for FASP transfers.

HTTP and FASP proxies

If you need to configure any network proxies or override network speeds, you can do so through the Connect **Network** option. For more information about configuring proxies, see "Network configuration" on page 39.

Limit transfer rates

You can limit the bandwidth that Connect uses. For example, your office might have limited bandwidth to share among its users.

Important: For the SaaS products Files and Aspera on Cloud, use this field to set the *default transfer speed*.

You can limit Connect transfer rates by launching the Connect Preferences dialog and go to the **Bandwidth** tab.
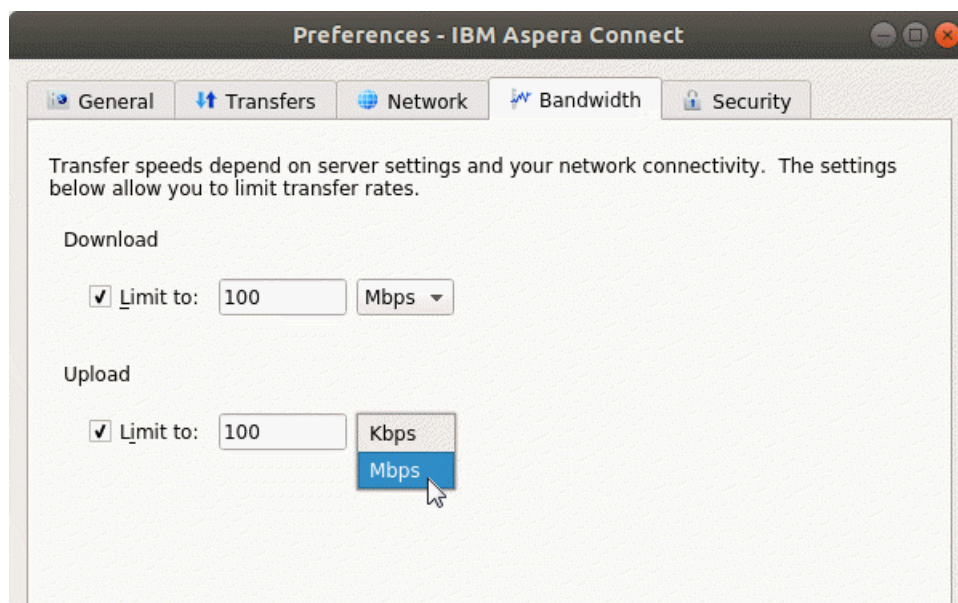
You can limit the download and upload transfer rates by selecting the respective check-boxes and entering a rate in either Mbps or Kbps. Setting a maximum speed doesn't guarantee your transfers achieve that speed. Actual performance depends on the following factors:

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

For more information about bandwidth configuration settings, see "Bandwidth configuration" on page 40.

Transferring files with Connect

Initiating a transfer

You can use Connect with the Aspera demo server to test basic transfer functions and also familiarize yourself with how to initiate uploads and downloads.

The following steps describe how to initiate a file transfer, and shows how to perform a download from Aspera demo server.

Important: 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 demo transfer server at https://aspera.pub/60OtzmU.
2. On the **AoC Demo** page, open the folder small.

   To select a file or folder you want to download, click the check-box 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 **Download**.
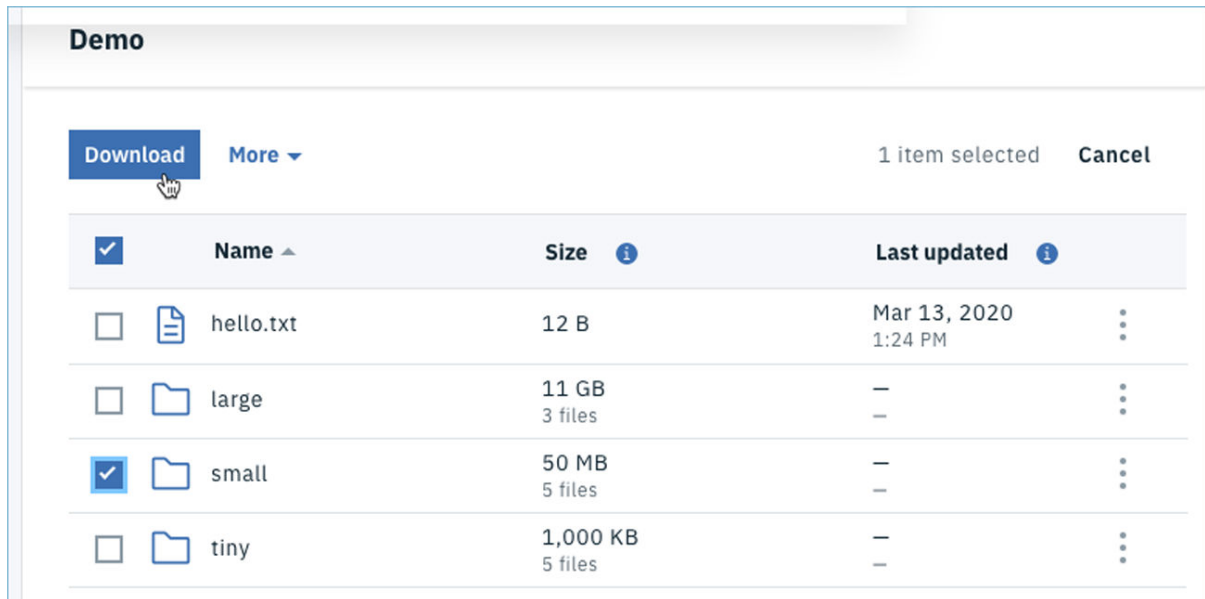
3. Confirm the download.

   A dialog appears asking whether you want to allow the server access to your machine. Select **Yes** to begin. To skip this dialog in the future, enable the check-box **Remember my choice for this site**. The server is then added to your **Trusted Hosts** list. For more information on trusted hosts and how to manage them, see "Security configuration" on page 40.

   The way hosts are granted access differs from previous Connect releases. Instead of prompting for permission to communicate with a transfer node when a transfer is about to start, Connect prompts for the website when the website first tries to interact with the Connect APIs. Thus, the address in the dialog is no longer a transfer server, but is instead the address of the website. As a result, sites that perform transfers with many different hosts no longer need to respond to access requests from each of those hosts because there will be only a single request for the website.

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, point your browser to your server's hostname.

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

Multi-session transfers

Data can be transferred faster by using multiple-session transfers (also known as parallel transfers and multi-part transfers) to and from multi-node servers and clusters, on premises, or in the cloud.

If a transfer meets the criteria that you configure in the Connect **Preferences** dialog, files are automatically transferred with multiple sessions.

Configuring multi-session transfers

Launch the Connect Preferences dialog and go to the **Transfers** tab.
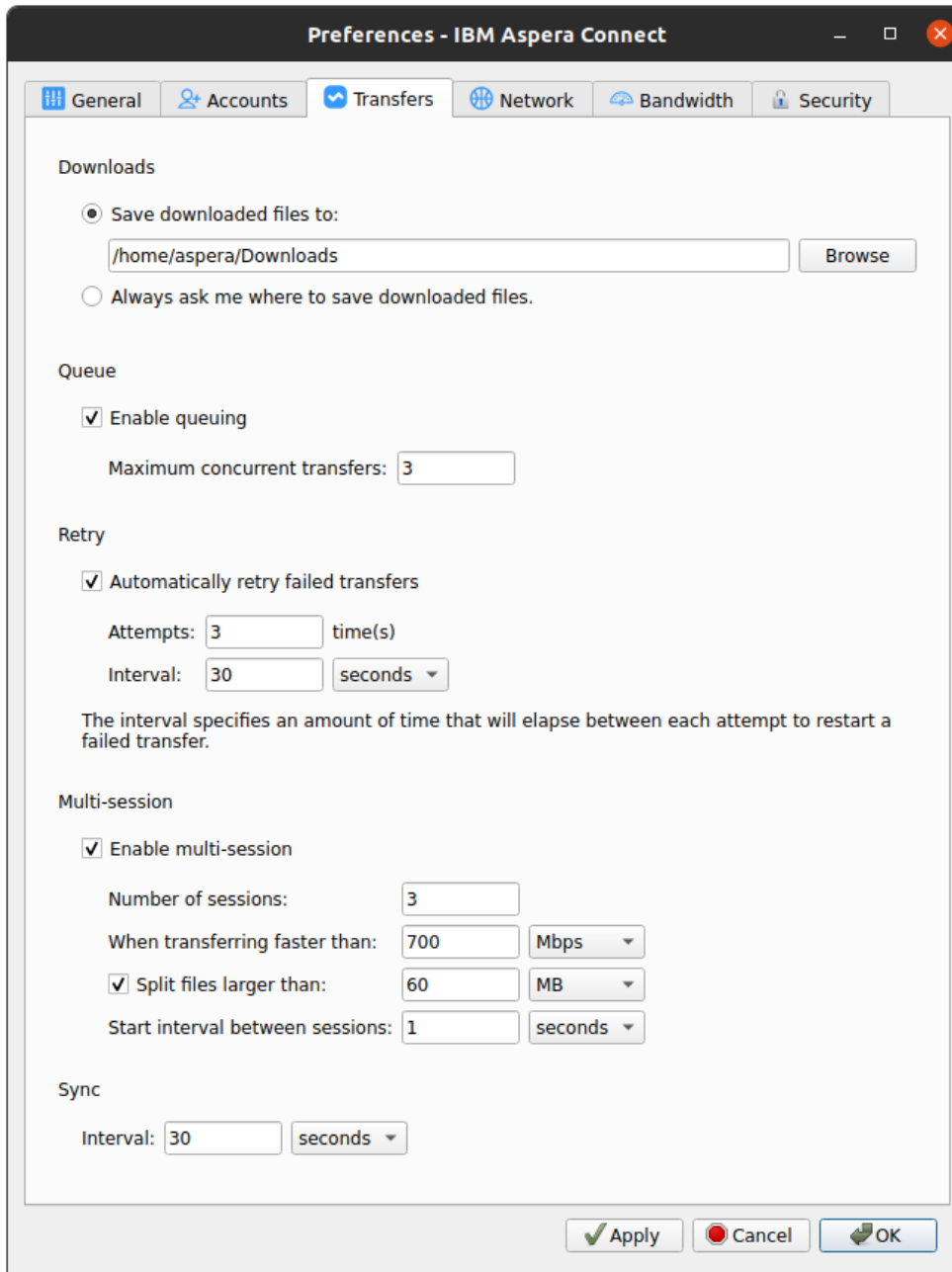
Field	Description	Default Setting
Enable multi-session	Enable multi-session transfers.	Unselected

| Field	Description	Default Setting
Number of sessions	The number of sessions you prefer (as guidance, not as a requirement).	3
When transferring faster than	The transfer speed that triggers multi-session transfers.	700 Mbps
Split files larger than	Enable file splitting for files larger than or equal to the specified size. This value is sometimes also referred to as the *multi-session threshold*. For example, by using the default size value (60 MB), if the source directory contains multiple files, all files less than 60 MB are distributed between sessions, while all files 60 MB or larger are split and then distributed between sessions. If the source directory contains only one file and the file is 60 MB or larger, the file is split, otherwise the file is transferred by one session.	60 MB
Startup interval between sessions	The amount of time to wait before the next session starts.	1 second

Limitations

- **Encryption-at-Rest (EAR)**: Files cannot be split when EAR is used. If EAR is specified, splitting is disabled.
- **Resuming transfers**: When file splitting is enabled, the **ascp** resume-transfer option is set to **-k 0** (always transfer the entire file again). If you need the ability to resume transfers, disable file splitting.
- **HTTP fallback**: HTTP fallback cannot be used with multi-session transfers. If specified, HTTP fallback is ignored.
- **Single-file transfers without splitting**: A multi-session transfer of a single file without file splitting potentially results in a slower transfer. The target rate for each session is 1/N of the total target rate. If a file is not split, only one session does productive work. This might not be an actual limitation if the single session is already taking advantage of all available bandwidth; for example, if a single session that transfers at maximum speed obtained the same transfer rate.

Advised practices

- **When to use multi-session**: Enable multi-session only when:
  - You must have a fast network connection (>1 Gbps).
  - The server has a slower network connection than your network connection (cloud virtual machines).
  - Extra servers are available to handle more traffic (cluster of servers).
- **Startup Interval**: If you have a large transfer that requires the transfer cluster to scale to meet the demand, set a higher startup interval to allow extra virtual machines to come online. It can take 5-15 minutes for new instances to become available.

The Activity window

Right-click Ⓖ and select **Activity** to open the **Activity** window, where you can view and manage all transfer sessions. From here you can stop a transfer, resume it, retry a failed transfer, and open the location that contains the content.
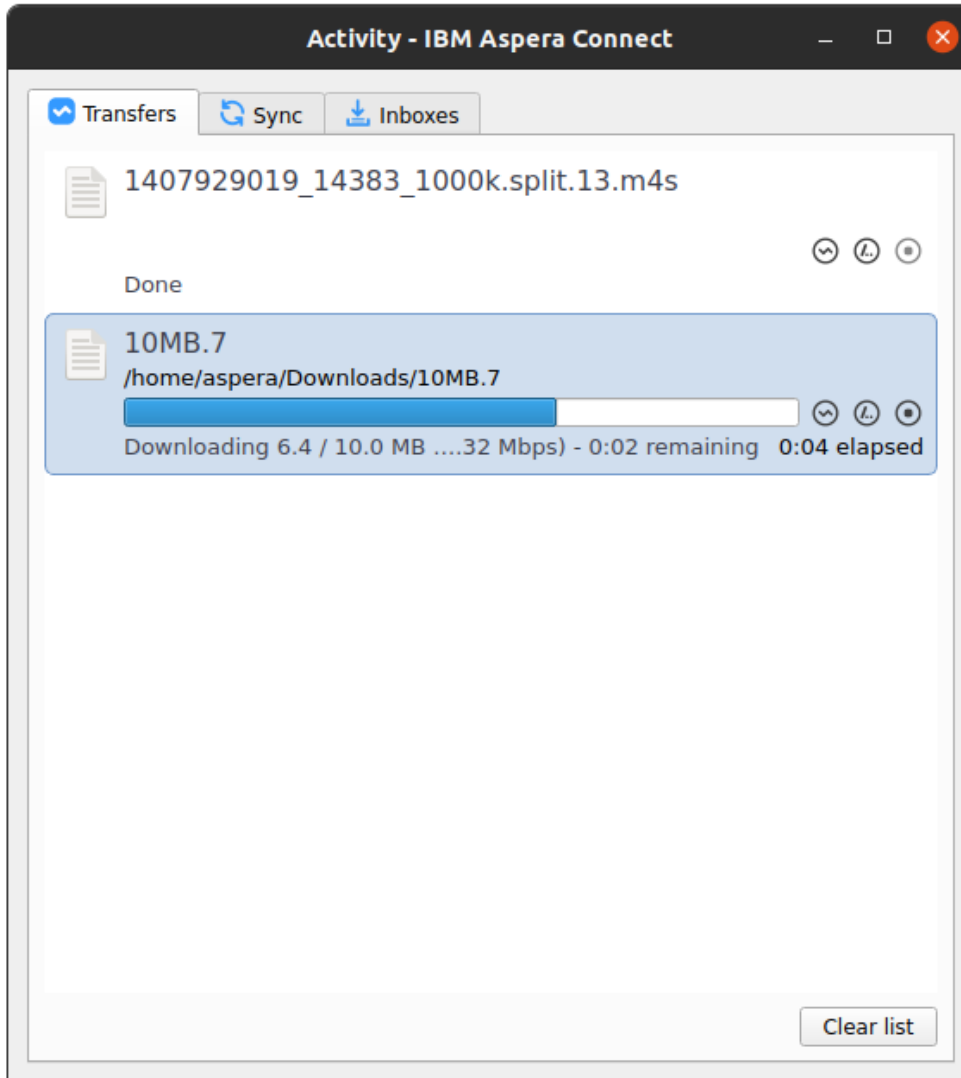
The Activity window contains the following controls:

- ⊙ Open the Transfer Monitor. For more information about this feature, see <u>Monitoring Transfers</u>.
- ⓛ 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 ⊙. You can also right-click on a started or stopped transfer to access various controls. The following example shows the right-click options for a stopped transfer.
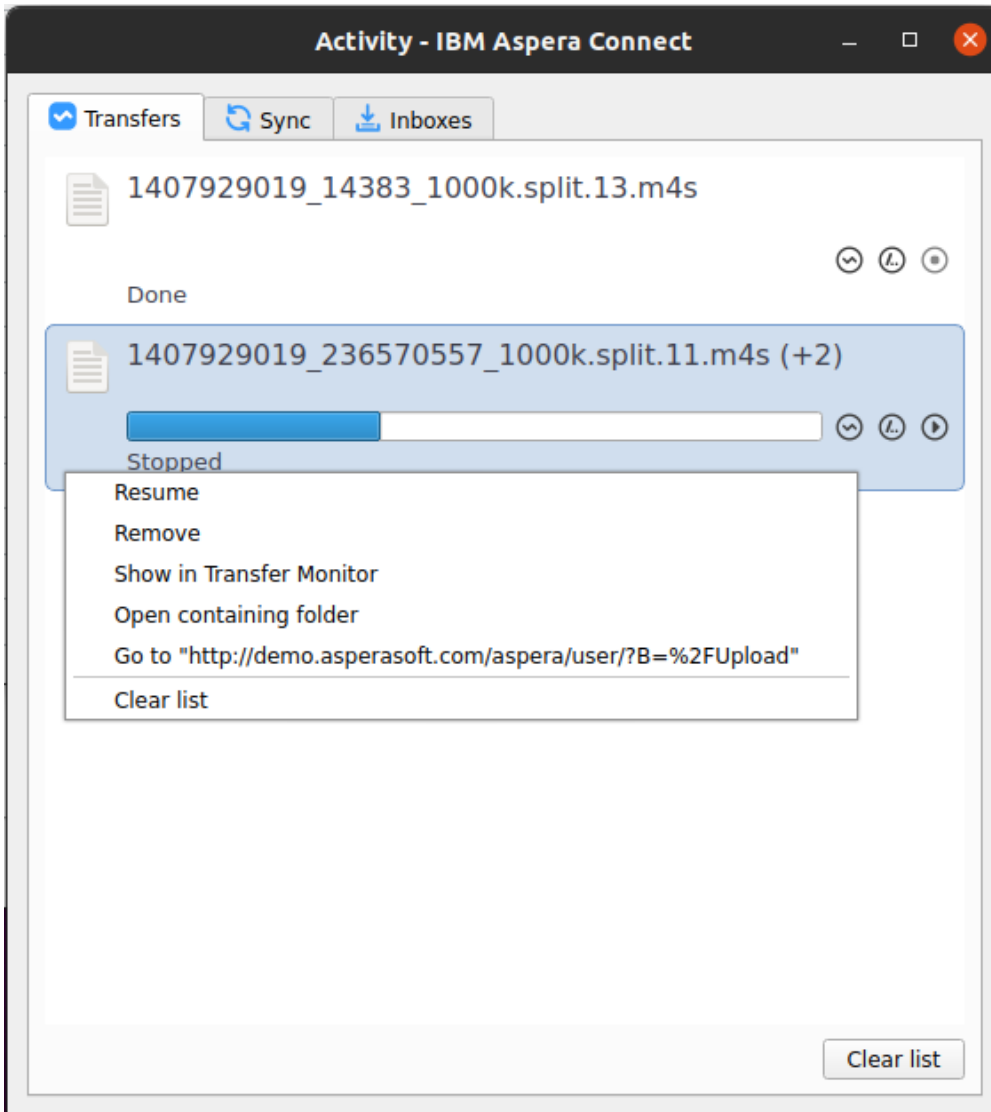
Monitoring transfers

From the Transfer Monitor window, you can monitor transfer progress. The Transfer Monitor provides a graphical interface to adjust file transfer speed, adjust the minimum transfer rate, and set rate policy, all while the transfer is in progress.

To monitor a transfer session shown in the **Activity** window, click the ⊙ icon that is shown with the session. The Transfer Monitor opens:
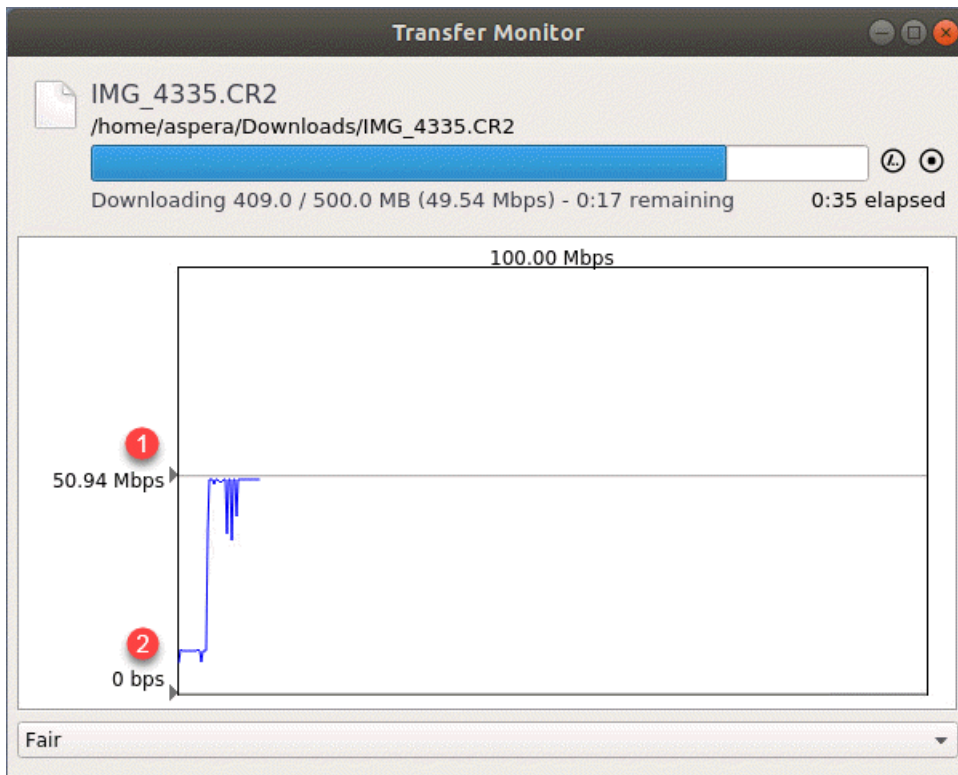
The following controls are available in this window:

- Ⓛ Open the folder on your computer that contains this content.
- ⊙ Stop the transfer.
- ⊙ 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 wanted 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 first slider ❶ and move it up or down to change the wanted rate. The actual rate depends on several factors.
- Minimum transfer rate – To set the minimum transfer speed, locate, and select the second slider ❷ and move it up or down to set the wanted rate. The actual minimum rate depends on several factors.
- Transfer policy – Select the transfer policy from the drop-down list. Your specified rate policy might be subject to external limitations:

    Fixed
    The transfer transmits data at a rate equal to the target rate, although this might impact the performance of other traffic present on the network.

    High
    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.

- More options – Right-clicking within the graph area opens the same menu available in the **Activity** window, offering options such as stop or remove transfers and access the folder containing the transfer.

File encryption

Connect provides a means to protect files with Aspera encryption when the files are uploaded to a content-protected server, and to decrypt those files when downloaded.

Whenever you upload files to a server configured as a content-protected host, Connect prompts you to create 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 is complete. 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 the Content Protection section of Security Config.

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**.

Once Aspera-encrypted files are uploaded to your server, you can identify them by an extra file extension, `.aspera-env` (Aspera Security Envelope).
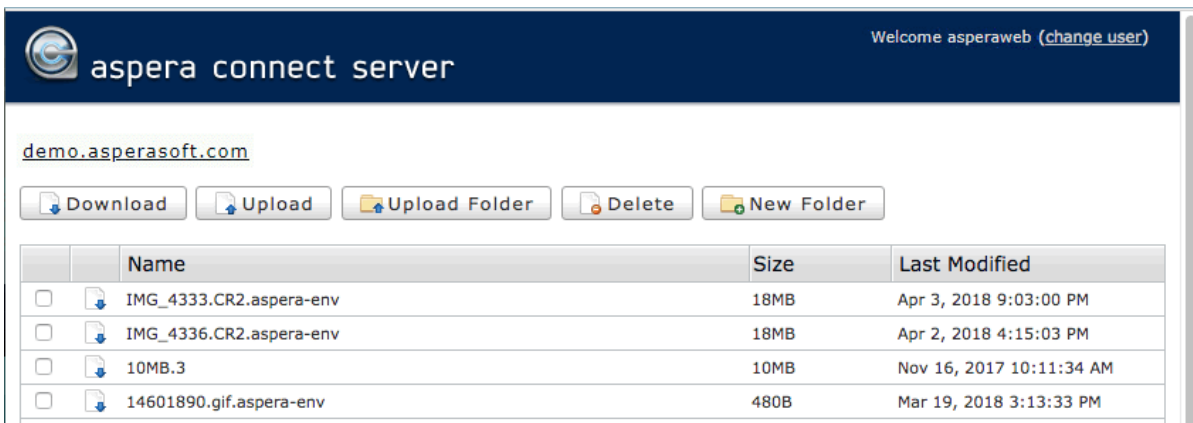
Decrypting Files During Download

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

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 anytime after the download is completed.

Note: If you choose to decrypt encrypted files during download, the transfer might fail if the password you supply doesn't apply to all the encrypted files. In this case, retry downloading and check the box for **Keep files encrypted**. You can then decrypt them after they are downloaded. See "Decrypting Files after download" on page 18 in the following section.

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 that you have chosen to keep encrypted, run the **IBM Aspera Crypt** utility. You can start **Crypt** by 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**:
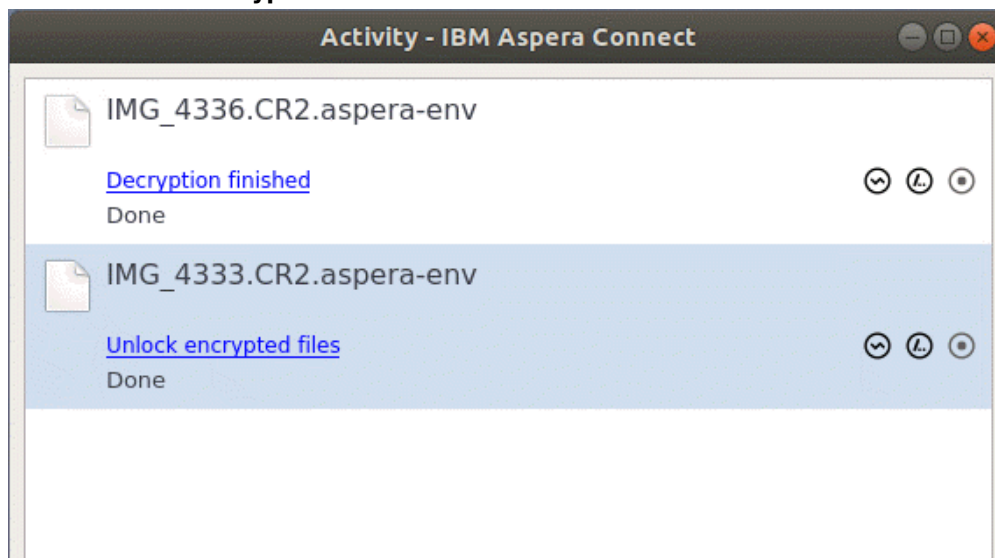
To start Crypt, click **Unlock encrypted files**. This is the most convenient method for unlocking protected files once they've been transferred. Depending on your preferences settings, you can also decrypt your files from here later, as the transfer records remain in the Connect Activity window until 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 start Crypt by opening an `.aspera-env` file from the menu or by double-clicking the file.
- From the Connect application menu: To open the application menu, click the Connect icon in the menu bar. To start Crypt, select **Unlock encrypted files**.

When you start Crypt, the following window opens:
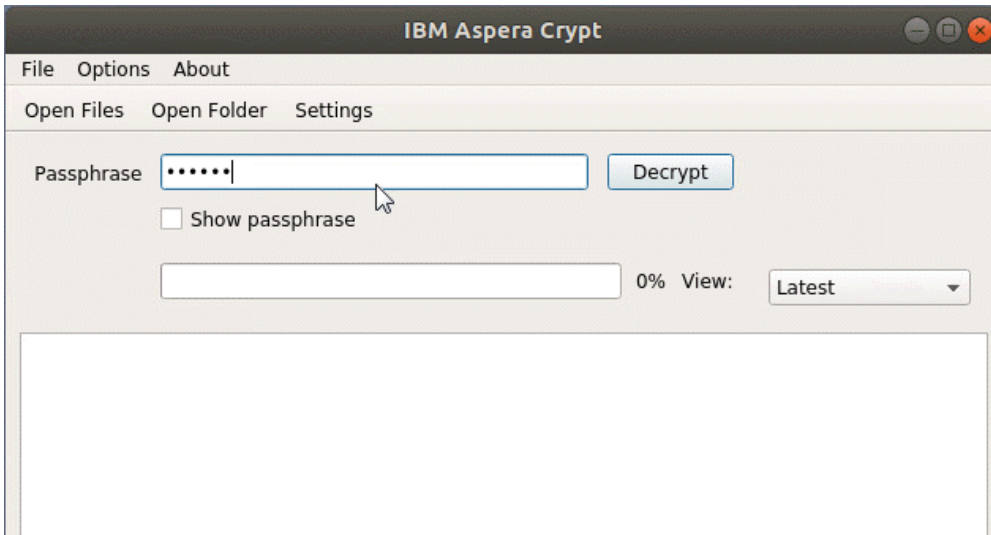
If you started Crypt from the Connect Activity window or by opening an `aspera-env file`, Crypt decrypts the files that were selected. From the Crypt window, you can also select **Open Files** or **Open Folder** and browse for files or folders to decrypt. When your encrypted contents are loaded into Crypt, a status message is displayed within the application's interface, displaying the number of items ready for decryption.

To unlock protected content, type the encryption passphrase and click **Decrypt**. The files are unlocked and the results that are displayed in the window:
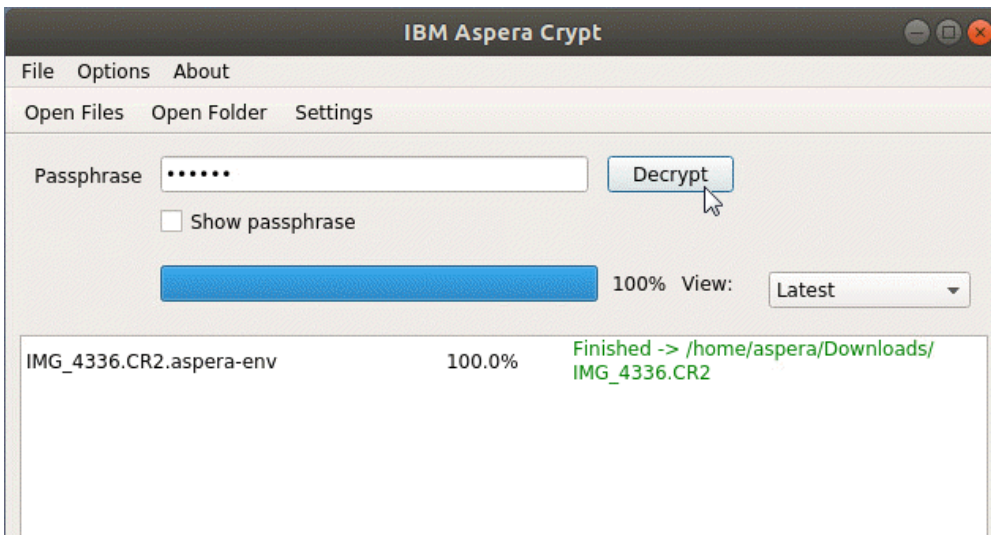
The decrypted files are placed in the same directory as the original encrypted files:

```
aspera@kbequa:~/Downloads$ ls -l
total 748792
-rw-rw-r-- 1 aspera aspera   19827846 Apr 16 18:21 IMG_4333.CR2
-rwxrwxrwx 1 aspera aspera   19827966 Apr 16 16:52 IMG_4333.CR2.aspera-env
-rw-rw-r-- 1 aspera aspera   19827846 Apr 16 18:25 IMG_4333(decrypted).CR2
-rw-rw-r-- 1 aspera aspera   19834559 Apr 16 16:58 IMG_4336.CR2
-rwxrwxrwx 1 aspera aspera   19834679 Apr 16 16:51 IMG_4336.CR2.aspera-env
-rw-rw-r-- 1 aspera aspera   19834559 Apr 16 18:26 IMG_4336(decrypted).CR2
```

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 file name, as in the previous example. However, if you decrypt the file yet again, the "**(decrypted)**" file is overwritten without notice.

Maintaining Your Connect Installation

Upgrading Connect

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

Note: Before you upgrade, verify that you don't have previous Connect installations on your system – either single-user or system-wide.

Note: If you need to revert to an earlier version of Connect, be sure to delete the Connect database before reverting. You can create a copy of the Connect database before the upgrade.

⚠️ **Attention: Upgrading IBM Aspera Connect 3.1X or earlier**

To avoid potential issues with performance and stability after upgrading Connect, you must clear all transfers (before proceeding with the upgrade) from the Activity window.

Restart Connect, and confirm that there are no transfers in the Activity window. Repeat the process as needed.

Tip: For all versions of Connect, it is a good idea to manually quit the application from time to time. This allows Connect to clear successful transfers accumulated over time from the database.

To download the latest version of Connect, go to https://www.ibm.com/aspera/connect/. Click **Download Now** and follow the on-screen instructions. This downloads the latest installer.

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

Required Steps

To enable Aspera uploads and downloads, you need to install
or upgrade to IBM Aspera Connect 4.2.7.

New
Step 1   Install Extension

Step 2   Install Connect

Already installed? Refresh / Troubleshoot

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

```
IBM Aspera Connect Diagnostic Tool
```

Connect and Aspera Drive

Note: Connect 4.0 and later include all Drive features and is the official upgrade path for Aspera Drive.

If you have IBM Aspera Drive installed, Connect prompts you to migrate your Drive settings to Connect. If you accept, Connect migrates Drive settings, and then prompts you to uninstall Drive.

Uninstalling

The Connect installation provides scripts for uninstalling Connect.

Uninstalling the Connect application

Important: You must quit Connect before uninstalling it.

After you quit the Connect application, run the following script to uninstall it:

```
$ ~/.aspera/connect/var/uninstall.sh
Uninstall finished.
```

Removing the Connect browser extension

For Chrome and Firefox, the browser extension is removed separately, described as follows.

Chrome

To remove the extension from Chrome, click the three-dot icon (Customize and control Google Chrome

⋮) of the Chrome window.

Note: In certain circumstances, the default three-dot icon might not be visible while displaced by other icons. For example, a circular yellow/orange icon with an arrow indicates Chrome needs to be updated.

In the drop-down menu that opens, choose **More Tools > Extensions**:
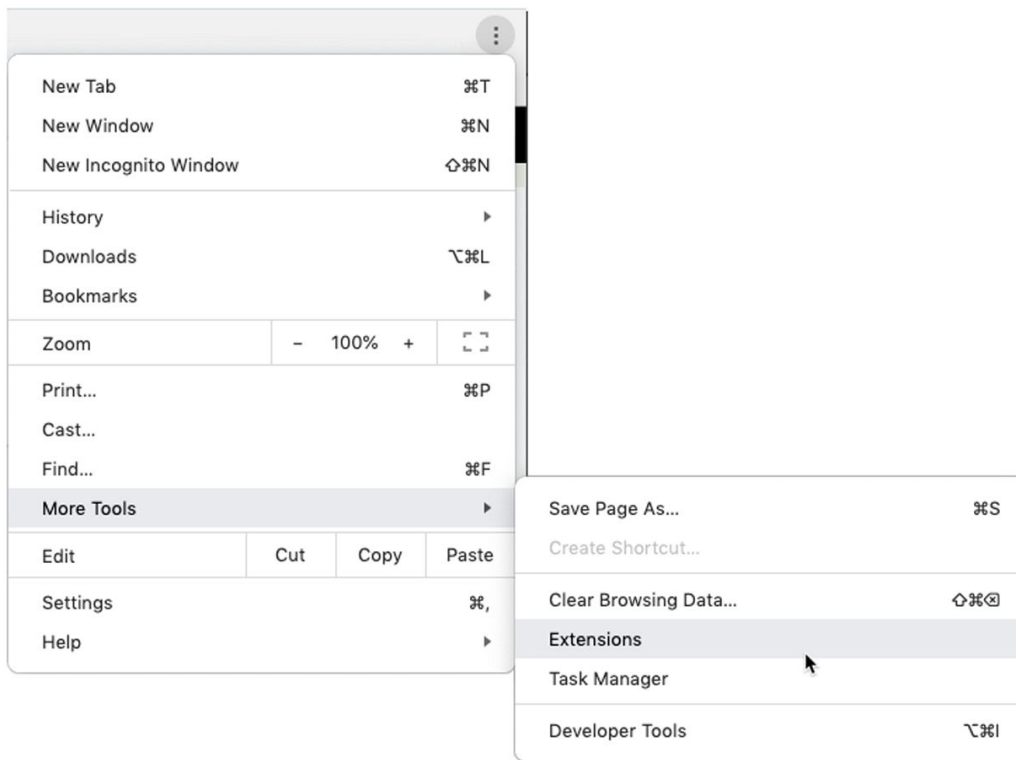
The **Extensions** tab opens. Look for the panel with the Connect extension and click **Remove**:
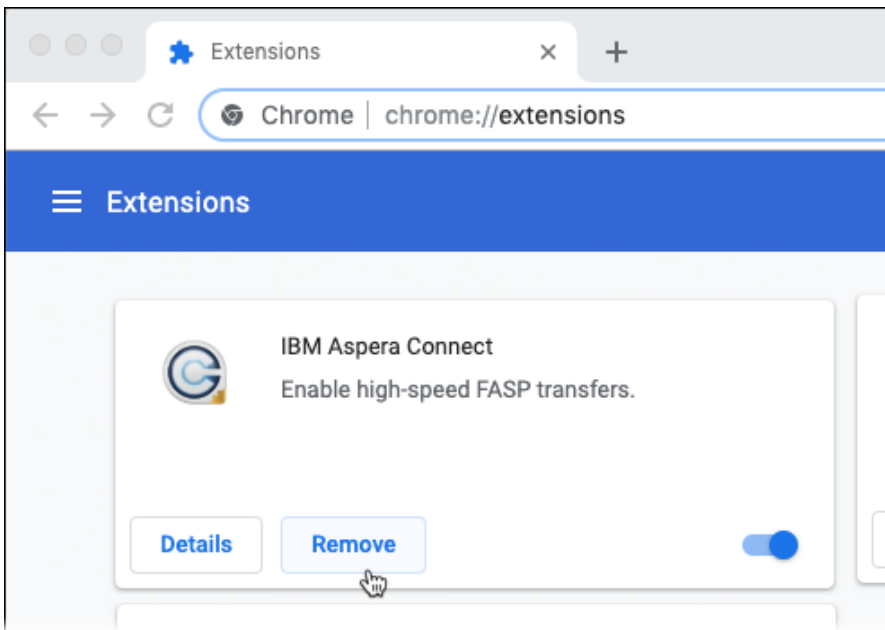
The Connect extension is now removed from Chrome.

<u>Firefox</u>

To remove the Connect extension for Firefox, click the three-bar icon (Open application menu ☰) of the browser window, and click **Add-ons**:
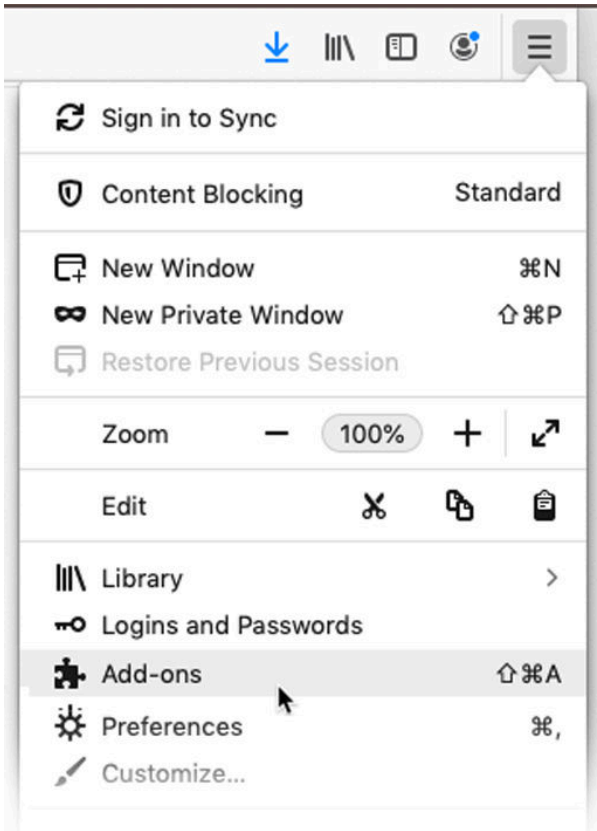
The **Add-ons Manager** tab opens. Look for the panel with the Connect extension and click **Remove**:
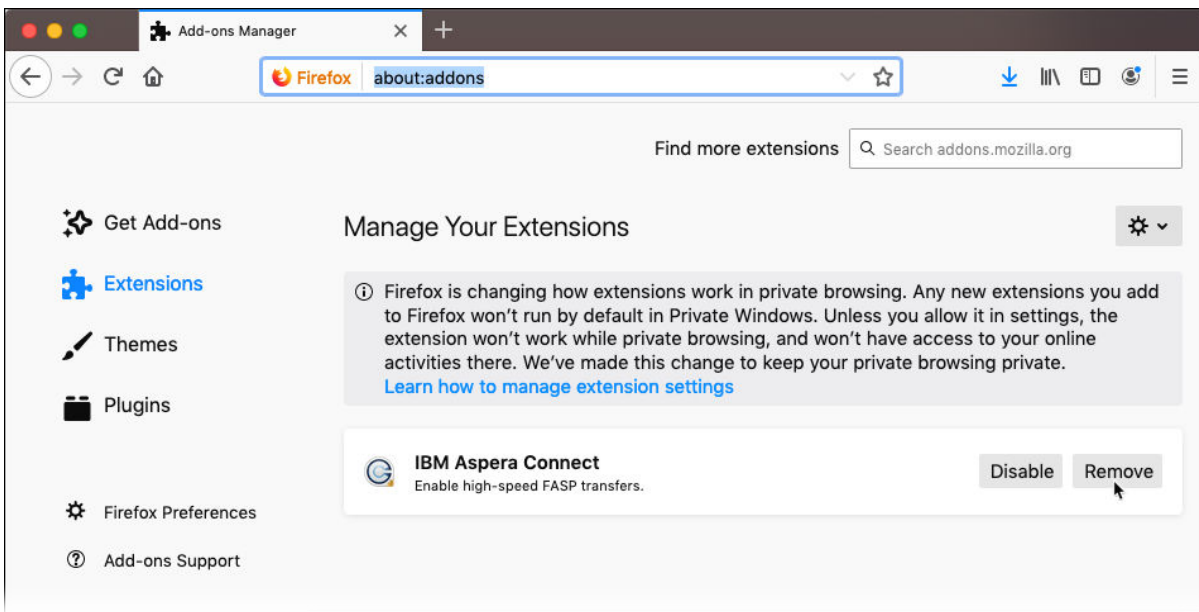
The Connect extension is now removed from Firefox.

Working with IBM Aspera High-Speed Transfer Server

Adding a High-Speed Transfer Server account to Connect

IBM Aspera High-Speed Transfer Server (HSTS) is the foundation under Connect transfers with Faspex and Shares, and under Connect transfers with AoC if your AoC uses an on-premises (*tethered*) transfer

node. Therefore, in any of these cases, the configuration of your HSTS is fundamental to your Connect implementation.

Mostly, your HSTS does not need special configuration to work with Connect. You configure your HSTS for use with Connect in the same way as you would for use with Aspera on Cloud, Aspera Faspex, or Aspera Shares.

Setting Group Ownership

Sometimes, you might want to control the permissions on files that are uploaded to a transfer server. To do this, you can set the SGID bit on the directory on the transfer server into which files are transferred.

The following steps set the SGID bit on a directory named **limited**. When the steps are complete, transfers to the **limited** directory has group ownership rather than user ownership.

Note: The change in ownership applies to Connect transfers to this directory, and to files created in this directory on the transfer server itself, but does *not* apply to transfers ran through sync actions.

1. Set the transfer server to ignore group ownership.

   ```
   asconfigurator -x "set_node_data;group_ownership,-"
   ```

2. Change the group associated with the **limited** directory to **mygroup**. The group that is named **mygroup** is not the user **xfer**'s primary group.

   ```
   chgrp -R mygroup limited/
   ```

3. Set the SGID bit for the destination directory **limited**.

   ```
   chmod -R ug=rwx limited/
   chmod -R g+s limited/
   ```

4. Verify your changes.

   ```
   ls -la limited/
   drwxrwsr-x 1 root mygroup 1234 Apr 23 10:42 .
   ```

   Your output might vary, but verify that the **s** is present in the group's permissions.

Working with IBM Aspera on Cloud

You can use Connect along with IBM Aspera on Cloud, a SaaS platform for file transfer and collaboration.

When Aspera on Cloud is integrated into Connect, you can do the following tasks:

• Share content with members of your organization.

• Send packages to an Aspera on Cloud inbox.

Note: Connect does not currently support adding metadata to packages when sending to a user, but you can send metadata to an Aspera on Cloud inbox.

Note: Connect does not currently support Oauth2 for AOC on Linux.

For more information about using Aspera on Cloud, see the Help Center within the Aspera on Cloud application.

Working with IBM Aspera Faspex

When working with Faspex, you can send and receive files and folders as packages.

IBM Aspera Faspex is a file-exchange application that is built on IBM Aspera High-Speed Transfer Server as a centralized transfer solution. With a web-based GUI, Faspex offers advanced management options for FASP high-speed transfer to match your organization's workflow.

Before configuring Faspex to work with Connect, you need the following requirements:

- A computer running the correct version of Faspex. For instructions on how to install Faspex, see IBM Aspera Faspex documentation.
- Credentials for a Faspex user account. You need one of these accounts to provide Connect access to Faspex.

Adding a Faspex account to Connect

Use the Connect account wizard to configure a new package transfer account.

Note: This information applies to IBM Aspera Faspex 4.0 and previous versions.

Have the following information available before you start configuring an account:

- The address of the server where Faspex is installed and running.
- The username and password that you have on the Faspex server.

The following steps assume that you have Connect installed and running.

To add a Faspex account to Connect, do the following procedure:

1. Launch the Connect Preferences dialog and go to the **Accounts** tab.
2. Click ⊞ to add a Connect account.
3. Select your IBM Aspera product:

    Click **IBM Aspera Faspex**.
4. Complete the fields with the following information about the Faspex transfer server:

Field	Description
Account name	A name for the account. The name is used only by Connect.
Server address	The URL for the server that is running Faspex.

    Click **Next**.
5. Select your Faspex server's authentication method:

    - **SAML Authentication**: Log in to the Faspex server with this user's SAML credentials.
    - **Basic Authentication**: Enter the username and password of the Faspex user.
6. If you are prompted to confirm the server's security certificate, indicate whether you trust the server.
7. Set up package downloading:

    - **Automatically download my packages to the following directory** and enter or browse to a location where you want to store your downloaded Faspex packages.
    - **I'd rather not set up automatic downloading now.** You can change this setting later if you want.
8. If you opted to set up package downloading in the previous step, now select a time frame:

    - Choose to download packages from a date in the past.

        Select **Download my packages from date sent** and choose an option from the drop-down list:

        - **Yesterday** (default).
        - **A week ago**.
        - **A month ago**.
        - **The beginning of time**.
    - Choose to download packages from now on.

    Click **Next**.
9. Set up how you are going to check for new packages:

    - Automatically: Select **Check for new packages** and select an automated time interval from the drop-down list.

- Manually: Select **I'll check manually using the Check Now option**.

10. Click **Finish** to complete your Faspex account setup.

Modifying your package download settings

You can modify the following aspects of a package transfer account:

- The local destination folder for downloading received packages.
- How often Connect must look for new packages.
- Whether to overwrite packages that have the same title.
- Whether to automatically decrypt downloaded packages.

The following steps assume that you have Connect installed and running, and that you created at least one Connect account that you want to modify.

1. Start the Connect Preferences dialog and go to the **Accounts** tab.
2. In the left section of the dialog, select the transfer server account that you want to modify.
3. Under **Account**, you can change the connection settings for the account:

Field	Description
Account name	The name of the account. The name is used only by Connect.
Server address	The URL for the server, and the port number (if applicable).
Username	The username that you have on the transfer server.
Password	The password that you have on the transfer server.
Do not verify host's SSL certificate	If selected, Connect bypasses the validation of your server's SSL certificate. Select this option if your server's certificate is not valid, but you trust the server.

4. In the **Services** section, click **Packages: Settings**.

   The **Packages** dialog appears.
5. Modify the fields as needed:

Field	Description
Download received packages to	Specify the folder where the downloaded packages are going to be saved. You can download packages to the default folder: , or you can click **Change** to provide a different folder name.
Overwrite packages that have the same title	When a received package has the same title as an existing package, Connect can either reuse the same folder (overwriting the existing package), or create a new folder for the received package. If you select this checkbox, packages with the same name as an existing downloaded package are going to be downloaded into the existing folder. If a downloaded file has the same name as an existing file, that file from the older package is overwritten. If you do not select this checkbox, Connect creates a new folder for the new package so that the existing one is not overwritten. For example, if you already downloaded a package with a title of **My_Files**, and then download another package with the same title, the files are placed in **My_Files(2)**.

Field	Description
	If you select this checkbox, Connect places the new package into the existing **My_Files** folder instead of creating a new **My_Files(2)** folder. If **My_Files** already contains a file with the same file name, the existing file is overwritten. By default, this checkbox is not selected.
Do not download packages sent by me	If this checkbox is selected, packages that you send to yourself or to workgroups that you belong to are not downloaded. If this checkbox is not selected, packages that you send to yourself or to workgroups that you belong to are downloaded. (By default, it is not selected.)
Packages are downloaded from **Note:** This field is not configurable.	Displays the date since which Connect searches for packages to download. For example, if this field displays **05/06/2014**, Connect downloads any packages that arrived since May 6, 2014.
Check for new packages	Select the interval in which to check for newly arrived packages.
Automatically unlock encrypted files on download	If you configured encryption for your packages, you can set Connect to automatically decrypt them when they are downloaded. To do so, select this check-box and enter the decryption passphrase in the **Passphrase** field.

6. Click **OK** to apply and save your settings, or click **Cancel** to cancel your selections.

Sending Faspex packages with Connect

To send packages to Faspex, you must first add a Faspex account to Connect. If you don't have a Faspex account, you cannot access the **Send Files** dialog. For instruction on how to add a Faspex account, see "Adding a Faspex account to Connect" on page 26.

1. Open the **Send Files** dialog:

   a) If not already running, start Connect:

   b) Right-click 🌀 > **Send to...**.

2. In the **Send Files** dialog enter:

Field or Button	Description
Account	The account that you use to send the package from (required).
Email or Group	The recipient of the package (required).
Title	A short, relevant title for the package (required).
Notes	A short message to the recipient of this package.
Files	A list of the files and folders in the package that are going to be sent. To add items to this list, click **Add files** or drag-and-drop from the into the **Send Files** dialog.
Encrypt sent files	Select this checkbox if you want to encrypt files before you send them. When you select **Encrypt sent files** and click **Send Package**, you are prompted to enter and confirm a passphrase.

Field or Button	Description
	When you send encrypted packages, you must provide the recipients with the encryption passphrases so that they can decrypt packages after they receive them.
Add files	Click **Add files** to add a file or files to the package for transfer. You can also drag-and-drop files from into this dialog.
Add folder	Click **Add folder** to add a folder to the package for transfer. You can also drag-and-drop folders from into this dialog.
Remove	To remove an item from the package to be sent, select it in the **Files** list and click **Remove**.

3. Click **Send** to send the package.

The Connect **Activity** window's **Transfers** tab opens to display the progress of the transfer.

Receiving Faspex packages with Connect

Getting more information about a transferred package

1. Right-click ⓖ and select **Activity**.
2. Click **Transfers** to view a list of the recent packages that you have sent or downloaded.
3. With the buttons in the **Transfers** tab, you can:

Butto n	Description
ⓧ	Opens the **Transfer Monitor** for more in-progress detail about the transfer. In the **Transfer Monitor**, you can adjust the transfer rate (if settings allow).
ⓛ	Opens a window to the transfer destination folder (the "**containing folder**").
⊙	Stops an in-progress transfer.
⊙	Resumes a stopped or suspended transfer.

In addition to those actions, you can also right-click a package and select **Remove** to remove it from the list.

Clearing a transfer
If a transfer is not currently queued or running, you can remove it from the list:

On the **Transfers** tab, right-click a transfer in the list and select **Remove**.

Looking for new packages

You can also do the following tasks:

- To stop checking for packages, click ⊙.
- To resume automatic checking for packages, click ⊙.
- To check for packages immediately, right-click an inbox and select **Check now**.

Decrypting received packages

If you receive an encrypted package, see "File encryption" on page 17.

Working with IBM Aspera Shares

IBM Aspera Shares is a multinode web transfer application that enables organizations to share content with internal and external users.

Connect accounts that are set up with Shares as the transfer server provide the following functions:

- You can set up Connect to sync folders automatically on the client computer and on the server whenever contents change. Content changes include
  - Modification of file contents
  - Changes in file and folder names
  - Creation and deletion of files and folders

  The sync feature can be configured to be one-way or bidirectional.

For more information about Shares, including system requirements, and installation instructions, see the IBM Aspera Shares documentation.

Adding a Shares account to Connect

Use the Connect account wizard to configure a new Shares transfer account.

To set up a transfer account, make sure that you have the following information from the system administrator who manages your Shares transfer server:

- A URL for the Shares transfer server, including a port and path (if applicable).
- A username and password that was set up on your Shares transfer server.

The following steps assume that you have Connect installed and running.

To add a Shares account to Connect:

1. Launch the Connect Preferences dialog and go to the **Accounts** tab.
2. Click ⊞ to add a Connect account.
3. Select your IBM Aspera product:

   Click **IBM Aspera Shares**.
4. Complete the fields with the following information about the Shares transfer server:

Field	Description
Account name	A name for the account. The name is used only by Connect.
Server address	The URL for the server that is running Shares.

5. If you are prompted to confirm the server's security certificate, indicate whether you trust the server.
6. Select your Shares server's authentication method:

   Either
   - SAML Authentication

     If you choose **SAML Authentication**, log in to the Shares server with this user's SAML credentials.

     Or
   - Basic Authentication

     If you choose **Basic Authentication**, enter the username and password that this user has on the Shares server.
7. If the transfer server supports synchronization, either:
   - Set up syncing now.

     To do so, either accept the default folder that is shown for **Place my files in the following directory**, or click **Change** to browse for a different folder (or create a new one).

By default, the sync folder is created inside your **Documents** folder, in a folder with the name you gave for the account in an earlier step. If you choose to use the default folder, it is created automatically.

Or

- Set up syncing later.

  To do so, click **I'd rather not set up file syncing now**.

8. If you opted to set up syncing on the previous screen, the Account Wizard prompts you to choose folders to sync.

   You can either:

   - Select **Synchronize with the selected remote folders** and then select the folders on Aspera on Cloud to sync.

     Click the arrows to expand or collapse the folder view, and select the check boxes for the folders you want to sync.

     Choose the sync direction:

     – **Two-Way**.
     – **Remote to Local** (default).
     – **Local to Remote**.

     Note: For a detailed explanation of your options for sync direction, see "Synchronization" on page 32.

     Or

   - Select **I'll choose the folders to sync later.**

9. When the screen displays a success message, click **Finish** to exit the Account Wizard.

Modifying a Connect account for Shares

The following steps assume that you have Connect installed and running, and that you created at least one Connect account that you want to modify.

To modify a transfer account, do the following tasks:

1. On the left side of the dialog, select the transfer server account that you want to modify.
2. Under **Account**, you can change the connection settings for the account:

Field	Description
Account name	The name of the account. The name is used only by Connect.
Server address	The URL for the server, and the port number (if applicable).
Username	The username that you have on the transfer server.
Password	The password that you have on the transfer server.
Do not verify host's SSL certificate	If selected, Connect bypasses the validation of your server's SSL certificate. Select this option if your server's certificate is not valid, but you trust the server.

3. Back in the **Preferences** dialog, click **Save** to put into effect any changes you have made.

Synchronization

With Connect transfer accounts for IBM Aspera High-Speed Transfer Server, IBM Aspera on Cloud, and IBM Aspera Shares, you can set up Connect to sync folders automatically on your client computer and the server whenever the folder's content changes in either location.

Content changes include

- Modification of file contents.
- Changes in file and folder names.
- Creation and deletion of files and folders.

Sync direction

When you set up sync, you must choose the direction of synchronization. Connect can be configured for the following direction settings:

- **Remote to Local**

  This is the default setting. In this configuration, the remote computer (usually a server) retains the primary version of the files. The latest content is copied from the server to users' workstations.

- **Local to Remote**

  In this configuration, the user's version of the content is assumed to be the primary version, and is copied to a central server. Typically, this setting is employed when users update content frequently.

- **Two-Way**

  In a two-way, or bidirectional, sync relationship, changes in each location are copied to the other location. With this type of sync, the contents of both remote and local are identical after the sync has completed.

  Note: When you have two-way sync that is configured, Connect runs these transfers by using the lowest nonzero bandwidth limit that you have set for automatic transfers. For more information about setting bandwidth limits for automatic transfers, see "Manual versus automatic transfers" on page 40.

  If no bandwidth limit is set, Connect runs two-way sync transfers at the maximum rate that the server and network conditions allow.

Avoiding Sync conflicts

To avoid unexpected results, understand what each sync direction setting means and choose carefully. For example, consider the following scenario:

The system is configured for remote-to-local sync. When the scheduled automatic sync occurs, the latest content is copied from the remote computer to the user's local desktop. A local user then creates a new file. The next automatic sync occurs, but this new file still exists only on the user's computer. *This is the expected behavior in remote-to-local sync*. In this scenario, the content on the destination is not necessarily identical to that on the source.

Initial synchronization

When you first set up a sync relationship between two computers, the system starts its initial transfer of content from the *source* location to the *destination* (or *target*) location. Depending on the size of the content, this can be a large operation.

Then, when the system performs the next automatic sync, any changes at the source location are copied to the target.

Automatic Sync versus Reset Sync

Automatic Sync

After the initial transfer, synchronization between the transfer server and client computers occurs automatically, at the regular interval you set in the Connect **Preferences** dialog.

In these automatic sync operations, the system transfers *only the changes since the most recent sync*.

Reset Sync

A reset operation is like starting over. Unlike automatic sync, a reset is a wholesale transfer of *all* the content, not just the changed content. Because a reset clears the sync records, you typically run a reset only after a conflict is resolved or by changing the sync configuration.

Use a signature file to prevent accidental directory deletion

Designate a file as the signature file (on either the local or remote storage, or both). Before you start the sync, Connect verifies that the signature file exists. If the signature file cannot be found, Connect halts the sync to prevent accidental deletion.

Configuring Sync in Connect

When you use Connect's synchronization capability, you can configure various aspects of the sync relationship. Start by selecting **Preferences > Accounts**. Connect's synchronization works with IBM Aspera High-Speed Transfer Server, IBM Aspera on Cloud, and IBM Aspera Shares.

Usually, you set up sync folders when you added accounts to Connect. If you opted not to set up sync with your accounts, or if you need to change the folders on the transfer server that you want the local computer to sync with, follow these steps:

1. On the **Accounts** tab, select the account for which you want to configure sync folders.
2. In the **Services** area of the tab, click **Sync: Settings**.

   The **Sync Settings** dialog appears.

   Note: If sync capabilities are made available for the transfer server *after* the account has been added to Connect, you must remove and then readd the account to Connect to use the **Sync Settings** dialog.
3. Select the folders on the remote server that you want to sync with the local computer.

   Browse through the nested folders shown under **Synchronize with the selected remote folders**, and select the ones that must be synced with.
4. Set the local path for the sync.

   Under **Local Folder Path**, the default path on the local computer is shown. If you want to change it, click **Browse** and go to the wanted location.
5. In the **Direction** drop-down list, choose **Two-Way**, **Remote to Local**, or **Local to Remote**.

   Connect's synchronization between the remote server and the local computer can be upload-only, download-only, or bidirectional. For a description of these sync direction options and their behavior, see "Synchronization" on page 32.
6. Choose whether Connect must use continuous mode.

   Connect usually checks for sync changes on an interval. When using continuous mode, Connect detects new changes almost immediately.
7. Designate a file as the signature file on either the local or remote storage, or both. Set **Local Mounts Signature Pathname** and **Remote Mounts Signature Pathname**.

   Before starting the sync, Connect verifies that the signature file exists. If the signature file cannot be found, Connect halts the sync to prevent accidental deletion.
8. Click **OK** to save.

Syncing content

Monitoring sync status

You can monitor the status of a sync operation on the **Activity Window > Sync** tab.

A progress bar shows in-progress synchronizations, and a countdown timer shows that when the next synchronization will take place.

Stopping and starting sync

You can stop and resume file syncing with the following buttons on the **Activity Window > Sync** tab:

Button	Description
⊙	Stops an in-progress synchronization.
⊙	Resumes a stopped synchronization.

Resolving sync conflicts

A sync conflict occurs when the file on one side does not match the file on the other side. Files and folders might not be synchronized for reasons such as insufficient permissions for the destination folder on the local computer.

If a file or folder cannot be synchronized, a conflict warning appears on the **Activity Window > Sync** tab.

To resolve the conflict, do the following steps:

1. Click the red **conflict** link.
2. In the dialog that appears, select the file or folder that is in a conflict state.
3. Click **Resolve Selected Conflicts**.

   Connect renames the content on the local file system, appending the phrase **conflict-mine**. For example, the file **log.txt** is renamed as **log.conflict-mine.txt**.

Resetting the Sync

You can reset the sync at any time, such as after changing the sync configuration, or after you resolve a sync conflict. When you reset the sync, your sync configuration settings are retained, but the repositories are rescanned for discrepancies. To reset the sync:

1. On the **Accounts** tab, select the account for which you want to configure sync folders.
2. In the **Services** area of the tab, open the **Settings** for the Sync service.

   The **Sync Settings** dialog appears.

   Note: If sync capabilities are made available for the transfer server *after* the account has been added to Connect, you must remove and then readd the account to Connect to use the **Sync Settings** dialog.
3. Select **Reset Sync** and click **OK**.

Requirements for using Sync with Aspera on Cloud

If you are using Aspera Connect with Aspera on Cloud, Connect can synchronize files and folders automatically between the remote server and the local computer.

Aspera on Cloud user permissions

Aspera on Cloud users who use Connect with sync features must be authorized to run *create*, *delete*, and *rename* file operations. The Aspera on Cloud admin can set these on the **Authorizations** tab.

Connect account configuration

You must have Connect accounts that can synchronize content with your Aspera on Cloud organization.

For more information, see Adding an Aspera on Cloud account to Connect.

Sync configuration in Connect and in Aspera on Cloud

Pay close attention to the configuration of the sync relationship. In all cases, *the settings in Aspera on Cloud override the settings locally in Connect*. Note that if your Aspera on Cloud transfer server nodes are not correctly configured, you might experience sync problems between Aspera on Cloud and Connect users.

For more information, see the Aspera Sync section in the IBM Aspera High-Speed Transfer Server documentation.

Requirements for using Sync with Shares

If you are using Aspera Connect with a Shares transfer server, Connect can synchronize files and folders automatically between the remote server and the local computer.

Shares server configuration

To set up sync with a Shares server, the server must be configured for sync in its `aspera.conf` file and must have the appropriate license.

For more information about your server's configuration file and license, see the IBM Aspera Shares documentation.

Shares user permissions

Shares users who use Connect with sync features must be authorized to run *create*, *delete*, and *rename* file operations. The Shares admin can set these on the **Authorizations** tab.

Connect account configuration

You must have Connect accounts that can synchronize content with a Shares server.

For more information, see "Adding a Shares account to Connect" on page 30.

Sync configuration in Connect and in Shares

Pay close attention to the configuration of the sync relationship. In all cases, *the settings on the Shares server override the settings locally in Connect*. If your Shares server is not correctly configured, you might experience sync problems between the server and Connect users.

For more information, see the Aspera Sync section in the IBM Aspera High-Speed Transfer Server documentation.

Configuration

In the Connect **Preferences** dialog, you can configure logging behavior and various options for file transfers. These options include transfer queuing, file download location, and the allowed number of transfer retries.

Start Connect and open the **Preferences** dialog:

If Connect is already running, go to **System Tray > Right-click Aspera Connect > Preferences**. If it is not running, you can run the application manually by running:

```
~/.aspera/connect/bin/asperaconnect &
```
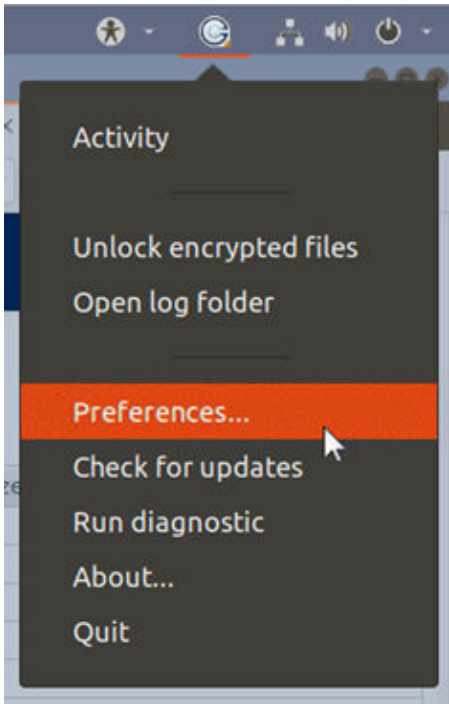
General configuration

To set your general preferences, launch the Connect Preferences dialog and go to the **General** tab.

Field	Description	Default
Remove transfer list items	Specify how to remove transfer sessions from the **Activity** window: Manually, or automatically on successful transfers. **Manually** is selected by default.	Manually
Logging level	⚠️ **Warning:** Do not change this setting unless requested by the Aspera Technical Support. Enabling **Debug** or **Trace** logging might impact performance. Choose the level of information to be recorded in the Connect logs. Options are: • **Info** – Default. Displays general messages about requests, **ascp** create 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.	Info
Disk space warning	Specify the disk space threshold for automatic transfers. If the available disk space is less than the specified threshold, a warning is displayed.	5 percent
Specify the maximum number of files and folders to display within a	1000	

Field	Description	Default
folder in the remote view.		

Account configuration

To set your account preferences, launch the Connect Preferences dialog and go to the **Accounts** tab.

Adding an account

- For instructions on adding Connect accounts for use with the Aspera on Cloud SaaS, see Adding an Aspera on Cloud account to Connect.
- For instructions on adding Connect accounts for use with a Shares transfer server, see "Adding a Shares account to Connect" on page 30.
- For instructions on adding Connect accounts for use with a Faspex transfer server, see "Adding a Faspex account to Connect" on page 26.

Removing an account

To remove an account, do the following:

1. In the list of accounts, select an account to be removed.

2. Click ▣ to remove the account.

   When you remove an account, all account transfers and services that are associated with that account are stopped and removed.

3. Click **Yes** to confirm the account removal, or click **No** to cancel the account removal.

Configuring Sync settings

For Connect accounts that are set up with Aspera on Cloud or Shares as the transfer server, you can configure synchronization settings, such as which remote folders to sync with, and the direction of the synchronization relationship.

For instructions on using synchronization features, see "Syncing content" on page 34.

Configuring package settings

For Connect accounts that are set up with Aspera on Cloud or Faspex, you can configure the following:

- The local folder for received packages.
- Whether to overwrite packages.
- How often Connect should look for new packages.

For instructions, see "Modifying your package download settings" on page 27.

Transfer configuration

To set your transfer preferences, launch the Connect Preferences dialog and go to the **Transfers** tab.

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 are going to be saved.

- **Always ask me where to save downloaded files**: Choose this option to select a location for each download.

Queue

Field	Description	Default Setting
Enable queuing	When this checkbox is selected, Connect limits the number of concurrent transfers. **Note:** When transfers are queued, you can start them manually from the **Activity > Transfers** window.	Selected
Maximum concurrent transfers	If **Enable queuing** is selected, you can enter a maximum number of concurrent transfers in this field. Any transfers above this value are queued and then started once the number of concurrent transfers drops below the specified value. When queuing is not enabled, this field is not available.	3

Retry

Field	Description	Default Setting
Automatically retry failed transfers	When this checkbox is selected, Connect retries failed transfers. If you want Connect to retry failed transfers, specify the number of attempts and the interval in which Connect tries to resend in seconds, minutes, or hours.	Selected
Attempts	When **Automatically retry failed transfers** is selected, Connect makes the number of retry attempts that you specify in this field.	3
Interval	When **Automatically retry failed transfers** is selected, Connect retries transfers at the interval you specify in this field.	30 seconds

Multi-session

For more information about configuring multi-session transfers, see "Multi-session transfers" on page 12.

Field	Description	Default Setting
Enable multi-session	Enable multi-session transfers.	Unselected
Number of sessions	The number of sessions you prefer (as guidance, not as a requirement).	3
When transferring faster than	The transfer speed that triggers multi-session transfers.	700 Mbps
Split files larger than	Enable file splitting for files larger than or equal to the specified size. This value is sometimes also referred to as the *multi-session threshold*. For example, by using the default size value (60 MB), if the source directory contains multiple files, all files less than 60 MB	60 MB

Field	Description	Default Setting
	are distributed between sessions, while all files 60 MB or larger are split and then distributed between sessions. If the source directory contains only one file and the file is 60 MB or larger, the file is split, otherwise the file is transferred by one session.	
Startup interval between sessions	The amount of time to wait before the next session starts.	1 second

Sync

Field	Description	Default Setting
Interval	If the sync feature is enabled, specify the interval between synchronizations.	30 seconds

Network configuration

To set your network preferences, launch the Connect **Preferences** dialog and go to the **Network** tab.

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 configured an HTTP proxy, the transfer continues over the HTTP protocol based on this proxy configuration.

Although the HTTP proxy is used primarily for the HTTP fallback feature, you can use it for all HTTP-related activities that Connect runs. However, it cannot be used for FASP transfers.

Field	Description
Use HTTP Proxy • **Username** • **Password** • **Address** and **Port**	• Your username • Your password • Your server's URL or IP address, and port number **Note:** For some proxies, the username and password are optional.

FASP Proxy

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

Field	Description
Use FASP Proxy (DNAT)	If your transfers use an IBM Aspera FASP Proxy server, select this checkbox.
Secure (DNATS)	Select this checkbox if your FASP Proxy uses a secure connection.
• **Username** • **Password** • **Address** and **Port**	Use these fields to define your FASP Proxy configuration. Type the following information: • Your server username • Your server password

Field	Description
	• Your server's URL or IP address, and port number **Note:** These fields are enabled only if **Use FASP Proxy (DNAT)** is selected.

Bandwidth configuration

Transfer speeds depend on server settings and your network connectivity. To limit transfer rates, launch the Connect **Preferences** dialog and go to the **Bandwidth** tab.

Manual versus automatic transfers

The limits that you set on the **Bandwidth** tab can be different for transfers that are initiated *manually* versus those that are *automatically* triggered. Automatic transfers can include sync-initiated transfers, script-initiated transfers, or any other background method of starting a Connect transfer.

Manual transfers

Field Name	Description
Downloads: Limit to	When the **Limit to** checkbox is selected, you can set the download rate in either megabits per second (Mbps) or kilobits per second (Kbps). The limit that you set here applies to downloads that users initiate manually.
Uploads: Limit to	When the **Limit to** checkbox is selected, you can set the upload rate in either megabits per second (Mbps) or kilobits per second (Kbps). The limit that you set here applies to uploads that users initiate manually.

Automatic transfers

New limits to download and upload transfer rates immediately apply to noncontinuous syncs. For new limits to take effect on continuous syncs, you must stop and restart those syncs for the new limits to take effect.

Field Name	Description
Background downloads: Limit to	When the **Limit to** checkbox is selected, you can set the download rate in either megabits per second (Mbps) or kilobits per second (Kbps). The limit that you set here applies to transfers that are initiated for Inbox downloads or sync actions.
Background uploads: Limit to	When the **Limit to** checkbox is selected, you can set the upload rate in either megabits per second (Mbps) or kilobits per second (Kbps). The limit that you set here applies to transfers that are initiated for sync actions.

Security configuration

With Connect security facilities that you can specify restricted and trusted hosts, encrypt content, and manage authentication credentials.

To configure security, launch the Connect Preferences dialog and go to the **Security** tab.

You can use these features to minimize security risks when you upload or download 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, and removing them from the **Passwords** tab.
- **Content protection** is a feature that allows uploaded files to be encrypted during a transfer, 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.

Managing hosts

When a transfer is initiated and the **Remember my choice for this site** option is enabled in the confirmation dialog, the server you are allowing or denying is added to the **Trusted Hosts** or **Restricted Hosts** list, respectively. To view, add or remove extra trusted hosts, go to **Security > Trusted Hosts**. Enter the host's address in the specified text field and click **Add**.
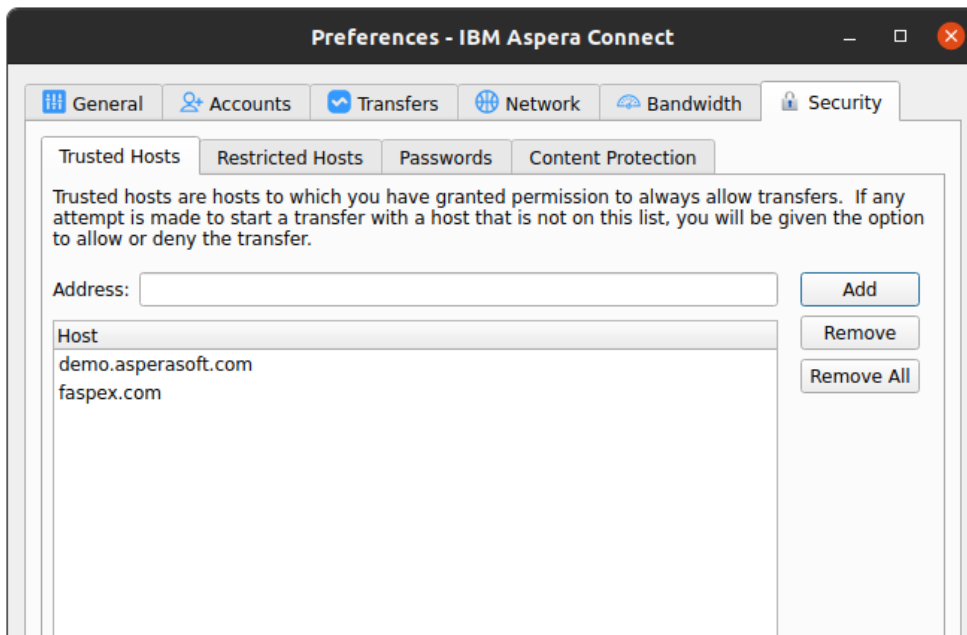
To view, add or remove restricted hosts, go to **Security > Restricted Hosts**. Here, enter the host's address in the specified text field and click **Add**.
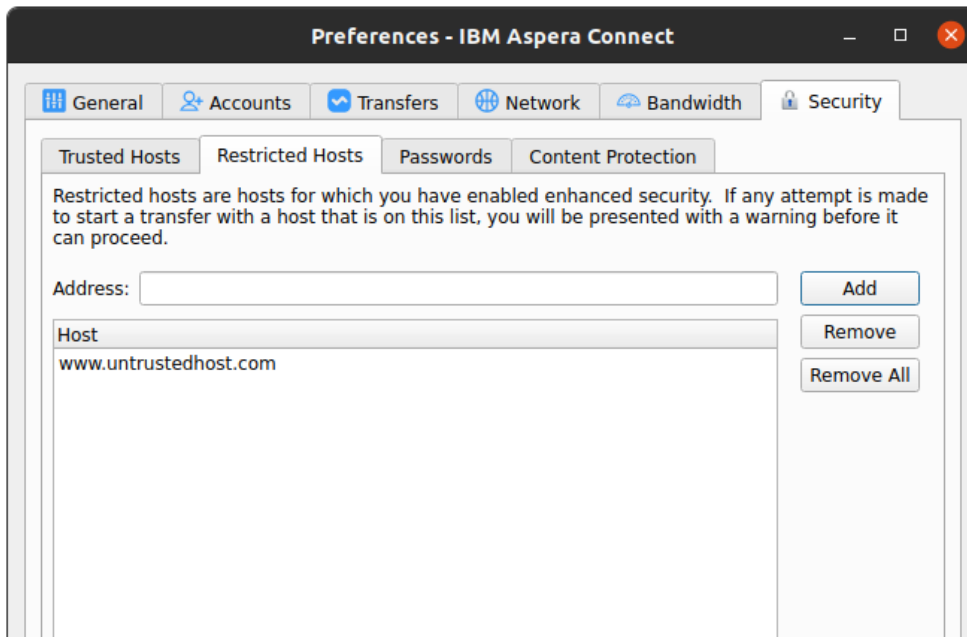
Whenever you initiate a transfer to or from a host in the **Restricted Hosts** list or a host that's not in the **Trusted Hosts** list, Connect displays a security warning asking whether you want to grant access to the host for this transfer:

Managing passwords

To view 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.
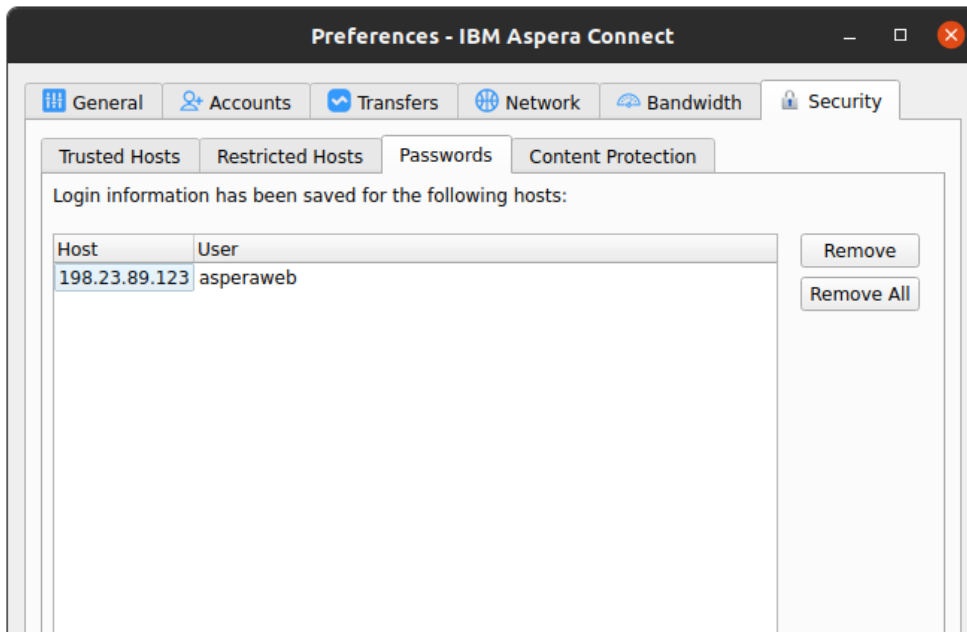
Whenever you attempt a transfer with a server where your credentials are not saved, you are prompted with an authentication dialog and offered a **Remember this password** check-box. Marking the check-box causes your login credentials to be saved and appear in the **Passwords** tab.

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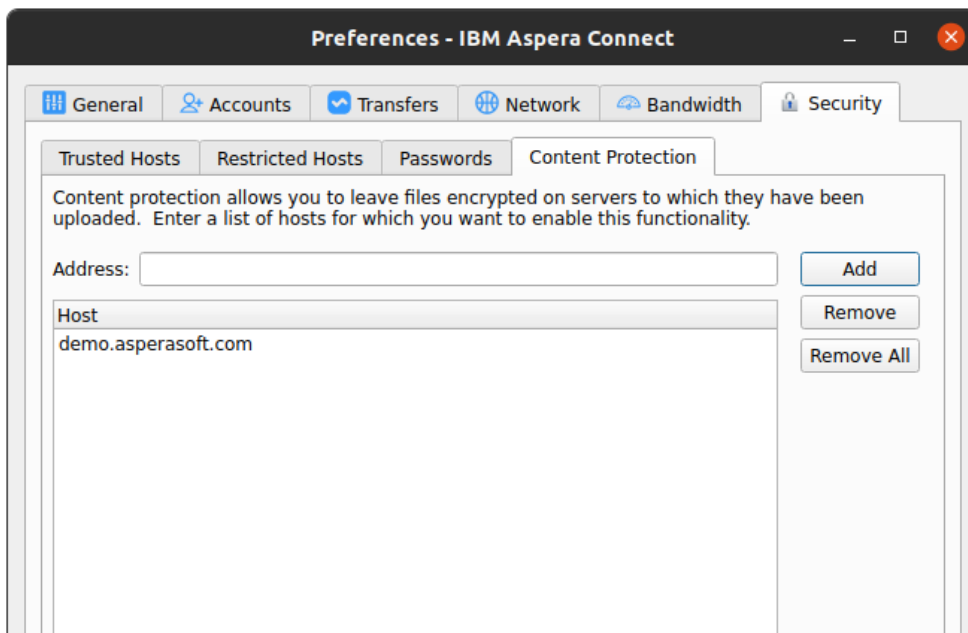
When uploading files to a server on the list, or one that is configured as a content-protected host, you are prompted for a passphrase to encrypt the files. You can also choose not to encrypt files if the server allows it.

For more information about encryption and decryption, see File Encryption.

Appendices

Configuring Faspex

To install and configure Faspex, follow the instructions in the IBM Aspera Faspex documentation.

Note: Connect does not currently support adding metadata to packages that it sends. Therefore, verify that Faspex is not configured to have any required metadata fields when sending packages. You can configure optional metadata fields, but Connect will ignore them.

Configuring Shares

Before configuring Shares to work with Connect, you need the following:

- A computer running the correct version of Shares and Enterprise Server.
- On each node on the Shares server, a supported version of Connect Server with a Connect-enabled license.

Note: If you use the synchronization feature, you must ensure that the Enterprise Server is configured to use token authentication.

1. Log in to your Shares server as administrator, and go to **Admin > Accounts > Users**.
2. For each Shares user account that will use Connect, click **Edit**.
3. On the **Security** tab, verify that the **API Login** checkbox is selected.

   On Shares 1.6 and later versions, this permission is enabled by default whenever new users are created.

4. Create shares, and authorize users for each share.

   For more instructions about creating shares and authorizing users, see IBM Aspera Shares documentation..
5. For each authorized user of a share, enable the following permissions to allow users to view, edit, or delete files and folders when using Connect:

To allow this action on Connect …	… Enable this checkbox on Shares
View	**browse**
	download
Edit	**upload**
	mkdir
	rename
Delete	**delete**

6. For each Shares user account that uses Connect, repeat these steps.

For more information about Shares, see IBM Aspera Shares documentation.

Log files

You can access Connect log files from within Connect or from your file system.

Log files

aspera-connect.log
　　log file for the Connect application

aspera-scp-transfer.log
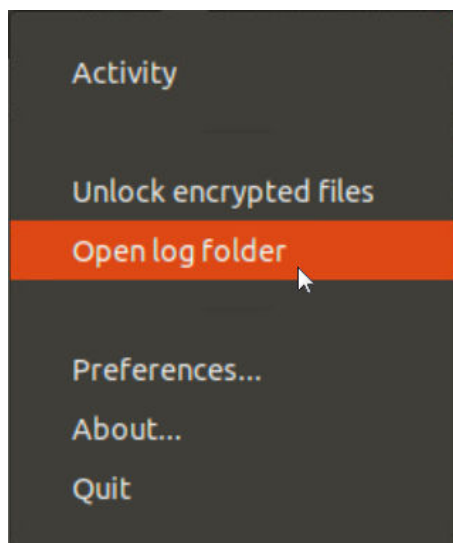　　log file for the ascp transfers

nativemessagehost.log
　　log file for host messages

Log file location

Log files are located in the following location:

```
~/.aspera/connect/var/log/
```

Deploying Connect extensions in closed environments

Locked-down or enterprise environments without access to the public internet generally require special steps to acquire and enable Connect web extensions. Depending on OS platform and browser, there are various methods for doing so.

Chrome

Method: Manual deployment by using drag-and-drop

1. Download the Connect extension CRX file from Google. To do so, right-click the following link and select **Save Link As**: Connect extension for Chrome
2. Open `chrome://extensions`
3. Enable developer mode.
4. Drag-and-drop the CRX file into the `chrome://extensions` window to install.

Firefox

Method: Manual deployment

1. Download the Connect extension XPI file from Mozilla. To do so, right-click this link Connect extension for Mozilla and select **Save Link As**.
2. Open `about:addons`
3. From the menu, select **Install add-on from file**.

Method: Deploying Aspera Connect add-on with custom build of Firefox

See Mozilla documentation: Extensions for your enterprise.

Allowlisting the Chrome extension

By default, all Chrome extensions that are allowlisted. However, if your organization blocklists all extensions by policy, you can override the blocklist and allow the Connect extension to be installed by adding it to the allowlist. For more information, see ExtensionInstallAllowlist.

The following instructional links also include information on other extension-related policy settings that you can use to enable automatically install Chrome, force-install Chrome, and other tasks.

Note: These policies are intended strictly for configuring instances of Google Chrome internal to your organization. Use of these policies outside of your organization (for example, in a publicly distributed program) is considered malware and will likely be labeled as malware by Google and anti-virus vendors.

Provisioning Policy Using Chrome Policy Templates

1. Install Chrome policy templates: Detailed instructions can be found here: Set Chrome Browser policies on managed PCs.
2. Set Chrome extension policies. Detailed instructions can be found here: Set Chrome app and extension policies (Linux).

   a. Create a file with the following contents in `/etc/opt/chrome/policies/managed/test_policy.json`:

   ```
   {
       "ExtensionInstallWhitelist": ["kpoecbkildamnnchnlgoboipnblgikpn"]
   }
   ```

   b. Restart Chrome.
   c. To verify that the policy has been applied, enter the following Chrome URL in the address bar:

   chrome://policy

Troubleshooting

Disabling SELinux

SELinux (Security-Enhanced Linux), an access-control implementation, can prevent web UI access.

To disable SELinux:

1. Open the SELinux configuration file: `/etc/selinux/config`.
2. Locate the following line:

   ```
   SELINUX=enforcing
   ```

3. Change the value to **disabled**:

   ```
   SELINUX=disabled
   ```

   Save your changes and close the file.

4. On the next restart, SELinux is permanently disabled. To dynamically disable it before the restart, run the following command:

   ```
   # setenforce 0
   ```

Disabling AppArmor

AppArmor is a Linux security module that uses mandatory access control (MAC) to restrict some applications' system access. It might prevent Connect from running correctly on some Linux systems.

To disable AppArmor, enter the following commands on the affected computer:

```
# /etc/init.d/apparmor stop
# update-rc.d -f apparmor remove
```

Connectivity issues

SSH connectivity errors: "Timeout establishing connection"

If you receive the error "`Timeout establishing connection`", the TCP connection between 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 (where Connect is installed). 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 might 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. Verify 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:

```
IBM Aspera Connect Diagnostic Tool
```

Transfer issues

Connect won't transfer `.partial` files

With the default configuration for Connect, if you try to transfer files that have a `.partial` extension, you are going to notice that these files are skipped. This is because the `.partial` extension has a special meaning for Connect. For a file in transit, `.partial` is the default temporary extension for the partial file on the receiving end before its transfer is complete. When the file's transfer is finished, the extension is removed.

You can transfer the skipped files by changing the name of the file name extension that Connect uses. Choose a name that you don't expect will be used by files you transfer.

To make this change:

1. Locate the Connect `aspera.conf` file on the machine at the receiving end of the transfer. The `aspera.conf` file is included in the Connect installation. Open it with a text editor:

   ```
   ~/.aspera/connect/etc/aspera.conf
   ```

2. Go to the line that begins with `<partial_file_suffix>`, and change `.partial` to a name your transfer files will not be using:

   ```xml
   <?xml version='1.0' encoding='UTF-8'?>
   <CONF version="2">

   <default>
       <file_system>
           <storage_rc>
               <adaptive>
                   true
               </adaptive>
           </storage_rc>
           <resume_suffix>.aspera-ckpt</resume_suffix>
           <partial_file_suffix>.partial</partial_file_suffix>
           <replace_illegal_chars>_</replace_illegal_chars>
       </file_system>
   </default>

   </CONF>
   ```

   Note: Removing the `<partial_file_suffix>` entry or setting it to a null value does not necessarily solve the problem. Doing so means the file extension that is used for partial files becomes whatever is set in the `aspera.conf` for **ascp**, which by default is `.partial`.

3. Save your changes to the Connect `aspera.conf` file. The changes will take effect with the next transfer.

Issues installing Connect on macOS Ventura

Sometimes, users might be unable to install Connect on macOS Ventura when running the installer from the Downloads directory.

To address this issue, it is necessary to grant the `Installer.app` permissions to the Downloads directory. To do this go to:

• `System Preferences > Privacy & Security > Files and Folders > Installer.app > Grant access to Downloads Folder.`

Alternatively, if that option is not available you can grant `Installer.app` more permissions by going to:

• `System Preferences > Privacy & Security > Full Disk Access > Grant full disk access to Installer.app.`

You can find the `Installer.app` at `/System/Library/CoreServices/Installer.app`

Downgrading Connect 4.x to Connect 3.11.x.

Downgrading from IBM Aspera Connect 4.x to 3.11.x is not supported since the database schema has been changed. Attempting this results in Connect fails whenever Connect is started. If you still plan to go through with the downgrade, you must delete the IBM Aspera Connect database after downgrading.

IBM®