

IBM Aspera Faspex Admin Guide 4.4.1

Linux

Revision:a351a2 Generated:06/04/2020 19:06

Contents

Introduction.....	8
Installing Faspex.....	9
Faspex Installation Scenarios.....	9
Installing Faspex with a Local Node.....	10
Before You Begin.....	10
Installing the Transfer Server Locally.....	10
Install Faspex on the server.....	11
First Time Log In and Licensing.....	13
Installing Faspex with a Remote Node.....	13
Before You Begin.....	14
Install Faspex on the Server.....	14
First Time Log In and Licensing.....	16
Provide Faspex with Credentials to the Remote Node.....	16
Migrating Faspex to a New Machine.....	17
Installing Faspex with a Setup File.....	18
Generate the Setup Files.....	18
Install Faspex Using the Setup Files.....	18
First Time Log In and Licensing.....	18
Configuring Faspex to Use a Remote Database (Faspex + MySQL).....	19
Configuring Faspex to Use a Remote Database (MySQL Only).....	20
Updating Your License.....	23
Enabling On Demand Entitlement for Faspex.....	23
Uninstalling Faspex.....	24
Logging In.....	24
Upgrading Faspex.....	25
Upgrading Faspex from 4.2.0 or Later.....	25
Before You Begin.....	25
Upgrading Faspex from 4.2.0 and Later.....	26
Logging In.....	27
Upgrading Faspex from Before 4.2.0.....	28
Before You Begin.....	28
Upgrading Faspex from Before 4.2.0.....	28
Logging In.....	29
Logging In to Faspex.....	30
Logging In to Faspex.....	30
Logging In with SAML.....	31
Requesting an Account.....	31
Configuring Faspex Settings.....	32
Configuring the Faspex Web Server.....	32
Configuring the Faspex Domain Name.....	32
Configuring Alternate Addresses for Faspex.....	33

Configuring Transfer Options.....	33
Setting Maximum Package Title Length.....	34
Configuring the Email Server.....	35
Enabling Post-Processing Scripts.....	35
Setting Up Bandwidth Measurement.....	37
Customizing New User Account Form.....	38
Modifying HTTP Server Settings.....	39
Changing the Default Language Used in Faspex.....	40
Configuring HTTP and HTTPS Fallback.....	40
Setting the Minimum IBM Aspera Connect Version.....	42
Configuring On-Demand Entitlement.....	42
Working with Sender Quotas.....	43
Sender Quota Overview.....	43
Configuring Sender Global Quotas.....	46
Configuring Sender Quota for a User Account.....	47
Securing Faspex.....	47
Firewall Settings.....	47
Configuring Security Settings.....	47
Securing Incoming and Outgoing Transfers.....	52
Verify Private and Public Key Authentication for SSH Server.....	53
Disabling SELinux.....	54
Securing Admin Login Attempts from Unknown IP Addresses.....	54
Enabling Terms of Service Agreement.....	55
Installing a Signed SSL Certificate Provided by Authorities.....	55
Generating and Installing a New Self-Signed SSL Certificate.....	57
Regenerating Self-Signed SSL Certificate (Apache).....	57
File Encryption Options.....	57
Obfuscating File Names in Packages.....	58
Adding Nodes and File Storage to Faspex.....	59
Adding a Node to Faspex.....	59
Setting Up a Linux Node.....	60
Setting Up a Windows Node.....	63
Setting Up an OS X Node.....	65
Adding File Storage to a Tethered Node.....	68
Configuring File Storage.....	68
Set Default Server Inbox.....	70
Enabling Cloud Referencing for Package Creation.....	70
Creating and Managing User Accounts.....	71
Creating a New Faspex User.....	71
Managing Faspex Users.....	72
Changing or Resetting a User's Password.....	72
Reactivating an Inactive Account.....	73
User Roles.....	73
Configuring Custom User Fields.....	74
Configuring Account Preferences.....	75
Updating Email and Connect Settings.....	75

Changing Your Language.....	77
Changing Your Password.....	78
Editing Contacts.....	78
Creating a Personal Distribution List.....	78
Check Data Usage and Sender Quota Limit.....	79
Transferring Files.....	79
Faspex and Connect.....	79
The Activity Window.....	80
Monitoring Transfers.....	81
Sending a New Package.....	82
Managing Pending Packages.....	85
Viewing and Downloading Packages.....	86
Package Recipient Expansion by Email Address.....	87
Package Details.....	87
Serving Connect Locally.....	88
Using Faspex with the HTTP Gateway Service.....	89
Enabling the HTTP Gateway Service.....	89
Limitations.....	89
Using HTTP Gateway Instead of IBM Aspera Connect.....	90
Working with External Senders.....	90
Allowing External Users to Send to Faspex Users.....	90
Allowing Users to Send to External Email Addresses.....	90
Inviting External Senders.....	91
Configuring Public URLs.....	91
Enabling and Sharing your Public URL.....	92
Removing External Users from Faspex.....	92
Viewing Packages and Managing Package Storage.....	92
Viewing and Downloading Packages.....	92
Configure Package Storage Expiration.....	93
Changing the Package Directory.....	94
Working with Workgroups.....	95
Creating a Workgroup.....	95
Managing Workgroups Members.....	95
Sending Packages to a Workgroup.....	96
Downloading Packages for Workgroup.....	98
Custom Inboxes.....	98
Archiving Packages in a Workgroup Inbox.....	99
Working with Dropboxes.....	99
Faspex Dropboxes.....	99
Creating a Dropbox.....	99
Managing Dropbox Members.....	102
Sending Packages to a Dropbox.....	103
Downloading Packages for Dropbox.....	104
Inviting an Outside Contributor to Send to Dropbox.....	105

Working with Relays.....	106
What is a Relay?.....	106
Package Relays.....	107
File Relays.....	107
Tracking Relay Progress and Status.....	108
Using Metadata Fields to Set Relay Destinations.....	108
 Working with Directory Services (DS).....	 110
Review Directory Service Requirements.....	110
Adding a Directory Service to Faspex.....	110
Import Directory Service Groups.....	111
Import Individual Directory Service Users.....	112
 Working with SAML.....	 112
SAML and Faspex.....	112
User Accounts Provisioned by Just-In-Time (JIT) Provisioning.....	114
Configuring Your Identity Provider (IdP).....	115
Creating a SAML Configuration in Faspex.....	116
Creating SAML Groups.....	117
Configuring a Domain URL for SAML.....	118
Configure SAML Options.....	119
Setting Up Custom SAML Fields.....	120
Bypassing the SAML Redirect.....	121
SAML Group Permissions.....	121
Customizing SAML Error Messages.....	123
 Managing User Self-Registration.....	 124
Enabling Self-Registration.....	124
Approving or Denying Pending Registrations.....	125
Configure Self-Registration Template User.....	125
 Creating Distribution Lists.....	 128
Creating a Personal Distribution List.....	128
Creating a Global Distribution List.....	129
Configure User Access to Global Distribution Lists.....	130
 Using Rake Tasks to Manage Faspex.....	 130
Configuring the Primary Transfer Address of the Default Node.....	130
Creating Users with Rake Tasks.....	131
Bulk Create and Manage Users with Rake Tasks.....	131
Force All Users to Reset Passwords with Rake Tasks.....	133
Bulk Import and Manage DS Users with Rake Tasks.....	133
Import SAML Users with Rake Tasks.....	134
Automating Importing SAML Users with Rake Tasks.....	135
Configuring Server Settings with Rake Tasks.....	136
Managing Packages with Rake Tasks.....	137
Encrypting and Decrypting Database Passwords.....	137
Exporting and Importing Global Distribution Lists.....	138

Customizing Faspex: Email Notifications, Server Instructions, Application

Appearance.....	138
Configuring Email Notification Templates.....	138
Posting Instructions for Sending New Packages.....	139
Posting Announcements on the Login Page.....	139
Configure Display Settings.....	140
Creating a Custom CSS File.....	141
Customize Faspex with the Custom CSS File.....	141
Creating CSS Classes to Use in Instructions.....	144
 Configuring Metadata.....	 145
Faspex Metadata.....	145
Creating Metadata Profiles.....	146
Applying Metadata Profile to Normal Packages.....	147
 Backing Up and Restoring Faspex.....	 148
Backing Up Faspex from the Application.....	148
Backing Up Faspex from the Command Line.....	149
Restoring your Faspex Database.....	149
 Configuring Faspex Using <code>faspex.yml</code>.....	 151
Configuring Signed SAML Authentication Requests.....	151
Handling Sender and Recipient Information in Tags.....	152
<code>faspex.yml</code> Configurations Reference.....	154
 Validating Packages and Files with IBM Aspera Validator.....	 159
Installing and Configuring the Validator Service.....	159
Monitoring Validation.....	159
Validation and Relays.....	160
Troubleshooting Validation.....	161
 Troubleshooting Faspex.....	 161
Common Errors in Faspex.....	161
Resetting Admin Password.....	162
Troubleshooting File Storage Errors.....	162
Changing Stats Collector Purge Frequency.....	163
Log Files.....	163
Restarting Faspex and Common Aspera Services.....	164
Restarting Aspera Services.....	165
 Appendix.....	 166
High Availability Configuration.....	166
Introduction.....	166
Architecture for High Availability Systems.....	167
Installation.....	171
Upgrading the Environment.....	181
Maintenance of the HA Environment.....	186

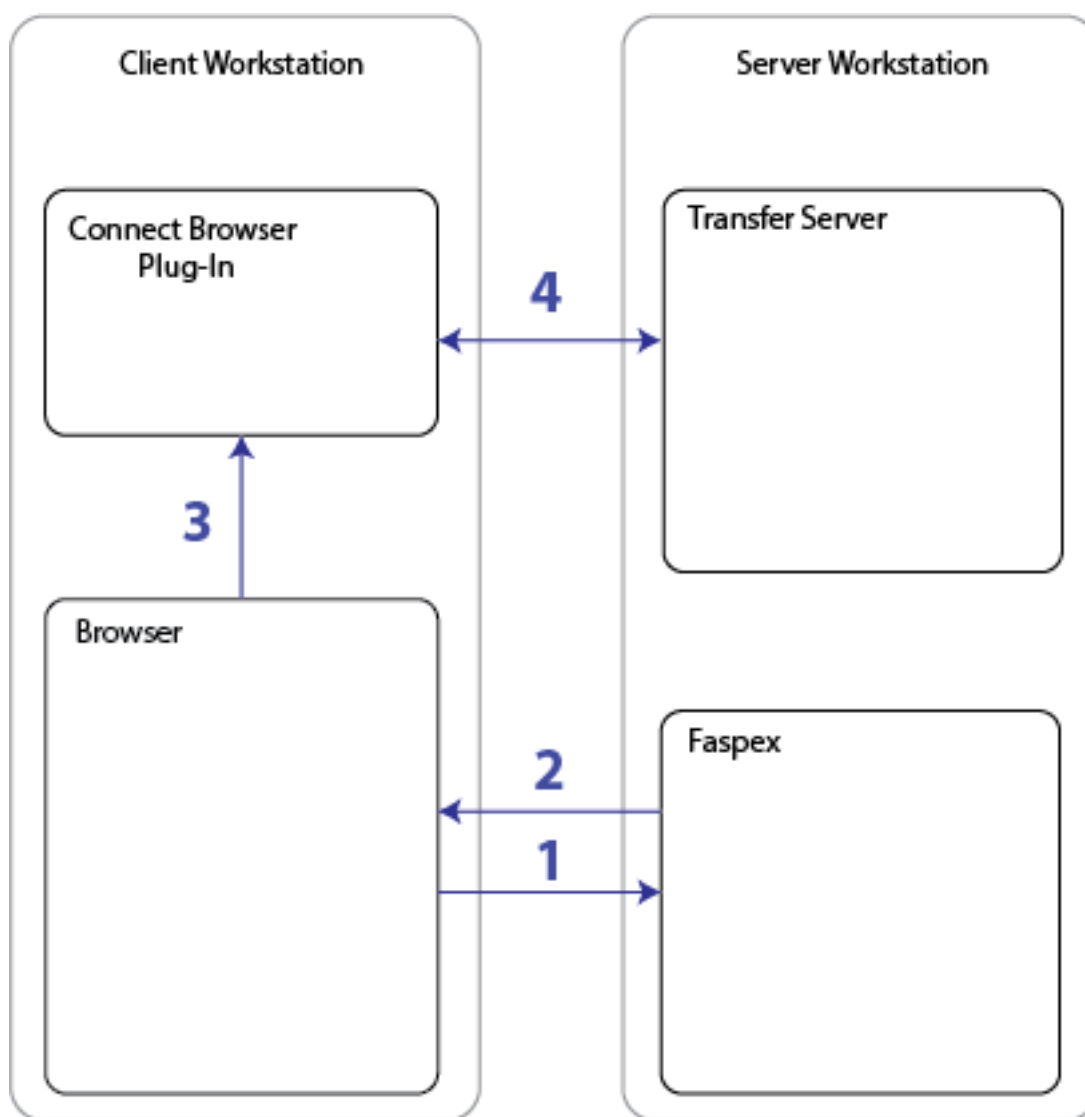
Suspending ACM.....	189
Appendix.....	194
Using the Health Check URL.....	198
asctl Command Reference.....	199
Faspex APIs.....	206
Enabling Faspex V4 APIs.....	206
Available HTML Tags and Attributes in Faspex.....	207
Directory Service Group Permissions Reference.....	207
Configure User Settings.....	209
Email Notification Template Types.....	213
Email Notification Template Text Strings.....	215
Partitioning Mongrel Processes between Faspex and Cargo.....	226
Aspera Ecosystem Security Best Practices.....	228
Securing the Systems that Run Aspera Software.....	228
Securing the Aspera Applications.....	232
Securing Content in your Workflow.....	239
Patch Versions.....	241

Introduction

Faspex is a file exchange application built on IBM Aspera High-Speed Transfer Server as a centralized transfer solution. With a web-based graphical user interface, Faspex offers more advanced management options for *fasp* high-speed transfer to match your organization's workflow. Faspex offers the following file-exchange and management features:

Feature	Description
Web/Email-based Interface	Simple web and email interface for exchanging files and directories.
Package Forwarding	Enable users to forward file packages on the server to others (without re-uploading).
Permission Management	Manage user permissions through workgroup/dropbox assignment or direct configuration.
Post-Processing	Execute custom scripts after a transfer when certain conditions are met.
Email Notification	Create customizable email notifications of Faspex events (such as receiving a package).
Directory Service	Seamlessly integrate your organization's Directory Service users and groups.

The following diagram illustrates how Faspex handles file transfers:



1. A user accesses the Faspex website through a web browser.
2. At this point, Faspex checks that IBM Aspera Connect is installed and up-to-date. If it is not, Faspex automatically prompts the user to download the latest version. Faspex displays the HST Server's file list or an upload page based on the user's request.
3. When the user selects a file for download or upload, transfer information is passed to Connect.
4. Connect establishes a connection with the HST Server and begins transferring the files.

Installing Faspex

Faspex Installation Scenarios

There are three main ways to install Faspex.

Use Case 1: Installing Faspex with the Transfer Server on the Local server

The simplest use case is to install both Faspex and the transfer server on the same server. When installing Faspex on the same server as a transfer server, Faspex automatically configures the local node's `aspera.conf` configuration file and sets up a Node API user to communicate with the Node API. During installation, you can also choose to

perform a streamlined installation which allows Faspex to configure advanced options to Faspex defaults. This streamlined installation is not available when the transfer server is on a remote server.

For instructions, see [Installing Faspex with a Local Node](#) on page 10.

Use Case 2: Installing Faspex with the Transfer Server on a Remote server

When installing Faspex on a machine without a transfer server, you must configure a remote transfer node for use with Faspex and connect that node to Faspex during the installation process.

For instructions, see [Installing Faspex with a Remote Node](#) on page 13.

Use Case 3: Installing Faspex Programmatically with a Setup File

You can automate Faspex installation by using setup files generated by the `asctl` command-line interface. The setup files define configuration options that are manually configured during a typical installation.

For instructions, see [Installing Faspex with a Setup File](#) on page 18.

Installing Faspex with a Local Node

The simplest installation scenario is to install both Faspex and the transfer server on the same server.



Warning: Due to incompatible common components, IBM Aspera Console and IBM Aspera Faspex *cannot* be installed on the same machine. IBM Aspera does not support this combination.

Note:

When installing Faspex on the same workstation as the transfer server, Faspex automatically configures the local node's `aspera.conf` configuration file and sets up a Node API user to communicate with the Node API. When installing Faspex on a machine without a transfer server, you must configure a remote transfer node for use with Faspex and connect that node to Faspex during the installation process.

Before You Begin...

Before beginning the installation process for Faspex, you must be logged into your computer as an admin .

1. Review the system requirements section of the release notes.
2. Download the latest version of IBM Aspera High-Speed Transfer Server, Common Components and IBM Aspera Faspex installers from the following locations:
 - HSTS: <http://downloads.asperasoft.com/en/downloads/1>
 - Common Components: <http://downloads.asperasoft.com/en/downloads/6>
 - Faspex: <http://downloads.asperasoft.com/en/downloads/6>

Installing the Transfer Server Locally

To install IBM Aspera High-Speed Transfer Server, log into your computer with root permissions.

1. Run the installer

To run the installer, run the following commands with the proper administrative permissions. Replace the product version accordingly.

```
$ rpm -Uvh aspera-entsrv-version.rpm
```

2. Install the license.

The license can be installed using the GUI or from the command line.

- **GUI:** Launch the application by running the following command as root:

```
# asperascp
```

If this is a fresh install, an **Enter License** window appears. Either click **Import License File** and select the license file, or click **Paste License Text** to copy-and-paste the license file's content. The license information appears in the window. Verify that it is correct and click **Close**.

- **Terminal:** Create the following file:

```
/opt/aspera/etc/aspera-license
```

Copy and paste your license key string into it, then save and close the file. To verify the license information, run the following command:

```
$ ascp -A
```

3. Review or update OpenSSH authentication methods.

Open your SSH Server configuration file from `/etc/ssh/sshd_config` with a text editor.

To allow public key authentication, set `PubkeyAuthentication` to `yes`. To allow password authentication, set `PasswordAuthentication` to `yes`, for example:

```
...
PubkeyAuthentication yes
PasswordAuthentication yes
...
```

Restart the `sshd` service:

```
$ sudo service sshd restart
```

To further secure your SSH Server, see the *IBM Aspera High-Speed Transfer Server Admin Guide: Securing Your SSH Server*.

Install Faspex on the server

Before installing Aspera Faspex:

- Disable SELinux (Security-Enhanced Linux) on your RedHat, CentOS or Fedora machine. SELinux, an access control implementation, causes the Faspex installation to fail with an error. Disable SELinux on your machine by following the instructions in [Disabling SELinux](#) on page 54.
- If you have an existing MySQL database installed, stop the MySQL service.
- If you have an existing Apache HTTP server installed, stop the Apache server.

1. Install the IBM Aspera Common Components.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-common-version.rpm
```

2. Launch the Faspex installer.

Note: The installer attempts to create a **faspex** system user and the associated `/home/faspex/` directory. If your organization does not allow you to use the `/home` directory, first create the **faspex** user and configure the user directory with the following commands:

```
# mkdir -p /home/faspex/faspex_packages
# chown faspex:faspex /home/faspex/
```

```
# chown faspex:faspex /home/faspex/faspex_packages
```

The installer uses the **faspex** user that you created and does not need to create the **faspex** user directory.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-faspex-version.rpm
```

3. Launch `asctl` to continue the Faspex setup process. Run the following command:

```
asctl faspex:setup
```

4. Choose to perform a `streamlined (s)` setup or a `detailed (d)` setup.

Follow the configuration instructions to complete the setup. The prompts the installer presents depends on whether this is a streamlined or detailed setup. See the table below for more information.

Prompt	Description	Streamlined or Detailed Setup?
What base port should the Mongrel servers start at?	The default is 3000	Detailed setup
Do you want to run the transfer server locally? (y/n)	You must choose <code>y</code> .	Detailed setup
Enter the directory to store Faspex packages	The directory to store packages uploaded to the Faspex server. If the chosen directory does not exist, Faspex prompts you to create it	Detailed setup
Choose a login name for the new admin user	The login name for the new Faspex admin user account.	Both
Enter the email address for admin	The email address to associate with the Faspex admin user account.	Both
Enter the password for admin	The password for the Faspex admin user account. Note: When you log in for the first time, Faspex requires you to change your password.	Both
Do you want to update SSL DHParams?	The default is <code>y</code> .	Both
What port would you like MySQL to listen on?	The default is 4406.	Detailed setup
Please enter a new MySQL root password	The password for the MySQL user account.	Both
Mysql will need to start/restart during configuration. Continue (y/n)?	You must choose <code>y</code> .	Both
Enter IP address of network interface for apache to listen on	The hostname or IP address of the server.	Detailed setup
What hostname or IP address should Apache use to identify itself (in the SSL certificate)?	The default is <code>127.0.0.1</code> .	Both

Prompt	Description	Streamlined or Detailed Setup?
What port would you like to run Apache http on?	The default is 80.	Both
What port would you like to run Apache https on?	The default is 443.	Both
Would you like to generate a self-signed SSL certificate, or install your own? ([g]enerate, [c]opy)	The default is generate (g).	Detailed setup
Aspera Central will need to restart when setup completes. This will stop any active transfers. Is this okay (y/n)?	If you choose n, you must restart these services yourself after installation. See Restarting Aspera Services on page 165.	Both
Aspera Node Server will need to restart when setup completes. Is this okay (y/n)?	If you choose n, you must restart these services yourself after installation. See Restarting Aspera Services on page 165.	Both
Aspera HTTPD will need to restart when setup completes. This will stop any HTTP fallback transfers. Is this okay (y/n)?	If you choose n, you must restart these services yourself after installation. See Restarting Aspera Services on page 165.	Both

First Time Log In and Licensing

1. Open a supported browser and enter the Faspex hostname or IP address followed by `/aspera/faspex` in the browser URL. For example:

`http://faspex.asperasoft.com/aspera/faspex`

or

`http://198.51.100.24/aspera/faspex`

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Enter the login credentials you created for the admin user and click **Login**.

When logging in for the first time, you must change your password and then login with the new password.

3. Configure a valid license.

You cannot interact with Faspex until configuring a valid license.

- a) Click **Browse** to upload a license file from your computer, or paste the contents of your license into the box.
- b) Click **Update and validate license**.

Installing Faspex with a Remote Node

Some use cases may require a user to install Faspex and the transfer server on separate machines. In such a case, first, configure the remote transfer server as a node. Then, install and configure the Faspex application.



Warning: Due to incompatible common components, IBM Aspera Console and IBM Aspera Faspex cannot be installed on the same machine. IBM Aspera does not support this combination.

When installing Faspex on the same workstation as the transfer server, Faspex automatically configures the local node's `aspera.conf` configuration file and sets up a Node API user to communicate with the Node API. When installing Faspex on a machine without a transfer server, you must configure a remote transfer node for use with Faspex and connect that node to Faspex during the installation process.

Before You Begin...

Before beginning the installation process for Faspex, you must be logged into your computer as an admin .

1. Review the system requirements section of the release notes.
2. Download the latest version of IBM Aspera High-Speed Transfer Server, Common Components and IBM Aspera Faspex installers from the following locations:
 - HSTS: <http://downloads.asperasoft.com/en/downloads/1>
 - Common Components: <http://downloads.asperasoft.com/en/downloads/6>
 - Faspex: <http://downloads.asperasoft.com/en/downloads/6>

Install Faspex on the Server

Before installing Aspera Faspex:

- Disable SELinux (Security-Enhanced Linux) on your RedHat, CentOS or Fedora machine. SELinux, an access control implementation, causes the Faspex installation to fail with an error. Disable SELinux on your machine by following the instructions in [Disabling SELinux](#) on page 54.
 - If you have an existing MySQL database installed, stop the MySQL service.
 - If you have an existing Apache HTTP server installed, stop the Apache server.
1. Install the IBM Aspera Common Components.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-common-version.rpm
```

2. Launch the Faspex installer.

Note: The installer attempts to create a **faspex** system user and the associated `/home/faspex/` directory. If your organization does not allow you to use the `/home` directory, first create the **faspex** user and configure the user directory with the following commands:

```
# mkdir -p /home/faspex/faspex_packages
# chown faspex:faspex /home/faspex/
# chown faspex:faspex /home/faspex/faspex_packages
```

The installer uses the **faspex** user that you created and does not need to create the **faspex** user directory.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-faspex-version.rpm
```

3. Launch `asctl` to continue the Faspex setup process. Run the following command:

```
asctl faspex:setup
```

4. When prompted to perform a streamlined or detailed setup, choose to perform a detailed (d) setup.

Follow the configuration instructions to complete the setup. The prompts the installer presents depends on whether this is a streamlined or detailed setup. See the table below for more information.

Prompt	Description	Streamlined or Detailed Setup?
What base port should the Mongrel servers start at?	The default is 3000	Detailed setup
Do you want to run the transfer server locally? (y/n)	You must choose n.	Detailed setup
What address or hostname should the Faspex web server use to communicate with the transfer server?	The hostname or IP address of your remote transfer node. Note: You can change this after installation using a rake command. For more information, see Configuring Server Settings with Rake Tasks on page 136.	Detailed setup
What address or hostname should end users (with Aspera Connect) use to communicate with the transfer server?	The hostname or IP address of the remote transfer node.	Detailed setup
Choose a login name for the new admin user	The login name for the new Faspex admin user account.	Both
Enter the email address for admin	The email address to associate with the Faspex admin user account.	Both
Enter the password for admin	The password for the Faspex admin user account. Note: When you log in for the first time, Faspex requires you to change your password.	Both
Do you want to update SSL DHParams?	The default is y.	Both
What port would you like MySQL to listen on?	The default is 4406.	Detailed setup
Please enter a new MySQL root password	The password for the MySQL user account.	Both
Mysql will need to start/restart during configuration. Continue (y/n)?	You must choose y.	Both
Enter IP address of network interface for apache to listen on	The hostname or IP address of the server.	Detailed setup
What hostname or IP address should Apache use to identify itself (in the SSL certificate)?	The default is 127.0.0.1.	Both
What port would you like to run Apache http on?	The default is 80.	Both
What port would you like to run Apache https on?	The default is 443.	Both

Prompt	Description	Streamlined or Detailed Setup?
Would you like to generate a self-signed SSL certificate, or install your own? ([g]enerate, [c]opy)	The default is generate (g).	Detailed setup
Aspera Central will need to restart when setup completes. This will stop any active transfers. Is this okay (y/n)?	If you choose n, you must restart these services yourself after installation. See Restarting Aspera Services on page 165.	Both
Aspera Node Server will need to restart when setup completes. Is this okay (y/n)?	If you choose n, you must restart these services yourself after installation. See Restarting Aspera Services on page 165.	Both
Aspera HTTPD will need to restart when setup completes. This will stop any HTTP fallback transfers. Is this okay (y/n)?	If you choose n, you must restart these services yourself after installation. See Restarting Aspera Services on page 165.	Both

First Time Log In and Licensing

1. Open a supported browser and enter the Faspex hostname or IP address followed by `/aspera/faspex` in the browser URL. For example:

`http://faspex.asperasoft.com/aspera/faspex`

or

`http://198.51.100.24/aspera/faspex`

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Enter the login credentials you created for the admin user and click **Login**.

When logging in for the first time, you must change your password and then login with the new password.

3. Configure a valid license.

You cannot interact with Faspex until configuring a valid license.

- a) Click **Browse** to upload a license file from your computer, or paste the contents of your license into the box.
- b) Click **Update and validate license**.

Provide Faspex with Credentials to the Remote Node

1. Go to **Server > File Storage**.

2.

Select **Edit** from the  drop-down menu.

3. Enter the Node API user credentials in the **Username** and **Password** fields.

4. Click **Test Connection**.

If Faspex displays an error instead of the message "Connection succeeded!", see [Troubleshooting File Storage Errors](#) on page 162 for help understanding the error.

5. Click **Update Node**.

Migrating Faspex to a New Machine

Move an existing Faspex server installation to a new system.

Important: You must migrate to the same version of Faspex.

1. Back up your Faspex MySQL database by running the following `asctl` command:

```
asctl faspex:backup_database
```

The `asctl` command uses `mysqldump` to backup Faspex's three MySQL databases to `/opt/aspera/faspex/backup/time_stamp-version_number.revision_number`

For example, the directory name may be **2016-04-15_140547-Faspex.4.0.0.100400**.

2. Move files from the current server to the new server.

- The database backup directory you just generated
- `/opt/aspera/faspex/config/secret.yml`
- `/opt/aspera/common/apache/conf/*.key` (if you have your own SSL certificates)
- `/opt/aspera/common/apache/conf/*.crt` (if you have your own SSL certificates)
- `/opt/aspera/faspex/config/faspex.yml` (if you made advanced Faspex configurations)
- `/opt/aspera/faspex/lib/daemons/np/etc/keystore.jks`

Note: You cannot use the same Faspex license on multiple systems as this is a violation of your license terms. You can only use the Faspex license from your original system on your new system if you are immediately uninstall Faspex on the original system. If your original Faspex installation needs to stay up and running for a short period you may ask your account manager for a temporary license to use on your new installation.

3. On the new machine, install Faspex. Again, make sure you install the same version of Faspex that you had on the original server.

For instructions on installing Faspex, see [Faspex Installation Scenarios](#) on page 9.

4. Restore the database with the backup directory:

```
asctl faspex:restore_database /path/to/your_backup
```

5. Restore `secret.yml`:

```
# cp /path/to/secret.yml /opt/aspera/faspex/config/secret.yml
```

6. If you copied `faspex.yml`, restore the configuration file:

```
# cp /path/to/faspex.yml /opt/aspera/faspex/config/faspex.yml
```

Open up `faspex.yml` in a text editor and look for the `production` section. Change `Hostname` and `BaseURL` to your new hostname or IP address.

7. If you copied over certificates that you would like to continue using for your new Faspex installation, restore the certificates:

```
asctl apache:install_ssl_cert cert_filekey_file[chain_file]
```

8. Clear the `fasp_nodes` table in MySQL:

```
# /opt/aspera/common/mysql/bin/mysql -uroot -ppassword -e 'delete from fasp_nodes;' faspex
```

9. Restart Faspex services

```
asctl all:restart
```

10. Update file storage for the tethered node:

- a) Go to **Server > File Storage** and select the drop-down menu next to **localhost**.
 - If the tethered node is local, select **Edit**. For **Username** and **Password** enter the Node API credentials.
 - If the tethered node is remote, select **Add File Storage**. Fill in the configuration details.
- b) Under **Advanced Configuration**, make sure the **Primary transfer address or name** reflects the new server's address or name.
- c) Click **Update Node**.

Installing Faspex with a Setup File

You can automate Faspex installation by using setup files generated by the `asctl` command-line interface. The setup files define configuration options that are manually configured during a typical installation.



Warning: Due to incompatible common components, IBM Aspera Console and IBM Aspera Faspex *cannot* be installed on the same machine. IBM Aspera does not support this combination.

Generate the Setup Files

1. Install the Aspera common applications and the Faspex packages, in that order.

```
# rpm -Uvh aspera-common-version
# rpm -Uvh aspera-faspex-version
```

Note: Do not run the `asctl faspex:setup` command. That command initiates a typical Faspex installation.

2. Create the setup files for the Aspera common and Faspex applications.

The filenames of the setup files must end with the **.yaml** extension. Run the following commands:

```
asctl apache:create_setup_file /path/to/apache_setup_file.yaml
asctl mysql:create_setup_file /path/to/mysql_setup_file.yaml
asctl faspex:create_setup_file /path/to/faspex_setup_file.yaml
```

You are prompted to set the desired configuration options used to install each application.

Install Faspex Using the Setup Files

Before installing Aspera Faspex:

- Disable SELinux (Security-Enhanced Linux) on your RedHat, CentOS or Fedora machine. SELinux, an access control implementation, causes the Faspex installation to fail with an error. Disable SELinux on your machine by following the instructions in [Disabling SELinux](#) on page 54.
- If you have an existing MySQL database installed, stop the MySQL service.
- If you have an existing Apache HTTP server installed, stop the Apache server.

Use the setup files to install the Aspera common and Faspex applications.

Run the following commands manually or through a script to install the applications:

```
asctl apache:setup_from_file /path/to/apache_setup_file.yaml
asctl mysql:setup_from_file /path/to/mysql_setup_file.yaml
asctl faspex:setup_from_file /path/to/faspex_setup_file.yaml
```

First Time Log In and Licensing

1. Open a supported browser and enter the Faspex hostname or IP address followed by **/aspera/faspex** in the browser URL. For example:

`http://faspex.asperasoft.com/aspera/faspex`

or

`http://198.51.100.24/aspera/faspex`

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Enter the login credentials you created for the admin user and click **Login**.

When logging in for the first time, you must change your password and then login with the new password.

3. Configure a valid license.

You cannot interact with Faspex until configuring a valid license.

- a) Click **Browse** to upload a license file from your computer, or paste the contents of your license into the box.
- b) Click **Update and validate license**.

Configuring Faspex to Use a Remote Database (Faspex + MySQL)

Configuring Faspex to use a remote database can make the application more responsive by putting the database and background processes on a separate server from the one that hosts the Faspex web application. Configure two Faspex servers: a *database server* and an *application server*. The *database server* runs the MySQL database, and the *application server* runs the web application.

If you want to set up a remote database that only runs MySQL, see [Configuring Faspex to Use a Remote Database \(MySQL Only\)](#) on page 20.

Aspera recommends that you use the database on the server that runs background processes. The server hosting the application can be remote.

1. Set up two identical Faspex instances on separate servers.

Each Faspex installation creates its own database, but the servers are configured to only use one.

2. On the database server, grant the application server access to the database.

Run the following commands to run the MySQL command line:

```
/opt/aspera/common/mysql/bin/mysql -umysql_username -pmysql_password
```

From the MySQL command line, allow remote connection to the Faspex database from only the remote node, and exit the MySQL command line:

```
mysql > grant all privileges on faspex.* to root@'ui_server_hostname'
identified by 'mysql_password';

mysql > end
```

These commands allow connections from the application server to access the specified database.

3. On the database server, decrypt the `database.yml` database configuration file.

```
asctl faspex:rake aspera:decrypt_database_passwords
```

4. Copy the `database.yml` and `secret.yml` files from the database server to the application server.
5. On both servers, encrypt the `database.yml` database configuration files.

```
asctl faspex:rake aspera:encrypt_database_passwords
```

6. On the application server, point Faspex to the database on the database server.

Open `/opt/aspera/faspex/config/database.yml` in a text editor. Locate the line for **host** in the **production** section and change the value to the hostname of the database server. Save your changes.

7. On both servers, set matching encryption keys.

On both the database server and application server, run the following command to set the encryption key to the same value:

```
asconfigurator -x "set_node_data;token_encryption_key,token_key"
```

The `token_key` must be identical on the servers.

8. On both servers, restart `asperacentral` and `asperanoded`.

Run the following command in a Terminal window to restart `asperacentral`:

```
# /etc/init.d/asperacentral restart
```

Run the following commands to restart `asperanoded`:

```
# /etc/init.d/asperanoded restart
```

9. On both servers, create the same node username and password.

This must be done after configuring `database.yml` and `secret.yml`. Run the following command:

```
asnodeadmin -a -u node_username -p node_password -x transfer_username
```

For example:

```
asnodeadmin -a -u nodeadmin -p -x faspex
```

10. In the web application, configure the localhost file server to use the new node user.

In the Faspex application, go to **Server > File Storage**. Click the arrow for localhost and click **Edit**. Enter the `node_username` from the previous step in the **Username** field and the `node_password` in the **Password** field.

Click **Update Node** to activate your changes.

11. On both servers, restart Faspex services.

```
asctl faspex:restart
```

12. On both servers, configure background processes.

On the database node: Disable the application by running the following command:

```
asctl faspex:mongrel:stop
```

On the application node: Disable all process but the application by running the following commands:

```
asctl all:stop
asctl faspex:mongrel:start
asctl apache:start
```

After following these instructions, you have one node running database and background services, and another node running only the application.

Configuring Faspex to Use a Remote Database (MySQL Only)

Faspex can be configured to use a remote database that only runs MySQL. To configure Faspex to use a remote database on a node that also runs Faspex background processes (so that the other Faspex node runs only the Faspex application), see [Configuring Faspex to Use a Remote Database \(Faspex + MySQL\)](#) on page 19.

1. Set up the remote database.

Note: For this operation, Faspex requires MySQL version 5.7 or later. Earlier versions are not supported.

2. On the Faspex server, stop Faspex services and back up the local database.

```
asctl faspex:stop
asctl faspex:backup_database
```

Record the location of the database backup, which you use in the next step to migrate the database.

3. Grant remote access privileges to Faspex.

```
mysql > CREATE USER 'root'@'faspex_ip_address' IDENTIFIED
BY 'mysql_password'; GRANT ALL PRIVILEGES ON *.* TO
'root'@'faspex_ip_address' WITH GRANT OPTION; FLUSH PRIVILEGES;
```

For example:

```
mysql > CREATE USER 'root'@'10.0.174.47' IDENTIFIED BY '*****'; GRANT
ALL PRIVILEGES ON *.* TO 'root'@'10.0.174.47' WITH GRANT OPTION; FLUSH
PRIVILEGES;
```

4. Migrate the local database to the remote database.

```
/opt/aspera/common/mysql/bin/mysql -h remote_db_ip_address -P port -
umysql_username -pmysql_password < path_to_db_backup
```

The default MySQL port is 4406. For example,

```
/opt/aspera/common/mysql/bin/mysql -h 54.182.111.111 -P 4406 -uroot -
pXR9sJFF5ja1BGLKHYLwzQ== < /opt/aspera/faspex/backup/2015-07-01_23458/
faspex.sql
```

5. Verify that the migration was successful.

Log in to the MySQL database:

```
/opt/aspera/common/mysql/bin/mysql -h remote_db_ip_address -P port -
umysql_username -pmysql_password
```

View the contents of the new database by running the following commands:

```
mysql use faspex;
mysql show tables;
mysql select * from e_packages;
```

6. On the Faspex server, configure Faspex to use the remote database.

- a) Back up the `/opt/aspera/common/mysql/database.rb.yml` files.
- b) Edit `/opt/aspera/common/mysql/database.rb.yml`.

Change:

- host to the IP address of the remote database.
- port to the MySQL port (4406, by default).
- password to the remote MySQL database password.
- user to the remote MySQL database user.

Note: By default, there is no `user` field. Faspex defaults to the `root` user. Add a new line to configure a different, non-root user. For example, `:user: remote_faspex_user`.

For example:

```
---
...
:hostname: 54.182.111.111
:port: 4406
:task status:
  ...
  ...
:user: remote_faspex_user
:password: XRs9sJFF5ja1BG1KHYLwzQ==
:setup_complete: true
```

Save your changes.

c) Edit `/opt/aspera/faspex/config/database.yml`.

Locate the production and change:

- host to the IP address of the remote database.
- port to the MySQL port (4406, by default).
- username to the remote MySQL database user.

Note: By default, Faspex also includes the user field, but uses the username field for the MySQL database user.

- password to the remote MySQL database password.

For example:

```
...
production:
  encoding: utf8
  port: 4406
  username: faspex
  adapter: mysql
  database: faspex
  host: 54.182.111.111
  user: root
  password: XRs9sJFF5ja1BG1KHYLwzQ==
```

Save your changes.

a) Edit `/opt/aspera/faspex/lib/daemons/np/etc/persistence.xml`.

Locate the `<properties>` section and change **hibernate.connection.url** to the IP address of the remote database, **port** to the MySQL port (4406, by default), and provide the username and password to the remote MySQL database.

```
...
  <properties>
    <property name="hibernate.connection.driver_class"
value="com.mysql.jdbc.Driver"/>
    <!-- connection URL: jdbc:mysql://HOST:PORT/DATABASE -->
    <property name="hibernate.connection.url"
value="jdbc:mysql://ip_address:port/faspex"/>
    <property name="hibernate.connection.username" value="username"/>
    <property name="hibernate.connection.password" value="password"/>
    ...
  </properties>
...
```

For example:

```
...
```

```

    <properties>
      <property name="hibernate.connection.driver_class"
value="com.mysql.jdbc.Driver"/>
      <!-- connection URL: jdbc:mysql://HOST:PORT/DATABASE -->
      <property name="hibernate.connection.url"
value="jdbc:mysql://54.182.111.111:4406/faspex"/>
      <property name="hibernate.connection.username" value="root"/>
      <property name="hibernate.connection.password" value="aspera"/>
      ...
    </properties>
    ...

```

Save your changes.

7. Shut down the local MySQL database and restart all other Faspex services.

```

asctl mysql:disable
asctl all:restart

```

If you need to restart the local MySQL database, revert the `.yaml` files and then run the following command:

```

asctl mysql:setup

```

Updating Your License

IBM Aspera Faspex requires you to install a valid license key before you can configure Faspex users and begin sending or receiving packages.

1. Locate your Faspex license key file.

Download the license file with the **.aspera-license** file extension in the authorization email sent to you by Aspera (for example, *aspera.faspex.companyname.aspera-license*).

Note: If you have not received this email or need it resent, contact IBM Aspera Support for assistance.

2. Go to **Server > Configuration > License**.
3. Click **Browse** to upload a license file from your computer or paste the contents of your license into the box. Then click **Update and validate license**.
4. Update the transfer server license.

When updating your Faspex license, make sure the license for the default transfer server is also up-to-date. For instructions on how to update your HSTS license, see *IBM Aspera High-Speed Transfer Server Admin Guide: Updating the Product License*.

Enabling On Demand Entitlement for Faspex

Customers who are manually installing Faspex in an Aspera on Demand system need to configure Faspex to use an On Demand Entitlement instead of using a standard license. To use entitlement on Faspex, you must have the IBM Aspera High-Speed Transfer Endpoint installed on the same system, so that Faspex can access the included `asperanoded` and its license API.

1. Log on to the server hosting Faspex as the `root` user.
2. Turn on entitlement.

```

export RAILS_ENV=production
asctl faspex:rake entitlement:turn_safe_net_entitlement_mode_on

```

3. Entitle the system with your entitlement key and entitlement customer ID.

```

export RAILS_ENV=production

```

```
asctl faspex:rake --trace entitlement:config_license_server EL_KEY="key"
EL_CUSTOMER_ID="id"
```

For example:

```
export RAILS_ENV=production
asctl faspex:rake --trace entitlement:config_license_server
EL_KEY="cd0904ae-f85a-4e3b-8ae0-615d79e5dea1" EL_CUSTOMER_ID="Test"
```

You can use the `--trace` option to debug issues.

If you do not want to use entitlement, you can turn it off with the following command:

```
export RAILS_ENV=production
asctl faspex:rake entitlement:turn_safe_net_entitlement_mode_off
```

Uninstalling Faspex

You must uninstall both IBM Aspera Faspex and IBM Aspera High-Speed Transfer Server to remove Faspex from your system.

1. Uninstall Faspex.

To uninstall Faspex, run the following commands in a Terminal window:

```
# asctl all:stop
# rpm -e aspera-faspex
# rpm -e aspera-common
```

2. Uninstall HSTS.

To uninstall HSTS, run the following command in a Terminal window:

```
# rpm -e aspera-entsrv
```

Logging In

1. Open a supported browser and enter the Faspex hostname or IP address followed by `/aspera/faspex` in the browser URL. For example:

```
http://faspex.asperasoft.com/aspera/faspex
```

or

```
http://198.51.100.24/aspera/faspex
```

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Log in with your credentials.

If SAML configurations are available, you can choose to log in with a configured SAML provider or with your Faspex user credentials.

If your administrator configured Faspex to use a default SAML configuration, Faspex automatically redirects you to the SAML login page. Login with your SAML credentials or login locally by bypassing the redirect.

If you need to login with your Faspex user credentials or if you need to log in using another SAML configuration, you can bypass the redirect by adding `login?local=true` to the end of the URL. For example:
<https://192.51.100.24/aspera/faspex/login?local=true>.

3. If prompted, install IBM Aspera Connect.

You must have the latest version of Connect installed to transfer packages using Faspex. Faspex prompts you to install the Connect Browser if you do not have it installed or if your version is not the latest. If you install Connect, refresh your browser to start using Connect.

For more information, see [Faspex and Connect](#) on page 79.

4. If your license is out-of-date or expired, you must first update the license before you can access Faspex.

Faspex prompts you to update your license . You cannot interact with Faspex until entering and saving a valid license. For more information, see [Updating Your License](#) on page 23.

5. If you are upgrading from a version of Faspex prior to 4.0.1 and you had SAML configured, you need to add your SAML configuration metadata to your SAML Identity Provider (IdP) again. Metadata URLs now contain numbers to support multiple SAML configurations.

For information about configuring the IdP, see [Configuring Your Identity Provider \(IdP\)](#) on page 115.

Upgrading Faspex

Upgrading Faspex from 4.2.0 or Later

Upgrade Faspex to the latest version from a post-4.2.0 version of Faspex.

Before You Begin...

Before beginning the installation process for Faspex, you must be logged into your computer as an admin .

Important: IBM Aspera supports direct upgrades to the current General Availability (GA) version from only two GA versions prior to the current release. To upgrade to the latest version, you must be within two GA versions of the current version. Upgrading from older version requires upgrading in steps. For example, if you are four GA versions behind, upgrade to two GA versions behind (GA - 2), and then upgrade to the current GA version.



Warning:

Prior to performing any upgrade, IBM Aspera strongly recommends customers:

1. Perform a full environment back up and ensure the back up is successful. In case the upgrade fails, the only reliable, short-term fix is to roll back the environment using the back up.
 2. Test the upgrade in a test environment comparable to the production environment.
 3. If upgrading the test environment is successful, upgrade the production environment, but do not bring the production environment back online.
 4. Prior to bringing the production environment back online, the customer must test the application to determine if an immediate rollback is needed. Otherwise, customers risk losing all data generated between upgrade and rollback.
1. Download the latest version of IBM Aspera High-Speed Transfer Server, Common Components and IBM Aspera Faspex installers from the following locations:
 - HSTS: <http://downloads.asperasoft.com/en/downloads/1>
 - Common Components: <http://downloads.asperasoft.com/en/downloads/6>
 - Faspex: <http://downloads.asperasoft.com/en/downloads/6>
 2. Make sure your MySQL password are easily accessible.
 3. Check the requirements in *IBM Aspera High-Speed Transfer Server Admin Guide: Before Upgrading*.

4. Install HSTS.

```
$ rpm -Uvh aspera-entsrv-version.rpm
```

Upgrading Faspex from 4.2.0 and Later

1. Back up your Faspex MySQL database by running the following `asctl` command:

```
asctl faspex:backup_database
```

The `asctl` command uses `mysqldump` to backup Faspex's three MySQL databases to `/opt/aspera/faspex/backup/time_stamp-version_number.revision_number`

For example, the directory name may be **2016-04-15_140547-Faspex.4.0.0.100400**.

2. Stop all Faspex services.

Before upgrading, stop all services related to Faspex, including Faspex, MySQL, and Apache. Use the following command:

```
asctl all:stop
```

3. Back up the host before upgrading.

If Faspex is installed on a physical host, perform a full file-system backup.

If Faspex is installed on a virtual machine, perform a full virtual-machine backup or take a snapshot.

In both cases, if a full backup is not viable, back up `/opt/aspera` as a minimal option.

4. If your server is using a remote database, you must set the `SKIP_MYSQL_UPGRADE` environment variable to `true` to perform a successful upgrade.

```
export "SKIP_MYSQL_UPGRADE=true"
```

For more information about using a remote database, see [Configuring Faspex to Use a Remote Database \(Faspex + MySQL\)](#) on page 19.

Important: If you are using a local database, do not skip the MySQL upgrade.

5. Install the IBM Aspera Common Components.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-common-version.rpm
```

6. Launch the Faspex installer.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-faspex-version.rpm
```

7. Run the `asctl:upgrade` command.

```
asctl faspex:upgrade
```

8. If you are upgrading from a version prior to 4.2.x, Faspex prompts you to provide the path to the database backup you made earlier:

```
Please provide the location of the Faspex database backup (e.g.
backup/20XX-XX-XX_XXXXXX-Faspex.4.1.1.XXXXXX):
```

9. Confirm that your previous Faspex settings are still applicable.

Faspex prompts you to confirm if your previous Faspex settings are still applicable. Enter `y` to continue, `n` to change settings.

10. If Faspex and HSTS are installed on the same server, restart the `service`.

Run the following commands to restart the `asperanoded` service:

```
# service asperanoded restart
```

11. If you are using IBM Aspera Validator with Faspex, you must enable the **Out-of-transfer file validation (otfv)** setting (**Server > Security**).

12. If you had the HTTP Gateway [BETA] service installed, and want to use Faspex with HTTP Gateway 2.0 and later, stop the process, and then remove the `/opt/aspera/httpgateway` from your server:

```
service aspera_httpgateway stop
rm -rf /opt/aspera/httpgateway
```

Logging In

1. Open a supported browser and enter the Faspex hostname or IP address followed by `/aspera/faspex` in the browser URL. For example:

```
http://faspex.asperasoft.com/aspera/faspex
```

or

```
http://198.51.100.24/aspera/faspex
```

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Log in with your credentials.

If SAML configurations are available, you can choose to log in with a configured SAML provider or with your Faspex user credentials.

If your administrator configured Faspex to use a default SAML configuration, Faspex automatically redirects you to the SAML login page. Login with your SAML credentials or login locally by bypassing the redirect.

If you need to login with your Faspex user credentials or if you need to log in using another SAML configuration, you can bypass the redirect by adding `login?local=true` to the end of the URL. For example:

<https://192.51.100.24/aspera/faspex/login?local=true>.

3. If prompted, install IBM Aspera Connect.

You must have the latest version of Connect installed to transfer packages using Faspex. Faspex prompts you to install the Connect Browser if you do not have it installed or if your version is not the latest. If you install Connect, refresh your browser to start using Connect.

For more information, see [Faspex and Connect](#) on page 79.

4. If your license is out-of-date or expired, you must first update the license before you can access Faspex.

Faspex prompts you to update your license. You cannot interact with Faspex until entering and saving a valid license. For more information, see [Updating Your License](#) on page 23.

5. If you are upgrading from a version of Faspex prior to 4.0.1 and you had SAML configured, you need to add your SAML configuration metadata to your SAML Identity Provider (IdP) again. Metadata URLs now contain numbers to support multiple SAML configurations.

For information about configuring the IdP, see [Configuring Your Identity Provider \(IdP\)](#) on page 115.

Upgrading Faspex from Before 4.2.0

Upgrading to Faspex 4.2.0 and later from a version prior to 4.2.0 requires additional steps to upgrade to a newer version of MySQL.



Warning:

Prior to performing any upgrade, IBM Aspera strongly recommends customers:

1. Perform a full environment back up and ensure the back up is successful. In case the upgrade fails, the only reliable, short-term fix is to roll back the environment using the back up.
2. Test the upgrade in a test environment comparable to the production environment.
3. If upgrading the test environment is successful, upgrade the production environment, but do not bring the production environment back online.
4. Prior to bringing the production environment back online, the customer must test the application to determine if an immediate rollback is needed. Otherwise, customers risk losing all data generated between upgrade and rollback.

Note: Aspera does not support a direct upgrade from Faspex versions prior to 3.1.1. Instead, first upgrade to version 3.9.3 before upgrading to 4.0+.

Before You Begin...

Before beginning the installation process for Faspex, you must be logged into your computer as an admin .

1. Download the latest version of IBM Aspera High-Speed Transfer Server, Common Components and IBM Aspera Faspex installers from the following locations:
 - HSTS: <http://downloads.asperasoft.com/en/downloads/1>
 - Common Components: <http://downloads.asperasoft.com/en/downloads/6>
 - Faspex: <http://downloads.asperasoft.com/en/downloads/6>
2. Make sure your MySQL password are easily accessible.
3. Check the requirements in *IBM Aspera High-Speed Transfer Server Admin Guide: Before Upgrading*.
4. Install HSTS.

```
$ rpm -Uvh aspera-entsrv-version.rpm
```

Upgrading Faspex from Before 4.2.0

1. Back up your Faspex MySQL database by running the following `asctl` command:

```
asctl faspex:backup_database
```

The `asctl` command uses `mysqldump` to backup Faspex's three MySQL databases to `/opt/aspera/faspex/backup/time_stamp-version_number.revision_number`

For example, the directory name may be **2016-04-15_140547-Faspex.4.0.0.100400**.

2. Stop all Faspex services.

Before upgrading, stop all services related to Faspex, including Faspex, MySQL, and Apache. Use the following command:

```
asctl all:stop
```



Warning: Faspex 4.2.0 and later uses a new version of MySQL included in the IBM Aspera Common Components. If you are upgrading from a version prior to 4.2.0, you must first back up and empty your MySQL database (`/opt/aspera/common/mysql/data`). You cannot upgrade the Common

Components until you have backed up and emptied your database. When running the upgrade script, you are required to provide the path to a back up.

3. If your server is using a remote database, you must set the `SKIP_MYSQL_UPGRADE` environment variable to `true`:

```
export "SKIP_MYSQL_UPGRADE=true"
```

Important: If you are using a local database, do not skip the MySQL upgrade.

4. If your server is *not* using a remote database, you must clear your MySQL database before upgrading to upgrade successfully.

Delete all the files and sub-directories in `/opt/aspera/common/mysql/data`.

5. Install the IBM Aspera Common Components.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-common-version.rpm
```

6. Launch the Faspex installer.

Use the following commands with proper administrative permissions to run the installers (replacing *version* accordingly):

```
rpm -Uvh ibm-aspera-faspex-version.rpm
```

7. Run the `asctl:upgrade` command.

```
asctl faspex:upgrade
```

8. Provide Faspex with the database backup when prompted:

```
Please provide the location of the Faspex database backup (e.g.
backup/20XX-XX-XX_XXXXXX-Faspex.4.1.1.XXXXXX):
```

9. Confirm that your previous Faspex settings are still applicable.

When prompted, enter `y` to continue, `n` to change settings.

10. If Faspex and HSTS are installed on the same server, restart the `service`.

Run the following commands to restart the `asperanoded` service:

```
# service asperanoded restart
```

Logging In

1. Open a supported browser and enter the Faspex hostname or IP address followed by `/aspera/faspex` in the browser URL. For example:

```
http://faspex.asperasoft.com/aspera/faspex
```

or

```
http://198.51.100.24/aspera/faspex
```

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Log in with your credentials.

If SAML configurations are available, you can choose to log in with a configured SAML provider or with your Faspex user credentials.

If your administrator configured Faspex to use a default SAML configuration, Faspex automatically redirects you to the SAML login page. Login with your SAML credentials or login locally by bypassing the redirect.

If you need to login with your Faspex user credentials or if you need to log in using another SAML configuration, you can bypass the redirect by adding `login?local=true` to the end of the URL. For example:

<https://192.51.100.24/aspera/faspex/login?local=true>.

3. If prompted, install IBM Aspera Connect.

You must have the latest version of Connect installed to transfer packages using Faspex. Faspex prompts you to install the Connect Browser if you do not have it installed or if your version is not the latest. If you install Connect, refresh your browser to start using Connect.

For more information, see [Faspex and Connect](#) on page 79.

4. If your license is out-of-date or expired, you must first update the license before you can access Faspex.

Faspex prompts you to update your license. You cannot interact with Faspex until entering and saving a valid license. For more information, see [Updating Your License](#) on page 23.

5. If you are upgrading from a version of Faspex prior to 4.0.1 and you had SAML configured, you need to add your SAML configuration metadata to your SAML Identity Provider (IdP) again. Metadata URLs now contain numbers to support multiple SAML configurations.

For information about configuring the IdP, see [Configuring Your Identity Provider \(IdP\)](#) on page 115.

Logging In to Faspex

Logging In to Faspex

1. Open a supported browser and enter the Faspex hostname or IP address followed by `/aspera/faspex` in the browser URL. For example:

`http://faspex.asperasoft.com/aspera/faspex`

or

`http://198.51.100.24/aspera/faspex`

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Log in with your credentials.

If SAML configurations are available, you can choose to log in with a configured SAML provider or with your Faspex user credentials.

If your administrator configured Faspex to use a default SAML configuration, Faspex automatically redirects you to the SAML login page. Login with your SAML credentials or login locally by bypassing the redirect.

If you need to login with your Faspex user credentials or if you need to log in using another SAML configuration, you can bypass the redirect by adding `login?local=true` to the end of the URL. For example:

<https://192.51.100.24/aspera/faspex/login?local=true>.

3. If you are logging in for the first time, you are prompted to change your password and then asked to login with the new password.

If you incorrectly enter your password too many times, Faspex locks your account. If enabled, you can select the **Forgot password** link from the login page to request a password reset email from Faspex. Once you reset your password, you can log into your account again.

4. If your license is out-of-date or expired, you must first update the license before you can access Faspex.

Faspex prompts you to update your license . You cannot interact with Faspex until entering and saving a valid license. For more information, see [Updating Your License](#) on page 23.

5. If prompted, install IBM Aspera Connect.

You must have the latest version of Connect installed to transfer packages using Faspex. Faspex prompts you to install the Connect Browser if you do not have it installed or if your version is not the latest. If you install Connect, refresh your browser to start using Connect.

For more information, see [Faspex and Connect](#) on page 79.

Logging In with SAML

If SAML configurations are available, you can choose to log in with a configured SAML provider.

1. Open a supported browser and enter the Faspex hostname or IP address followed by **/aspera/faspex** in the browser URL. For example:

`http://faspex.asperasoft.com/aspera/faspex`

or

`http://198.51.100.24/aspera/faspex`

Note: For security reasons, Faspex versions 4.0.3 and later by default only allow login using the hostname that is configured in the `faspex.yml` configuration file (the hostname you designated during installation). If you try to log in to the application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, follow the instructions in [Configuring the Faspex Web Server](#) on page 32.

2. Log in with your credentials.

If SAML configurations are available, you can choose to log in with a configured SAML provider or with your Faspex user credentials.

If your administrator configured Faspex to use a default SAML configuration, Faspex automatically redirects you to the SAML login page. Login with your SAML credentials or login locally by bypassing the redirect.

If you need to login with your Faspex user credentials or if you need to log in using another SAML configuration, you can bypass the redirect by adding `login?local=true` to the end of the URL. For example:

<https://192.51.100.24/aspera/faspex/login?local=true>.

3. If prompted, install IBM Aspera Connect.

You must have the latest version of Connect installed to transfer packages using Faspex. Faspex prompts you to install the Connect Browser if you do not have it installed or if your version is not the latest. If you install Connect, refresh your browser to start using Connect.

For more information, see [Faspex and Connect](#) on page 79.

Requesting an Account

If you do not have an account and Faspex is configured to allow users to self-register, the login page displays the **Request an Account** link.

Note: If you do not see this link, contact your admin.

1. Click the **Request an Account** link to request access to Faspex.
2. After clicking on this link, complete the following form and click the **Request an account** button.

Note: Faspex can be configured to force external users to register a Faspex account to download packages sent to them. If you are requesting an account in order to download a package, your login and email are automatically set to the external address.

3. Once you receive your account confirmation email, enter your user credentials and click **Login**.
4. If prompted, install IBM Aspera Connect.

You must have the latest version of Connect installed to transfer packages using Faspex. Faspex prompts you to install the Connect Browser if you do not have it installed or if your version is not the latest. If you install Connect, refresh your browser to start using Connect.

For more information, see [Faspex and Connect](#) on page 79.

Configuring Faspex Settings

Configuring the Faspex Web Server

Go to **Server > Configuration > Web Server** to access the Web Server configuration page, which displays the IP address or domain name of the server and the HTTP/HTTPS ports that users connect to when accessing the application. These settings were initially configured when you first installed Faspex.

Server Information

Field	Description
Server's external address or name	The Faspex server's primary IP address or domain name. To change the address or name, run the following command: <pre>asctl apache:hostname host</pre>
HTTP port	The Faspex server's HTTP port number. To change the port, run the following command: <pre>asctl apache:http_port port</pre>
HTTPS port	The Faspex server's secure HTTP (HTTPS) port number. To change the port, run the following command: <pre>asctl apache:https_port port</pre>

Configuring the Faspex Domain Name

Create a domain name for Faspex to prevent email providers from flagging emails sent by Faspex as spam or junk.

If Faspex is configured to identify itself by IP address (rather than by domain name), then the URLs in your notification emails contain an IP address (for example, "https://10.0.0.1/aspera/faspex"). Some Web-based email services (such as Yahoo or Ymail, and Hotmail) have been known to automatically flag emails containing IP address links as "Spam," and move them to your Junk/Spam folder. If you do not have a domain name immediately available, then you can first configure Faspex with an IP address and then change it to use a domain name later.

If you know that you will not be setting up a domain name, make sure that users add your Faspex "From" email address (for example, admin@faspex.example.com) to their address book or contact list. Doing so typically "white-lists" the address so that emails from Faspex are not automatically flagged and routed the Junk/Spam folder.



CAUTION: Do not configure Faspex to use a domain name or hostname that contains underscore characters. Doing so could prevent you from logging into the server or cause other connectivity problems. Internet standards for domain names and hostnames do not support underscore characters.

Configuring Alternate Addresses for Faspex

If you have a group of external users who must log into Faspex through a different IP address or domain name, you can configure alternate IP addresses or domain name to use to authenticate to Faspex.

1. Select **Enable alternate address** > **Add alternate address** to add a new address.

Note:

Alternate addresses support comma-delimited Classless Inter-Domain Routing (CIDR), allowing you to specify multiple subnets or a specific range of addresses. For example:

198.51.100.24,192.168.0.0/18,10.0.0.*

2. Fill in the address name and the description to include in email notifications.
3. Choose whether this alternate address is available for email templates to use.
4. Click **Update** to finish.

You can include any configured alternate IP addresses with the **Show in emails option enabled** the `ALTERNATE_ADDRESS_#` email variable, where # is the number corresponding to the alternate address you want to include. For more information about customizing email notifications, see [Configuring Email Notification Templates](#) on page 138.

Configuring Transfer Options

Download During Transfers

Field	Description
Enable downloads during transfers	When enabled, users can download files from packages in an ongoing transfer. This feature is enabled by default. Note: If you are using IBM Aspera Validator to perform file validation, you must disable this feature.

Download Over HTTP

Field	Description
Enable HTTP fallback	Use HTTP for transfers when Connect is unavailable.

Initial Default Transfer Rate

Field	Description
Initial upload rate	Specify the target upload rate
Initial download rate	Specify the target download rate

Field	Description
Lock minimum rate and policy	Prevent clients from adjusting their transfer policy or minimum transfer rate

Server Information

Field	Description
Upload target rate cap	Specify the maximum upload rate
Download target rate cap	Specify the maximum download rate

Aspera Connect Settings

Field	Description
Minimum connect version	The minimum version of the IBM Aspera Connect that can be used to transfer with Faspex. The version must be in the form "X.Y.Z" (for example, 0.0.0.) Note: If you are serving Connect locally, you must remember to update the minimum Connect version for each new version of Faspex to ensure your end users use a version supported by the current version of Faspex.
Locally host Connect	Serve Connect using the local Connect SDK instead of the Aspera CDN. For more information, see Serving Connect Locally on page 88. Note: If you are serving Connect locally, you must remember to manually update the version of the hosted Connect SDK for each new version of Faspex to support the latest Faspex features.
Prefer http over extension	[Chrome only] Enforce the browser to use HTTP to communicate with Connect instead of using the browser extension.
Lock Connect SDK version	Prevent Faspex from updating the local Connect SDK if a new version becomes available. This setting persists across upgrades. Note: Faspex periodically checks for updates and does not immediately download a new version if this option is disabled.

Server-to-Server Relay Transfer Settings

Field	Description
Outgoing bandwidth	Set the outgoing bandwidth for relay transfers.

Setting Maximum Package Title Length

When Faspex saves a package, it names the package using the title of the package. By default, Faspex limits the package name to 200 characters to prevent problems caused by unnecessarily long package titles. You can change this limit by going to **Server > Configuration > Package Storage** and adjusting the **Maximum package title length in storage paths** option to limit the maximum number of characters Faspex uses to name package titles.

Configuring the Email Server

IBM Aspera Faspex uses a SMTP server to communicate various events with users.

1. Go to **Server > Notifications** and select **E-mail Configuration**.
2. Choose **open** or **login** authentication. If you choose **login** authentication, you are required to enter login credentials for the SMTP server.
3. Enter your **SMTP Mail Server** and its **Server Port**.
4. To enable TLS, select **Use TLS if available**.

Important: Faspex confirms whether the name in your TLS security certificate matches your mail server's configured address (fully qualified domain name or IP address). If it does not, Faspex displays an error. If your fully qualified domain name does not resolve with your internal DNS, you must add the IP address and name to your `/etc/hosts` file (or ensure the name resolves using DNS).

5. Enter the domain of the SMTP server.
6. If you chose **login** authentication, enter your login credentials.
 - **User:** The email account that you are sending the notification from (be sure to include the domain).
 - **Password:** The password for the email account.
7. Configure email details.
 - **Faspex "From" name:** The "From" name that appears on Faspex-generated emails.
 - **Faspex "From" email:** The "From" email address that appears on Faspex-generated emails.
 - **Packages received "From":** Choose from **Sender**, **Faspex**, and **Sender via Faspex**. Selecting **Sender** shows package notifications as received from the sender's name. Selecting **Faspex** shows package notifications received from "Faspex". Selecting **Sender via Faspex** shows package notifications as received from the sender's name "via Faspex".
8. Click **Save**.
9. Test your SMTP server settings. Enter your email address and click **Save and Send Test Email** to send a test email.

You should receive a confirmation email titled "Email settings test" with the message, "If you received this message, your email settings are configured correctly."

Enabling Post-Processing Scripts

Faspex admins have the ability to execute post-processing scripts on the server to accomplish tasks such as virus checking, moving files, and creating backups once packages arrive. Post-processing uses a set of filtering options to determine when to execute customized scripts. Aspera Faspex can execute shell scripts and Windows batch scripts, where information about the package is passed to the script by means of environment variables.

Post-processing scripts that have been activated execute automatically after the initial transfer to a default inbox. The relay of a package to a custom inbox does not trigger script execution.

In the event that a Faspex Administrative account is compromised, post-processing can be a serious threat to your server's security. Thus, Aspera strongly recommends that you update your administrative users' permissions in order to prevent unauthorized users from executing post-processing on Faspex by restricting the IP addresses from which a user can log into an admin account. For more information, see [Configure User Settings](#) on page 209.

Note: By default, post-processing is enabled. To disable it for security reasons, see the instructions at the end of this topic.

1. Prepare the post-processing script.

Generate your post-processing script and place it in a directory on the machine running your Faspex. Take note of, or copy, your script's full system path on the server. You can utilize the following environment variables in your

post-processing scripts, but be sure to use the proper format. For example, the variable **faspex_pkg_directory** will be available as **\$faspex_pkg_directory** in shell scripts, and **%faspex_pkg_directory%** in Windows batch files.

Variable	Description
faspex_pkg_directory	Storage directory of the package. See cautionary note below.
faspex_pkg_name	Package title.
faspex_pkg_note	Package note.
faspex_pkg_id	Package ID.
faspex_pkg_delivery_id	Package delivery ID for use with API endpoints that accept package delivery ID to interact with packages in the system.
faspex_recipient_list	Comma-separated list of recipients. (for example, "admin, johndoe")
faspex_recipient_count	Number of recipients. (for example, "3")
faspex_recipient_i	Name of the recipient. (# starts at "0", for example, faspex_recipient_0, faspex_recipient_1 ...).
faspex_sender_id	The sender's ID.
faspex_sender_name	The sender's full name.
faspex_sender_email	The sender's e-mail.
faspex_pkg_total_bytes	Size of the package in bytes.
faspex_pkg_total_files	Number of files in the package.
faspex_pkg_uuid	The package's UUID (36 characters).
faspex_metadata_fields	Comma separated list of the metadata fields defined for the package.
faspex_metadata_field	The value of the metadata field named <i>field</i> . In the field name, spaces are converted to underscores, non alphanumeric characters or underscores are stripped. For example, "my field" becomes "my_field"; "*my_group" becomes "mygroup".

Set up post-processing in the Faspex Web UI.

2. Go to **Server > Post-Processing** and click **Create New**.
3. Configure the script.

Script to run

Item	Description
Name	A descriptive name for this script.
Path to script on server	Enter the full path to the executable script that exists on the server. Important: The system user faspex should have the proper permissions to access and execute this file.
Active	Check to enable this script.

Execution criteria

All specified criteria must match the uploaded package's attributes for the script to be run on that package. All match fields in this section are optional. When **Exact match** is checked, the package attribute has to match the specified criterion exactly for the script to be run, the entered text will be matched anywhere in the field.

Item	Description
Package name	Execute when the package name matches the string.
Sender name	Execute when the sender name matches the string.
Sender email	Execute when the sender email matches the string.
Recipient name	Execute when the recipient name matches the string.
Recipient email	Execute when the recipient email matches the string.
Package note	Execute when the package note matches the string.
Package date	Execute when the package date falls into the determined range.
Package size	Execute when the package size falls into the determined range.
Package file count	Execute when the package file count falls into the determined range.

For security reasons, you may optionally disable post-processing in **faspex.yml**. The `DisablePostProcessing` setting can be found in the **faspex.yml** found at:

```
/opt/aspera/faspex/config/faspex.yml
```

Important: Aspera strongly recommends backing up **faspex.yml** before modifying.

Within **faspex.yml**, change `DisablePostProcessing: false` to `DisablePostProcessing: true`:

```
production:
  ...
  DisablePostProcessing: true
  ...
```

For more information on **faspex.yml**, see [faspex.yml Configurations Reference](#) on page 154.

Setting Up Bandwidth Measurement

You can enable bandwidth measurement to make all uploads perform a bandwidth measurement prior to transferring regardless of the target rate setting for the server or the transferring user (downloads are not affected).

1. Stop Faspex.

Execute the command to stop Faspex:

```
$ asctl faspex:stop
```

2. Open **faspex.yml** with a text editor.

Locate **faspex.yml** in the following location:

```
/opt/aspera/faspex/config/faspex.yml
```

Before editing **faspex.yml**, create a backup. Open it with a text editor:

3. Add the bandwidth measurement parameter in **faspex.yml**.

Before editing **faspex.yml**, create a backup. Open it with a text editor, and add this line at the end of the file:

```
...
MeasureBandwidthOnUpload: yes
```

4. Start Faspex.

Execute the command to start Faspex with the new setting:

```
$ asctl faspex:start
```

To verify bandwidth measurement, open IBM Aspera Connect and go to **Preferences > Bandwidth**, click **Remove All** and make sure **Automatically cache measurements obtained during transfer** is unchecked. Now log into Faspex and send a package. In the first few seconds of the transfer, Connect should show a status of *Measuring Bandwidth....*

Customizing New User Account Form

You can customize the New User Account form admins must fill out to create new accounts by marking certain fields required. For example, if you mark the option **Password expires** as required, that field becomes required when creating a user.

The following fields can be marked as required:

- Password expires
- Account expires
- Allowed IP addresses for login
- Allowed IP addresses for download
- Allowed IP addresses for upload

Important:

- Modifying `faspex.yml` is for advanced administrative users only.
- Be sure to back up `faspex.yml` before modifying.

1. Stop Faspex.

Execute the command to stop Faspex:

```
$ asctl faspex:stop
```

2. Open `faspex.yml` with a text editor.

Locate `faspex.yml` in the following location:

```
/opt/aspera/faspex/config/faspex.yml
```

Before editing `faspex.yml`, create a backup. Open it with a text editor:

3. Write the required-field parameters into your `faspex.yml` file.

Write the following parameters into the file. When a required field is specified, the option is checked and grayed-out; When a required field with default value is specified, a default value is presented in the option.

Parameter	Description
RequireUserPasswordExpires: yes	Make "Password expires" required. A value is required.
RequireUserAccountExpires: yes	Make "Account expires" required. A value is required.
RequireUserDescription: yes	Make "description" required.
RequireUserDescriptionWithDefault: "Default_value"	Make "description" required, and insert default value.
RequireUserAllowedIpAddressesForLogin: yes	Make "Allowed IP addresses for login" required.

Parameter	Description
RequireUserAllowedIpAddressesForLoginWithDefault: "Default_value"	Make "Allowed IP addresses for login" required, and insert default value.
RequireUserAllowedIpAddressesForDownload: yes	Make "Allowed IP addresses for download" required.
RequireUserAllowedIpAddressesForDownloadWithDefault: "Default_value"	Make "Allowed IP addresses for download" required, and insert default value.
RequireUserAllowedIpAddressesForUpload: yes	Make "Allowed IP addresses for upload" required.
RequireUserAllowedIpAddressesForUploadWithDefault: "Default_value"	Make "Allowed IP addresses for upload" required, and insert default value.

For example, to make "Account expires" required, and "Allowed IP addresses for download" required with default value "10.0.*", add the following lines in *Faspex.yml*:

```
...
RequireUserAccountExpires: yes
RequireUserAllowedIpAddressesForDownloadWithDefault: "10.0.*"
```

4. Start Faspex.

Execute the command to start Faspex with the new setting:

```
$ asctl faspex:start
```

To verify the modified fields are now required, log into Faspex with an admin account and go to **Accounts > New User**. Red asterisks appear near the fields that have been marked as required. Trying to create a user without specifying values for these field result in an error message to that effect.

Modifying HTTP Server Settings

You may configure the IBM Aspera Faspex Apache HTTP Server to use different host name, communication port, and namespace.

Important: For help on regenerating the self-signed SSL certificate (due to a host name change) that is installed with this Aspera Web application, see [Regenerating Self-Signed SSL Certificate \(Apache\)](#) on page 57. For instructions on creating and enabling a CA-signed certificate, see [Installing a Signed SSL Certificate Provided by Authorities](#) on page 55.

1. Update the hostname.

The hostname used by apache is configured when you first install Faspex. Use this command to print the current hostname:

```
$ asctl apache:hostname
```

To change the hostname, use the following command. Replace **HOSTNAME** with the new hostname:

```
$ asctl apache:hostname HOSTNAME
```

Also update your SSL certificate to reflect the new hostname:

```
$ asctl apache:make_ssl_cert HOSTNAME
```

2. Change HTTP and HTTPS ports.

By default, Faspex uses standard ports for HTTP (80) and HTTPS (443). Use the following commands to update these ports:

Item	Command
HTTP	<code>\$ asctl apache:http_port NEW_HTTP_PORT</code>
HTTPS	<code>\$ asctl apache:https_port NEW_HTTPS_PORT</code>

3. Change Faspex namespace.

Faspex uses the namespace */aspera/faspex* by default. Use this command to print the current namespace:

```
$ asctl faspex:uri_namespace
```

To set the namespace to, for example, */faspex*, use the following command:

```
$ asctl faspex:uri_namespace /faspex
```

When the namespace is updated, advise your users of the new URL. For example, if your faspex server's address is `https://198.51.100.24/aspera/faspex` and you change the namespace to */faspex*, they would use the following URL: `https://198.51.100.24/faspex`.

For a complete `asctl` command reference, see [asctl Command Reference](#) on page 199.

Changing the Default Language Used in Faspex

Change the default language used in Faspex. The default language is English.

1. Stop all Faspex services:

```
asctl:all stop
```

2. Change the `I18n.default_locale` option in `/opt/aspera/faspex/configinitializers/i18n_defaults`.

For example, to set the default language to Dutch:

```
# I18n.default_locale = "en"
I18n.default_locale = "nl"
```

3. Start all Faspex services:

```
asctl:all stop
```

Configuring HTTP and HTTPS Fallback

HTTP fallback serves as a secondary transfer method when the Internet connectivity required for Aspera FASP transfers (UDP port 33001, by default) is unavailable. When HTTP fallback is enabled and UDP connectivity is lost or cannot be established, the transfer will continue over the HTTP protocol. These instructions describe how to enable and configure HTTP/HTTPS fallback.

Prerequisites:

- To enable HTTP fallback for IBM Aspera Faspex, you must configure the feature in both Faspex and the associated transfer node that is running IBM Aspera High-Speed Transfer Server.

When Faspex and the HSTS are installed on the same machine, the Faspex installation process configures both automatically. When HSTS is remote, configure the transfer server and firewall ports in either of the following ways:

- Set HTTP/HTTPS to default ports (8080 + 8443) and open firewall ports on 8080/8443.
- Set HTTP/HTTPS to standard ports (80 + 443) and open firewall ports on 80/443.

Additionally, the transfer server fallback settings must match the Faspex fallback settings. If the settings don't match, Faspex returns a "Package creation failed" error. Ensure that transfer server has HTTP/HTTPS fallback enabled.

- Configure your HSTS web UI. For additional information on configuring different modes and testing, see the Aspera KB Article ["HTTP fallback configuration, testing and troubleshooting."](#)
- Your Aspera HTTP daemon () is running with sufficient privileges so that it can modify file ownership.

Limitations:

- Folders that are symbolic links cannot be downloaded directly by using HTTP fallback. Folders that are symbolic links are processed correctly when their parent folder is the source.
- HTTP fallback can only follow symbolic links. Settings in `aspera.conf` or in the command line are ignored.
- HTTP fallback attempts to transfer at the target rate but is limited by TCP.
- HTTP fallback does not support pre-post processing or inline validation.

Process:

1. Go to **Server > Configuration > Transfer Options** and select **Enable HTTP Fallback**.
2. Go to **Server > Configuration > Security** and select **Encrypt Transfers**.

Note: If HTTPS fallback is enabled on the transfer server, encrypted transfers must be enabled in Faspex.

3. Confirm your HTTP fallback port number.

To confirm your HTTP fallback port number, run the following `asctl` command:

```
asctl faspex:http_fallback_port
```

If you need to modify the Faspex HTTP port, add the `port_number` to the command:

```
asctl faspex:http_fallback_port port_number
```

Important: Do not use this command if Faspex and your transfer server are on the same machine. If you modify the HTTP fallback port, HTTP fallback fails because Apache is hard-coded to route traffic to `asperahttpd` on port 8080.

4. (In HSTS) Configure HTTP/HTTPS fallback settings.

You can configure HTTP/HTTPS fallback from the HSTS GUI or by editing `aspera.conf`.

Configuring HTTP/HTTPS fallback from the GUI:

Launch the transfer server and go to **Configuration > Global > HTTP Fallback**.

Review the following settings:

- In the **Enable HTTP** row, select **Override** and set to **true**.
- If you want to allow fallback over HTTPS, in the **Enable HTTPS** row, select **Override** and set to **true**.

Configuring HTTP/HTTPS fallback by editing `aspera.conf`:

Run the following commands:

- To view the current HTTP settings in `aspera.conf`:

```
$ asuserdata -b -t
```

Confirm the HTTP fallback settings in `aspera.conf` as shown in the example below. `enable_http` should be set to `true`, while the value shown for `http_port` should match what was displayed when you ran the command `asctl faspex:http_fallback_port` (default: 8080).

```
<CONF version="2">
...
<http_server>
...
  <enable_http>true</enable_http>      <!-- Enable HTTP -->
  ...
  <http_port>8080</http_port>          <!-- HTTP port -->
  ...
</http_server>
</CONF>
```

To manually inspect `aspera.conf`, open it from the following directory:

5. After enabling HTTP fallback and setting a token encryption key, restart `,` and `.`

Run the following command in a Terminal window to restart `asperacentral`:

```
# /etc/init.d/asperacentral restart
```

Run the following commands to restart `asperanoded`:

```
# /etc/init.d/asperanoded restart
```

Run the following commands to restart `asparahttpd`:

```
# /etc/init.d/asparahttpd restart
```

Setting the Minimum IBM Aspera Connect Version

Setting the minimum Connect version ensures your end users are using a version that supports the latest Faspex features. Users are prompted to upgrade their version of Connect if their version does not meet the minimum requirement.

Note: To use the file name obfuscation feature, your end users must be running Connect 3.9.8 or higher.

1. Go to **Server > Transfer Options**.
2. In the **Aspera Connect Settings** section, change the minimum Connect version.

Configuring On-Demand Entitlement

Manually install Faspex for use in Aspera on Demand need to use an On Demand entitlement.

Aspera highly recommends using pre-configured images available in Aspera-supported cloud providers for greater reliability and for ease of configuration. These instructions are for customers who are manually installing Faspex for use in Aspera on Demand need to use an On Demand entitlement.

Faspex entitlement requires that you have IBM Aspera High-Speed Transfer Server installed on the same server as Faspex. Faspex uses the `asperanoded` service's license API for entitlement.

Note: Faspex uses the `asctl` command to configure entitlement. You must run `asctl` as the `root` user.

Turn On Entitlement

```
export RAILS_ENV=production
```

```
asctl faspex:rake entitlement:turn_safe_net_entitlement_mode_on
```

Turn Off Entitlement

```
export RAILS_ENV=production
asctl faspex:rake entitlement:turn_safe_net_entitlement_mode_off
```

Register Entitlement Key

```
export RAILS_ENV=production
asctl faspex:rake --trace entitlement:config_license_server
EL_KEY="entitlement_key" EL_CUSTOMER_ID="id"
```

For example:

```
asctl faspex:rake --trace entitlement:config_license_server
EL_KEY="cd0904ae-f85a-4e3b-8ae0-615d79e5deal" EL_CUSTOMER_ID="Test "
```

Note:

- 1) You must turn on entitlement before you can register the key.
- 2) The `--trace` option is not required, but it is helpful for debugging issues.

Working with Sender Quotas

Sender Quota Overview

Sender quotas allow Faspex admins to control the maximum volume of data that specific Faspex users can send to specific recipients over a rolling period, based on settings at the global and user account levels.

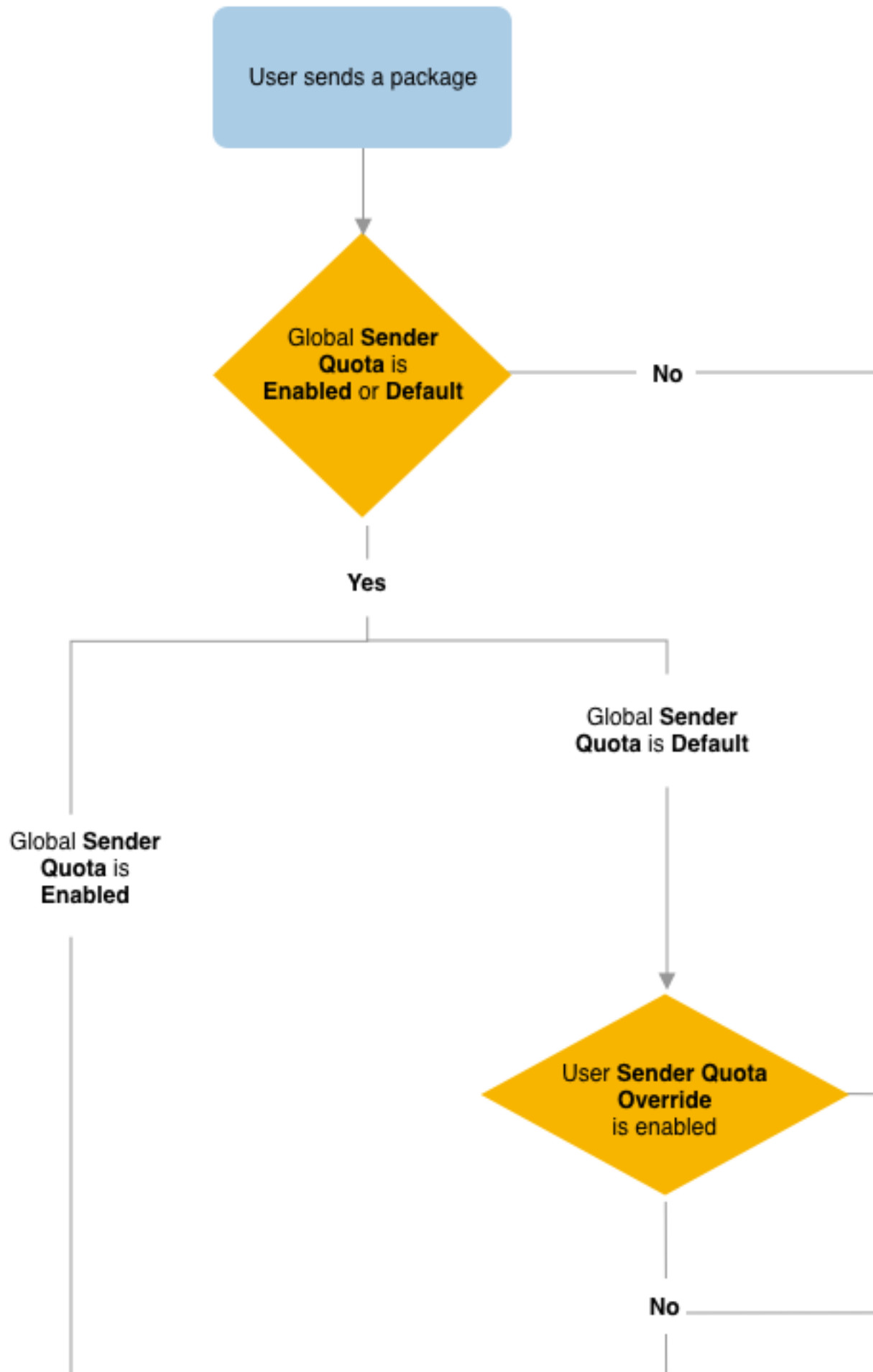
For example, admins can prevent all Faspex users from individually sending more than 25 GB over a twenty-four hour period, while allowing some of those users to send an unlimited amount of data.

Sender quotas can be applied based on who is sending, who is receiving, or both.

Senders and recipients can be exempted from sender quota enforcement based on their email address domain name.

Sender Quota Verification Logic

Faspex uses this logic to determine whether to verify sender quotas for a package being sent:



Data Allowed for a New Package When Enforcing Sender Quota

If the sender quota is being verified for a package, then the maximum number of bytes (in MB) allowed for the package is defined by the global sender quota configuration and possibly the sender's sender quota configuration:

Global and Current Account Sender Quota Configurations	Package Maximum Size
Global sender quota = Enabled	Global default sender quota minus bytes already sent by that user to non-whitelisted recipients within the current rolling period
Global sender quota = Default Sender's Sender Quota Override is selected and the Sender Quota value has a value greater than 0 MB	User account sender quota minus bytes already sent by that user to non-whitelisted recipients within the current rolling period
Global sender quota = Default Sender's Sender Quota Override is selected and the Sender Quota value has a value of 0 MB	0 MB (no package can be sent)
Global sender quota = Default Sender's Sender Quota Override is selected and the Sender Quota value is empty	Unlimited (normally based on file storage)

Note: Faspex takes into account all user data sent within the current period (duration configured by **Sender quota duration**), even if sender quotas were not yet enabled. For example, a user sends 100 MB of data in the current period. An admin then enables sender quotas with a maximum of 4000 MB. The user has 3900 MB available in the current period.

Over-Quota Warnings and Enforcement

When users start the process of sending a new package, Faspex warns users as soon as possible that the package might go over quota:

- If the user is over quota, Faspex notifies the user when they attempt to create a new package that they cannot send more data until the end of the current rolling period.

Note:

Faspex cannot determine the size of the package before its files are uploaded. Instead, Faspex relies on the HST Server node to pre-calculate the package size. Faspex uses that information to determine if senders will reach or exceed their sender quotas. The node must have the `pre_calculate_job_size` enabled (set to `yes` or `any`) for Faspex to use this information.

If the option is disabled (set to `no`), Faspex determines the size of the package as the transfer goes and stops the transfer when it determines the sender has reached or exceeded the sender quota. In the worst-case scenario, Faspex might not stop a transfer until most of the package is transferred.

Therefore, IBM Aspera recommends enabling the `pre_calculate_job_size` setting on the HST Server node (by default, set to `any`).

- If the user is still under quota, Faspex allows the user to initiate a transfer. When the package size reaches or exceeds the sender quota, Faspex notifies the user that the user went over quota. Faspex then cancels the transfer and deletes the package.

Note:

During a transfer, Faspex checks a sender's available quota every 5 seconds. The polling frequency can allow some packages to go beyond the quota limit if Faspex does not check the in-transfer package at least once. For example, a user creates a new package while under quota and the transfer completes in under 5 seconds due to a

small, package size and a high, transfer speed. Nevertheless, that package size is accounted for in the user's sender quota for any, future quota verification.

Sender Quota Exceptions

Admins can exempt individual accounts from sender quota enforcement by overriding the account sender quota and leaving the sender quota value empty. That requires the global sender quota setting to be set as **Default**.

Admins can also choose to whitelist email domains to exempt senders or recipients from sender quota enforcement based on their email addresses.

Note:

If users change their email address, that can impact their inclusion in sender or recipient whitelists, and therefore also impact sender quota enforcement.

This can be prevented by disabling the **Allow users to change their email address** setting (**Server > Configuration > Security > Allow users to change their email address**).

Configuring Sender Global Quotas

Enable sender quotas globally to limit the amount of data users can send in a specified rolling period.

1. Go to **Faspex > Configuration > Security** and go to the Sender Quota section.
2. Set the **Sender quota option** option to **Enabled** or **Default**.

Option	Sender Enforcement
Enabled	Faspex enforces the default sender quota for all non-whitelisted user accounts in Faspex, regardless of the override option set at the user level.
Default	Faspex enforces the default sender quota for all non-whitelisted user accounts in Faspex, unless an admin sets a specific sender quota for the account. Instead, the specific sender quota is enforced.
Disabled	Faspex does not enforce sender quotas for any user accounts in Faspex, even if an admin had set a specific sender quota for the account.

3. Set the **Sender quota duration** in hours. Faspex resets a user account's sent bytes (in MB) after the specified duration. The value must be a positive number between 1 – 9999 hours.
4. Set the **Sender quota limit** to a value in megabytes (MB). The value must be a positive number.

If the limit set to 0, users cannot send packages.

The default is 4000 MB.

If the **Sender quota option** is set to **Default**, admins can configure sender quotas for specific account. For more information, see [Configuring Sender Quota for a User Account](#) on page 47.

5. Define a list of **Approved recipient domains** to whitelist. Sender quotas are not enforced when sending to recipients with email addresses in these domains.

For example: "@aspera.com; @ibm.com".

Note: Whitelists do not support individual email addresses. You can whitelist only domain names.

6. Define a list of **Approved sender domains** to whitelist. Sender quota are not enforced for users with email addresses in these domains.

For example: "@aspera.com; @ibm.com".

Note: Whitelists do not support individual email addresses. You can whitelist only domain names.

7. Click **Update**.

Configuring Sender Quota for a User Account

Admins can override sender quotas for specific account if the global sender quota setting is set to **Default**.

1. Go to **Accounts** > *user_account*.
2. Select **Override security sender quota**.
3. Set the **Sender quota limit** to a value in megabytes (MB).

To exempt the user from sender quota enforcement, do not set a value.

To prevent a user from sending packages, set the value to 0 MB.

4. Click **Update User**.

Securing Faspex

Firewall Settings

An Aspera server runs one SSH server on a configurable TCP port (22 by default).

Your firewall should be configured as follows:

- To ensure that your server is secure, Aspera strongly recommends allowing inbound connections for SSH on TCP/33001 (or on another non-default, configurable TCP port), and disallowing inbound connections on TCP/22. If you have a legacy customer base utilizing TCP/22, then you can allow inbound connections on both ports.

Open your SSH configuration file in a text editor. The configuration file is located in the following directory: `/etc/ssh/sshd_config`.

Add the line `Port 33001` to the configuration file to enable access to port 33001. If you are also using port 22 for shell access to the server you also need to add or uncomment the line `Port 22` in the config file.

Restart the SSH server to apply your new settings:

```
# service sshd restart
```

- Allow inbound connections for FASP transfers, which use UDP/33001 by default, although the server may also choose to run FASP transfers on another port.
- If you have a local firewall on your server (such as `iptables`), verify that it is not blocking your SSH and FASP transfer ports (TCP/UDP 33001).
- For the Faspex application, allow inbound connections for HTTP and/or HTTPS Web access (TCP/80, TCP/443).

The firewall on the server side must allow the open TCP port to reach the Aspera server. No servers listen on UDP ports. When a transfer is initiated by an Aspera client, the client opens an SSH session to the SSH server on the designated TCP port and negotiates the UDP port for the data transfer.

Configuring Security Settings


Modify security settings for Faspex user accounts, self-registration, external senders and encryption. Go to **Server** > **Configuration** > **Security** to view or modify your server's security settings for Faspex user accounts, self-registration, external senders, and encryption.

Faspex Accounts

Configuration Option	Description
Session timeout	Sessions time out after the specified number of minutes of inactivity.
Lock users	<p>Lock a user account based on the number of failed login in attempts in a given number of minutes, or based on account inactivity.</p> <p>By default, Faspex locks an account after the user fails to login five times in a row within five minutes. The maximum failed login attempts and the rolling period for failed attempts must be positive numbers between 0 and 99.</p> <p>You can also select After number days of inactivity to lock accounts based on inactivity.</p> <p>An administrators must reactivate a locked account before the user can use the account again. For more information, see Reactivating an Inactive Account on page 73.</p>
Remove users	Remove users after the specified number of days of inactivity. Local, directory service, and SAML users can be configured separately.
Prevent concurrent login	If enabled, users can only be logged in from one client at a time.
Passwords expire	<p>When activating global password expiration, all users with default password policies are updated with a password expiration date specified by the password expiration interval. Admins can override this global policy in a user's account settings. See Configure User Settings on page 209.</p> <p>Note: When changing password expiration interval, changes to password expiration date do not occur until next password change for each user if password expiration is already active.</p>
Prevent password reuse	Prevent users from reusing passwords. Enter the number of previous passwords users cannot reuse.
Use strong passwords	<p>If enabled, requires newly created passwords to contain at least one letter, one number and one symbol. Existing passwords remain valid.</p> <p>You can change the strong password criteria by editing the <i>faspex.yml</i> file, which is located in the following directory: <code>/opt/aspera/faspex/configfaspex.yml</code>. For more information on faspex.yml, see faspex.yml Configurations Reference on page 154</p>
Require new users to change password on first login	New users must enter a new password when they first log in.
Allow locked out users to unlock themselves	Locked out users can select the Forgot my password button to have a password reset email sent to them. Using the link, they can reset their email and log in.
Keep user directory private	<p>When set to Yes, prevents a Faspex user (even if they have permissions to send to all Faspex users) from being able to see the entire user directory. You can override this setting on a user-by-user basis by editing their permissions.</p> <p>Important: When the privacy setting is turned on (set to Yes), users who have been assigned the role of Workgroup Admin can still view the entire list of Faspexusers via the Workgroup Members page.</p>
Allow users to create normal packages	If this feature is disabled, users cannot access the New Packages site and can only create dropbox packages (only if they are a member of a dropbox). This option can

Configuration Option	Description
	also be set for individual users by going to Accounts > Users , clicking the username, and selecting an option for Can create normal packages .
Users can see global distribution lists by default	Select to give all users access to the global distribution lists. If this option is disabled, admins must configure a user's settings to grant access to global distribution lists.
Ignore invalid recipients	Prevent a package from failing to send even when addressed to invalid recipients. Faspex skips any invalid user and delivers the package to all valid recipients in the list.
Allow users to change their email address	Enable users to change their own email addresses in their account preferences (see Updating Email and Connect Settings on page 75). If this feature is disabled, only admins can change a user's email address.
Send welcome email to all new users	Faspex sends a welcome email to all users. The welcome email includes a link to download Aspera products, a password reset link, and a link to login to Faspex. Note: The password reset link expires after one week.

Registrations

Configuration Option	Description
Self-registration	<p>Choose whether non-users can create or request user accounts.</p> <ul style="list-style-type: none"> • None: Non-users are not allowed to create or request user accounts. • Moderated: An admin must approve the account before it is created. • Unmoderated: Once a user registers, his or her account is automatically created. <p>If you allow self-registration, Aspera recommends the moderated setting for security.</p> <p> Warning: If self-registration is enabled, then it could be utilized to find out whether a certain account exists on the server. That is, if you attempt to self-register a duplicate account, you receive a prompt stating that the user already exists.</p> <p>After a user self-registers (either moderated or unmoderated), his or her account inherits the permissions of the configured template user and automatically becomes a member of designated workgroups. To configure the template user, go to Accounts > Pending Registrations and select the user. To set the workgroups that newly created users join, click the workgroups link. Although self-registered users are, by default, not allowed to send packages to other self-registered users, you can modify this setting by selecting Self-registered users can send to one another.</p> <p>Important: To prevent a self-registered account from having the same email address as a full Faspex user, Admins can add a special option to faspex.yml. You can find faspex.yml in the following directory:</p> <pre>/opt/aspera/faspex/config/faspex.yml</pre> <p>Inside faspex.yml, within the "Production:" section, paste the following option and set it to "true":</p> <pre>EnforceSelfRegisteredUserEmailUniqueness: true</pre>
Terms of service	Enter a statement that users are required to accept in order to self register an account. If you do not enter a statement, users are not required to accept terms of service to create an account.

Configuration Option	Description
Notify the following emails to approve	<p>This field appears when you choose the Moderated registration policy. Enter one or more email addresses to notify for moderation.</p> <p>Note: These email addresses are not validated against existing Faspex admins or managers.</p>
Require external users to register	<p>Force external users to register a Faspex account to download packages sent to them. External users register with the same process as self-registered users. For more information about requesting accounts, see Requesting an Account on page 31.</p> <p>Note: You must first allow users to send packages to external email addresses by selecting the Allow sending to external email addresses. For more information, see the description for the option below.</p> <p>Important: You cannot</p> <p>if you using external flag in Faspex, please do not use "require the external user to register" option. Only one option permitted at the time.</p>
Use default registration policy for external users	<p>Use the same registration policy you chose for self registration for external users registering accounts.</p> <p>Note: This option appears when you selected Require external users to register. You must choose a registration policy for self registration to select this option.</p>
Registration policy for external users	<p>If you do not use the default registration policy, choose either Moderated or Unmoderated.</p> <ul style="list-style-type: none"> • Moderated: An admin must approve the account before it is created. • Unmoderated: Once a user registers, his or her account is automatically created.
Terms of service for external users	<p>Enter a statement that external users are required to accept in order to create an account. If you do not enter a statement, users are not required to accept terms of service to create an account.</p>
Notify the following emails to approve external users	<p>This field appears when you choose the Moderated registration policy. Enter one or more email addresses to notify for moderation.</p> <p>Note: These email addresses are not validated against existing Faspex admins or managers.</p>
Self-registered users can send to one another	<p>Select to allow self-registered users to send packages to other self-registered users.</p> <p>Note: Self-registered users must have permission to send to all Faspex users. If a self-registered user does not have permission to send to all Faspex users, the Self-registered users can send to one another option has no effect. For more information giving a user permission to send to all Faspex users, see Configure User Settings on page 209.</p>

Important: If users are allowed to self-register, they see the **Request an account** link on the login page. After a user clicks this link and completes the form, admins are prompted under **Accounts > Pending Registrations > Actions** to **Approve** or **Deny** the account.

Outside email addresses

Configuration Option	Description
Allow inviting external senders	<p>When Allow inviting external senders is selected, external senders (those who do not have Faspex accounts) can be invited to send a package to a user. For more</p>

Configuration Option	Description
	<p>information on external senders, see Allowing Users to Send to External Email Addresses on page 90.</p> <p>Important: An admin can enable or disable this feature for specific users while still retaining the server-wide setting of enabled or disabled. Go to Accounts and select the user to enable or disable this feature. For more information on this setting, see Configure User Settings on page 209.</p>
Invitation link expires	<p>Select to set a global policy for invitation link expiration times for personal and dropbox invitations. You can set a time in days, expire the link after one successful upload, allow users to set a custom link expiration policy, or a combination. For example, you can select both a time in days and allow users to set a custom policy. If the default policy is to expire links after 5 days, then users can set links to expire after less than 5 days but not longer than 5 days.</p> <p>Clear this option to never let invitation links expire.</p>
Allow public URL	<p>Allow a user to send a Public URL to users without Faspex accounts. These external users can submit packages to registered Faspex users through this public URL. For more information about Public URLs, see Configuring Public URLs on page 91.</p> <p>Select Allow public submission URLs to globally enable the feature and allow admins to configure this feature on a user-by-user basis. Set the server default to Allow or Deny.</p> <p>Tip: An admin can enable or disable this feature for specific users while still retaining the server setting.</p>
Allow sending to external email addresses	<p>Select Allow sending to external email addresses to enable all Faspex users to send packages to external email addresses.</p> <p>This feature is enabled by default. Select Allow sending to external email addresses to globally enable the feature and allow admins to configure this feature on a user-by-user basis. Set the server default to Allow or Deny.</p> <p>Tip: An admin can enable or disable this feature for specific users while still retaining the server setting.</p>
Package link expires	<p>This field appears when you select Allow sending to external email addresses.</p> <p>When enabled, the package link expire after the specified number of days.</p>
Expire after full package download	<p>This field appears when you select Allow sending to external email addresses.</p> <p>If this checkbox is enabled, the package link expires after one download. This is also applicable when the link is forwarded. After the first download, the files must be re-sent in a new package through Faspex for the recipient to be able to download them again.</p>

Encryption

Configuration Options	Description
Encrypt transfers	Select to encrypt all transfers with the AES-128 encryption method. HTTP fallback transfers are also encrypted.
Use encryption-at-rest	Encryption-at-Rest (EAR) requires users, on upload, to enter a password to encrypt the files on the server.

Configuration Options	Description
	<p>Package recipients are required to enter the encryption password to decrypt protected files as they are being downloaded. If a user chooses to keep downloaded files encrypted, they are not required to enter a password until they attempt to decrypt the files locally. Encryption-at-Rest is supported by the IBM Aspera Connect</p> <ul style="list-style-type: none"> • Always: Always use EAR. Users must enter an encryption password when sending a password. • Never: Do not use EAR. This is the default setting. • Optional: Users may choose to encrypt when uploading a package. <p>Note: This EAR setting only applies to transfers initiated through Faspex. Transfers initiated using <code>ascp</code> from the command line or the High Speed Transfer Server GUI are handled by the configured <code>aspera.conf</code> file. Transfers initiated by High Speed Transfer Server version 3.7.4 and above are encrypted with AES-128 by default. For more information on encrypting <code>ascp</code> transfers, see the <i>IBM Aspera High-Speed Transfer Server Admin Guide</i>.</p>
Allow dropboxes to have their own encryption settings	Select to allow admins to adjust Encryption-at-Rest settings for each dropbox. For more information on creating and configuring dropboxes, see Creating a Dropbox on page 99.

Important: You must click the **Update** button to apply and save your changes.

Securing Incoming and Outgoing Transfers

This section describes how to configure IBM Aspera Faspex to deny all transfers except for ones initiated by or sent to permitted users. This is accomplished by updating the global authorization settings for your installation of IBM Aspera High-Speed Transfer Server (HSTS).

1. Modify **Incoming Transfers** and **Outgoing Transfers** settings within the **aspera.conf** file, which is located at: `/opt/aspera/etc/aspera.conf`

```
<default>
...
<authorization>
<transfer>
<in>
<value>deny</value>          <!-- Incoming Transfer -->
</in>
<out>
<value>deny</value>          <!-- Outgoing Transfer -->
</out>
</transfer>
...
</authorization>
...
</default>
```

You can then set transfer permissions on an individual user basis using their sections in the **aspera.conf** file.

2. (Complete this step if your system is a dedicated FaspexServer and is not performing transfers with IBM Aspera High-Speed Transfer Server or HSTS) Only allow user "faspex" within HSTS

You can verify the *faspex* user and corresponding settings within the `aspera.conf` file, which is located at `/opt/aspera/etc/aspera.conf`.

```

        <aaa>
        <realms>
        <realm>
        <users>
        <user>
        <name>faspex</name>
        <authorization>
        <transfer>
        <in>
        <value>token</value>
        </in>
        <out>
        <value>token</value>
        </out>
        </transfer>
        <token>
        <encryption_key>CRYPTOGRAPHIC_STRONG_RANDOM_STRING</
encryption_key>
        </token>
        <authorization>
        <file_system>
        <access>
        <paths>
        <path>
        <absolute>E:\faspex_packages</absolute>
        <read_allowed>>false</read_allowed>
        <dir_allowed>>false</dir_allowed>
        <write_allowed>>false</write_allowed>
        </path>
        </paths>
        </access>
        </file_system>
        </user>
        </realm>
        </realms>
        </aaa>

```

Verify Private and Public Key Authentication for SSH Server

This topic describes the process for **disabling** *password authentication* in the `sshd_config` file and **enabling** *private/public key authentication* to ensure that private and public key authentication is enabled for your SSH server.

1. Open your SSH server configuration file in a text editor.

The configuration file is located in the following directory:

```
# /etc/ssh/sshd_config
```

2. Ensure that `PubkeyAuthentication yes` has been added or uncommented, and that `PasswordAuthentication yes` has been commented out with a `#`.

The section should look like the following:

```
...
PubkeyAuthentication yes
```

```
#PasswordAuthentication yes
PasswordAuthentication no
...
```

3. You must restart or reload the SSH server to apply your new settings. Restarting or reloading your SSH server does not impact currently connected users.

To restart or reload your SSH server, use the following commands:

OS Version	Instructions
RedHat (restart)	<pre>\$ sudo service sshd restart</pre>
RedHat (reload)	<pre>\$ sudo service sshd reload</pre>
Debian (restart)	<pre>\$ sudo /etc/init.d/ssh restart</pre>
Debian (reload)	<pre>\$ sudo /etc/init.d/ssh reload</pre>

Private and public key authentication should now be enabled for your SSH server.

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 reboot, SELinux is permanently disabled. To dynamically disable it before the reboot, run the following command:

```
# setenforce 0
```

Securing Admin Login Attempts from Unknown IP Addresses

IBM Aspera Faspex admins have the ability to execute post-processing scripts on the server. In the event that an admin account is compromised, this capability can be a serious threat to your server's security. As such, Aspera strongly recommends that you update your admin user permissions in order to prevent unauthorized users from executing post-processing scripts on Faspex. You can disallow login attempts to Faspex admin accounts from unknown IP addresses.

1. Go to **Accounts** and select the admin account.
2. Scroll down to the **Permissions** section and enter the IP address or address range to allow in the **Allowed IP addresses for login** field.

3. Click **Save**.

Enabling Terms of Service Agreement

You can require that users agree to a Terms of Service prior to sending packages. When this option is enabled, users must select the checkbox next to a customizable Terms of Service text field before clicking **Send**. Otherwise, sending the package fails.

1. On the Faspex Server admin page, go to **Server > Configuration > Security > Faspex Accounts**.
2. Enter text for the Terms of Service agreement.
By entering text in the **Terms of service for sending** text box, the feature is automatically enabled. Users must accept the statement in order to send a package.
3. Click **Update** to apply your changes.

Installing a Signed SSL Certificate Provided by Authorities

In a default IBM Aspera Faspex installation, Apache generates and uses a self-signed SSL certificate. Install a signed certificate provided by authorities to secure your server.

1. Generate your Private Key (.key) and Certificate Signing Request (CSR) (.csr):
 - a) Run the following openssl command, where *key_name* is the name of the unique key that you are creating and *csr_name* is the name of your CSR:

```
$ openssl req -new -nodes -newkey rsa:2048 -keyout key_name.key -
out csr_name.csr
```

- b) Configure the certificate's X.509 attributes.

Important: The Common Name field must be filled in with the fully qualified domain name of the server to be protected by SSL. If you are generating a certificate for an organization *outside of the US*, see <https://www.iso.org/obp/ui/#search/code/> for a list of 2-letter, ISO country codes.

For example:

```
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'my_key_name.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]: US
State or Province Name (full name) [Some-State]: CA
Locality Name (eg, city) []: Emeryville
Organization Name (eg, company) [Internet Widgits Pty Ltd]: IBM Aspera
Organizational Unit Name (eg, section) []: ASP
Common Name (i.e., your server's hostname) []: faspex.asperasoft.com
Email Address []: faspex@asperasoft.com
```

- c) When prompted, you can enter extra attributes, including an optional challenge password.

Manually entering a challenge password when starting the server can be problematic in some situations (for example, when starting the server from system boot scripts). You can skip entering values for any extra attribute by hitting the Enter button.

```
...
Enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

After finalizing the attributes, the private key and CSR are saved to your root directory.

Important:

- If you make a mistake when running the OpenSSL command, discard the generated files and run the command again.
- After successfully generating your key and Certificate Signing Request, secure your private key, as it cannot be re-generated.

2. Send CSR to your signing authority.

You now need to send your newly generated, unsigned CSR to a Certifying Authority (CA). Once the CSR has been signed, you have a real certificate. Follow the key provider's instructions to generate and submit both your private key and the Certificate Signing Request (CSR) to acquire the certificate.

Important: Some Certificate Authorities provide a Certificate Signing Request generation tool on their Website. Check with your CA for additional information.

3. If your CA returns the SSL certificates to you in PFX (.pfx) format, use the `openssl` command convert the certificates to PEM (.pem) format:

```
openssl pkcs12 -in path/to/pfx_cert_name.pfx -nocerts -out path/to/
key_name.key -nodes
openssl pkcs12 -in path/to/pfx_cert_name.pfx -nokeys -out path/to/
cert_name.crt -nodes
```

4. Store your certificates on your server.

For example:

- `my_server.crt`
- `my_server.key`

Your certificate provider may require you to also install an Intermediate CA Certificate file. Copy the file to `apacheconfserver-ca.crt`

5. Install the SSL certificate with the following command:

```
asctl
apache:install_ssl_cert cert_file_path key_file_path [chain_file_path]
```

For example:

```
asctl
apache:install_ssl_cert my_server.crt my_server.key apacheconfserver-
ca.crt
```

You can find the installed certificate and key at the following locations:

- `apacheconfserver.crt`
- `apacheconfserver.key`

Generating and Installing a New Self-Signed SSL Certificate

Generate a self-signed certificate if you don't plan on sending your certificate to be signed by a Certified Authority (CA), or if you want to test your SSL implementation while waiting for the CA to sign your certificate.

A self-signed certificate is a temporary certificate that is valid for 365 days. Self-signed certificates are not meant to be used in your production environment. Users accessing your server are warned by their browser warn them that your server is not secure.

By default, IBM Aspera Faspex uses a generated, self-signed certificate as a placeholder until you can install a certificate signed by authorities.

You can find the installed certificates at:

- confserver.crt
- confserver.key

Generate a self-signed certificate using `openssl` command, where *key_name* is the name of the unique key that you are creating and *cert_name* is the name of your certificate file:

```
openssl x509 req -days 365 -in csr_name.csr -signkey key_name.key -
out cert_name.crt
```

Regenerating Self-Signed SSL Certificate (Apache)

When you initially set up Faspex on your system a pregenerated, self-signed SSL certificate is also installed. If you have changed your Apache hostname, regenerate the self-signed certificate by following the instructions below.

1. Open a terminal window and run the `asctl` command.

In a terminal window, run the following command to generate a new, self-signed SSL certificate for your installation of Faspex (where you will replace the **HOSTNAME** with your Apache server's IP address or host name):

```
$ asctl apache:make_ssl_cert HOSTNAME
```

Answer **yes** when prompted to overwrite the existing certificate.

2. Confirm that your certificates are updated.

Check the following location to confirm your self-signed SSL certificates have been updated:

- /opt/aspera/common/apache/conf/server.crt
- /opt/aspera/common/apache/conf/server.key

File Encryption Options

Use Faspex and IBM Aspera High-Speed Transfer Server together to encrypt files before they are transferred, encrypt files at the destination, and encrypt data transferred over the network.

Encryption Options

Option	Description	Use Case	Instructions
Client-Side Encryption-at-Rest (CSEAR)	CSEAR provides end-to-end encryption on uploaded packages. When enabled, Faspex requires	Give the sender complete control over who has access to the data.	Enable CSEAR by going to Server > Configuration > Security and set Use

Option	Description	Use Case	Instructions
	<p>users to set an encryption password when uploading packages using IBM Aspera Connect. Connect encrypts the files with that password and transfers the packages to Faspex.</p> <p>Encrypted files are given the <code>.aspera-env</code> extension. When a package recipient downloads these <code>.aspera-env</code> files, they must use the password to decrypt the files and access their contents.</p> <p>The sender must give the recipient the password.</p>		<p>encryption-at-rest to Always.</p> <p>Note: Do not use CSEAR if you are validating files with IBM Aspera Validator.</p>
Server-Side Encryption-at-Rest (SSEAR)	<p>SSEAR is not a Faspex feature, but an HSTS.</p> <p>When a user sends a package, the HSTS encrypts the transferred files at the destination using a password defined in the <code>aspera.conf</code> configuration file.</p>	Protect data on untrusted storage (for example, cloud storage connected to HSTS).	To enable SSEAR, see <i>IBM Aspera High-Speed Transfer Server Admin Guide: Server-Side Encryption-at-rest (EAR)</i> .
Encryption-in-Transit	Encrypt transfers using the AES-128 encryption standard.	Protect data transfer through an untrusted or insecure network.	Enable encryption-in-transit by going to Server > Configuration > Security and select Encrypt transfer .

Obfuscating File Names in Packages

For security reasons, you may want to obfuscate the names of files in your packages. The original file names are not visible in Faspex or in logs.

Faspex performs obfuscation when:

- A user initiates a transfer through Connect.
- A user initiates a transfer through the HTTP Gateway.
- A user initiates a transfer from a remote source (file storage on tethered nodes).

If enabled, Faspex obfuscates the file names of all uploaded files. In the case of a directory file structure, Faspex also obfuscates the folder name, the names of all files within the folder, and the names and files of any nested directories.

Faspex does not obfuscate the file extensions of files. For example, after obfuscation, a file with the `.txt` extension may be named `Nqu7ORqTEC2R9GHK8ISFw.txt`.

Note:

- File name obfuscation when transferring through Connect requires Connect version 3.9.8 or higher. Set the minimum Connect version in Faspex to 3.9.8 (**Server > Configuration > Transfer Options**) if you enable file name obfuscation. Faspex does not obfuscate file names if transferring with an older version of Connect.
- File name obfuscation in Faspex is irreversible.

Configure Global File Name Obfuscation

Go to **Server > Security**. In the Obfuscation section, you can set the global option to:

- **Always**
- **Never**
- **Optional**

If set to **Optional**, users can choose whether to obfuscate file names at package creation time.

Adding Nodes and File Storage to Faspex

Adding a Node to Faspex

You can add multiple nodes to Faspex from the File Storage page (**Server > File Storage**). The File Storage page lists tethered nodes and file storage. File storages are directories made available to use as inboxes (locations where Faspex packages can be received and stored) or as the source from which users can choose files to include in a package.


On a fresh install, the node you configured during Faspex installation is the only tethered node, and its default storage directory, `packages`, is the default inbox destination.

Nodes do not have to run on the same server as the Faspex server. You can tether a remote node to Faspex. All nodes must be configured to interact with Faspex before they can be added to Faspex:

- **Windows:** [Setting Up a Windows Node](#) on page 63
- **Linux:** [Setting Up a Linux Node](#) on page 60
- **OS X:** [Setting Up an OS X Node](#) on page 65

To add a configured node to Faspex:

1. Go to **Server > File Storage**.
2. Click **Add New Node**.
3. Enter a unique name to identify the node.
4. To encrypt the connection to the node using SSL, enable the **Use SSL** checkbox.
5. To verify the SSL certificate, enable the **Verify SSL Certificate** checkbox.
6. Configure the following file storage details:

Field	Description
Host	The node's hostname or IP address.  CAUTION: To avoid connectivity problems, do not specify a hostname that contains underscores.
Port	The Node API port number. By default, the port is 9092.
Username	The Node API username on the node machine.
Password	The Node API password on the node machine.

7. Choose the storage type for the node.

If you are connecting to a node using Windows Azure or Windows Azure SAS storage, specify which storage you are using. Otherwise, choose **Default**.

8. Test the node connection by selecting **Test Connection**.

If the connection is successful, Faspex displays: "Connection succeeded!" Otherwise, Faspex displays an error. For more information about troubleshooting the connection, see [Troubleshooting File Storage Errors](#) on page 162.

9. If you want to designate a primary transfer address or configure a secondary IP address to allow users to start transfers from different IP addresses, expand the **Advanced Configuration** section and see [Configuring File Storage](#) on page 68 for more details.

10. Create the node.

- Select **Create** to simply create your node.
- Select **Create and Add File Storage** to create your node and proceed to add file storage to your node. For more information on file storage and instructions on how to add it to your node, see [Adding File Storage to a Tethered Node](#) on page 68.

Setting Up a Linux Node

A *node* is any server running IBM Aspera High-Speed Transfer Server. Aspera web applications, such as IBM Aspera Faspex, communicate with a node through the IBM Aspera Node API. When a node is added to Faspex, it is called a *tethered node*.

The instructions below assume you have already installed HSTS on your server. For instructions on installing IBM Aspera High-Speed Transfer Server Admin Guide: Installing HSTS.

1. Aspera recommends setting up the node as the `root` user. If you do not have access to the `root` user, you must give the current system user permissions to make changes to the `/opt/aspera/etc/aspera.conf` configuration file.

Change ownership of the `aspera.conf` file to the current system user:

```
# chown system_user:root /opt/aspera/etc/aspera.conf
```

2. Verify that the node is running IBM Aspera High-Speed Transfer Server with a valid Connect Server license on your transfer server:

Run the following command:

```
# ascp -A
```

In the resulting output, look for the following phrase:

```
Connect Server License max rate
```

If you need to update your transfer server license, follow the instructions in *IBM Aspera Enterprise Server Admin Guide: Updating Product License*.

3. Create the `faspex` system user account on the node.

Run the following commands to create the system user `faspex`.

```
# groupadd -r faspex
# useradd -r faspex -g faspex
```

4. Create and configure the `faspex_packages` directory.

Run the following commands to create the `faspex_packages` directories and configure the `faspex` user directories:

```
# mkdir -p /home/faspex/faspex_packages
# chown faspex:faspex /home/faspex/
```

```
# chown faspex:faspex /home/faspex/faspex_packages
```

The `asconfigurator` utility modifies the `aspera.conf` configuration file, located at: `/opt/aspera/etc/aspera.conf`.

5. Add the user to `aspera.conf` and set the *docroot*.

The directory you choose for the docroot is the absolute path for the transfer user. When this node is added to Faspex, users cannot access files or folders outside of the docroot.



CAUTION: Aspera recommends that you not use spaces in your docroot. If your docroot contains spaces, you may not receive all email notifications relating to transfer activity.

Run the following `asconfigurator` command with the transfer username and the docroot path:

```
# asconfigurator -x "set_user_data;user_name,username;absolute,/docroot/path"
```

For example:

```
# asconfigurator -x "set_user_data;user_name,faspex;absolute,/home/faspex/faspex_packages"
```

6. Set up token authorization for the user in `aspera.conf`.

Run the following `asconfigurator` commands to set the encryption key for the user:

```
# asconfigurator -x "set_user_data;user_name,username;authorization_transfer_in_value,allow"
# asconfigurator -x "set_user_data;user_name,username;authorization_transfer_out_value,allow"
# asconfigurator -x "set_user_data;user_name,username;token_encryption_key,encryption_key"
```

The encryption key can be any string of numbers. Aspera recommends a string that is at least 20 characters long. For example:

```
# asconfigurator -x "set_user_data;user_name,faspex;authorization_transfer_in_value,allow"
# asconfigurator -x "set_user_data;user_name,faspex;authorization_transfer_out_value,allow"
# asconfigurator -x "set_user_data;user_name,faspex;token_encryption_key,gj5o930t78m34ejme9dx"
```

7. Set the IP address or hostname for the node in the `aspera.conf` file with the following `asconfigurator` command:

```
# asconfigurator -x "set_server_data;server_name,ip_or_hostname"
```

For example:

```
# asconfigurator -x "set_server_data;server_name,aspera.example.com"
```

8. Configure the node for HTTP and HTTPS fallback.

The fallback settings on the node must match the fallback settings on Faspex. If the settings don't match, Faspex returns a "Package creation failed" error. Set the HTTP and HTTPS ports to the ports you configured in Faspex. For more information about HTTP fallback, see [Configuring HTTP and HTTPS Fallback](#) on page 40.

```
$ asconfigurator -x "set_http_server_data;enable_http,true"
$ asconfigurator -x "set_http_server_data;http_port,8080"
$ asconfigurator -x "set_http_server_data;enable_https,true"
$ asconfigurator -x "set_http_server_data;https_port,8443"
```

Restart the **asperahttpd** service by running the following commands:

```
# /etc/init.d/asperahttpd restart
```

9. Configure a HSTS transfer user account with a Node API username and password.

Faspex communicates to the HSTS transfer user account through the Node API to start transfers on the node.

For instructions on adding users to HSTS, see the *IBM Aspera High-Speed Transfer Server Admin Guide: Setting Up Users*.

a) Set up the Node API user:

```
# /opt/aspera/bin/asnodeadmin -a -u node_api_username -
p node_api_passwd -x system_username
```

Note: Aspera recommends that you use different names for the system user account and transfer user account in order to minimize confusion when tracing transactions and events.

For example:

```
# /opt/aspera/bin/asnodeadmin -a -u node_user -p -x faspex
```

b) Run the following command to check the system user was successfully added to asnodeadmin:

```
# /opt/aspera/bin/asnodeadmin -l
```

Given a node user named **node_user** and a system user named **faspex**, the result should be similar to the following example:

user	system/transfer user	acls
=====	=====	=====
node_user	faspex	

10. Copy the IBM Aspera Connect public key to `authorized_keys` to allow Connect to connect to Faspex.

a) If the `.ssh` folder does not already exist in the `faspex` system user's home directory, run the following command to create the folder:

```
# mkdir -p /home/username/.ssh
```

For example:

```
# mkdir -p /home/faspex/.ssh
```

b) If the `authorized_keys` file does not already exist, add the `aspera_tokenauth_id_rsa.pub` public key to the file by running the following command:

```
# cat /opt/aspera/var/aspera_tokenauth_id_rsa.pub >> /home/
username/.ssh/authorized_keys
```

c) Transfer the `.ssh` folder and `authorized_keys` file ownership to the system user by running the following commands:

```
# chown -R username:username /home/username/.ssh
# chmod 600 /home/username/.ssh/authorized_keys
# chmod 700 /home/username
# chmod 700 /home/username/.ssh
```

You can now add this node to Faspex.

Setting Up a Windows Node

A *node* is any server running IBM Aspera High-Speed Transfer Server. Aspera web applications, such as IBM Aspera Faspex, communicate with a node through the IBM Aspera Node API. When a node is added to Faspex, it is called a *tethered node*.

The instructions below assume you have already installed HSTS on your server. For instructions on installing IBM Aspera High-Speed Transfer Server Admin Guide: Installing HSTS.

1. Verify that the node is running IBM Aspera High-Speed Transfer Server with a valid Connect Server license on your transfer server:

Run the following command:

```
> ascp -A
```

In the resulting output, look for the following phrase:

```
Connect Server License max rate
```

If you need to update your transfer server license, follow the instructions in *IBM Aspera Enterprise Server Admin Guide: Updating Product License*.

2. Create the **faspex** system user account on the node.

Click **Control Panel > User Accounts** and add a new account named **faspex**. This system user account is associated with the Node API account in the steps below.

After creating a Windows user account, log in as that user at least once for Windows to set up the user's home folder.

3. Create and configure the **faspex_packages** directory.

Create the following directory:

```
> cd C:\
> mkdir faspex_packages
```

The **asconfigurator** utility modifies the **aspera.conf** configuration file, located at: **C:\Program Files (x86)\Aspera\Enterprise Server\etc\aspera.conf**.

4. Add the transfer user to **aspera.conf** and set the *docroot*.

The directory you choose for the docroot is the absolute path for the transfer user. When this node is added to Faspex, users cannot access files or folders outside of the docroot.



CAUTION: Aspera recommends that you not use spaces in your docroot. If your docroot contains spaces, you may not receive all email notifications relating to transfer activity.

Run the following **asconfigurator** command with the transfer username and the docroot path:

```
> asconfigurator -x "set_user_data;user_name,username;absolute,/docroot/path"
```

For example:

```
> asconfigurator -x "set_user_data;user_name,faspex;absolute,/home/faspex/faspex_packages"
```

5. Set up token authorization for the user in **aspera.conf**.

Run the following **asconfigurator** commands to set the encryption key for the user:

```
> asconfigurator -x
"set_user_data;user_name,username;authorization_transfer_in_value,allow"
```

```
> asconfigurator -x
"set_user_data;user_name,username;authorization_transfer_out_value,allow"
> asconfigurator -x
"set_user_data;user_name,username;token_encryption_key,encryption_key"
```

The encryption key can be any string of numbers. Aspera recommends a string that is at least 20 characters long. For example:

```
> asconfigurator -x
"set_user_data;user_name,faspex;authorization_transfer_in_value,allow"
> asconfigurator -x
"set_user_data;user_name,faspex;authorization_transfer_out_value,allow"
> asconfigurator -x
"set_user_data;user_name,faspex;token_encryption_key,gj5o930t78m34ejme9dx"
```

6. Set the IP address or hostname for the node in the `aspera.conf` file with the following `asconfigurator` command:

```
> asconfigurator -x "set_server_data;server_name,ip_or_hostname"
```

For example:

```
> asconfigurator -x "set_server_data;server_name,aspera.example.com"
```

7. Enable HTTP and HTTPS fallback.

The fallback settings on the node must match the fallback settings on Faspex. If the settings don't match, Faspex returns a "Package creation failed" error. Set the HTTP and HTTPS ports to the ports you configured in Faspex. For more information about HTTP fallback, see [Configuring HTTP and HTTPS Fallback](#) on page 40.

```
> asconfigurator -x "set_http_server_data;enable_http,true"
> asconfigurator -x "set_http_server_data;http_port,8080"
> asconfigurator -x "set_http_server_data;enable_https,true"
> asconfigurator -x "set_http_server_data;https_port,8443"
```

Restart the `asperahttpd` service. Go to **Control Panel > Administrative Tools > Computer Management > Services and Applications > Services**, click **Aspera HTTPD**, and click **Restart**.

8. Configure a HSTS transfer user account with a Node API username and password.

Faspex communicates to the HSTS transfer user account through the Node API to start transfers on the node.

For instructions on adding users to HSTS, see the *IBM Aspera High-Speed Transfer Server Admin Guide: Setting Up Users*.

- a) Run the following commands to set up the Node API user:

```
> asnodeadmin -a -u node_api_username -p node_api_passwd -
x system_username
```

Note: Aspera recommends that you use different names for the system user account and transfer user account in order to minimize confusion when tracing transactions and events.

For example:

```
> asnodeadmin -a -u node_user -p -x faspex
```

- b) Run the following command to check that the system user was successfully added to `asnodeadmin`:

```
> asnodeadmin -l
```


Given a node user named `node_user` and a system user named `faspex`, the output should be:

user	system/transfer user	acls
=====	=====	=====
node_user	faspex	

9. Copy the IBM Aspera Connect public key to `authorized_keys` to allow Connect to connect to Faspex.
 - a) If the `.ssh` folder does not already exist in the system user's home directory, run the following commands to create the folder:

```
> cd "C:\Documents and Settings\username"
> mkdir .ssh
```

For example:

```
> cd "C:\Documents and Settings\faspex"
> mkdir .ssh
```

- b) If the `authorized_keys` file does not already exist, use a text editor to create or edit the following file: `C:\Documents and Settings\username\.ssh\authorized_keys`.
- c) Copy the contents of the `aspera_tokenauth_id_rsa.pub` (`C:\Program Files (x86)\Aspera\Enterprise Server\var\aspera_tokenauth_id_rsa.pub`) public key to the file.

The file must be named "authorized_keys" without file extensions. Some text editors add a `.txt` extension to the filename automatically. Be sure to remove the extension if it was added to the filename.

You can now add this node to Faspex.

Setting Up an OS X Node

A *node* is any server running IBM Aspera High-Speed Transfer Server. Aspera web applications, such as IBM Aspera Faspex, communicate with a node through the IBM Aspera Node API. When a node is added to Faspex, it is called a *tethered node*.

The instructions below assume you have already installed HSTS on your server. For instructions on installing IBM Aspera High-Speed Transfer Server Admin Guide: Installing HSTS.

1. Verify that the node is running IBM Aspera High-Speed Transfer Server with a valid Connect Server license on your transfer server:

Run the following command:

```
# ascp -A
```

In the resulting output, look for the following phrase:

```
Connect Server License max rate
```

If you need to update your transfer server license, follow the instructions in *IBM Aspera Enterprise Server Admin Guide: Updating Product License*.

2. Create the `faspex` system admin account on the node.
 - a) Go to **System Preferences # Users & Groups**.
 - b) Click the lock button and enter your admin credentials to make changes.
 - c) Click the add button.
 - d) Name the user `faspex`.
 - e) Select **Administrator** from the New Account drop-down menu.
 - f) Name the account.
 - g) Enter and verify a password for the account.

- h) Click **Create User**.
- i) Click **Login Options** in the users panel.
- j) Click the **Join** button next to Network Account Server.
- k) Click **Open Directory Utility**.
- l) In the Directory Utility window, click the lock button and enter an administrator account and password to make changes.
- m) From the menu bar, select **Edit # Enable Root User**.
- n) Enter and verify the password.
- o) Click **OK**.

The `asconfigurator` utility modifies the `aspera.conf` configuration file, located at: `/Library/Aspera/etc/aspera.conf`.

3. Add the user to `aspera.conf` and set the `docroot`.

The directory you choose for the `docroot` is the absolute path for the transfer user. When this node is added to Faspex, users cannot access files or folders outside of the `docroot`.



CAUTION: Aspera recommends that you not use spaces in your `docroot`. If your `docroot` contains spaces, you may not receive all email notifications relating to transfer activity.

Run the following `asconfigurator` command with the transfer username and the `docroot` path:

```
# asconfigurator -x "set_user_data;user_name,username;absolute,/docroot/path"
```

For example:

```
# asconfigurator -x "set_user_data;user_name,faspex;absolute,/home/faspex/faspex_packages"
```

4. Set up token authorization for the user in `aspera.conf`.

Run the following `asconfigurator` commands to set the encryption key for the user:

```
# asconfigurator -x "set_user_data;user_name,username;authorization_transfer_in_value,allow"
# asconfigurator -x "set_user_data;user_name,username;authorization_transfer_out_value,allow"
# asconfigurator -x "set_user_data;user_name,username;token_encryption_key,encryption_key"
```

The encryption key can be any string of numbers. Aspera recommends a string that is at least 20 characters long. For example:

```
# asconfigurator -x "set_user_data;user_name,faspex;authorization_transfer_in_value,allow"
# asconfigurator -x "set_user_data;user_name,faspex;authorization_transfer_out_value,allow"
# asconfigurator -x "set_user_data;user_name,faspex;token_encryption_key,gj5o930t78m34ejme9dx"
```

5. Set the IP address or hostname for the node in the `aspera.conf` file with the following `asconfigurator` command:

```
# asconfigurator -x "set_server_data;server_name,ip_or_hostname"
```

For example:

```
# asconfigurator -x "set_server_data;server_name,aspera.example.com"
```

6. Configure the node for HTTP and HTTPS fallback.

The fallback settings on the node must match the fallback settings on Faspex. If the settings don't match, Faspex returns a "Package creation failed" error. Set the HTTP and HTTPS ports to the ports you configured in Faspex. For more information about HTTP fallback, see [Configuring HTTP and HTTPS Fallback](#) on page 40.

```
# asconfigurator -x "set_http_server_data;enable_http,true"
# asconfigurator -x "set_http_server_data;http_port,8080"
# asconfigurator -x "set_http_server_data;enable_https,true"
# asconfigurator -x "set_http_server_data;https_port,8443"
```

Restart the **asperahttpd** service by running the following commands:

```
# sudo launchctl stop com.aspera.asperahttpd
# sudo launchctl start com.aspera.asperahttpd
```

7. Configure a HSTS transfer user account with a Node API username and password.

Faspex communicates to the HSTS transfer user account through the Node API to start transfers on the node.

For instructions on adding users to HSTS, see the *IBM Aspera High-Speed Transfer Server Admin Guide: Setting Up Users*.

a) Run the following commands to set up the Node API user:

```
# /Library/Aspera/bin/asnodeadmin -a -u node_api_username -
p node_api_passwd -x system_username
```

Note: Aspera recommends that you use different names for the system user account and transfer user account in order to minimize confusion when tracing transactions and events.

For example:

```
# /Library/Aspera/bin/asnodeadmin -a -u node_user -p -x faspex
```

b) Run the following command to check the system user was successfully added to asnodeadmin:

```
# /Library/Aspera/bin/asnodeadmin -l
```

Given a node user named **node_user** and a system user named **faspex**, the result should be similar to the following example:

user	system/transfer user	acls
=====	=====	=====
node_user	faspex	

8. Copy the IBM Aspera Connect public key to authorized_keys to allow Connect to connect to Faspex.

a) If the `.ssh` folder does not already exist in the system user's home directory, run the following commands to create the folder:

```
# mkdir "/Users/username/.ssh"
```

For example:

```
# mkdir "/Users/faspex/.ssh"
```

b) If the `authorized_keys` file does not already exist, use a text editor to create or edit the following file: `/Users/username/.ssh/authorized_keys`.

c) Copy the contents of the `aspera_tokenauth_id_rsa.pub` (`/Library/Aspera/Enterprise Server/var/aspera_tokenauth_id_rsa.pub`) public key to the file.

The file must be named `authorized_keys` without file extensions. Some text editors add a `.txt` extension to the filename automatically. Be sure to remove the extension if it was added to the filename.

You can now add this node to Faspex.

Adding File Storage to a Tethered Node

File storages are directories made available to use as inboxes (locations where Faspex packages can be received and stored) or as the source from which users can choose files to include in a package.

You can add file storage on both the local tethered node or on remote tethered nodes.

Only registered Faspex users can browse remote file storage. External senders are not permitted to access remote file storage. Every registered Faspex user can access all file storage, which means that you cannot limit file storage access to certain registrants. However, a registered Faspex user cannot send from remote sources unless the user account is configured to **Create packages from remote sources** and their permission settings give them access to the source.

To add file storage:

1. Go to **Server > File Storage**.

2.

Choose a tethered node and select **Add File Storage** from the  drop-down menu.

3. Enter a name for the file storage.

4. Choose the directory for the file storage. Click **Browse**, select a directory, and click **Select**.

You can perform the following actions to help find the desired directory.

- You can perform a simple search for a directory by entering it into the name field and clicking **Search**.
- You can perform an advanced search by clicking the **Show Filters** link, and entering your criteria.
- You can sort the directory list by **Name**, **Type**, **Largest first**, **Smallest first**, **Newest first**, or **Oldest first** in descending order.

Important: You are only able to browse within the docroot that was associated with your transfer service user and API username. The path `/` means the docroot, not the root directory of the node.

5. If the node is running a Linux operating system and you want to enable symlinks for this file storage, select **Enable linking**. This setting is ignored if the option is not supported by the node (in other words, non-Linux nodes).

6. If you are using this file storage as cloud storage, select **Enable cloud referencing**.

Note: For more information, see [Enabling Cloud Referencing for Package Creation](#) on page 70.

7. Click **Create File Storage**.

You should now see your tethered node and file storage listed on the File Storage page. The display shows the name and status of each node. The **Active** and **Error** links provide more detail on the node status. The display indicates which location is the current default inbox, and the permission level for access to sources in that location. By default, source directories are private.

You can configure read permissions and transfer rate limitations of your file storage by selecting the drop-down arrow next to the file storage's name and selecting **Edit**. For more information about configuring your file storage, see [Configuring File Storage](#) on page 68.

Configuring File Storage

You can configure read permissions and transfer rate limitations of your file storage. Go to **Server > File Storage**, select the drop-down arrow next to the file storage's name, and select **Edit**.

Choose Directory

Click **Browse** and select a directory in the pop-up window. Choose one of the following options:

- You can perform a simple search for a directory by entering it into the name field and clicking **Search**.
- You can perform an advanced search by clicking the **Show Filters** link, and entering your criteria.
- You can sort the directory list by **Name**, **Type**, **Largest first**, **Smallest first**, **Newest first**, or **Oldest first** in descending order.

Read Permissions

Set the read permission. Choose from one of the following options:

- **Private:** No one can use this file storage as a remote source.
- **Public:** Any user with the **Create packages from remote source** permission can use it as a remote source.
- **Limited:** Set a list of users who can use this file storage as a remote source. When you select **Limited**, Faspex displays the Custom Access Control section. Users must have the **Create packages from remote source** permission to use the file storage as a source.

File storage read permissions are set to **Private** by default.

Transfer Settings

If you want to override the default transfer settings, select **Override default transfer settings** to configure the following settings:

Initial Default Transfer Rate

Item	Default
Initial upload rate:	10000 kbps
Initial download rate:	10000 kbps

Selecting **Lock minimum rate and policy** disables the ability to adjust transfer policies or minimum transfer rates for clients accessing this file storage. (Clients are, for example, Connect and HSTS.)

Default Maximum Allowed Rate

Item	Default
Maximum upload rate:	20000 kbps
Maximum download rate:	20000 kbps

Relay Transfer Rate

Item	Default
Incoming relay rate:	45000 kbps
Outgoing relay rate:	45000 kbps

When a relay takes place between two servers with differing transfer rates, the transfer uses the smaller transfer rate between the two servers. For example, if there is a relay from server A to server B where the outgoing relay rate of server A is 20,000 kbps and the incoming relay rate of server B is 10,000 kbps, then the resulting relay transfer rate will be 10,000 kbps.

Note: Faspex uses Relay Transfer Rates for packages with files from remote sources and for relays to custom inbox or to relay destinations.

Advanced Configuration

In the Advanced Configuration options, you can specify secondary server addresses for a group of users that need to use a different address to authenticate to Faspex.

Note:

Alternate addresses support comma-delimited Classless Inter-Domain Routing (CIDR), allowing you to specify multiple subnets or a specific range of addresses. For example:

```
198.51.100.24,192.168.0.0/18,10.0.0.*
```

Specify rules for when these secondary server addresses apply.

Use if requester's address matches: Use secondary server addresses when the user's IP address matches the given range of addresses. For example: `192.168.0.*`

Use if browser hostname matches: Use secondary server addresses when the user accesses Faspex through a URL that matches the given hostnames. For example: `faspex-internal.com`

Set Default Server Inbox

The default server inbox is the location where Faspex stores packages uploaded to the server.

1. Go to **Server > File Storage**.
2. Select your desired inbox under the **Default Inbox** column.

On a fresh install, the default inbox is the **packages** directory on the tethered node. You can change the default inbox to any file storage directory on any active node. If the node's connection status is **Error**, the option is be grayed out and not selectable.

3. Click **Update**.

Related tasks

[Adding a Node to Faspex](#) on page 59

Enabling Cloud Referencing for Package Creation

Cloud referencing links package files to source files in the cloud instead of copying source files to create a package.

Important:

- The source and destination of a package must be in the same cloud storage attached to an HST Server running in the cloud, or attached to the Aspera on Cloud Transfer Service (if compatible).
- Faspex currently supports file storages run by these cloud providers:

- AWS (S3)
- Azure

1. Go to **Server > File Storage** and edit the file storage of the remote cloud service node. Select **Enable cloud referencing**.

2. Enable trap links for the remote storage.

For example, on Azure nodes, edit `/opt/aspera/etc/trapd/azure.properties` and set `aspera.session.support.symlink = true`.

```
# Defines whether symlink support is wished
# Default is false
aspera.session.support.symlink = true
```

Enable the configuration changes by running:

```
$ sudo service asperatrapd restart
```

Note: When creating a package, both the source and the default inbox need to be on the same cloud node for the cloud referencing feature to work.

3. Enable specific users to create packages from remote sources.

Go to **Accounts** and click the name of the user. Under Permissions, select **Create packages from remote sources** to enable the feature for that user.

Creating and Managing User Accounts

Creating a New Faspex User

These instructions demonstrate how to create local user accounts. For information on adding directory service users or groups, see [Working with Directory Services \(DS\)](#) on page 110.

1. Go to **Accounts**.
2. Click **New User** or select **Faspex User** from the **Add Account** drop-down menu if directory services are enabled.
3. Enter a username in the **Login** field.

If an admin creates a user with the same username and email address as an external user, Faspex merges the external user with this new account. If the new user shares only an email address with the external user, the two accounts are not merged. For more information about external users, see [Working with External Senders](#) on page 90.

Important: Usernames cannot contain semi-colons.

4. Enter a valid email address. Faspex uses this email address for email notifications.
5. If you want to manually set the account password, select **Set password**. Enter and confirm a password. The password must conform to current server password requirements.

By default, Faspex enforces the creation of strong passwords. Faspex defines strong passwords as passwords that are at least six characters long, with at least one letter, one number, and one symbol. You can disable strong passwords by going to **Server > Security** and disabling the **Use strong passwords** option.

6. Optional: Edit Additional Permissions.

Click the **Edit Additional Permissions** link at the bottom of the form to access additional user settings. These settings include the following:

- Account Details
- Permissions
- Package Deletion
- Advanced Transfer Settings
- Welcome E-mail

For more information on specific settings, see [Configure User Settings](#) on page 209.

7. When finished with the configuration, click **Create Account**.

Unless disabled by an admin, Faspex sends a welcome email to every new account. The email includes a reset password link and a login link for users that already know their password. The password reset link in the welcome email expires after one week. Admins can disable the welcome email by going to **Server > Configuration > Security** and disabling the **Send welcome email to all new users** option.

If you manually set a password, provide the account credentials to the user.

Managing Faspex Users

You can edit, manage and remove IBM Aspera Faspex user accounts from the **Accounts** menu.

Editing a Faspex Account

Clicking the account name opens the Edit User page for the account. For more information, see [Configure User Settings](#) on page 209. In addition, the Edit User page includes the **Workgroup Memberships**, **Change Password**, and **Reset Password** links. For more information, see [Changing or Resetting a User's Password](#) on page 72.

Sorting or Filtering Accounts

To sort users, click the header bar to sort them. For example, by clicking **Login**, you can sort all accounts alphabetically by account name. Click again to sort in reverse order.

You can also use the filter controls to search for users or restrict display of users of a certain type. The filter searches through the following fields:

- First name
- Last name
- Username
- Email
- Description

To search, enter keywords in the **Filter** field or select a user type from the drop menu.

Note: You can also sort or filter accounts by custom fields. For more information on setting up custom fields, see [Configuring Custom User Fields](#) on page 74.

Activating, Deactivating, or Removing Faspex Accounts

- To activate users, select one or more accounts on the user listing page and click **Actions > Activate**.
- To deactivate users, select one or more accounts on the user listing page and click **Actions > Deactivate**.
- To remove users, select one or more accounts on the user listing page and click **Actions > Remove**.

Note: A user account must be active for the user to log in to Faspex. In the user account list, inactive accounts are shown in gray.

Changing or Resetting a User's Password

Changing a User's Password

Go to **Accounts** and click the username of the user you want to edit. Click the **Change/Reset Password** link.

Enter and confirm a password. The password must conform to current server password requirements. By default, Faspex enforces the creation of strong passwords. Faspex defines strong passwords as passwords that are at least six characters long, with at least one letter, one number, and one symbol. You can disable strong passwords by going to **Server > Security** and disabling the **Use strong passwords** option.

Resetting a User's Password

Go to **Accounts** and click the username of the user you want to edit. Click the **Change/Reset Password** link.

Confirm when prompted to send the user an email notification allowing them to log in and change their password with a password reset link. The password reset link expires after one hour.

Reactivating an Inactive Account

A user account can become inactive if an admin deactivates the user or the user account has been locked because an incorrect password was entered too many times. An inactive or locked account cannot be logged into and its password cannot be reset by clicking **Forgot my password** from the login page.

1. Go to **Accounts.**

In your list of accounts, you may see users that are Active, Inactive, Pending approval, or Locked. You can reactivate inactive and locked accounts. For more information on pending accounts, see [Approving or Denying Pending Registrations](#) on page 125.

Status
Active
Locked
Pending approval
Inactive

2. Click the name of the user account you want to reactivate.

3. Under the user account's Account Details section, select **Account activated.** The user can now login to this account using the existing password.

4. You can reactivate an account by selecting **Account activated or by changing the user's password.**

You can also reactivate an account by changing the user's password. For instructions on changing a user's password, see [Changing or Resetting a User's Password](#) on page 72.

User Roles

An IBM Aspera Faspex user's permissions are defined by its specific user settings and its user role. Admins assign user roles to an account when creating a new account or when configuring an account's permissions. For more information on configuring an accounts permissions, see [Configure User Settings](#) on page 209.

User accounts can have the following roles:

- Admin
- Manager
- User
- Workgroup Admin

To set permissions for an account in Faspex, go to **Accounts** for a list of existing users. Click the name of the account you want to change permissions for and choose the desired role.

Tip: You can also define a user as a workgroup admin. This role is assigned and managed from **Workgroups**, whereas the other user roles are assigned and managed from **Accounts**. For more information, see [Working with Workgroups](#) on page 95.

User

All users can send packages through Faspex. Normal users typically do not manage other users or workgroups.

Manager

The manager role gives a user permissions to manage other Faspex accounts. Managers can create, edit, or delete workgroups and regular users. However, they cannot create new managers, edit admin accounts, or promote another user to admin or manager roles. Managers do not have access to the **Server** tab, nor can they change the Faspex server configuration (a privilege limited to admins).

Tip: Assigning the manager role to users allows you to separate server administration and account administration, delegating the burden of administration to two different groups.

Admin

Admins can configure Faspex from the **Server** tab. They can create, edit, and delete every type of Faspex user (admins, managers, and regular users) as well as create, edit, or delete workgroups.

Workgroup Admins



The workgroup admin role is assigned and managed when configuring Workgroups, not from a user's account settings. For details, see [Working with Workgroups](#) on page 95. A user can be designated as a "workgroup admin" (by a Faspex admin or manager). Workgroup admins manage specific workgroups according to the permissions set for that role in that workgroup.

Configuring Custom User Fields

Admins can create additional custom fields for a user to fill out when creating a new IBM Aspera Faspex user. Custom fields can be required or optional. You can view information gathered by these custom fields on the **Accounts** page and you can use these fields to sort and filter user accounts. Custom fields are also used to configure SAML. For more information on SAML, see [SAML and Faspex](#) on page 112.

Note: Custom user fields do not apply to Directory Service users.

1. To create custom fields, go to **Server > User Profile**.
2. Click the **Add User Profile Field** button to create additional custom fields to a maximum of five fields.
3. Configure the custom field. The following section describes configuration options for a custom field:

Configuration Option	Description
Enabled	Select this box to enable or disable the custom field. (Fields are enabled by default.)
Name	Enter the desired name of your custom field into the text box. This field applies to Local users.
Required	Require new users to fill out the field. Clearing the box makes the field optional. (Fields are required by default.)
	Click the  button to delete a field. Faspex opens a pop-up that prompts you to confirm by clicking OK to delete the field. Note: Deleting a field permanently deletes the custom field and all its data from all existing users.

4. Click **Save Fields**.

To view your custom fields, go to **Accounts**. Click the **Toggle Columns** button and select the fields you want displayed.



Configuring Account Preferences

Click the profile icon in the top-right of the banner and select **Account** from the drop-down menu. You can change your Faspex account preferences including language, notification options, and password. You can also manage your contacts and distribution lists.

Updating Email and Connect Settings

Click the profile icon in the banner and select **Account** from the drop-down menu and go to **Preferences** to update your Faspex email preferences and Connect settings.

Email Settings

Option	Description
E-mail	Enter your email address to receive electronic notifications from Faspex. Admins have the ability to disable users from changing their email addresses. For more information, see Configuring Security Settings on page 47.
Upload notifications	If you would like to be notified (via email) after you have uploaded a package successfully, select Upload notification and input your faspex account. Notify additional users from your contacts list by clicking the  button.
Download notifications	If you would like to be notified (via email) after recipients download your package successfully, select this feature and enter your faspex account. Notify additional users from your contacts list by clicking the  button.
Email me when I receive a package	Select to be notified when new packages are received.
Email me when I download a package	Select to be notified when new packages are downloaded.
Include me in workgroup notifications for packages I send	Select to be notified when a workgroup receives your packages.

Misc

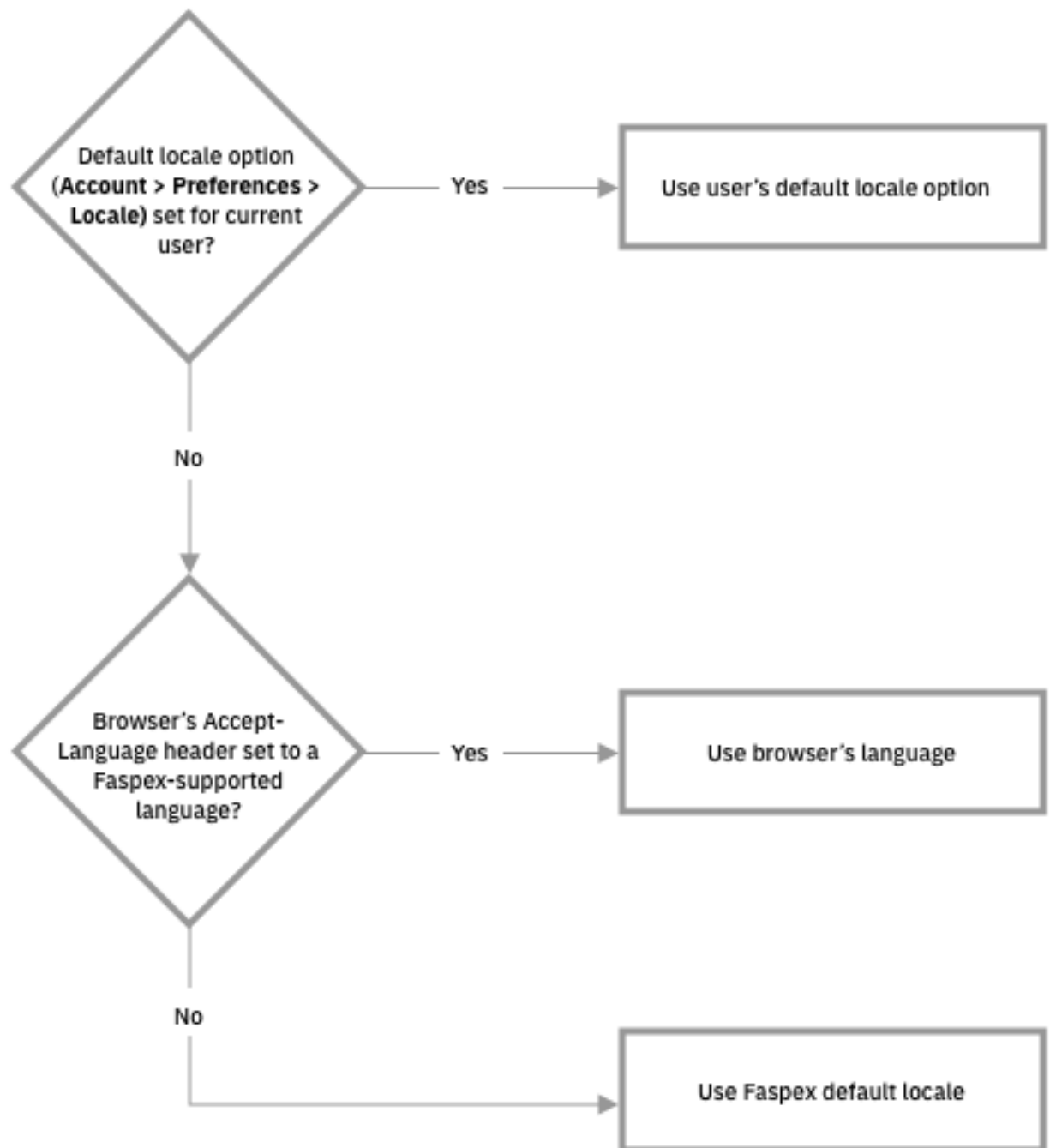
Option	Description
Disable Aspera Connect plugin	Prevent Faspex from checking for and using IBM Aspera Connect. When Connect is disabled, Faspex uses the HTTP Gateway service instead.
Max rows per page	For a package or an account list, set how many rows are displayed per page.
Enable public URL	<p>Note: This field and checkbox does not appear if (1) Public URLs are disabled server-wide or (2) Public URLs have been disabled for this particular user.</p> <p>A public URL allows external senders to submit packages to registered users and dropboxes. External senders no longer need to be individually invited to submit a package, although that functionality still exists. For more information, see Enabling and Sharing your Public URL on page 92.</p>

Option	Description
	You can enable or disable the Enable public URL feature for your account, as long as Public URLs are allowed by your admin.

Changing Your Language

Change your default language to another supported language.

How Faspex determines on a user-to-user basis the language to use for the web UI:



1. Click the profile icon in the top-right of the banner and select **Account** from the drop-down menu.

2. Under **Locale**, select your language from the drop-down menu.
3. Click **Update Preferences**.

Changing Your Password

Change your account password.

1. Click the profile icon in the top-right of the banner and select **Account** from the drop-down menu.
2. Go to the **Change Password** tab.
3. Enter your current password in the **Old Password** field.
4. Enter and confirm a new password.
By default, the requirement is a strong password that contains at least six characters (with a minimum of one letter, one number and one symbol).
5. Click **Change Password**.

Editing Contacts

Whenever you send packages to an external email address, Faspex automatically saves the email address in your contact list.

If your account has also been configured with **Keep user directory private** set to **Yes**, each recipient of your packages and each sender that sends a package to your account is automatically added to your contact list.

To remove contacts:

1. Click the profile icon in the top-right of the banner and select **Account** from the drop-down menu.
2. Go to the **Edit Contacts** tab.
3. Click the **Remove** link for each contact you want to remove.

Creating a Personal Distribution List

You can configure personal distribution lists to send packages to a list of email addresses and Faspex users. Each distribution list consists of a comma-separated list of email addresses or Faspex usernames.



On the Edit Distribution Lists page, you can create, edit, or delete personal distribution lists. Although you cannot edit global distribution lists, you can duplicate the list and then edit the duplicated list. For more information on creating and editing global distribution lists, see [Creating a Global Distribution List](#) on page 129.

To create a new list:

1. Click the profile icon in the top-right of the banner and select **Account** from the drop-down menu.
2. Go to the **Edit Distribution Lists** tab.
3. Click **Add New Distribution List** or **Duplicate** a global list.
4. Name the distribution list.

Do not give your personal distribution list the same name as a user account or workgroup name.

Do not give your personal distribution list same name as a global distribution list, unless you want Faspex to use personal list instead of the global list when sending a package.

5. Enter up to 50 contacts. You can:
 - Type email addresses or Faspex usernames into the Contacts field.
 -  Click  to import contacts from your Faspex contacts list.
 - Click the **Browse** button to upload contacts from a CSV file.

Note: The CSV file must include a single column containing only email addresses.

You cannot send packages to a distribution list if any recipient in the list is an invalid user. For example, if a user is an external user and the option to send to external users is disabled, the external user is considered invalid and package sending fails.

If the admin enables the **Ignore invalid recipients** option, package sending does not fail even if the list contains an invalid user. Faspex skips any invalid user and delivers the package to all valid recipients in the list. (Go to **Server > Security** and, under the Faspex accounts section, select **Ignore invalid recipients**.)

Note: To send explicitly to external users, you must append (`external`) to the email address (or Faspex automatically expands the email to existing Faspex users or creates a Faspex user for the email. For example, to send to `faspex_user@example.com`, add `faspex_user@example.com (external)` to the distribution list. For more information on email expansion, see [Package Recipient Expansion by Email Address](#) on page 87.

The items in the list are not validated until you try to send a package to the list.

6. Click **Create**.

After creating a distribution list, the list appears on the Editing Distribution Lists page. You can edit the name and contacts list, or import contacts by clicking **Import Contacts from CSV**. After making changes, click **Update Distribution Lists** to save the changes. You can also delete distribution lists by clicking the **Delete** link for the list.

Check Data Usage and Sender Quota Limit

If sender quotas are enabled, you can check your sender quota limit and the amount of data you've sent in your personal preferences.

Click the profile icon in the banner and select **Account** from the drop-down menu. Go to **Sender Quota**.

The page shows your remaining available data in the current rolling period and the quota limit set for your account. When the remaining available data drops to zero, you cannot send packages until the rolling period expires and your available data is reset.

Transferring Files

Faspex and Connect

Transfers initiated in the IBM Aspera Faspex web application are conducted using the IBM Aspera Connect Browser Plug-in. The Connect Plug-In is an install-on-demand web browser plug-in that facilitates high-speed uploads and downloads with an Aspera transfer server.

The Connect Install Dialog

When a user first logs in, Faspex checks if Connect has been installed on their browser. If they have an outdated version or do not have the plug-in installed, Faspex prompts the users to download and install the plug-in.

Clicking **Download latest version** connects the user to Aspera's CloudFront CDN from which they can download the Connect installer.

Transfers with HTTP Gateway Service

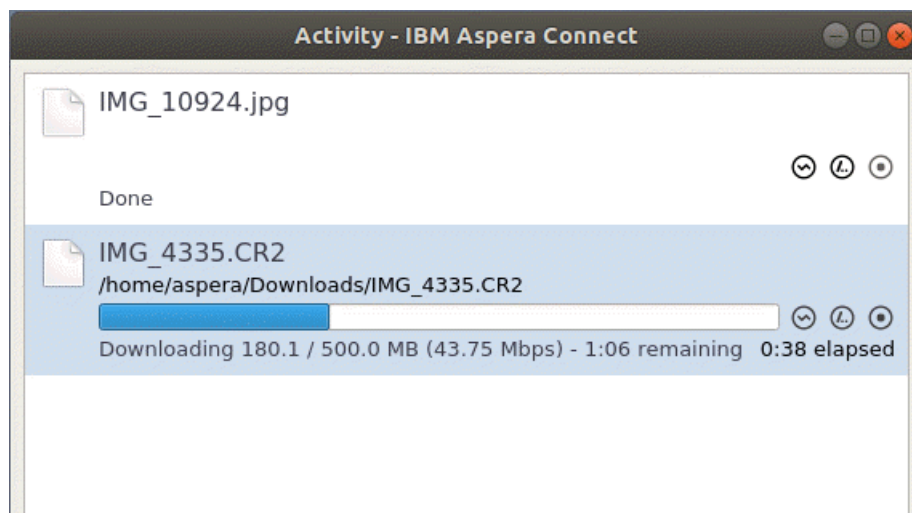
You can choose to use the HTTP Gateway service instead of Connect to make transfers using Faspex. For more information about transferring with HTTP Gateway, see [Using HTTP Gateway Instead of IBM Aspera Connect](#) on page 90.

Serving Connect Locally

If you are operating within a closed system, you may want to host the IBM Aspera Connect installers and plug-ins for locally rather than having the downloads served from Aspera's CloudFront CDN. This also enables you to enforce a certain version of the Connect plug-in. you can host the IBM Aspera Connect Plug-in SDK installers locally. For more information on serving the Connect plug-in locally, see [Serving Connect Locally](#) on page 88.

The Activity Window

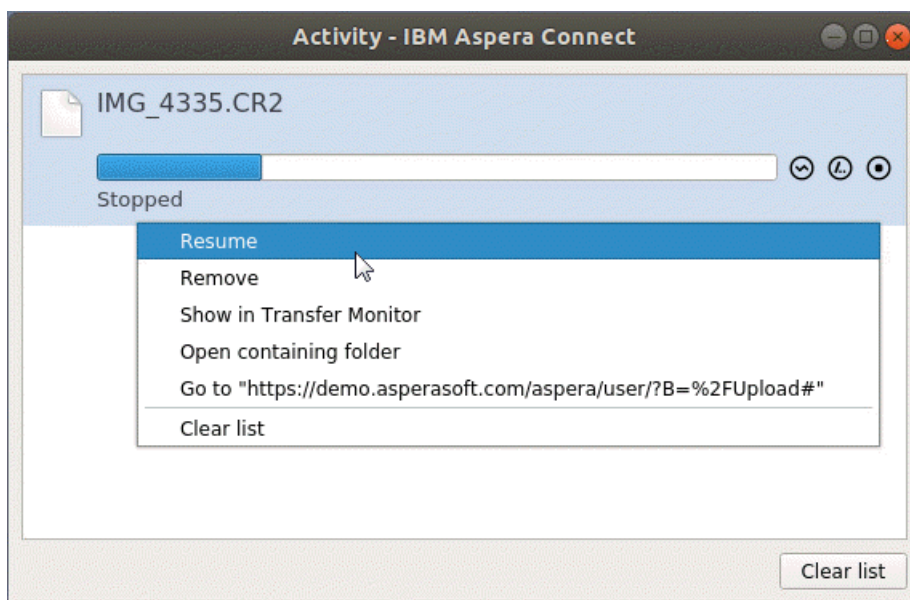
In the Activity window, you can view and manage all transfer sessions.




The Activity window contains the following controls:

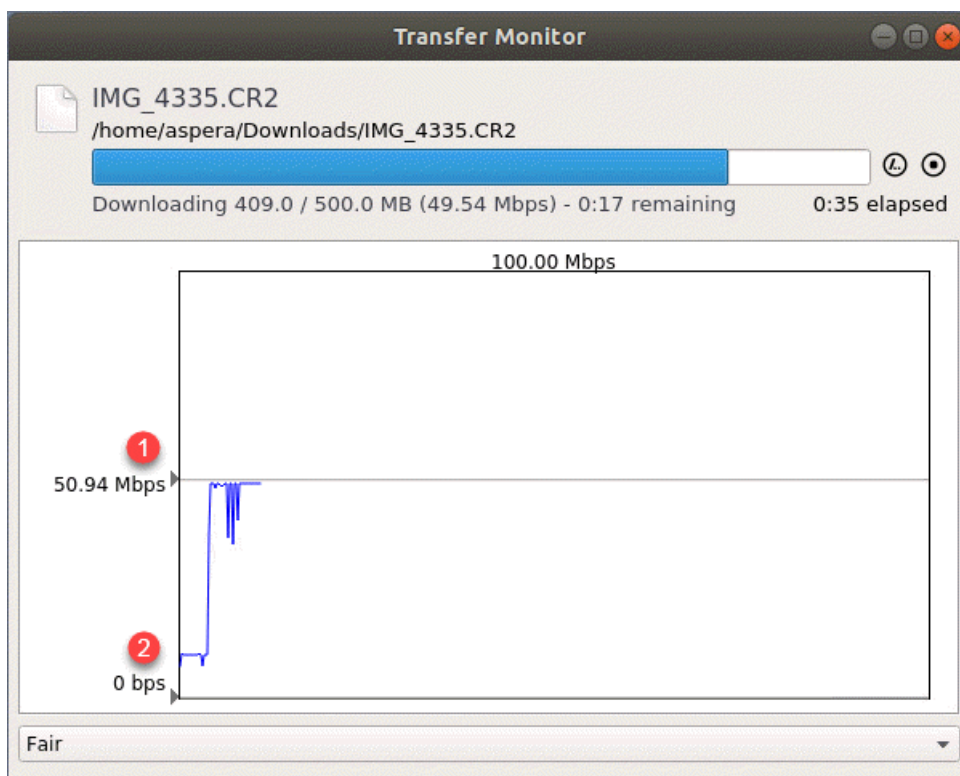
- Open the Transfer Monitor. For more information on this feature, see [Monitoring Transfers](#).
- Open the folder on your computer that contains this content.
- Stop the transfer.
- Resume a stopped transfer, or retry a failed transfer.

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 button. You can also right-click on a started or stopped transfer to access various controls. The example below shows the right-click options for a stopped transfer.






Monitoring Transfers



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  icon 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 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  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  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

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.

Sending a New Package

When a local transfer is initiated, IBM Aspera Faspex prompts IBM Aspera Connect to start a session. You must allow the Connect to run in order to send packages with Faspex.

Note: Remote transfers do not prompt the Connect.

1. Go to **New Package**.


Note: If the **New Package** button opens a drop-down menu, choose **Normal Package**. Other options send packages to your dropboxes. For more information about dropboxes, see [Working with Dropboxes](#) on page 99.

2. Specify package recipients in the following fields:

Enter the package recipients on the **To** line. A recipient can be any one of the following:

- A Faspex account name.
- The email address of an external user (if this is permitted for your account). For more information on sending to external users, see [Allowing Users to Send to External Email Addresses](#) on page 90.
- A workgroup name, which begins with an asterisk (*).
- A name of a distribution list.

Note: Valid delimiters when entering multiple recipients are commas (,) and semi-colons (;).

You can also add recipients from your contact list by clicking the  button. The contact list shows the Faspex users, workgroups, and distribution lists you can access.

If you are permitted to send packages to external email addresses, Faspex saves the external email address to your contact list when you send files to a new address. To remove an email address from your contact list, go to **Account > Edit Contacts**.

Note: For recipient fields, Faspex automatically converts email address to existing Faspex users with the corresponding email addresses. For more information, see [Package Recipient Expansion by Email Address](#) on page 87.

3. If you want to send packages as a BCC (blind carbon-copy), click **Show Private Recipients** and enter Faspex account names, external email addresses (if allowed), or distribution lists in the **To (private)** field.
4. Specify recipients of CC notifications in the following fields:

Option	Description	Triggered Email Template
CC Upload	<p>You can notify others when packages are uploaded by enabling this field and entering Faspex account names or email addresses.</p> <p>You cannot enter workgroups in these fields. To hide CC options, click Hide CC.</p>	<ul style="list-style-type: none"> • Upload Result CC
CC Download	<p>You can notify others when packages are downloaded by enabling this field and entering Faspex account names or email addresses.</p> <p>You cannot enter workgroups in these fields. To hide CC options, click Hide CC.</p>	<ul style="list-style-type: none"> • Package Downloaded CC
CC Receipt	<p>If your account has Allow editing of receipt addresses on package creation enabled, you can add Faspex users or email address to the CC Receipt list. These users and email addresses receive the same notifications as the package sender regarding this transfer.</p> <p>If an admin has included CC Receipt recipients for your account, the CC Receipt field is auto-populated with those accounts and emails. If allowed to edit, you can modify that list.</p>	<ul style="list-style-type: none"> • Package Received CC • Package Sent CC • Package Downloaded CC • Upload Result CC

Note: Valid delimiters when entering multiple recipients are commas (,) and semi-colons (;).

Admins can configure CC notification templates by going to **Server > Notifications**. For additional information, see "[Notifications](#)".

5. Enter a package title.
6. Fill out custom metadata fields added by the admin.

Faspex allows the admin to add custom metadata fields to the New Package form. For more information on custom metadata, see [Faspex Metadata](#) on page 145.

7. Schedule package delivery by selecting a **Release Policy** option.

Faspex users can specify when uploaded packages are delivered. External submitters do not have this option. The following three policies are available:

- **Release Now:** Deliver the package as soon as it is uploaded (default).
- **Release Later - Set Date Now:** Delay delivery and set a delivery time. Click in the **Release Date** text box to open the date and time setting popup.
- **Release Later - Set Date Later:** Delay delivery and set a delivery time later. Packages that are created with this option are listed in **Pending Packages** with the option to **Set now** under **Send Date**.

Delayed delivery can be used to stagger package delivery, moderating the load on the Faspex server if there are many recipients, or to prepare the package but wait to deliver until the desired release date.

Packages that are created with a **Release Later** option are listed on the **Pending** page. The send date or **Set now** is listed in the **Send Date** column. You can edit the send date by clicking on it. For more information, see [Managing Pending Packages](#) on page 85.

8. If enabled by an admin, and if you want to obfuscate the file names in your package, select **Use obfuscation on filenames**.

If enabled, Faspex obfuscates the file names of all uploaded files. In the case of a directory file structure, Faspex also obfuscates the folder name, the names of all files within the folder, and the names and files of any nested directories.

Faspex does not obfuscate the file extensions of files. For example, after obfuscation, a file with the .txt extension may be named Nqu7ORqTEC2R9GHK8ISFw.txt.

Note:

- File name obfuscation when transferring through Connect requires Connect version 3.9.8 or higher. Set the minimum Connect version in Faspex to 3.9.8 (**Server > Configuration > Transfer Options**) if you enable file name obfuscation. Faspex does not obfuscate file names if transferring with an older version of Connect.
- File name obfuscation in Faspex is irreversible.

9. If enabled by an admin, and if you want to secure your packages, enable the encryption-at-rest feature for this transfer.

Select **Use encryption-at-rest** to encrypt the package's contents on the server. If enabled, recipients are required to decrypt the package with a password to access its contents. For more information about encryption, see [Configuring Security Settings](#) on page 47.

10. If enabled by an admin, set package expirations for the package.

Select from one of the following auto-deletion rules:

- **Do nothing:** Do not auto-delete after the package is downloaded.
- **Delete files after any recipient downloads all files:** Delete after *any* recipient downloads *all* files in the package once.

Important: When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option.

- **Delete files after all recipients download all files:** Delete if *all* files in the package have been downloaded by *all* recipients.

For more information about package expiration, see [Changing the Package Directory](#) on page 94.

11. Select your content source if your Faspex account is allowed to create packages from remote sources.

Select your content source from the **Source** drop-down list. For example, select whether to create a package from files on your local computer, another computer, or cloud storage.

Important: Outside submitters are not be able to create packages from remote sources.

12. Select content to include in your package.

- Browse for files: Upload specified files to Faspex.
- Browse for folders: Upload specified folders to Faspex.

- Drag-and-drop: Drag files and folders to the browser to upload files.¹

13. To prevent recipients from downloading this package over HTTP (HTTP Gateway or HTTP fallback), select **Prevent HTTP download for this package**.

14. If transfers through HTTP Gateway is enabled, select (from the **Transfer With** drop-down menu) whether Faspex should use HTTP Gateway or Connect for the transfer.

15. Click **Send Package** when you are finished.

Depending on your Package Storage settings, file packages sent from Faspex are either stored on the server for a specified duration or until they are manually deleted. You can find your sent packages by going to the tab **Sent** in the Faspex menu.

You can shorten the list of packages by archiving or deleting packages. If the option is available, click the **Delete** button or the **Archive** button. To locate archived packages, click **View Full History**.

Note: Only global admins and workgroup admins can archive packages. Regular workgroup members cannot archive packages.

Managing Pending Packages

When package delivery is delayed, you can view pending packages on the **Pending** page of the Faspex UI.

aspera faspex server

Hi admin [Account](#) [Sign out](#)

New Package ▾ Received Sent **Pending** Workgroups Accounts Server

Pending Packages [View Full History](#)

Recipients	Title	Send Date	Upload Date	Size	Files	Status	Action
jason@aspera.com	Revisions you requested	Jun 28	3:52 PM	4.2 MB	1	Complete	Archive Delete
jason@aspera.com	Proofs 6-16-2017	Set Now	3:48 PM	5.7 MB	2	Complete	Archive Delete

Edit or Set the Send Date

To update or set the package date, click the link in **Title** or **Send Date** column. In the **Send Date** field, click **Edit** to set or edit the send date, or **Release Now** to send the package immediately.

¹ The drag-and-drop capability is not supported on some platforms. See the IBM Aspera Faspex Release Notes for the feature support matrix.

Archive One or All Pending Packages

If you are logged in as an admin, you can hide some or all pending packages from your **Pending Packages** view. To hide a single package, click **Archive** in that row. To hide all pending packages, click **Archive All**. You can view archived pending packages by clicking **View Full History**.

Delete a Pending Package

If you decide you do not want to send a package and want to delete it, click **Delete** to completely remove the package and its contents from the Faspex server.

Viewing and Downloading Packages

1. View your received packages.

- Download a package you received: Go to **Received**.
- Download a package you sent: Go to **Sent**.
- Download any package sent through Faspex: Go to **Server > Packages**.

Tip: Admins can shorten their received packages list by moving packages into archive. To do so, click the **Archive** link within the corresponding package row (under the Action column). To locate archived packages, click **View Full History** link.

2. Optional: Sort your packages.

In the packages list, you can click the header bar links to sort your packages. For example, when clicking **Sender**, all packages are sorted alphabetically by sender's name.

Three additional columns exist when viewing all packages sent through Faspex:

Header	Description
Downloads Full/Partial	The number of times the corresponding package has been fully or partially downloaded.
Files on Server?	States whether the package is currently stored on the server: <ul style="list-style-type: none"> • yes: All files in the package have been uploaded. • partial: Some of the files in the package have been uploaded. • deleted: The package and its files have been deleted from the server.
Action	If you see an active <u>Delete</u> hyperlink, click it to delete the corresponding package from the server. If the package has already been deleted from the server, the entire row is grayed out and the field Files on Server? displays deleted .

Important: You can also perform a batch deletion for packages that are older than "X" number of days. To do so, scroll to the bottom of the packages list and enter the number of days in the **for packages [#] days or older** field. The number is set to 30 days, by default. Click **Delete files** to proceed with the deletion.

3.



Click the button to download a package.

Faspex prompts the IBM Aspera Connect to start a session. When the Confirm window appears, click **Allow** to begin.

Note: When downloading an encrypted package, the Connect prompts the user for a passphrase. The Connect also prompts for a passphrase if the package contains any **.aspera-env** files within the folder hierarchy, even if the package also contains unencrypted files or files encrypted with different passphrases. If you choose to keep downloaded files encrypted, you do not need to enter a password until you attempt to decrypt the files locally.

Package Recipient Expansion by Email Address

Faspex automatically converts email addresses in recipient fields to existing Faspex users associated with the same email addresses. If there are multiple users associated with an email address, the address expands to all matching users. If a user exists whose username is the entered email address, the email address is not expanded and the package or notification is sent to that user only.

Faspex expands emails in the following fields:

- New package To field
- New package CC Upload field
- New package CC Download field
- New package CC Recipients field
- Distribution lists Contacts field

Package Recipient Expansion with External users

When creating a new package, if the sender enters an email address in the To field, Faspex detects whether there are existing Faspex users associated with the entered email and handles entered email addresses in one of the following ways:

- If there are existing users, the To field suggestions drop-down is auto-populated with the Faspex users that the sender has permissions to send to.
- If there are no existing users or the sender does not have permissions to send to any existing users, the To field does not display any suggestions. If the sender sends to the email address anyway, Faspex notifies that the sender does not have adequate permissions.
- If there are no existing Faspex users share the email address and the sender is allowed to send to external email addresses, Faspex automatically creates a new external user with the email address.

If you explicitly append **(external)** to an entered email address (for example, `faspex_user@example.com(external)`), Faspex does not check for the associated users and transfers the package to the external email address. For more information on sending to external users, see [Allowing Users to Send to External Email Addresses](#) on page 90.

Package Details

You can view details for any sent or received package on the Package Details page. To open the Package Details page:

- Go to **Received** and click on a package name.
- Go to **Sent** and click on a package name.
- Go to **Server > Packages** and click on a package name.
- Go to **Workgroups**, select your workgroup or dropbox, and click on a package name.

Note: If you do not see the **Workgroups** tab, you do not have access to any workgroups or dropboxes.

The Package Details page displays the following information:

A **Package - File Type Comparison** [Return to List](#) [Forward](#) **B**

D Company Name: Aspera
Note:

E Browse and Download Contents or [Download Entire Package](#)

Path: / PKG - File Type Comparison

Name	Size
jpeg-n-png-123-photo.jpg	93.7 KB

Download selected Select: [All](#) , [None](#) [More Details](#)

Package Details **C**

Status: Complete
Size: 93.7 KB
Files: 1
Upload stats:
Elapsed: less than 5 seconds
Average rate: 7.1 Mbps

Full Package Downloads: 0
Partial Package Downloads: 0
Active Downloads: 0

Item	Name	Description
A	Download Icon	Click the icon to download the complete package.
B	Forward	If package forwarding is permitted for your account, click the link to forward this package.
C	Package Details	The package's information and download activity.
D	Package Note and Metadata	The package's note and metadata, if any. For more information on metadata, see Faspex Metadata on page 145.
E	Browse and Download Contents	Navigate into folders in this package, or select folders and files to download.

Serving Connect Locally

You may want to host your own IBM Aspera Connect SDK for your applications rather than having the downloads served from Aspera's CloudFront CDN. This also enables you to make users download the Connect plug-in from a server of your choice.

Note: If you choose to locally serve connect, you must manually update your Connect plug-in version to support the latest Faspex features. Different versions of Faspex require a different minimum version of the Connect plug-in. You can check the minimum Connect plug-in version of your Faspex by going to **Server > Transfer Options** and looking under Aspera Connect Version.

1. Download the Connect SDK zip file from the [Aspera Developer Network](#) and unzip the folder into a temporary location.
2. Create this folder: `/opt/aspera/faspex/public/connect`
3. Extract the Connect SDK to the connect folder.
4. Give Faspex permissions and ownership of the new Connect directory.

```
# chown -R faspex:faspex /opt/aspera/faspex/public/connect
# chmod -R 755 /opt/aspera/faspex/public/connect
```

5. In the Faspex UI, go to **Server > Configuration > Transfer Options** and select **Locally host Connect**.

Using Faspex with the HTTP Gateway Service

The HTTP Gateway is a service that allows a client to download files from and upload files to a HSTS node without using IBM Aspera Connect. If configured, Faspex users can choose to use HTTP Gateway instead of Connect for transfers.

Enabling the HTTP Gateway Service

Provide Faspex with the URL to your configured HTTP Gateway service.

Note: HTTP Gateway is a standalone product that has separate documentation. For instructions on installing and configuring HTTP Gateway, see the *IBM Aspera HTTP Gateway Admin Guide*.

To enable HTTP Gateway transfers in Faspex:

1. Go to **Server > Transfer Options** and enter the URL (with namespace `/aspera/http-gwy/v1`) of your HTTP Gateway.
For example: `https://http_gateway.example.com/aspera/http-gwy/v1`
2. Click **Update preferences**.

Faspex users can choose to use HTTP Gateway for downloads by selecting **Disable Aspera Connect plugin** in their account preferences.

Limitations

HTTP Gateway-based transfers are limited by the same limitations of HTTP/HTTPS transfers and the native download manager of the client's web-browser.

General Limitations

- Since uploads and downloads leverage HTTP/HTTPS between the web browser and HTTP Gateway, the transfer performance depends on the performance of HTTP/HTTPS, which can be affected by distance between clients and servers, and by other network-related issues. For this reason, IBM Aspera highly recommends following best practice by deploying HTTP Gateway as close as possible to end users.
- Empty (0-byte) files are not supported for uploads and downloads.
- HTTP Gateway does not support resuming transfers.

Download Limitations

When downloading more than one file, HTTP Gateway bundles the files in-memory. Bundling the files allows end users to download multiple files at once as one archive. Bundling the files also allows preserving a directory structure in the archive.

The total size of the archive cannot be communicated to the web browser, because files are bundled and transferred in-memory. Therefore, the download manager cannot show progress based on the total size.

Upload Limitations

- Since web browsers do not have an upload manager, IBM Aspera provides an upload mechanism through a JavaScript SDK. The upload mechanism allows sending multiple files as chunks, allowing the web page implementing the SDK to send large amounts of data. Because the web page sends the chunked data in the background, the user must stay on the same web page until the upload finishes.

Note: You can find the JavaScript SDK documentation on the [IBM Developer website](#).

- HTTP Gateway supports uploading only files and not directories.

Using HTTP Gateway Instead of IBM Aspera Connect

Use HTTP Gateway instead of Connect to transfer files.

Note: If HTTP Gateway is not enabled, you cannot choose to disable Connect.

1. Go to your account.
2. Select **Disable Aspera Connect plugin**.
3. Click **Update preferences**.

Working with External Senders

Allowing External Users to Send to Faspex Users

Configure IBM Aspera Faspex to allow external senders, those who do not have Faspex accounts, to send packages to Faspex users.

1. Go to **Server > Configuration > Security** and find the Outside Email Addresses section.
2. Select **Allow inviting external senders** and set the default to **Allow**.

When set to **Allow**, all Faspex users are able to invite external senders by default. An Admin can enable or disable this feature for specific users from the Accounts page, while retaining server-wide settings. For instructions on inviting external users, see [Inviting External Senders](#) on page 91.

Whenever a user sends to an external user, Faspex saves the email address to the database. Admins can view and remove external users from the database by going to **Accounts > External Users**.

Allowing Users to Send to External Email Addresses

Configure IBM Aspera Faspex to allow users to send packages to external email addresses not associated with a Faspex account.

1. Go to **Server > Configuration > Security** and find the Outside email addresses section.
2. Select **Allow sending to external email addresses** and choose **Allow**.

Choosing **Allow** enables all users to send to external email addresses by default. An admin can enable or disable this feature for specific users from the **Accounts** page, while still retaining the global setting.

3. Configure invitation link expiration.

You can choose to expire the invitation link after a set number of days, after one successful upload, both, or none.

If **After one successful upload** is configured, this limit applies even if the package download link is forwarded.

After the first download, the package must be resent for a recipient to download the package again.

4. Allow users to set a custom link expiration policy. This is enabled by default.

All your Faspex accounts can now send packages to external email addresses. You can configure permissions for each individual user by going to **Accounts** and selecting the user you want to configure. For more information on configuring user permissions, see [Managing Faspex Users](#) on page 72.

When a user sends to an external email address that is not associated with an existing Faspex user, Faspex creates a new external user with that email address. To explicitly send a package to an existing external user, add **(external)** to the email address. For example, enter **johndoe@faspex.example.com (external)**.

Inviting External Senders

The following steps assume an admin has configured Faspex to allow inviting external senders (users who do not have Faspex accounts). For more information, see [Allowing External Users to Send to Faspex Users](#) on page 90.

1. Go to **Received** and click the **Invitations** link.
2. Click on **New** to send an invitation.
3. Enter the outside sender's email address
4. If you want to offer further information or further instruction, enter a description.
5. Choose a link expiration policy. If you do not enable **Custom link expiration policy**, Faspex uses the server default link expiration setting.

The submission link expiration options include the following:

- **After one upload:** Delete the submission link after one successful upload
- **After 3 days:** Delete the submission link on a specific date (which you need to input)

You can enable both features. The link expires whenever either of the conditions are met.

6. Click **Save**.
Faspex sends the external user an email with a submission link. The external user can upload a package to Faspex from that link.

You can view all your invitations by going back to **Received > Invitations**.

Here, you can perform the following operations:

- You can **Resend** the submission link email.
- You can **Delete** the invitation, which removes the sender from this list and prevents them from using the submission link.
- You can see the URL submission link that was sent to the user.

Configuring Public URLs

A public URL allows external senders to submit packages to registered users and dropboxes. External senders no longer need to be individually invited to submit a package, although that functionality still exists. When a public URL is enabled and shared to an external sender, the external sender can take the following actions to send a package.

1. The external sender clicks the Public URL (which could be for either a dropbox or a registered Faspex user).
2. The sender is directed to page and asked to enter an email address.
3. A private link is automatically emailed to the sender.
4. The sender clicks the private link and is automatically redirected to a dropbox or Faspex user package submission page.
5. Once the package is submitted through the private link, the dropbox or Faspexuser can download the package by going to **Received**.

The following describes how to enable a public links.

1. Go to **Server > Configuration > Security** and find the Outside Email Addresses section.
2. Select **Allow public submission URLs** and choose **Allow**.
Choosing **Allow** turns on the public URL feature for all Faspex dropboxes and registered users.
3. Select **Allow dropboxes to individually enable/disable their own public URLs** to allow dropbox and global admins to override the server setting and turn off this feature for individual dropboxes.

When public URLs are allowed, all users can use public submission unless otherwise configured by an admin. Users must enable the feature in their user preferences. For more information, see [Enabling and Sharing your Public URL](#) on page 92. Admins can enable or disable the Public URL feature for specific users despite global settings by

going to **Accounts**, selecting the user, going to the Permissions section, and choosing **Allow**, or **Deny** for **Allow public submission urls**.

Enabling and Sharing your Public URL

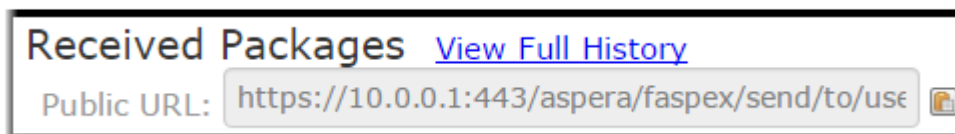
A public URL allows external senders to submit packages to registered users and dropboxes. When a public URL is enabled and shared to an external sender, the external sender can take the following actions to send a package.


1. The external sender clicks the shared Public URL.
2. The sender is directed to a page and asked to enter an email address.
3. A private link is automatically emailed to the sender.
4. The sender clicks the private link and is automatically redirected to a package submission page.
5. Once the package is submitted through the private link, the user can download the package by going to **Received**.

The following describes how to enable a public link on your account. An admin must first enable the Public URL feature for your account or for the server. For more information, see [Configuring Public URLs](#) on page 91.

1. Click the **Account** link next to your username.
2. Go to the Misc section on the Preferences page and select **Enable public URL**.
3. Click **Update preferences**.
4. Go to **Received**.

Your public URL is displayed under Received Packages.



5. Click the  button to copy the public URL to your clipboard.
6. Send the public URL to the external sender.

Removing External Users from Faspex

Whenever a user sends to an external user, Faspex saves the external user's email address to the database.

1. Go to **Accounts > External Users**.
2. Select the users you want to delete.
3. Select **Remove** from the **Actions** drop-down menu.
4. Confirm and click **OK**.

Viewing Packages and Managing Package Storage

Viewing and Downloading Packages

1. View your received packages.
 - Download a package you received: Go to **Received**.
 - Download a package you sent: Go to **Sent**.
 - Download any package sent through Faspex: Go to **Server > Packages**.

Tip: Admins can shorten their received packages list by moving packages into archive. To do so, click the **Archive** link within the corresponding package row (under the Action column). To locate archived packages, click **View Full History** link.

2. Optional: Sort your packages.


In the packages list, you can click the header bar links to sort your packages. For example, when clicking **Sender**, all packages are sorted alphabetically by sender's name.

Three additional columns exist when viewing all packages sent through Faspex:

Header	Description
Downloads Full/Partial	The number of times the corresponding package has been fully or partially downloaded.
Files on Server?	States whether the package is currently stored on the server: <ul style="list-style-type: none"> yes: All files in the package have been uploaded. partial: Some of the files in the package have been uploaded. deleted: The package and its files have been deleted from the server.
Action	If you see an active <u>Delete</u> hyperlink, click it to delete the corresponding package from the server. If the package has already been deleted from the server, the entire row is grayed out and the field Files on Server? displays deleted .

Important: You can also perform a batch deletion for packages that are older than "X" number of days. To do so, scroll to the bottom of the packages list and enter the number of days in the **for packages [#] days or older** field. The number is set to 30 days, by default. Click **Delete files** to proceed with the deletion.

3.

Click the  button to download a package.

Faspex prompts the IBM Aspera Connect to start a session. When the Confirm window appears, click **Allow** to begin.

Note: When downloading an encrypted package, the Connect prompts the user for a passphrase. The Connect also prompts for a passphrase if the package contains any **.aspera-env** files within the folder hierarchy, even if the package also contains unencrypted files or files encrypted with different passphrases. If you choose to keep downloaded files encrypted, you do not need to enter a password until you attempt to decrypt the files locally.

Configure Package Storage Expiration

Change the default package expiration time, as well as what to do with packages after they are downloaded by recipients. Within the IBM Aspera Faspex Web UI, go to **Server > Configuration > Package Storage** to view or modify your server's package expiration and deletion behavior. After modifying these settings, you must click the **Update** button to save your changes.

•

- **Time-based content expiration:** This setting determines how long Aspera on Cloud maintains contents of a package. For example, if you configure this setting for 10 days, Faspex deletes package contents 10 days after the package becomes available to the intended recipients. You can apply a separate time-based expiration policy to Draft packages in the workspace. **Note:** Content expiration also applies to packages in failed transfers.
- **Download-based content expiration:** This setting determines whether Aspera on Cloud deletes package contents after all recipients have downloaded the package (either the entire package or all the individual contents of the

package in one operation). If desired, you can configure a grace period that delays deletion for the number of days you configure, even after all recipients have downloaded the package.

Configuration Option	Description
Packages expire	Once a package is uploaded to Faspex, the link to view the package will expire after the specified number of days.
After packages are downloaded	<p>Select from one of the following auto-deletion rules:</p> <ul style="list-style-type: none"> • Do nothing: Do not auto-delete after the package is downloaded. • Delete files after any recipient downloads all files: Delete after <i>any</i> recipient downloads <i>all</i> files in the package once. <p>Important: When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option.</p> <ul style="list-style-type: none"> • Delete files after all recipients download all files: Delete if <i>all</i> files in the package have been downloaded by <i>all</i> recipients.
Allow all users to set their own delete setting on a package-by-package basis	Enable users to set package expiration when creating a new package.

Important: The package storage location is your local docroot plus the directory specified under your file storage settings. The source location is the remote node's docroot plus the file share location.

Important: When a package is marked for deletion after download, any packages that point to the files contained therein will not be accessible once the original package is downloaded. This condition could potentially lead to forwarded package files being inaccessible if they are forwarded before being downloaded by the original recipient.

Changing the Package Directory

The package directory is the directory where IBM Aspera Faspex stores packages uploaded to the Faspex server. When a user requests to download a package, Faspex searches this directory for that package. The package directory is created and specified during the installation process. By default, it is located at: `/home/faspex/faspex_packages`

You can change the package directory, but you must do so on the Faspex server. Changing the package directory within the application UI does not move the packages or create the directory.

1. On the Faspex server, view the current package directory by running the following command:

```
asctl faspex:package_dir
```

2. Create the new directory on the server. You can now move packages into it or wait until after you have set the directory as Faspex's package directory.
3. To set the Faspex's package directory, run the following command and specify the path to the new directory:

```
asctl faspex:package_dir /new_directory
```

SPECIAL CONSIDERATIONS:

If you are storing Faspex packages in a network directory, ensure that the directory is configured as follows:

- The network share is accessible to the OS system account that Faspex server is running under, with permissions to read/write/delete/traverse directories, and create new files and folders.
- The share will be auto-mounted on boot.

Working with Workgroups

Workgroups define a group of users that can be sent packages as a collective whole. A Faspex administrator determines who has permissions to send packages to a workgroup and where those packages are stored. The administrator also determines whether members can see and send packages to other workgroup members.

Creating a Workgroup

Note: Admins and managers can set up workgroups, but workgroup admins cannot create workgroups. Workgroup admins manage specific workgroups according to the permissions set in that workgroup.

1. To create a workgroup, go to **Workgroups > Create New > Workgroup**.
2. Enter a workgroup name and a description of the workgroup.
3. Set the inbox destination, where packages sent to the workgroup are stored:
 - **Server default:** Use the server default node and directory.
 - **Custom:** Choose from a list of local and remote nodes as the default location for your custom inbox.
 - Incoming packages are stored in both the custom inbox and the default server inbox. Deleting packages from the default inbox through the web UI do not automatically remove the same packages from the custom inbox.
 - Use the **Upload directly to custom inbox** option to prevent Faspex from storing a copy in the default inbox if the workgroup or dropbox is the only recipient of a package.

Note: If a user sends a package to two workgroups or dropboxes, even if both workgroups and dropboxes are configured to upload directly to the custom inbox, Faspex stores the package on the default inbox and then relays the packages to the custom inboxes.

4. If you want to forward package to remote destinations, set up file relay. Select **Enable Relay**. For each desired destination:
 - a) Check **Relay**.
 - b) If you want to overwrite files if they exist on the destination, check **Overwrite**.
 - c) If you want to notify users on relay start, error, or completion, enter a list of usernames or email addresses in the relevant field.

For more information about file relay, see [File Relays](#) on page 107.

5. Set workgroup permissions for sending packages to the workgroup. **Restricted** is the default.
6. Set workgroup permissions for workgroup members sending packages to each other. **Restricted** is the default.
7. Set permissions for workgroup admins.
8. Click **Create**.

Managing Workgroups Members

Workgroups in Faspex are listed under **Workgroups**, along with the number of associated members (see link on right side of table). To add or remove members, or add members via a Directory Service group that you have [imported into Faspex](#), click the *Members* link for the workgroup.

1. Add a user to the workgroup.
 - Add directory service user: If your Faspex server has Directory Services (DS) configured and you have imported one or more DS groups, then you can also add DS users or groups from the Directory Service Groups drop-down menu. For more information about configuring DS, see [Working with Directory Services \(DS\)](#) on page 110.

- Add an existing user: Type in the user's name and click the **Add User** button.
- Create a new user: Click the **Create new user** link. For more information on creating new users, see the topic [Managing Faspex Users](#) on page 72.

The account appears in the members list.

2. Manage user settings.

You can manage members by checking the appropriate members and selecting the **Members actions...** drop-down menu and choosing one of the following actions and clicking **OK**:

Action	Description
Set standard access	Designate selected members as standard users of the workgroup. Permissions are defined by the workgroup settings.
Set as workgroup admin	Designate selected members as workgroup admins. Workgroup admins manage specific workgroups according to the permissions set for that role in that workgroup. If allowed by an admin, workgroup admins can add or remove workgroup members and can create new regular users to add to the workgroup. Note: <ul style="list-style-type: none"> • Workgroup admins cannot change the workgroup settings. That can only be done by Faspex admin or manager. • Workgroup admins cannot set a custom workgroup inbox. That can only be done by Faspex admin or manager. • Workgroup admins cannot delete workgroup packages, but they can archive them.
Deactivate	Deactivate a member. A deactivated member cannot perform workgroup functions, but the account remains in the dropbox list.
Activate	Activate a deactivated member.
Remove	Remove a member from the workgroup. This action does not remove the user from Faspex.

Sending Packages to a Workgroup

If you are an IBM Aspera Faspex workgroup member and have been assigned the proper permissions, follow the steps below to send a package to the workgroup.


1. Select **New Package** and select the dropbox you wish to send a package to from the drop-down menu.

Selecting **Normal Package** takes you to the New Package form. For more information on sending a normal package, see [Sending a New Package](#) on page 82.

Note: If the New Package button does not open a drop-down menu, you do not have permission to send to any dropboxes. If you don't see the **New Package** button at all, your account does not have permission to send users or to dropboxes.

2. Specify package recipients.

Enter your package recipients. Workgroup names are preceded by an asterisk (*).

You can also choose recipients from your contact list. To view your contact list, click the  button. The contact list shows your Faspex users, workgroups, and distribution lists. If you are permitted to send packages to external email addresses, Faspex also saves the email address to your contact list when you send files to a new address. To remove an email address from your contact list, go to **Account > Edit Contacts**.

3. If you want to send packages as a BCC (blind carbon-copy), click **Show Private Recipients** and enter Faspex account names, external email addresses (if allowed), or distribution lists in the **To (private)** field.
4. Specify recipients of CC notifications in the following fields:

Option	Description	Triggered Email Template
CC Upload	<p>You can notify others when packages are uploaded by enabling this field and entering Faspex account names or email addresses.</p> <p>You cannot enter workgroups in these fields. To hide CC options, click Hide CC.</p>	<ul style="list-style-type: none"> • Upload Result CC
CC Download	<p>You can notify others when packages are downloaded by enabling this field and entering Faspex account names or email addresses.</p> <p>You cannot enter workgroups in these fields. To hide CC options, click Hide CC.</p>	<ul style="list-style-type: none"> • Package Downloaded CC
CC Receipt	<p>If your account has Allow editing of receipt addresses on package creation enabled, you can add Faspex users or email address to the CC Receipt list. These users and email addresses receive the same notifications as the package sender regarding this transfer.</p> <p>If an admin has included CC Receipt recipients for your account, the CC Receipt field is auto-populated with those accounts and emails. If allowed to edit, you can modify that list.</p>	<ul style="list-style-type: none"> • Package Received CC • Package Sent CC • Package Downloaded CC • Upload Result CC

Note: Valid delimiters when entering multiple recipients are commas (,) and semi-colons (;).

Admins can configure CC notification templates by going to **Server > Notifications**. For additional information, see "[Notifications](#)".

5. Enter a package title.
6. Fill out custom metadata fields added by the admin.


Faspex allows the admin to add custom metadata fields to the New Package form. For more information on custom metadata, see [Faspex Metadata](#) on page 145.

7. If enabled by an admin, and if you want to secure your packages, enable the encryption-at-rest feature for this transfer.
Select **Use encryption-at-rest** to encrypt the package's contents on the server. If enabled, recipients are required to decrypt the package with a password to access its contents. For more information about encryption, see [Configuring Security Settings](#) on page 47.
8. Select your content source if your Faspex account is allowed to create packages from remote sources.
Select your content source from the **Source** drop-down list. For example, select whether to create a package from files on your local computer, another computer, or cloud storage.
Important: Outside submitters are not be able to create packages from remote sources.
9. Select content to include in your package.
 - Browse for files: Upload specified files to Faspex.
 - Browse for folders: Upload specified folders to Faspex.
 - Drag-and-drop: Drag files and folders to the browser to upload files. ²
10. Click **Send Package** when you are finished.

Downloading Packages for Workgroup

If you are a member of an IBM Aspera Faspex Workgroup, you can download file packages that have been sent to your Workgroup from the **Workgroups** tab.

Downloading a Package

To download a package, click  or click the package name to advance to its Details page.

From the Details page, you can either browse and download individual files, or click the **Download Entire Package** link to download the entire package.

Once you have initiated the download, you are asked to confirm your download directory. Faspex prompts IBM Aspera Connect to start a session. When the Confirm window appears, click **Allow** to begin.

Archiving Old Packages

You can shorten the downloaded packages list by moving packages into archive. To archive a package, click the **Archive** link within the under the Actions column. To view archived packages, click the **View Full History** link.

Note: Only global admins and workgroup admins can archive packages. Regular workgroup members cannot archive packages.

Custom Inboxes

You can set a custom inbox (custom storage location) for a workgroup or a dropbox. Custom inboxes are directories on a tethered node.

Note: Only Faspex admins can set custom inboxes. Workgroup and dropbox admins do not have this power.

How Faspex Stores Packages for Custom Inboxes

- Incoming packages are stored in both the custom inbox and the default server inbox. Deleting packages from the default inbox through the web UI do not automatically remove the same packages from the custom inbox.

² The drag-and-drop capability is not supported on some platforms. See the IBM Aspera Faspex Release Notes for the feature support matrix.

- Use the **Upload directly to custom inbox** option to prevent Faspex from storing a copy in the default inbox if the workgroup or dropbox is the only recipient of a package.

Note: If a user sends a package to two workgroups or dropboxes, even if both workgroups and dropboxes are configured to upload directly to the custom inbox, Faspex stores the package on the default inbox and then relays the packages to the custom inboxes.

- Even if symbolic links are enabled for a storage location, packages sent to a workgroup or dropbox with a custom inbox are not symbolic links. The default inbox location contains symbolic links, but custom inboxes contain actual files.

Related tasks

[Adding a Node to Faspex](#) on page 59

[Creating a Workgroup](#) on page 95

Archiving Packages in a Workgroup Inbox

Archive packages to clean up the workgroup inbox or to hide specific packages from view.

Go to **Workgroups** > *workgroup_name* and click the **Archive** link for the package you want to hide.

Working with Dropboxes

Faspex Dropboxes

Dropboxes provide a file submission system that users can drop their packages into. dropbox members can submit files as well as view them. Admins can also invite external users (people who don't have a Faspex account) to submit to a dropbox.

Faspex users submit files to a dropbox they have membership in by selecting the dropbox from the **New Package** drop-down. However, users don't necessarily have to be a member or even a Faspex user to submit to a dropbox.

Admins can invite external users to submit to a dropbox using an emailed, private link. Admins can also distribute a public URL that allows those who access it to obtain a private link to the dropbox submission page.

Users can view submitted files on the **Workgroup** page.

Common Uses

dropboxes can be used to:

- Allow file submission for various projects and business processes with different, required metadata for each.
- Allow outside users to drop packages in file submission areas without having full access to Faspex.

Creating a Dropbox

Only administrators can create dropboxes. Administrators can provide specific instructions for submitters, set custom package expiration policies, and configure permissions for dropbox admins.

1. Go to **Workgroups** from the Faspex menu and select **Create New > dropbox**.
2. Name the dropbox.
3. If you want, enter instructions for submitters.

You can use HTML tags and CSS classes in your instructions.

For a list of available tags, see [Available HTML Tags and Attributes in Faspex](#) on page 207.

For more information on using CSS classes, see [Creating a Custom CSS File](#) on page 141.

4. If an administrator created metadata profiles for Faspex, you can apply a metadata profile to the dropbox. The metadata profile defines additional, optional and required fields for the dropbox package submission form.

For more information on setting up your metadata profiles for dropbox and normal package submissions, see [Faspex Metadata](#) on page 145.

5. If an administrator created metadata profiles for Faspex, you can choose to save the metadata information to the server's root directory as the `aspera-metadata.xml` file.

If `SaveMetadataInPackage` is set to `true` in the `faspex.yml` configuration file, Faspex includes the `aspera-metadata.xml` file in submitted packages instead of saving it to the server.

For more information about `faspex.yml` options, see [faspex.yml Configurations Reference](#) on page 154.

6. If you want to set an expiration policy for all submitted packages, select **Custom package expiration policy** and configure the expiration.
 - a) To set time-based package expiration, select **Packages expire** and set the number of days Faspex makes the package available.
 - b) Select an option for download-based package expiration:

- **Do nothing:** Do not delete the submitted package after it is downloaded.
- **Delete files after any member of this dropbox downloads all files:** Delete the submitted package if *any* dropbox member downloads all the files in the package.

Important: When this option is selected, a forwarded package can be deleted before the original recipient has downloaded it.

- **Delete files after all members of this dropbox download all files:** Delete if *all* dropbox members have downloaded all the files in the package.

Note:

This policy overrides the global package expiration setting. If global package expiration is enabled, but you want to disable time-based and download-based package expiration for only this dropbox, select **Custom package expiration policy**, but clear **Packages expire** and select **Do nothing**.

For more information about global package expiration, see [Configure Package Storage Expiration](#) on page 93.

7. If you want to set an expiration policy for invitation links, select **Custom invitation link expiration policy** and configure the expiration.
 - a) To set time-based link expiration, select **Invitation links expire** and set the number of days Faspex keeps the link available.
 - b) To set download-based link expiration, select **After one successful upload**. The link expires after an outside submitters uploads one package.

Note:

This policy overrides the global link expiration setting. If global link expiration is enabled, but you want to disable time-based and download-based link expiration for only this dropbox, select **Custom invitation link expiration policy**, but clear all settings for **Invitation links expire**.

8. Configure encryption-at-rest (EAR). The **Require encryption-at-rest** only appears when enabled for dropboxes by an admin.

Choose from the following options.

- **Use server default:** Use the globally configured option (displayed in parentheses).
- **Always:** Always use EAR. Users must enter an encryption password when sending a password.
- **Never:** Do not use EAR. This is the default setting.
- **Optional:** Users may choose to encrypt when uploading a package.

For more information on encryption-at-rest, see [Configuring Security Settings](#) on page 47.

9. Allow submission of packages from a public URL. The **Allow submission via public URL** option only appears when enabled for dropboxes by an admin. For more information on public URLs, see [Configuring Public URLs](#) on page 91.

Important:

A Public URL can be used by external senders to submit packages to both registered Faspex users and dropboxes. Public URLs allow external senders to submit a package without being individually invited to submit a package. When a Public URL is enabled and sent to an email, instant message, website, and so on, the following workflow occurs:

- The external sender clicks the Public URL for the dropbox.
- The sender is directed to page where he or she is asked to enter and submit an email address.
- A private link is automatically emailed to the sender.
- The sender clicks the private link and is automatically redirected to the dropbox package submission page.
- Once the package is submitted through the private link, the dropbox receives the package.

Select **Allow** to enable the Public URL feature for this dropbox. Select **Deny** to disable the feature for this dropbox. Changing the dropbox setting overrides the system default set in the Faspex **Server** settings.

10. Choose your dropbox's inbox destination. Packages sent to the dropbox are stored at this location.

- **Server default:** Use the server default node and directory.
- **Custom:** Choose from a list of local and remote nodes as the default location for your custom inbox.
 - Incoming packages are stored in both the custom inbox and the default server inbox. Deleting packages from the default inbox through the web UI do not automatically remove the same packages from the custom inbox.
 - Use the **Upload directly to custom inbox** option to prevent Faspex from storing a copy in the default inbox if the workgroup or dropbox is the only recipient of a package.

Note: If a user sends a package to two workgroups or dropboxes, even if both workgroups and dropboxes are configured to upload directly to the custom inbox, Faspex stores the package on the default inbox and then relays the packages to the custom inboxes.

When selecting a **Custom** inbox destination, note the following:

- Only Faspex admins can set the location of a dropbox inbox. dropbox admins do not have this power.
- Incoming packages are stored in two locations: the custom location and the server default location. When packages are deleted from the default location through the Web UI, they are not automatically removed from the custom location.

Tip: If you do not want packages stored in two locations, you can select **Senders upload directly to custom inbox**. When this feature is enabled, packages sent to this dropbox are not stored in the default location but only in the custom inbox.

- Even if symbolic links are enabled for a storage location, packages sent to a dropbox with a custom inbox will not be symbolic links. The default inbox location contains symbolic links, but custom inboxes contain actual files.

11. If you want to forward package to remote destinations, set up file relay. Select **Enable Relay**. For each desired destination:

- a) Check **Relay**.
- b) If you want to overwrite files if they exist on the destination, check **Overwrite**.
- c) If you want to notify users on relay start, error, or completion, enter a list of usernames or email addresses in the relevant field.

For more information about file relay, see [File Relays](#) on page 107.

12. Set permissions for dropbox admins and standard dropbox users.

13. Click the **Create** button.

Your new dropbox should now be listed on the **Workgroups** page along with any other existing dropboxes or workgroups.

Managing Dropbox Members

Dropboxes in Faspex are listed under the Workgroups page. The Workgroups page displays a list of workgroups; dropboxes are designated by **Dropbox** under the Type column.

1. To add or remove members, select the Dropbox from the list by clicking its name. Then click **View Members**.
2. Add a user to the dropbox.
 - Add directory service user: If your Faspexserver has Directory Services configured and you have imported one or more DS groups, then you can also add the DS users or groups. For more information about configuring DS, see the topic [Working with Directory Services \(DS\)](#) on page 110.
 - Add an existing user: Type in the user's name and click the **Add User** button.
 - Create a new user: Click the **Create new user** link. For more information on creating new users, see [Managing Faspex Users](#) on page 72.

The account appears in the members list. For information on adding outside submitters, see [Inviting an Outside Contributor to Send to Dropbox](#) on page 105

3. Manage user settings.

You can manage members by checking the appropriate members and selecting the **Members actions** drop-down menu and choosing one of the following actions and clicking **OK**:

Action	Description
Set standard access	Designate selected members as standard users of the dropbox. Permissions are defined by the dropbox settings.
Set submit-only access	Limit selected users to only submit packages to the dropbox and prohibit them from downloading packages.
Set as dropbox admin	Designate selected members as dropbox admins. Dropbox admins manage specific dropboxes according to the permissions set for that role in that dropbox. If allowed by an admin, dropbox admins can add or remove dropbox members and can create new regular users to add to the dropbox. Note: <ul style="list-style-type: none"> • Dropbox admins cannot change the dropbox settings. That can only be done by Faspex admin or manager. • Dropbox admins cannot set a custom dropbox inbox. That can only be done by Faspex admin or manager.
Deactivate	Deactivate a member. A deactivated member cannot perform dropbox functions, but the account remains in the dropbox list.
Activate	Activate a deactivated member.
Remove	Remove a member from the dropbox. This action does not remove the user from Faspex.

Sending Packages to a Dropbox

If you are a member of a dropbox and have the proper permissions, follow the steps below to send a package to a dropbox.

1. Select **New Package** and select the dropbox you wish to send a package to from the drop-down menu.

Selecting **Normal Package** takes you to the New Package form. For more information on sending a normal package, see [Sending a New Package](#) on page 82.

Note: If the New Package button does not open a drop-down menu, you do not have permission to send to any dropboxes. If you don't see the **New Package** button at all, your account does not have permission to send users or to dropboxes.

Note: You do not have access to the **To** and **To (private)** fields, because you are sending to a designated dropbox.

2. Specify recipients of CC notifications in the following fields:

Option	Description	Triggered Email Template
CC Upload	You can notify others when packages are uploaded by enabling this field and entering Faspex account names or email addresses. You cannot enter workgroups in these fields. To hide CC options, click Hide CC .	<ul style="list-style-type: none"> • Upload Result CC
CC Download	You can notify others when packages are downloaded by enabling this field and entering Faspex account names or email addresses. You cannot enter workgroups in these fields. To hide CC options, click Hide CC .	<ul style="list-style-type: none"> • Package Downloaded CC
CC Receipt	If your account has Allow editing of receipt addresses on package creation enabled, you can add Faspex users or email address to the CC Receipt list. These users and email addresses receive the same notifications as the package sender regarding this transfer. If an admin has included CC Receipt recipients for your account, the CC Receipt field is auto-populated with those accounts and emails. If allowed to edit, you can modify that list.	<ul style="list-style-type: none"> • Package Received CC • Package Sent CC • Package Downloaded CC • Upload Result CC

Note: Valid delimiters when entering multiple recipients are commas (,) and semi-colons (;).


Admins can configure CC notification templates by going to **Server > Notifications**. For additional information, see ["Notifications"](#).

3. Enter a package title.
4. Fill out custom metadata fields added by the admin.
Faspex allows the admin to add custom metadata fields to the New Package form. For more information on custom metadata, see [Faspex Metadata](#) on page 145.
5. If enabled by an admin, and if you want to secure your packages, enable the encryption-at-rest feature for this transfer.
Select **Use encryption-at-rest** to encrypt the package's contents on the server. If enabled, recipients are required to decrypt the package with a password to access its contents. For more information about encryption, see [Configuring Security Settings](#) on page 47.
6. Select your content source if your Faspex account is allowed to create packages from remote sources.
Select your content source from the **Source** drop-down list. For example, select whether to create a package from files on your local computer, another computer, or cloud storage.
Important: Outside submitters are not be able to create packages from remote sources.
7. Select content to include in your package.
 - Browse for files: Upload specified files to Faspex.
 - Browse for folders: Upload specified folders to Faspex.
 - Drag-and-drop: Drag files and folders to the browser to upload files.³
8. Click **Send Package** when you are finished.

Downloading Packages for Dropbox

If you are a member of an IBM Aspera Faspex Dropbox, you can download file packages that have been sent to your Dropbox from the **Workgroups** tab.

Downloading a Package

To download a package, click  or click the package name to advance to its Details page.

From the Details page, you can either browse and download individual files, or click the **Download Entire Package** link to download the entire package.

Once you have initiated the download, you are asked to confirm your download directory. Faspex prompts IBM Aspera Connect to start a session. When the Confirm window appears, click **Allow** to begin.

Archiving and Deleting Old Packages

You can shorten the downloaded packages list by moving packages into archive. To archive a package, click the **Archive** link within the under the Actions column. To view archived packages, click the **View Full History** link.

You can also delete a package by clicking the **Delete** link.

Note: Only global admins and dropbox admins can archive and delete packages. Regular dropbox members cannot archive packages.

³ The drag-and-drop capability is not supported on some platforms. See the IBM Aspera Faspex Release Notes for the feature support matrix.

Inviting an Outside Contributor to Send to Dropbox

If you someone to upload files to Faspex without a user account, you can invite them to send their packages to a dropbox as an outside submitter. Outside submitters can submit files to the dropbox using a submission link, but they cannot view files in the dropbox.

When outside submitters are invited to access a dropbox, they are not prevented from sharing the upload link with others. Faspex records the IP address used to submit packages, but Faspex cannot verify that the person using the link is the intended contributor. If this is a concern, set a custom link expiration policy for the invitation link. the submission link expires after one successful upload completion or the submission link expires on a specific date. In the case of expiration after the completion of a successful upload, it *is* possible for an outside submitter to initiate parallel uploads using a single link to submit multiple packages.

1. Go to **Workgroups** and select your dropbox.
2. Select **Invite Outside Submitter**.
3. Enter the external email address of the invited submitter.
4. Write a description that is included in the email invitation.
5. Select **Custom invitation link expiration policy** submission link expiration options:
 - a) To set time-based link expiration, select **Invitation link expires** and set the number of days Faspex keeps the link available.
 - b) To set download-based link expiration, select **After one successful upload**. The link expires after an outside submitters uploads one package.



Warning: When outside submitters are invited to access a dropbox, they are not prevented from sharing the upload link with others. Faspex records the IP address used to submit packages, but Faspex cannot verify that the person using the link is the intended contributor. If this is a concern to your organization, you can identify one of two security options when sending an invitation to an outside submitter: the submission link expires after one successful upload completion or the submission link expires on a specific date. In the case of expiration after the completion of a successful upload, it *is* possible for an outside submitter to initiate parallel uploads using a single link to submit multiple packages.

6. Click **Save** to send an invitation email to the email address with the submission link.

You can configure your invitation email by modifying the email template. For more information on configuring email templates, see [Configuring Email Notification Templates](#) on page 138.

Note: After inviting an outside submitter, you can view the upload access URL or resend the invitation. Go to **Workgroups** and select your dropbox. Select **View Members**. Find the outside contributor in the members list and select either **see access URL** or **resend invitation**.

Working with Relays

What is a Relay?

Relays transfer copies of uploaded files to specified destinations (custom inboxes). There are two types of relays: package relays and file relays.

Overview

There are three types of transfers to Faspex file destinations: direct uploads, package relays, and file relays.

Transfer type	Description	Starts when	Transferred files directory structure on the destination node
Direct upload	A direct upload transfers files to the default inbox or to a custom inbox with direct upload configured. Faspex makes these files available to the designated recipients. Faspex also uses these files when performing a relay.	A user sends a package to a recipient, workgroup, or dropbox.	<pre> package_title - package_id.aspera- package/ -- PKG - package_title -- folder1 -- file1 -- file2 </pre>
Package relay	A package relay transfers copies of files uploaded to a source node to specified nodes. Package relays preserve the package directory structure.	<p>A user sends a package to a workgroup or dropbox with a custom inbox that does not have direct upload configured.</p> <p>A user sends a package with relay metadata (see Using Metadata Fields to Set Relay Destinations on page 108).</p>	<pre> package_title - package_id.aspera- package/ -- PKG - package_title -- folder1 -- file1 -- file2 </pre>
File relay	A file relay transfers copies of files uploaded to a source node to specified nodes. File relays do not preserve the package directory structure.	A user sends a package to a workgroup or dropbox with relays configured.	<pre> folder1 -- file1 file2 </pre>

Order of Operations

If a transfer triggers both package and file relays, Faspex performs transfers in this order:

1. Direct upload
2. Package relay
3. File relay

If the direct package upload fails, Faspex does not relay the package to custom inboxes or file relay destinations.

If the direct package upload succeeds, Faspex performs both relays. If the package relays fail, Faspex still performs the file relays.

Package Relays

A package relay transfers copies of files uploaded to a source node to specified nodes. Package relays preserve the package directory structure.

When a user uploads files to a custom inbox with direct upload or to the default inbox, Faspex creates the following package directory structure on the destination node:

```
package_title - package_id.aspera-package/
|-- PKG - package_title
|   |-- folder1
|       |-- file1
|       |-- file2
```

Once the initial transfer to the initial destination node has completed, then Faspex starts the package relay to copy that entire directory structure to the new destination. The new destination can be:

- A workgroup or dropbox custom inbox without direct upload configured.
- Destinations specified by package metadata.

File Relays

A file relay transfers copies of files uploaded to a source node to specified nodes. File relays do not preserve the package directory structure. File relays transfers files to storage in a flat structure. This is ideal for ingesting files without having to parse nested data from package structure (such as providing files for API consumption).

File Relay Options

When you configure file relays on a workgroup or dropbox, you can set the file relay to overwrite existing files with the same name at the destination. By default, Faspex skips files with the same name that exist at the destination node.

You can also configure email notifications for file relays. In the **Server > Notifications** section, you can use the **Relay Started CC** email template to notify users when package forwarding is started, a **Relay Finished CC** email template to let users know when package forwarding is completed, and a **Relay Error CC** email template to notify users when package forwarding has failed. For details see [Configuring Email Notification Templates](#) on page 138.

Comparing File Relays to Package Relays

When a user uploads files to a custom inbox with direct upload or to the default inbox, Faspex creates the following package directory structure on the destination node:

```
package_title - package_id.aspera-package/
|-- PKG - package_title
|   |-- folder1
|       |-- file1
|       |-- file2
```

File relays do not preserve this directory structure, but transfers the contents of the package in a flat structure to the destination node:

```
folder1
|-- file1
file2
```

If the destination node already had the `existing_file1` and `existing_folder1` files, the resulting directory snapshot would be:

```
existing_file1
existing_folder1
|-- existing_file2
folder1
|-- file1
file2
```

Tracking Relay Progress and Status

You can track the progress of a relay by going to **Server > Packages > Relay**.

Faspex reports the following relay statuses:

- Uploading
- Complete
- Relaying
- Complete or Error

If a transfer triggers both package and file relays, Faspex first reports the package relay status. If the package relay succeeds, Faspex then reports the file relay status. However, if the package relay fails, Faspex reports the error and does not report the file relay status.

Note: The **Server > Packages > Relay** page lists ongoing and failed relays, but does not list successful relays.

Using Metadata Fields to Set Relay Destinations

Use the `SenderShareId`, `RecipientShareIds`, `OverrideShareIds` metadata fields to configure relays for a package upload.

Metadata field names for relay destinations use the term *share*. A *share* in this context is a file storage used as a relay destination.

You use the `share_id` of a file storage to designate it as a relay destination. To determine the `share_id` of a file relay destination, go to **Server > File Storage**, select the node, and click **Edit** from the drop-down menu. Find `share_id` in the page URL.

For example, if the page URL is `https://faspex.aspera.us/aspera/faspex/admin/nodes/4/edit`, the `share_id` is 4.

Metadata field	Description	Format	Example
<code>SenderShareId</code>	Defines the file storage destination (defined by <i>share_id</i>) for the initial upload of a new package. If set, override the default inbox storage setting in Faspex with the file storage destination. If not set, use the default inbox destination as the file storage destination. Use <code>SenderShareId</code> to control where the	<i>share_id</i>	3

Metadata field	Description	Format	Example
	sender uploads to and downloads the sent package from. When the sender downloads the package from the Sent page, Faspex transfers the package to the sender from this file storage.		
RecipientShareIds	<p>Defines extra recipients (defined by <i>user_name</i>) and their respective file storage locations (defined by <i>share_id</i>). Faspex performs a package relay transfer from the initial transfer destination to the targets defined in the metadata.</p> <p>Use RecipientShareIds to control where recipients download the package from. When recipients download the package from the Received page, Faspex transfers the package to the recipients from the specified file storages.</p>	<pre>{ "user_name": share "another_user": sha ... }</pre> <p>Note: Value must be valid JSON.</p>	<pre>{ "admin": 4, "other_user": 5 }</pre>
OverrideShareIds	Defines additional file relays from the initial transfer destination host to designated file storages (defined by <i>share_id</i>).	<p>[<i>share_id</i>, ...]</p> <p>Note: Value must be valid JSON.</p>	[1, 2, 3]

Example

share_id	Node for file storage with specified share_id
1	node1 (default inbox)
2	node2
3	node3
4	node4
5	node5

The sender (sender_user) sends a package to the recipients (recipient_user1, recipient_user2, and recipient_user3) and configures file transfers using the metadata:

- **SenderShareId** = 2
- **RecipientShareIds** = recipient_user1: 3, recipient_user2: 4
- **OverrideShareIds** = 5

Faspex performs the following transfers:

1. Faspex uploads the package directly to node2.
2. Faspex performs a package relay from node2 to node3 and node4.
3. Faspex performs a file relay from node2 to node5.

When a user downloads the uploaded package, Faspex uses the metadata to determine from which node to serve the content:

User	Downloading from	Package source node
sender_user	Sent page	node2 (share_id: 2)
recipient_user1	Received page	node3 (share_id: 3)
recipient_user2	Received page	node4 (share_id: 4)
recipient_user3	Received page	node2 (share_id: 2)

In this scenario, the sender uploads the package to the node2 as defined by the `SenderShareId`, and not the server-default inbox. When `recipient_user3` (who is not defined in `RecipientShareIds`) downloads the package, the user downloads from node2, since there is no package in the server-default inbox. In this scenario, Faspex treats the share configured with **SenderShareId** as the default inbox.

Working with Directory Services (DS)

Review Directory Service Requirements

IBM Aspera Faspex supports the Lightweight Directory Access Protocol (LDAP) and can be configured to connect to a directory service. The following directory service databases are supported:

- 389/Red Hat/Fedora Directory Server
- Apple Open Directory
- Microsoft Active Directory (AD)

Important Information

- Directory service syncing is accomplished through a Faspex background service that must be kept running.
- When removing a directory service group, users in that group are deactivated instead of removed.
- When an user exists in multiple directory service groups, removing one of the groups doesn't affect the user. The user is deactivated only when all the user's directory service groups are removed.
- An activated directory service group is shown as "Active" in the status column. If it shows otherwise, click **View Operation History** to read the Active Directory operation log and identify the problem.
- Directory services and SAML should not be enabled together.

Adding a Directory Service to Faspex

1. Go to **Server > Authentication > Directory Services**.
2. To configure your directory service to work with IBM Aspera Faspex, check **Enable Directory Service** and enter your configuration details (example displayed below).

Option	Description
Directory Service Name	Your name for this directory service.

Option	Description
Enable Directory Service	Activate this directory service for Faspex.
Directory Service Type	Select from one of the following options: <ul style="list-style-type: none"> • 389/Red Hat/Fedora Directory Server • Apple Open Directory • Microsoft Active Directory (AD)
Use secure mode (TLS)	Note: <i>Aspera highly recommends turning this setting on to secure your server.</i> By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by enabling TLS. The port number will automatically change to 636 when TLS is enabled.
Server	The directory server's address.
Port	The directory server's port number. By default, unsecured LDAP uses port 389, unsecured global catalog uses port 3268, and global catalog over SSL uses port 3269. If TLS is enabled, then the port number automatically changes to 636.
Treebase	The search treebase (<i>for example, dc=myCompany,dc=com for myCompany.com</i>)
Username Attribute	The attribute for the type of login name for users of this directory service. For example, for Microsoft Active Directory, the mail attribute specifies the DS user login should be an email address, and samaccountname specifies it should be a pre-Windows 2000 login name.
Login Method	<ul style="list-style-type: none"> • Anonymous • Provide Credentials <p>If <i>Provide Credentials</i> is selected, then you are required to input your directory service login and password below.</p>
Login	Directory service user name, which is typically a Distinguished Name (DN) (for example, CN=Admin,CN=Users,DC=myCompany,DC=com).
Password	Directory service password.

When finished, click **Save and Test**. If Faspex successfully connects to your directory server, it displays the following information:

```
Connected: YES
Authenticated: YES
Success
```

Note: If the same user (identified by the username attribute) is a member of more than one directory, the user is only imported once from the first sync. The duplicated user from the second directory is not imported, and a warning is logged in the sync history.

Import Directory Service Groups

Important: When IBM Aspera Faspex imports Active Directory (AD) groups, it is bounded by the AD server parameter "MaxValRange." If you want to import a larger AD group, change the "MaxValRange" parameter on your AD server.

When importing a Directory Service group, all users listed under that group are added into Faspex. To import a group, start by going to **Accounts** and select the **Directory Service Group** tab. Any DS groups that you have previously imported are shown in the list.

1. Click the **+ New Group** button and enter the directory service group attributes.

Typing three characters or more brings up the group list with matching keywords.

Important: All DS groups must have unique names. You cannot import multiple Directory Service (DS) groups of the same name, regardless of whether they are on the same DS server.

2. Click **Edit Additional Permissions** to specify permissions for the DS group.

For more information on setting additional permissions for the DS group, see to [Configure User Settings](#) on page 209.

3. Click **Done > Import** when finished.

When adding directory service groups, Faspex searches for groups recursively to import users. For example, if group A contains Group 1, importing Group A also imports Group 1's members. Once imported, the directory service group's members are added to Faspex and the import page is updated with a link to view or edit the new group.

Click the **View** link to go back to the **Accounts** screen. Your imported DS users appear in the accounts list, along with the type column identification *DS*.

Import Individual Directory Service Users

1. Go to **Accounts > Users > +Add Account > Directory Service User**.
2. Select the directory service that contains the users you want to import from the Directory Service (DS) drop-down box.
3. In the Search Term box, enter a search string or substring for the user you want.
A list of DS user accounts containing that string is displayed.
4. Select the name of the user to import. You can only import one user at a time.
5. Click **Edit Additional Permissions** at the bottom of the page.

In the page that appears, fill in the **Account Details** section, specifying whether this user is an admin, a manager, or a regular user. Then scroll down and fill in **Permissions**, **Package Deletion**, and other remaining sections.

Important: IBM Aspera Faspex syncs individual directory service users every hour. You cannot sync them manually.

Once directory service users (or groups) are imported, the corresponding users can authenticate with and log in to Faspex. Directory service accounts are similar to Faspex user accounts, although options such as changing the login password are deactivated (since this information is configured on the directory server).

Working with SAML

SAML and Faspex

IBM Aspera Faspex supports Security Assertion Markup Language (SAML) 2.0, an XML-based standard that allows secure web domains to exchange user authentication and authorization data. With the SAML model, you can configure IBM Aspera Faspex as a SAML *online service provider (SP)* that contacts a separate online *identity provider (IdP)* to authenticate users. Authenticated users can then use IBM Aspera Faspex to access secure content.

With SAML enabled, IBM Aspera Faspex redirects a user to the IdP sign-on URL. The user signs in with the IdP and the IdP sends a SAML assertion back to IBM Aspera Faspex. When a SAML user logs in to IBM Aspera Faspex for the first time, IBM Aspera Faspex automatically creates a new user account based on the information provided by the

SAML response. Any changes subsequently made to the account on the DS server are not automatically picked up by IBM Aspera Faspex. For more information about user provisioning for SAML users, see [User Accounts Provisioned by Just-In-Time \(JIT\) Provisioning](#) on page 114.

IdP Requirements

To use SAML with IBM Aspera Faspex, you must already have an identity provider (IdP) that meets the following requirements:

- Supports SAML 2.0
- Able to use an HTTP POST Binding.
- Able to connect to the same directory service that IBM Aspera Faspex uses.
- Not configured to use pseudonyms.
- Can return assertions to IBM Aspera Faspex that include the entire contents of the signing certificate.
- If prompted, set to sign the SAML response. (Signing the SAML assertion is optional.)

Configure the SAML IdP

Before configuring SAML in IBM Aspera Faspex, make sure you configure your IdP to send a correct SAML response to IBM Aspera Faspex. For more information, see [Configuring Your Identity Provider \(IdP\)](#) on page 115.

For instructions on configuring SAML, see [Creating a SAML Configuration in Faspex](#) on page 116.

SAML and Directory Services

IBM Aspera Faspex supports the use of both SAML and directory services. If you configure both services to IBM Aspera Faspex, ensure the services use different Active Directory domains. Aspera advises against configuring LDAP directly to IBM Aspera Faspex if the SAML IdP acts as a frontend for the same Active Directory domain.

Multiple SAML Configurations in Faspex

Faspex supports multiple SAML configurations on the same server. Faspex redirects users to the default SAML IdP, but if no default is specified, Faspex directs users to the local login page where users can choose to log into publicly visible SAML configurations or log in locally.

In the following example, East Department and West Department are the names of two SAML configurations.

The image shows a web form titled "Faspex Login". Below the title is the instruction "Use this option to log in with your Faspex account". There are two input fields: "Username" and "Password". Below the password field is a link "Forgot password". A "Log In" button is positioned below the links. A horizontal line with the text "or log in with" is below the button. Underneath, there are two sections: "East Department log in here." with an "East Department" button, and "West Department log in here." with a "West Department" button.

To configure multiple SAML configurations in Faspex, first create a new SAML configuration (see [Creating a SAML Configuration in Faspex](#) on page 116) and then configure a domain URL for the configuration (see [Configuring a Domain URL for SAML](#) on page 118).

Bypassing the Default SAML IdP

IBM Aspera Faspex provides a mechanism for users to bypass the SAML redirect and log in using a local username and password. This feature allows admins to correct server settings, including a mis-configured SAML setup, without logging in through SAML.

To bypass the SAML login, add `login?local=true` to the end of the login URL. For example:

```
https://198.51.100.48/login?local=true
```

If users need to access a SAML IdP that is not the default IdP, users can use domain URLs to directly access a SAML configuration. For more information, see [Bypassing the SAML Redirect](#) on page 121.

User Accounts Provisioned by Just-In-Time (JIT) Provisioning

When a SAML user logs in to IBM Aspera Faspex for the first time, IBM Aspera Faspex automatically creates a new user account based on the information provided by the SAML response. If the SAML response also contains group information, and that group does not yet exist in IBM Aspera Faspex automatically creates a new SAML group for each group of which the user is a member. For more information about SAML groups, see [Creating SAML Groups](#) on page 117.

Note: If an admin enables the **Restrict access to known groups** feature for the SAML configuration, only members of existing IBM Aspera Faspex SAML groups can log in. This also means that new SAML groups are not automatically created when SAML users log in. For more information about SAML configuration options, see [Configure SAML Options](#) on page 119.

SAML Users and External Users

When a SAML user logs in to IBM Aspera Faspex checks for existing external users matching the email address of the SAML user. If such a user exists, IBM Aspera Faspex merges the two accounts.

Group Permissions

A SAML user belonging to multiple groups is given the permissions and settings of all groups it belongs to with permissions overriding restrictions. For example, if Group A disallows sending to external users but Group B does not, users who belong to both groups are allowed to send to external users. Settings that require specific handling are as follows:

- Account expiration is only enabled if all groups to which a user belongs specify account expiration. If account expiration is enabled, the expiration date is set to the latest expiration date from among all groups.
- For any settings that use **Server Default**, **Yes** or **Allow**, and **No** or **Deny**, the setting is set to **Yes** if any group specifies **Yes**, and it is set to **No** if all groups are set to **No**. Otherwise, it is set to use the server default.
- For package deletion policy, override is enabled if all groups specify override, or if the least restrictive group setting is less restrictive than the server-wide setting. If override is enabled, the least restrictive group setting is used. **Do nothing** is less restrictive than **Delete files after all recipients download all files**, which in turn is less restrictive than **Delete files after any recipient downloads all files**.
- For advanced transfer settings, override is enabled if all groups specify override or if any group specifies any transfer rate that is higher than the server default. If override is enabled, each transfer rate is set to the higher of the highest value from among the groups and the server default. The minimum rate policy is locked only if all groups specify the setting.

For more information on these settings, see [SAML Group Permissions](#) on page 121.

Configuring Your Identity Provider (IdP)

IdP Requirements

To use SAML with IBM Aspera Faspex, you must already have an identity provider (IdP) that meets the following requirements:

- Supports SAML 2.0
- Able to use an HTTP POST Binding.
- Able to connect to the same directory service that IBM Aspera Faspex uses.
- Not configured to use pseudonyms.
- Can return assertions to IBM Aspera Faspex that include the entire contents of the signing certificate.
- If prompted, set to sign the SAML response. (Signing the SAML assertion is optional.)

IdP Metadata Formats

You must configure formats to set up your IdP to work with IBM Aspera Faspex:

Tag	Format
NameID Format	Faspex supports the following formats: <ul style="list-style-type: none"> • urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified • urn:oasis:names:tc:SAML:1.1:nameid-format:transient • urn:oasis:names:tc:SAML:1.1:nameid-format:persistent • urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Entity ID	<code>https://faspex_ip/aspera/faspex/auth/saml/metadata/saml_id</code>
Binding	<code>urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST</code>
Callback URL	<code>https://faspex_ip/aspera/faspex/auth/saml/callback?id=saml_id</code>

If the IdP is capable of reading SAML XML metadata for a service provider, you can upload a saved XML metadata file to configure the IdP. You can retrieve the XML metadata for an existing IBM Aspera Faspex by going to `https://server_ip/aspera/faspex/auth/saml/metadata/saml_id` and saving the XML as an XML file.

Note: The *saml_id* specifies the SAML configuration. For example, in the case of multiple SAML configurations, the first configuration is associated with the SAML ID "1", the next configuration "2", and so on.

SAML Assertion Requirements

IBM Aspera Faspex: expects assertion from an IdP to contain the following elements:

Default Attribute	IBM Aspera Faspex User Field	Required
NameID / SAML_SUBJECT	Username	Yes, with the format: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
email	Email address	Yes
given_name	First name	Yes
surname	Last name	Optional
member_of	SAML group	Necessary for SAML groups

Tip: You can configure the IBM Aspera Faspex user fields to map to different attributes in the IBM Aspera Faspex SAML configuration settings.

Creating a SAML Configuration in Faspex

Before configuring SAML in Faspex, make sure you have properly configured your SAML IdP (see [Configuring Your Identity Provider \(IdP\)](#) on page 115).

1. In Faspex, go to **Server > Authentication > SAML Integration**.
2. Optional: Import a SAML IdP's metadata to auto-populate the fields for SSO URL, fingerprint, and certificate. You can import from a URL, from a saved file, or from pasted text. Click **Import Settings From Metadata URL**.
3. Enter a name for your configuration in the **Name** field. This name is used by Faspex to differentiate between multiple SAML configurations.
4. Optional: Configure the following SAML options.
 - **Publicly Visible:** Determines whether Faspex allows users to choose this IdP as an option from the local login page.
 - **Public Login Instructions field:** Displays a description of the IdP and instructions on how to log in.
 - **Restrict access to known groups:** Prevents SAML users that are not members of existing Faspex SAML groups from logging into this IdP.
 - **Default SAML Configuration:** Determines if accessing the Faspex URL redirects to this IdP or the local faspex login page.
 - **Domain URL:** Directs users to this IdP when they access this alternate URL. For more information, see [Configuring a Domain URL for SAML](#) on page 118.

For more information on these options, see [Configure SAML Options](#) on page 119.

If you chose to import a metadata file, the **SSO target URL**, **Name ID Format**, **Fingerprint**, and **Certificate** fields have already been auto-populated with information.

5. In the **SSO target URL** field, enter your IdP Single Sign-On URL.
6. Choose the **Name ID Format** used to authenticate with the SAML IdP.

The Name ID format must match the format used with your IdP. Faspex supports the following formats:

Unspecified, **Transient**, **Persistent**, or **Email Address**. When set to **Unspecified**, any Name ID format returned by the IdP is accepted.

7. Enter the IdP **Fingerprint** or **Certificate**. Only one of these two fields is required to authenticate with the SAML IdP.
8. Optional: In the **Allowable clock drift** field, configure the milliseconds allowed for clock drift between Faspex and the SAML IdP.
9. Configure the default profile fields. These fields must map to attributes in your SAML IdP's SAML response. Enter the **SAML Name** for each of the required fields: **username**, **email**, **first_name**, and **last_name**.

Important: Once you set the value for **username**, do not change it. If **username** is changed, existing SAML users can no longer log into their existing Faspex accounts, but are instead given new accounts with new usernames.

10. Optional: Configure local custom profile fields.

These are custom user attributes that only apply to this IdP. **Name** is the name of the attribute displayed in Faspex. **SAML Name** is the name of the attribute as configured in the IdP. To add a field, click **Add Local Profile Field**. For more information, see [Setting Up Custom SAML Fields](#) on page 120.

Note: If you've configured custom attributes (**Server > User Profile**), these fields show up as Global Custom Profile Fields that, if required, you must map to valid SAML names. For more information about custom attributes, see [Configuring Custom User Fields](#) on page 74.

11. Click **Create SAML Configuration**.

After creating a new SAML configuration, Faspex redirects you to the SAML Configurations page and displays the existing SAML configurations.

Users can now access Faspex through SAML instead of going through the local login page. For information about bypassing the SAML redirect, see [Bypassing the SAML Redirect](#) on page 121.

Creating SAML Groups

SAML groups are created in IBM Aspera Faspex one of two ways:

- Creating a SAML group in IBM Aspera Faspex using the application and then logging in as a SAML user in the new group. The IBM Aspera Faspex SAML group is mapped to the external SAML group.
- Logging in using SAML credentials creates a Shares SAML group mapped to the external SAML group.

The following instructions describe how to create a SAML group in IBM Aspera Faspex using the web application.

1. When SAML is enabled, you can create SAML groups by navigating to **Accounts > SAML Groups**.
2. Click **New Group** to create a SAML group.
3. Enter the group name, which is the distinguished name (DN).

For example: CN=Aspera Group, OU=Groups, Ou=asperaex, DC=aspera, DC=

4. Click **Edit Additional Permissions** to configure parameters such as keeping the user directory private, IP addresses for downloading and uploading, and package deletion parameters.
5. Click **Create** to create the SAML group.

To view and manage your SAML group, click **Actions** to activate, deactivate, or remove existing groups. The Sync option is not available for SAML groups.



Note: If a user belongs to only one group and that group is deactivated, the user cannot login anymore. However, if a user belongs to multiple groups and at least one of these groups is active, the user is able to log in.

Configuring a Domain URL for SAML

These instructions assume you have already created a SAML configuration in Faspex. For instructions to do so, see .

Domain URLs allow users to directly access a SAML IdP. A user may use a domain URL to bypass the default SAML IdP if the user is not a member of that IdP. Configuring a domain URL requires you to access Faspex through a browser to access the metadata file for the SAML configuration.

1. Go to **Server > Authentication > SAML Integration** and select your SAML configuration.
2. Enter an alternate hostname in the **Domain URL** text field. For example, you may enter `shibboleth.faspex.example.com`.

Note: Verify with your IT department that the domain URL resolves to your Faspex server's hostname in your DNS.

3. Click **Update SAML Configuration**.
4. Go to the SAML Configurations page in Faspex (**Server > Authentication > SAML Integration**). Click the **Metadata** link.

Faspex redirects you to page displaying the metadata in XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  ID="_2b0828b0-bf02-0133-9ed1-0050569f0e72"
  entityID="https://10.0.200.158/aspera/faspex/auth/saml/metadata/1">
  <md:SPSSODescriptor AuthnRequestsSigned="false"
    WantAssertionsSigned="true"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    </md:NameIDFormat>
    <md:AssertionConsumerService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://10.0.200.158/aspera/faspex/auth/saml/callback?
        id=1" index="0" isDefault="true"/>
    </md:SPSSODescriptor>
  </md:EntityDescriptor>
```

5. Change the URL in the browser to match the domain URL's hostname instead of the Faspex IP address. The domain URL's hostname is represented by the `entityID` attribute in the `<md:EntityDescriptor>` XML tag.

For example, if your Faspex IP address is **198.51.100.24**, your metadata URL may be:

`https://198.51.100.24/aspera/faspex/auth/saml/metadata/1`. If your domain URL is **shibboleth.faspex.example**, change the URL to `https://shibboleth.faspex.example/aspera/faspex/auth/saml/metadata/1`.

Enter the new URL in your browser and go to that page.

6. Save the page as an XML file to your machine.

7. Follow the instructions provided by your IdP to configure the domain URL's metadata in the IdP.

Once configured in your SAML IdP, accessing the domain URL redirects you to the IdP. Log in to the IdP to access Faspex.

Configure SAML Options

To configure an existing SAML IdP, go to **Server > Authentication > SAML Integration** and click the name of the IdP.

Option	Description
Name	Give this configuration a name.
Publicly Visible	<p>Determine whether Faspex allows users to choose this IdP as an option from the local login page. If selected, Faspex displays this IdP as a login option. If not selected, Faspex does not display this IdP and users must access the IdP using a domain URL.</p> <p>Note: If the admin does not specify a SAML configurations as the default, Faspex automatically redirects users to the local login page. For more information on bypassing the SAML redirect, see Bypassing the SAML Redirect on page 121.</p>
Public Login Instructions	This option becomes available when Publicly Visible is selected. Enter a description of the IdP and specify instructions for logging into the IdP.
Restrict access to known groups	<p>Prevent SAML users that are not members of existing Faspex SAML groups from logging into this IdP. If a user is a member of multiple groups, the user can log in as long as one of those groups exists in Faspex.</p> <p>Note: If this feature is enabled, Faspex does not create new groups for users that are a member of multiple SAML groups. For more information about automatically creating new groups, see User Accounts Provisioned by Just-In-Time (JIT) Provisioning on page 114. For more information about SAML groups, see Creating SAML Groups on page 117.</p>
Redirect to SAML logout page on logouts	When SAML users log out of Faspex, they are redirected to the SAML logout page instead of the local login page. From the SAML logout page, users can log back into Faspex with SAML.
Restrict access to known users	Prevent users that are not existing Faspex SAML users from logging into this IdP.
Default SAML Configuration	<p>Determine if accessing the Faspex URL redirects users to this IdP or to the local Faspex login page. If selected, accessing the Faspex URL directs them to this IdP. If not selected, users arrive at the local login page instead.</p> <p>Note: Setting a default SAML configuration does not affect the workflow for client applications such as IBM Aspera Drive. Even if a configuration is set as default,</p>

Option	Description
	the client application still presents all public SAML configurations.
Domain URL	<p>Enter an alternate Faspex domain URL that directs users to this IdP when they access it. This URL overrides the default URL.</p> <p>Tip: You do not need to enter a full URL. For example, you can use <code>idp.faspex.com</code> instead of <code>https://idp.faspex.com</code>.</p> <p>Domain URLs require further configuration. For more information, see Configuring a Domain URL for SAML on page 118.</p>

Setting Up Custom SAML Fields



Faspex can import SAML fields in your SAML identity provider (IdP) as user profile fields. (For more information on user profile fields, see [Configuring Custom User Fields](#) on page 74).

You can import different custom fields for each individual IdP.

1. Add new SAML fields in your SAML identity provider. These fields must be correctly mapped to the SAML directory service.
2. Go to **Server > Authentication > SAML Integration** and click the SAML configuration for which you want to configure custom attributes.

Go to the Attribute Mapping section and add custom fields to Local Custom Profile Fields. These are custom user attributes that only apply to this IdP. Click **Add Local Profile Field** for each field you want to configure.

The following section describes configuration options for a SAML custom field:

Configuration Option	Description
Enabled	Select this box to enable or disable the custom field. (Fields are enabled by default.)
Name	Enter the desired name of your custom field into the text box. This field applies to Local users.
SAML Name	<p>Enter the name of the SAML field found in your IdP.</p> <p>Important: The Faspex SAML Name must be correctly mapped to your SAML fields in IdP. If the names are incorrectly mapped, Faspex rejects the user login. For more information on custom SAML fields, see Setting Up Custom SAML Fields on page 120.</p>
Required	Require that a SAML response includes the SAML name mapped to this custom field. SAML user login fails when the field is required, but the SAML response does not include the required custom attributes.
	<p>Click the  button to delete a field. Faspex opens a pop-up that prompts you to confirm by clicking OK to delete the field.</p> <p>Note: Deleting a field permanently deletes the custom field and all its data from all existing users.</p>

3. Click **Update SAML Configuration**.

Bypassing the SAML Redirect

If Faspex has been configured with a default SAML IdP for authentication, Faspex automatically redirects you to the SAML login page of the default SAML IdP. If you need to authenticate with a different SAML IdP, you can access the correct IdP through the methods below.

Logging In to a SAML IdP from the Local Login Page

To bypass the automatic redirect and go to the local login page, add `login?local=true` to the end of the Faspex url. For example:

`https://192.51.100.24/aspera/faspex/login?local=true`.

On the local login page, you can choose to log in with the SAML IdPs an admin has chosen to display on the local login page.

Accessing a SAML IdP Using a Domain URL

Admins can configure a domain URL for a SAML IdP, which users can access to authenticate to Faspex with the corresponding IdP. If an admin has configured a domain URL for your IdP, you can follow that URL to authenticate with that IdP. need to access a SAML IdP that is not the default IdP, you can use domain URLs to directly access a SAML configuration. For more information on configure domain URLs, see [Configuring a Domain URL for SAML](#) on page 118.

SAML Group Permissions

Account Details

Option	Description
Account expires	Select to set an expiration date for users in this group. All users in this SAML group become inactive on the expiration date.

Permissions

Option	Description
Allowed to	<ul style="list-style-type: none"> • Uploads allowed: Select to allow users to send packages. • Downloads allowed: Select to allow users to download received packages. A user who does not have download permissions still receives packages, but cannot download the files. • Forwarding allowed: Select to allow users to forward received packages to other users. The package becomes available to the forwarded users in their Faspex accounts. • Can create from remote: Select to allow users to create a package from a remote source such as a remote server. Users allowed to access remote sources can access the Source drop-down menu when sending a new package. <p>You must first add remote sources to Faspex to see the Source drop-down menu. For more information on adding remote sources, see Adding a Node to Faspex on page 59.</p> <p>Note: This setting is disabled by default and must be set on a per-user basis (in other words, there is no global option).</p>

Option	Description
Allow inviting external senders	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable this user to invite users without Faspex accounts to upload a package to Faspex.</p>
Allow public submission URLs	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable users to send a Public URL to users without Faspex accounts. These external users can submit packages to registered Faspex users through this public URL. For more information about Public URLs, see Configuring Public URLs on page 91.</p> <p>Note: Even if the Public URL feature is enabled for registered Faspex users, they can override the feature for their own account by going to their user Account > Preferences > Misc and clearing Enable public URL.</p>
Can send to external email	<p>Select Allow to allow users to send packages to external email addresses.</p> <p>Faspex sends a download link through email. By default, this link expires after three days, but admins can change the duration or disable expiration by going to Server > Security. For more information, see Configuring Security Settings on page 47.</p>
Can send to all faspex users	<p>Select Allow to allow users to send packages to all Faspex users.</p> <p>If this feature is enabled, all existing Faspex users appear in the contact list. If disabled, users can, only send packages to members of workgroups they are part of.</p>
Keep user directory private	Select Yes to prevent users from being able to see the entire user directory, even if they have permissions to send to all Faspex users.
Can see global distribution lists.	Select Yes to give users access to global distribution lists. For more information on global distribution lists, see Creating a Global Distribution List on page 129.
Allowed IP addresses for login	Specify the IP addresses that a Faspex user can login from. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1, 198.51.100.2, 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for download	Specify the IP addresses that a Faspex user can login from to download packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1, 198.51.100.2, 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for upload	Specify the IP addresses that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1, 198.51.100.2, 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).

Package Deletion

Select from the following options to specify behavior after downloading a package:

Option	Description
After download	<p>You can override the server default by selecting Override system default. If you choose override, select one of the following policies:</p> <ul style="list-style-type: none"> Do nothing: Do not auto-delete after the package is downloaded.

Option	Description
	<ul style="list-style-type: none"> • Delete files after any recipient downloads all files: Delete after <i>any</i> recipient downloads <i>all</i> files in the package once. <p>Important: When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option.</p> <ul style="list-style-type: none"> • Delete files after all recipients download all files: Delete if <i>all</i> files in the package have been downloaded by <i>all</i> recipients.
Allow user to set own delete setting on a package-by-package basis	Select Allow to allow this user to choose a package expiration policy when sending a new package.

Advanced Transfer Settings

By default, Faspex uses the transfer settings from the Aspera Central Server section. Select **Override default settings** to set user-specific transfer settings, which take precedence over the server-wide settings.

Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option Lock minimum rate and policy is checked, the user is not able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the maximum upload and download transfer rate for this user.

Customizing SAML Error Messages

You can customize SAML error messages by modifying them in the **en.yml** error configuration file.

Open the **en.yml** error configuration file in a text editor. You can find the **en.yml** file at: `/opt/aspera/faspex/config/locales/en.yml`

```
...

login:
  new:
    login: Log In
    login_using_saml_idp: Log in using SAML IdP
  logged_out:
    message: You have been logged out of Faspex; you might still need to
log out of your corporate single-sign-on account.
    log_in_again: Log in again
  errors:
    saml_not_authorized: You are not authorized to use Faspex
    invalid_saml_response: Invalid response from SAML Identity Provider.
    saml_login_failed: Login Failed.
    saml_exception: SAML response Error. Please check the logs.

...
```

Managing User Self-Registration

Enabling Self-Registration

IBM Aspera Faspex gives you the ability to allow non-registered users to request accounts on the Faspex login page. This relieves the workload of admins and managers. You must ensure that proper security settings have been put into place before allowing self-registration.

1. The self-registration feature is turned off by default. Go to **Server > Security** and find the Registrations section.
2. From the **Self registration** drop down menu, choose between three options:
 - **None**: Self-registration is not allowed.
 - **Moderated**: An admin must approve the account before it is created.
 - **Unmoderated**: Once a user registers an account, the account is automatically created.

If you allow self-registration, Aspera recommends you use the **Moderated** setting for security purposes.



Warning: If self-registration is enabled, a user can use it to find out whether a certain account exists on the server. If a user attempts to self-register a duplicate account, then the user receives a prompt stating that the user already exists.

3. Configure the moderation settings in the table below:

Configuration	Description
Terms of service	If text is set, Faspex requires users to accept the terms of service in order to register an account
Notify the following emails to approve	The email addresses Faspex notifies for moderation. This option is only available if you are using the Moderated self-registration setting Note: These email addresses are not validated against existing Faspex admins or managers, but only admins and managers can approve account requests.
Block the following email domains from self-registering	New users are not allowed to register accounts using emails from these email domains
Require external users to register	Require external users to register a Faspex account to download packages
Registration instructions	Text that appears above the Create an account button on the Faspex login page
Self-registered users are allowed to send packages to one another	Self-registered users can send packages to other self-registered users.

4. Click **Update** to save changes.
5. (Optional) To prevent a self-registered account from having the same email address as a full Faspex user, admins can add a special option to **faspex.yml**.

You find **faspex.yml** in the following directory:

```
/opt/aspera/faspex/config/faspex.yml
```

Inside **faspex.yml**, within the Production section, paste the following option and set it to **true**:

```
EnforceSelfRegisteredUserEmailUniqueness: true
```

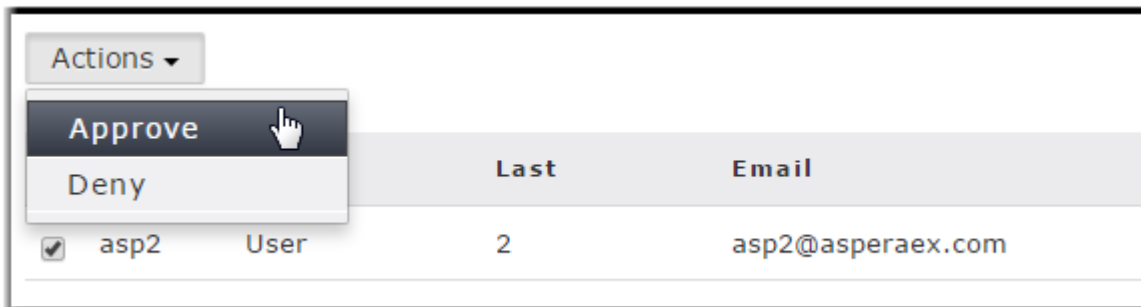
If users are allowed to self-register, they see the option to **Create an account** on the login page. After a user clicks this button and completes the form, admins are required to **Approve** or **Deny** the account. For more information on approving or denying accounts, see [Approving or Denying Pending Registrations](#) on page 125.

After a user self-registers, the new account inherits the permissions of the configured template user and automatically becomes a member of designated workgroups. To configure the template user, go to **Accounts > Pending Registrations** and click the **template user** link. For more information about configuring the template user, see [Configure Self-Registration Template User](#) on page 125.

Approving or Denying Pending Registrations

This topic assumes that you have turned on the **Moderated** self-registration setting. For more information on enabling self-registration, see [Enabling Self-Registration](#) on page 124.

1. Go to **Accounts > Pending registrations** to manage requests. Once a user self-registers, the request appears in the Pending Registrations page.
2. Select a pending registration or group of pending registrations.
3. Select either **Approve** or **Deny** from the **Actions** drop-down list.




Approved users automatically inherit the permissions of the template user and will become members of a workgroup, if configured to do so. For more information about the template user, see [Configure Self-Registration Template User](#) on page 125. After creation, you can update the permissions and workgroup memberships of these users from the **Users** tab.

Configure Self-Registration Template User

Changing Permissions for the Template User

When self-registration requests are approved, the new users inherit the permissions of the template user. This user has default settings, which you can view and modify by clicking **template user** link. On the **Edit Template User** page, you will find the following settings:

Option	Description
New accounts will expire	<p>Enable this setting if you would like a self-registered user's account to expire after a set number of days. Once the account expires, Faspex deactivates the account and that user will no longer be able to log into Faspex, unless you reactivate the account.</p> <p>Note: In the Accounts list, inactive accounts are shown in gray. Packages sent to this user will remain on the server (if configured to do so).</p>

Option	Description
New accounts will be deleted	<p>Enable this setting to automatically delete a self-registered user's account after a set number of days.</p> <p> Warning: If this setting is enabled, the user's account will be completely removed from the Faspex database and you cannot re-activate it. Packages sent to this user will remain on the server (if configured to do so).</p>

Permissions

Option	Description
Allowed to	<ul style="list-style-type: none"> • Uploads allowed: Select to allow users to send packages. • Downloads allowed: Select to allow users to download received packages. A user who does not have download permissions still receives packages, but cannot download the files. • Forwarding allowed: Select to allow users to forward received packages to other users. The package becomes available to the forwarded users in their Faspex accounts. • Can create from remote: Select to allow users to create a package from a remote source such as a remote server. Users allowed to access remote sources can access the Source drop-down menu when sending a new package. <p>You must first add remote sources to Faspex to see the Source drop-down menu. For more information on adding remote sources, see Adding a Node to Faspex on page 59.</p> <p>Note: This setting is disabled by default and must be set on a per-user basis (in other words, there is no global option).</p>
Allow inviting external senders	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable this user to invite users without Faspex accounts to upload a package to Faspex.</p>
Allow public submission URLs	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable users to send a Public URL to users without Faspex accounts. These external users can submit packages to registered Faspex users through this public URL. For more information about Public URLs, see Configuring Public URLs on page 91.</p> <p>Note: Even if the Public URL feature is enabled for registered Faspex users, they can override the feature for their own account by going to their user Account > Preferences > Misc and clearing Enable public URL.</p>
Can send to external email	<p>Select Allow to allow users to send packages to external email addresses.</p> <p>Faspex sends a download link through email. By default, this link expires after three days, but admins can change the duration or disable expiration by going to Server > Security. For more information, see Configuring Security Settings on page 47.</p>
Can create normal packages	<p>Select Allow to allow users to create packages on the New Package page. Select Deny to prevent the user from accessing the New Packages site. In this case, the user can only create dropbox packages and only if they are a member of a dropbox.</p>

Option	Description
	To change the server default, go to Server > Configuration > Security and edit the setting for Allow users to create normal packages .
Can send to all faspex users	Select Allow to allow users to send packages to all Faspex users. If this feature is enabled, all existing Faspex users appear in the contact list. If disabled, users can, only send packages to members of workgroups they are part of.
Keep user directory private	Select Yes to prevent users from being able to see the entire user directory, even if they have permissions to send to all Faspex users.
Can see global distribution lists.	Select Yes to give users access to global distribution lists. For more information on global distribution lists, see Creating a Global Distribution List on page 129.
Allowed IP addresses for login	Specify the IP addresses that a Faspex user can login from. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for download	Specify the IP addresses that a Faspex user can login from to download packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for upload	Specify the IP addresses that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).

Package Deletion

Select from the following options to specify behavior after downloading a package:

Option	Description
After download	You can override the server default by selecting Override system default . If you choose override, select one of the following policies: <ul style="list-style-type: none"> • Do nothing: Do not auto-delete after the package is downloaded. • Delete files after any recipient downloads all files: Delete after <i>any</i> recipient downloads <i>all</i> files in the package once. Important: When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option. • Delete files after all recipients download all files: Delete if <i>all</i> files in the package have been downloaded by <i>all</i> recipients.
Allow user to set own delete setting on a package-by-package basis	Select Allow to allow this user to choose a package expiration policy when sending a new package.

Advanced Transfer Settings

By default, Faspex uses the transfer settings from the Aspera Central Server section. Select **Override default settings** to set user-specific transfer settings, which take precedence over the server-wide settings.

Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option Lock minimum rate and policy is checked, the user is not able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the maximum upload and download transfer rate for this user.

Creating Distribution Lists

Creating a Personal Distribution List

You can configure personal distribution lists to send packages to a list of email addresses and Faspex users. Each distribution list consists of a comma-separated list of email addresses or Faspex usernames.

On the Edit Distribution Lists page, you can create, edit, or delete personal distribution lists. Although you cannot edit global distribution lists, you can duplicate the list and then edit the duplicated list. For more information on creating and editing global distribution lists, see [Creating a Global Distribution List](#) on page 129.

To create a new list:

1. Click the profile icon in the top-right of the banner and select **Account** from the drop-down menu.
2. Go to the **Edit Distribution Lists** tab.
3. Click **Add New Distribution List** or **Duplicate** a global list.
4. Name the distribution list.

Do not give your personal distribution list the same name as a user account or workgroup name.


Do not give your personal distribution list same name as a global distribution list, unless you want Faspex to use personal list instead of the global list when sending a package.

5. Enter up to 50 contacts. You can:

- Type email addresses or Faspex usernames into the Contacts field.

-



Click  to import contacts from your Faspex contacts list.

- Click the **Browse** button to upload contacts from a CSV file.

Note: The CSV file must include a single column containing only email addresses.

You cannot send packages to a distribution list if any recipient in the list is an invalid user. For example, if a user is an external user and the option to send to external users is disabled, the external user is considered invalid and package sending fails.

If the admin enables the **Ignore invalid recipients** option, package sending does not fail even if the list contains an invalid user. Faspex skips any invalid user and delivers the package to all valid recipients in the list. (Go to **Server > Security** and, under the Faspex accounts section, select **Ignore invalid recipients**.)

Note: To send explicitly to external users, you must append (`external`) to the email address (or Faspex automatically expands the email to existing Faspex users or creates a Faspex user for the email. For example, to send to `faspex_user@example.com`, add `faspex_user@example.com (external)` to the distribution list. For more information on email expansion, see [Package Recipient Expansion by Email Address](#) on page 87.

The items in the list are not validated until you try to send a package to the list.

6. Click **Create**.

After creating a distribution list, the list appears on the Editing Distribution Lists page. You can edit the name and contacts list, or import contacts by clicking **Import Contacts from CSV**. After making changes, click **Update Distribution Lists** to save the changes. You can also delete distribution lists by clicking the **Delete** link for the list.

Creating a Global Distribution List



Admins can configure global distribution lists that can be used by all users to send packages to a list of email addresses and Faspex users. Each distribution list consists of a comma-separated list of email addresses or Faspex usernames. The items in the list are not validated until a user tries to send a package to the list. Admins can configure whether all users can see these lists or whether admins have to grant access to individual users. For more information on granting access to global distribution lists, see [Configure User Access to Global Distribution Lists](#) on page 130.

1. Go to **Server > Configuration > Global Distribution Lists** and click **Add New Distribution List**.
2. Name the distribution list.

Do not give your personal distribution list the same name as a user account or workgroup name.

Do not give your personal distribution list same name as a global distribution list, unless you want Faspex to use personal list instead of the global list when sending a package.

3. Enter up to 50 contacts. You can:

- Type email addresses or Faspex usernames into the Contacts field.
-  Click  to import contacts from your Faspex contacts list.
- Click the **Browse** button to upload contacts from a CSV file.

Note: The CSV file must include a single column containing only email addresses.

You cannot send packages to a distribution list if any recipient in the list is an invalid user. For example, if a user is an external user and the option to send to external users is disabled, the external user is considered invalid and package sending fails.

If the admin enables the **Ignore invalid recipients** option, package sending does not fail even if the list contains an invalid user. Faspex skips any invalid user and delivers the package to all valid recipients in the list. (Go to **Server > Security** and, under the Faspex accounts section, select **Ignore invalid recipients**.)

Note: To send explicitly to external users, you must append (external) to the email address (or Faspex automatically expands the email to existing Faspex users or creates a Faspex user for the email. For example, to send to faspex_user@example.com, add faspex_user@example.com (external) to the distribution list. For more information on email expansion, see [Package Recipient Expansion by Email Address](#) on page 87.

The items in the list are not validated until you try to send a package to the list.

4. Click **Create**.

After creating a distribution list, the list appears on the Global Distribution Lists page. You can edit the name and contacts list, or import contacts by clicking **Import Contacts from CSV**. After making changes, click **Update Distribution Lists** to save the changes. You can also delete distribution lists by clicking the **Delete** link for the list.

Global Distribution Lists [Add New Distribution List](#)

Name	Contacts
Advent Vide	<div> james@adventvp.co m, madison@adventvp.c om, sara@adventvp.com, boyu@adventvp.com, </div> <div> + </div> <div> Import Contacts From CSV </div> <div> Delete </div>

Update Distribution Lists

Configure User Access to Global Distribution Lists

Configure Default Access to Global Distribution Lists

Go to **Server > Security**. Under the Faspex accounts section, select **Users can see global distribution lists by default** to give all users access to global distribution lists by default. Deselect the option to require an admin manually grant a user access to global distribution lists.

Enable or Disable Access for a User

Go to **Accounts** and click the name of the user you want to grant or deny access to global distribution lists. Under **Permissions**, there are three settings for the **Can see global distribution lists** permission. You can choose to permanently allow or deny access to global distribution lists, or you can choose to use the server default configured by enabling or disabling the **Users can see global distribution lists by default** option in the server security settings.

Using Rake Tasks to Manage Faspex

Configuring the Primary Transfer Address of the Default Node

You can configure the primary address Faspex uses to connect with the primary Faspex node. The primary node address is the node address you provided when you installed Faspex locally or remotely. To configure the address, run the following rake task command:

```
asctl faspex:rake aspera:set_node_ext_address
EXTERNAL_ADDRESS="hostname_or_IP"
```

You can also see and configure the primary address by going to **Server > File Storage**, selecting **Edit** from the drop-down menu for the default node, and clicking **Advanced Configuration**.

Creating Users with Rake Tasks

The following rake tasks allow you to create, update, and delete individual, local users.

Command	Description
<code>asctl faspex:rake users:create -- -n <i>username</i> -f <i>firstname</i> -l <i>lastname</i> -e <i>email</i> -p <i>password</i></code>	Create the user with the specified user name, first name, last name, and email address. Setting a password is optional.
<code>asctl faspex:rake users:update -- -n <i>username</i> [<i>optional arguments</i>]</code>	Update the user with the specified <i>username</i> and any additional arguments.
<code>asctl faspex:rake users:delete -- -n <i>username</i></code>	Delete the user with the specified <i>username</i> .

For more details on the options, see the table below.

Rake Task Options

Options (Short Form)	Options (Long Form)	Description
<code>-n <i>username</i></code>	<code>--name <i>username</i></code>	User's Faspex username used to log into this account.
<code>-p <i>password</i></code>	<code>--password <i>password</i></code>	User's password (optional).
<code>-f <i>first_name</i></code>	<code>--first_name <i>first_name</i></code>	User's first name (required for <code>users:create</code>).
<code>-l <i>last_name</i></code>	<code>--last_name <i>last_name</i></code>	User's last name (required for <code>users:create</code>).
<code>-e <i>email_address</i></code>	<code>--email <i>email_address</i></code>	User's email address (required for <code>users:create</code>).
<code>-h</code>	<code>--help</code>	Print out help information for this rake task.

Bulk Create and Manage Users with Rake Tasks

Rake Commands

To create and manage users in bulk, use the following commands:

```
asctl faspex:rake users:bulk_create -- -u userfile -p propertyfile
asctl faspex:rake users:bulk_update -- -u userfile -p propertyfile
asctl faspex:rake users:bulk_delete -- -u userfile
```

Note: The `users:bulk_create` and `users:bulk_update` rake tasks do not support setting passwords for users. An admin must manually set the passwords for the created users.

Create and Update Options

Option	Description
userfile (required)	<p>Full path to the CSV file specifying attributes to be applied to individual users.</p> <p>For example:</p> <pre>name,first_name,last_name,email,welcome_email user1,John,Doe,jdoe@example.com,jdoe@example.com user2,Susan,Lee,slee@example.com,slee@example.com user3,Jay,Johnson,jjohnson@example.com</pre> <p>Faspex sends a welcome email to a user if you provide a welcome email in the entry. You can forgo the welcome email by leaving that column blank. In the example above, Faspex sends a welcome email to user1 and user2, but not to user3.</p>
propertiesfile (required)	<p>Full path to the CSV file specifying attributes to be applied to all users. Use this file to determine the type of user.</p> <p>The properties file for adding local members of a directory service follows this format:</p> <pre>type,authorization_domain_id DirectoryServiceUser,3</pre> <p>Set the <code>authorization_domain_id</code> to the ID of a configured LDAP. You can obtain the ID by going to Accounts > Directory Service Groups, selecting the LDAP, and finding the ID in the URL (for example, the 3 in <code>aspera/faspex/admin/authorization_domains/3/edit</code>)</p> <p>The properties file for adding local users follows this format:</p> <pre>type LocalUser</pre>

Delete Options

Option	Description
userfile (required)	<p>Full path to the CSV file specifying attributes to be applied to individual users.</p> <p>For example:</p> <pre>name user1 user2 user3</pre>

Force All Users to Reset Passwords with Rake Tasks

You can force all users to reset their passwords when they next log in.

Rake Command

```
asctl faspex:rake users:force_password_reset
```

Bulk Import and Manage DS Users with Rake Tasks

To import and manage DS users in bulk, use the following commands:

```
asctl faspex:rake users:bulk_create -- -u userfile -p propertyfile
asctl faspex:rake users:bulk_update -- -u userfile -p propertyfile
asctl faspex:rake users:bulk_delete -- -u userfile
```

Rake Task Options

Option	Description
userfile (required)	<p>Full path to the CSV file specifying attributes to be applied to individual users.</p> <p>For example:</p> <pre>name,first_name,last_name,email,ad_objectguid user1,John,Doe,jdoe@example.com,e43f8A9d325ed74 user2,Susan,Lee,slee@example.com,2b42959ff79507 user3,Jay,Johnson,jjohnson@example.com,cc07cacc</pre> <p>The objectGUID is the DS Distinguished Name (DN).</p> <p>Important: If you are importing from Active Directory, you must find the objectGUID attribute for a user and copy it in hexadecimal format. Edit the user and go to Properties > Attribute Editor > objectGUID. Edit the attribute, select hexadecimal format, and copy the whole string.</p> <p>This string is different from the string displayed on the main page. Use this string instead of the one on the main page.</p> <p>When entering the string into the CSV file, enter it as one string without spaces. For example, if the string is "E4 3F 8A 9D 32 5E D7 40 B8 DB EF B3 CA 0F 7B B8", enter it as "E43F8A9D325ED740B8DBEFB3CA0F7BB8".</p>
propertiesfile (required)	<p>Full path to the CSV file specifying attributes to be applied to all users.</p> <p>The properties file for adding DS users to Faspex would look like this:</p> <pre>type,authorization_domain_id</pre>

Option	Description
	<p><code>DirectoryServiceUser, id_num</code></p> <p>The <code>authorization_domain_id</code> can be found by going to Server > Authentication > Directory Services and editing the Directory Service. Look at the URL and find the ID number after <code>"authorization_domains</code>. For example, if the URL is <code>https://198.51.100.24/aspera/faspex/admin/authorization_domains/1/edit</code>, the ID number is "1"</p>

Delete Options

Option	Description
userfile (required)	<p>Full path to the CSV file specifying attributes to be applied to individual users.</p> <p>For example:</p> <pre>name user1 user2 user3</pre>

Import SAML Users with Rake Tasks

You can run a rake task to build import SAML user information from a JSON file into Faspex. Faspex also imports entries for existing SAML users and imports updates the users in Faspex with the new values. The rake task follows this syntax:

```
asctl faspex:rake users:import_saml_users RESOURCE=path/to/json_file_or_url
```

You must point the rake task to a local file or to a URL referencing a JSON file with the following format:

```
{ "users": [
  { "username": "username",
    "email": "email_address",
    "given_name": "first_name",
    "saml_configuration_id": saml_config_id },
  ...
]}
```

Attribute	Description
Username	The Faspex username associated with the SAML user.
Email	The email address associated with the account.
Given Name	The first name associated with the account.
SAML Configuration ID	The ID associated with the SAML configuration. The <code>saml_id</code> specifies the SAML configuration. For example, in the case of multiple SAML configurations, the first

Attribute	Description
	<p>configuration is associated with the SAML ID "1", the next configuration "2", and so on.</p> <p>Note: You must first configure the SAML configuration in Faspex to associate the users with the correct SAML IdP through the SAML ID. For more information on configuring a SAML configuration, see Creating a SAML Configuration in Faspex on page 116.</p>

An example entry for a user might look like the following:

```
{ "username": "johndoe",
  "email": "johndoe@faspex.example.com",
  "given_name": "John",
  "saml_configuration_id": 1 }
```

Tip: You can also automate the process of importing SAML users from a JSON file. For more information, see [Automating Importing SAML Users with Rake Tasks](#) on page 135.

Automating Importing SAML Users with Rake Tasks

You can automate the process of importing SAML users from a JSON file by editing the faspex.yml file. You must provide the path to a JSON file with the following format:

```
{ "users": [
  { "username": "username",
    "email": "email_address",
    "given_name": "first_name",
    "saml_configuration_id": saml_config_id },
  ...
]}
```

Attribute	Description
Username	The Faspex username associated with the SAML user.
Email	The email address associated with the account.
Given Name	The first name associated with the account.
SAML Configuration ID	<p>The ID associated with the SAML configuration. The <i>saml_id</i> specifies the SAML configuration. For example, in the case of multiple SAML configurations, the first configuration is associated with the SAML ID "1", the next configuration "2", and so on.</p> <p>Note: You must first configure the SAML configuration in Faspex to associate the users with the correct SAML IdP through the SAML ID. For more information on configuring a SAML configuration, see Creating a SAML Configuration in Faspex on page 116.</p>

Important: Backup faspex.yml before making your changes. For more information about the faspex.yml file, see [faspex.yml Configurations Reference](#) on page 154.

1. Edit faspex.yml which can be found at: `/opt/aspera/faspex/config/faspex.yml`.

Under the "Production" section, provide the path to a local JSON file or a URL referencing a JSON file. Set the frequency for Faspex to import user data from the JSON file.

```
production:
  ...
  DisableSAMLUserImportBackgroundJob: false
  SAMLUserImportJSONResourceFQN: full_path_of_JSON_file
  SAMLUserImportFrequencyInSeconds: time_in_seconds
  ...
```

2. Save and restart Faspex processes.

```
asctl faspex:restart
```

Faspex now automatically imports updates you make to the JSON file. Faspex also imports entries for existing SAML users and imports updates the users in Faspex with the new values.

Configuring Server Settings with Rake Tasks

The following rake tasks are used to configure Faspex server settings related to file storage and nodes.

Configure SMTP Server

The syntax of the command to configure the Faspex SMTP server is as follows:

```
asctl faspex:rake aspera:smtp -- [options]
```

Options	Description
<code>--server <i>server</i></code>	The SMTP server address
<code>--port <i>port</i></code>	The SMTP port
<code>--domain <i>domain</i></code>	The email domain name
<code>--tls <i>true/false</i></code>	Whether to use TLS if available
<code>--username <i>username</i></code>	The email username
<code>--password <i>password</i></code>	The email password
<code>--from <i>email</i></code>	The email sender's address that will appear in the 'from' field

For example:

```
asctl faspex:rake aspera:smtp -- --auth=open --
server=smtp_example.aspera.us --port=25 --domain=aspera.us
--tls=ON --username=example@aspera.com --from_name=Faspex --
from_email=aspera_faspex@aspera.com
```

Configure the Server Default Inbox Path

To configure the path for the default inbox, run the following rake task:

```
asctl faspex:rake aspera:set_storage_share_directory DIRECTORY="/path/to/
directory"
```

Note: The specified path should be relative to the docroot. For example, if the docroot is `/home/faspex/faspex_packages`, and the new default inbox path is `/home/faspex/faspex_packages/johndoe`, specify `/johndoe`.

Create a Node API User

To create a Node API user mapped to the "faspex" transfer user, run the following rake task:

```
asctl faspex:rake aspera:setup_node_user USERNAME="username"
PASSWORD="password"
```

Create or Update a Remote Node

To create and add a remote node or update an existing remote node, run the following rake task:

```
asctl faspex:rake aspera:source_server NAME="remote_node_name"
HOST="remote_node_hostname" PORT="node_api_port"
USERNAME="node_api_username" PASSWORD="node_api_password"
USE_SSL=["true"/"false"] VERIFY_SSL=["true"/"false"]
```

The USE_SSL and VERIFY_SSL arguments are optional and can be set to either "true" or "false".

Update the Directory Path of an Existing File Storage

To create a new file storage or update an existing file storage, run the following rake task:

```
asctl faspex:rake aspera:source_directory NODE_NAME="node_name"
SOURCE_NAME="file_storage_name" DIRECTORY="/path/to/directory"
```

You can make this directory the default directory by adding `--make_default` to the command. For example:

```
asctl faspex:rake aspera:source_directory NODE_NAME="faspex_node"
SOURCE_NAME="packages" DIRECTORY="aspera_files" --make_default
```

Note: The specified path should be relative to the docroot. For example, if the docroot is `/home/faspex/`, `faspex_packages`, and the new default inbox path is `/home/faspex/faspex_packages/johndoe`, specify `/johndoe`.

Managing Packages with Rake Tasks

Clean Records of Deleted Packages

To clean records of packages deleted from Faspex, run the following rake task:

```
asctl faspex:rake packages:clean_deleted OLDER_THAN_DAYS=days
```

Delete Expired Packages from Custom Inboxes and Workgroup Relays

```
asctl faspex:rake packages:delete_expired_packages DELETE_INTERVAL=interval
```

This rake task iterates through expired packages in custom inboxes and workgroup relays and deletes their contents one by one, waiting the DELETE_INTERVAL in seconds between each delete. The default interval value is 5s.

Encrypting and Decrypting Database Passwords

You can use the following rake tasks to encrypt and decrypt passwords in your `database.yml` configuration file.

Encrypting Passwords

Run the following command to encrypt passwords:

```
asctl faspex:rake aspera:encrypt_database_passwords
```

Decrypting Passwords

Run the following command to decrypt passwords:

```
asctl faspex:rake aspera:decrypt_database_passwords
```

Exporting and Importing Global Distribution Lists

You can use the following rake tasks to export and import global distribution lists in JSON file format.

Exporting Global Distribution Lists

Run the following command to encrypt passwords:

```
asctl faspex:rake aspera:export_distribution_list  
FILE_LOCATION=file_location
```

For example:

```
asctl faspex:rake aspera:export_distribution_list  
FILE_LOCATION=~/.faspex_dlist.json
```

Importing Global Distribution Lists

Run the following command to decrypt passwords:

```
asctl faspex:rake aspera:import_distribution_list  
FILE_LOCATION=file_location
```

For example:

```
asctl faspex:rake aspera:import_distribution_list  
FILE_LOCATION=~/.faspex_dlist.json
```

Customizing Faspex: Email Notifications, Server Instructions, Application Appearance

Configuring Email Notification Templates

1. Go to **Server > Notifications** and select an email template. For a list of supported email templates, see [Email Notification Template Types](#) on page 213.
2. When you select one of these notification types, you can edit its respective content by clicking **Customize Using Template** or **Edit HTML**.

- **Customize Using Template:** Create an email template by filling out a form. You can use special text strings that are replaced in the actual email by the appropriate values. For a list of the available text strings for each notification type, see [Email Notification Template Text Strings](#) on page 215.

Tip: You can select the **Show all recipients in package information** option to list all public and CC recipients in the email notification.

Important: Do not use HTML code or the < and > symbols when customizing using the template.

- **Edit HTML:** Create an email template with HTML code.

Tip: For a list of allowed HTML tags and attributes, see [Available HTML Tags and Attributes in Faspex](#) on page 207.

3. Click **Generate E-mail and Save**.

If you made changes you want to revert, you can reload the template's default settings by clicking **Load Defaults**.

Posting Instructions for Sending New Packages

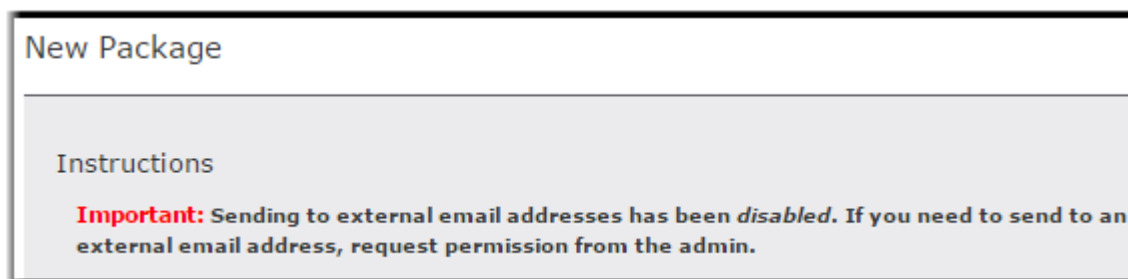
Post instructions for users who are sending new, normal packages (in other words, *not* dropbox packages). Once saved, your instructions appear on the Faspex New Package page. For information about posting instructions for sending dropbox packages, see [Creating a Dropbox](#) on page 99.

1. Go to **Server > Notifications > Package Instructions**
2. Enter your instructions.

You can use HTML tags and CSS classes in your instructions. For a list of available tags, see [Available HTML Tags and Attributes in Faspex](#) on page 207. For more information on using CSS classes, see [Creating CSS Classes to Use in Instructions](#) on page 144.

For example:

```
<p><b class="red" style="font-size:14px">Important:</b> Sending to external
email addresses has been <i>disabled</i>. If you need to send to an
external email address, request permission from the admin.</p>
```



Posting Announcements on the Login Page

Post an announcement on the login page to welcome users and provide further login information.

1. Go to **Server > Notifications > Login Announcement**.
2. Enter your announcement.

You can use HTML tags and CSS classes in your instructions. For a list of available tags, see [Available HTML Tags and Attributes in Faspex](#) on page 207. For more information on using CSS classes, see [Creating CSS Classes to Use in Instructions](#) on page 144.

For example:

```
<h1 class="red" style="text-align:center">Welcome to Faspex!</h1>
Login with your Faspex credentials. If you do not have an account, contact
the admin at <a href="mailto:johndoe@faspex.com">johndoe@faspex.com</a>.
```



Configure Display Settings

Go to **Server > Configuration > Display Settings**.

Important: You must click the **Update** button to save any changes you make to the following settings.

Custom Logo

Click the **Browse** button to replace the default logo in the menu bar with your custom logo.

Note: Your custom logo cannot be larger than the default logo, which is 295x51 pixels.

To remove the logo, click the **Remove custom logo** that appears if you have uploaded a custom logo.

Date Format

View or modify your server's date display format. The following list displays the available variables:

Variable	Description and Sample
%a	The abbreviated weekday name (for example, "Sun").
%A	The weekday name (for example, "Sunday").
%b	The abbreviated month name (for example, "Jan").
%B	The month name (for example, "January").
%d	Day of the month (for example, "01~31").
%j	Day of the year (for example, "001~366").
%m	Month of the year (for example, "01~12").
%y	The abbreviated year (for example, "09").
%Y	The year (for example, "2009").

Account display name format

The **Account display name format** option determines whether users see the login or the full name associated with an account when viewing package information. For example, given a user "jdoe" with full name "John Doe", Faspex displays "jdoe" if **Username** is selected and "John Doe" if **Full Name** is selected.

Login Page

You can configure the login page text using the **Login page header** and **Local login instructions** field options. The header is the title of the login form and the instructions appear above the local login option. For example, in the picture below, the header has been changed to "My Company Login" and the instructions read "Your username is firstname@mycompany.com and your password is your personal ID number (for example, 5GH012)."

You can further customize the login page by adding an announcement or by customizing the login page with a CSS file. For more information, see [Posting Announcements on the Login Page](#) on page 139 and [Customize Faspex with the Custom CSS File](#) on page 141.

Creating a Custom CSS File

1. Create a file at the following location: `/opt/aspera/faspex/public/stylesheets/custom/customize.css`
2. Edit this new `customize.css` file instead of the default `faspex.css` and `bootstrap.css` files. Those files are located at:
 - `faspex.css`: `opt/aspera/faspex/public/stylesheets/faspex.css`
 - `bootstrap.css`: `opt/aspera/faspex/public/stylesheets/third-party/bootstrap/bootstrap.css`

You do not need to copy the entire contents of `faspex.css` and `bootstrap.css` into `customize.css`. You only need to add the changed values and their surrounding functions. The values in `customize.css` take precedence over the defaults. For details on the custom css file, see [Customize Faspex with the Custom CSS File](#) on page 141.

3. Update references to images in the `customize.css` file.

When the `faspex.css` file references images, it references `../images/` to find the images. Since the `customize.css` file is in a different filepath than `faspex.css`, you must specify `../../images/` instead when referencing images in the `customize.css` file.

Customize Faspex with the Custom CSS File

While Faspex does not yet support skinning, it is possible to modify some files in order to personalize colors and images of the Faspex interface.

Folders and Files Handling the Application Appearance

The public folder is located at: `/opt/aspera/faspex/public`. Most of the pictures are located in the "images" sub-folder. The "stylesheets" sub-folder contains the `faspex.css` and `bootstrap.css` files. The `.css` files are located at:

- `faspex.css`: `opt/aspera/faspex/public/stylesheets/faspex.css`
- `bootstrap.css`: `opt/aspera/faspex/public/stylesheets/third-party/bootstrap/bootstrap.css`

Important: Aspera does not recommend editing the `faspex.css` and `bootstrap.css` files to personalize Faspex, because these files are not preserved when upgrading Faspex. Instead, follow the instructions in [Creating a Custom CSS File](#) on page 141 to create and modify the `customize.css` file that takes precedence over these default files.

Customize Faspex Colors

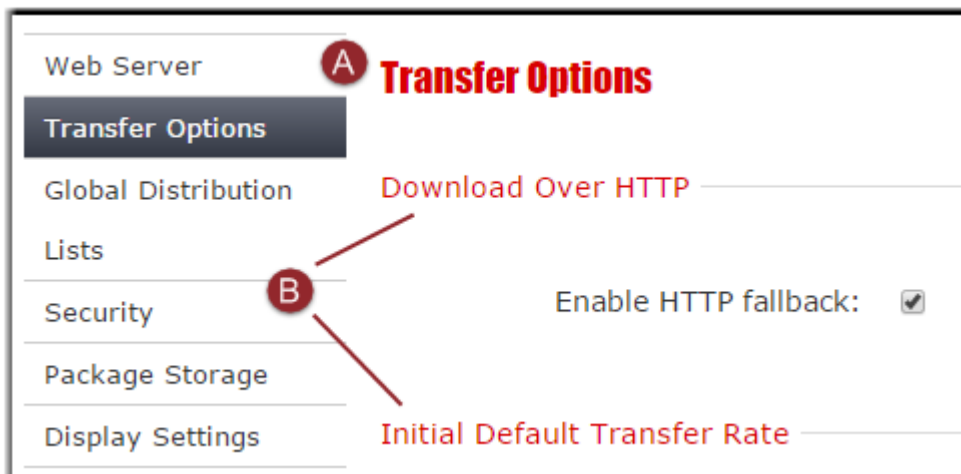
Use the `custom.css` file created in [Creating a Custom CSS File](#) on page 141 to change the color of the global navigation bar, the header, and the active tab. For example, to change the Faspex header and main navigation bar background colors to blue (`#1d2873`):

```
/* MAIN GLOBAL NAV */
.main_tabs
{
  margin: auto;
  float: left;
  width: 100%;
  background: #1d2873;
}

/* Header */
div#header
{ width: 100%; height: 60px; color: white; background: #1d2873 }

/* Active Tab */
.main_tabs ul li a.selected {
background: linear-gradient(to top, #5aaafa 4px, #1d2873 4px)
}
```

Customize Subtitles



Label	Description
A	Sub-menu Title
B	Section Titles

A: Sub-menu Title

To change the font, size, and color of sub-menu titles, edit the following tags (defaults found in bootstrap.css):

```
h1, h2, h3, h4, h5, h6 {
  margin: 0;
  font-family: Verdana, helvetica, sans-serif;
  font-weight: bold;
  color: inherit;
  text-rendering: optimizelegibility;
}
```

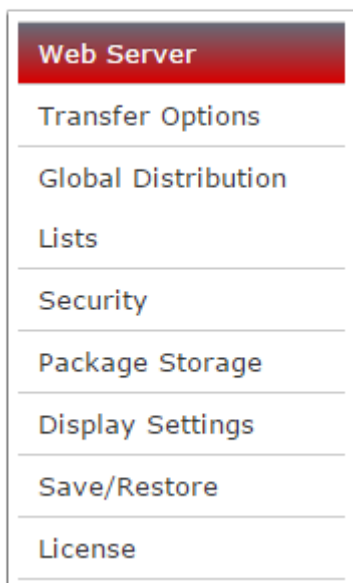
```
h1, h2, h3, h4, h5, h6 {
  font-weight: normal;
  line-height: normal;
  margin-bottom: 20px;
}
```

A: Titles

To change the font, size, and color of section titles, edit the following tags (defaults found in bootstrap.css):

```
legend {
  width: inherit;
  font-size: 108%;
  font-weight: normal;
  background: transparent;
  line-height: 1.5;
  color: #1952bb;
  margin: 12px 0;
  padding-right: 5px;
  border: 0;
}
```

Customize Vertical Menus



To change the color of tabs for the vertical menu, edit the following two sections (default found in faspex.css):

```
.v_menu li a {
  display: block;
  text-decoration: none;
  color: #333;
  line-height: 30px;
```

```
border-top:1px solid #ccc;
padding-left:10px;
cursor:pointer;
}
```

```
.v_menu .active a,
.v_menu .selected a {
  color:#fff;
  background-color:#343945;
  background-image: -moz-linear-gradient(top, #676c79, #343945);
  background-image: -webkit-gradient(linear, left top, left bottom,
  from(#676c79), to(#343945));
  filter:progid:DXImageTransform.Microsoft.gradient(startColorstr=#ff676c79,endColorstr=#ff343945);
  -ms-filter:
  "progid:DXImageTransform.Microsoft.gradient(startColorstr=#ff676c79,endColorstr=#ff343945)";
}
```

Customize the Drag and Drop Picture

To change the Drag and Drop picture on the New Package page, replace the original `dragndrop.jpg` with an equivalent `jpg` of your own.

Creating CSS Classes to Use in Instructions

You can create CSS classes in the `customize.css` file (`/opt/aspera/faspex/public/stylesheets/custom/customize.css`), which you can then use when editing email notifications or package instructions. For more information on the `customize.css` file, see [Creating a Custom CSS File](#) on page 141.

1. Create the `customize.css` file at `/opt/aspera/faspex/public/stylesheets/custom/customize.css` if it does not yet exist.
2. In this file, create a CSS class.
For example, create a class for the color red:

```
.red {
  color:red;
}
```

You can reference any classes you create when editing email notifications or package instructions. For example, when editing login instructions to Faspex, you can make the text red as follows:

```
<h1 class="red" style="text-align:center">Welcome to Faspex!</h1>
Login with your Faspex credentials. If you do not have an account, contact
the admin at <a href="mailto:johnndoe@faspex.com">johnndoe@faspex.com</a>.
```



Configuring Metadata

Faspex Metadata

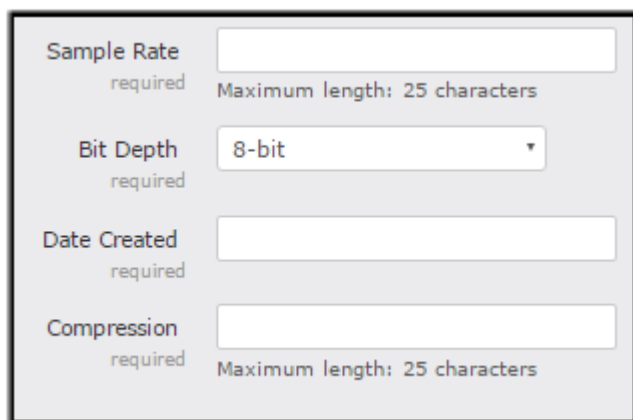
Metadata refers to the additional information that an IBM Aspera Faspex user can send with a file package. For example, an admin can require that, when a user sends an audio-file package to a producer, the user must also specify the sample rate, bit depth, and compression of the package. The admin sets these requirements by creating a new metadata profile that the admin can then apply to all new, normal packages or to individual dropboxes.

The Metadata Profiles (go to **Server > Metadata**) page displays any profiles you have previously created.

Metadata Example

In the example metadata file below, the Audio Details metadata profile contains the following fields:

- Sample rate (text input field)
- Bit Depth (option list that includes 8-bit, 16-bit and 24-bit)
- Compression (text input field)
- Date Created (date picker)



The screenshot shows a form titled 'Audio Details' with the following fields:

- Sample Rate**: A text input field with a 'required' label and a note 'Maximum length: 25 characters'.
- Bit Depth**: A dropdown menu with a 'required' label, currently showing '8-bit'.
- Date Created**: A date picker field with a 'required' label.
- Compression**: A text input field with a 'required' label and a note 'Maximum length: 25 characters'.

Applying Metadata Profiles

Admins choose which configured metadata profile to apply to new, normal packages or to individual dropboxes. Admins can choose to assign (**none**) as a metadata profile in cases where no metadata fields are required. For information about applying metadata profiles to normal packages, see [Applying Metadata Profile to Normal Packages](#) on page 147. For information about applying metadata profiles to dropboxes, see [Creating a Dropbox](#) on page 99.

Forwarding Packages with Metadata

When you forward a package, the original metadata is preserved in the **Note** field. The preserved metadata does not change even if the applied metadata profile has been changed. No new **aspera-metadata.xml** file is created, even if **Save metadata to file** is enabled for the metadata.

Faspex Metadata Reporting for IBM Aspera Console

If a Faspex instance is added to IBM Aspera Console as a managed node, Console monitors transfer details of transfers in Faspex. Custom metadata fields applied to normal packages or to dropboxes are included as metadata tags in the transfer details and as transfer cookies for Console to use in running reports.

A Faspex transfer cookie is formatted in the following way:

```
{ "aspera" :
```

```
{ "faspex" :
  { "key1": "val1", ... , "key3": "val3" }
}
```

The corresponding JSON match value is shown below:

```
[ aspera ][ faspex ][ key1 ] val1
```

Creating Metadata Profiles

Metadata profiles include a set of fields that, if applied, require users to include additional information when sending a package. Metadata profiles can be applied all new, normal packages or to individual dropboxes.

1. Go to **Server > Metadata** and click **Add New Profile**.
2. Name the metadata profile and click **Create**.
Faspex redirects you to the Edit Metadata Profile page.
3. You can set the max length and restrict illegal characters for the package title and note. You can also disable the ability to add a note to the package by clearing the **Enabled** checkbox.
4. Select a field option from the drop-down menu and then click **Add Field**. You can add multiple metadata fields.
 - **Text Field**: Create a single-line text field.
 - **Text Area**: Create a multiline text field.
 - **Option List**: Create a radio button-based options list.
 - **Date Field**: Create a date picker.

Each field option has its own template. The following instructions differ depending on the field option you selected.

5. Enter a descriptive name for the metadata field in the **Label** field. This text is displayed beside the field option on the New Package / Send to Dropbox page.
6. Create a metadata field. You can create one of the following types of fields:
 - Text Field / Text Area: Restrict users from using the character specified in the **Illegal Characters** field. Fields are validated for illegal characters when the user tries to send the package. Warning messages appear listing the illegal characters.

For Text Fields and Text Areas, set the max number of characters for the field. The maximum length must be between 1 and 999.

Note: The sum total maximum length of all fields (including labels, options, and date fields) must be less than 2000 characters. If the sum total exceeds 2000 characters, all max length fields are reset to the default (100 characters).
 - Option List: Enter the list of options a user can choose from in the **Options** field.
 - Date Field: Configure the **Date format** of the date picker.
7. If you want to make a field required for a user, select **Required** for that field.
8. Configure restrictions for a package title.
Under Title, set the max number of characters for the Title of a package in the **Max length** field. Restrict users from using the character specified in the **Illegal Characters** field.
9. Configure restrictions for a package note.
Under Note, set the max number of characters for the note of a package in the **Max length** field. Restrict users from using the character specified in the **Illegal Characters** field.

You can also disable the note by clearing the **Enabled** checkbox.
10. Preview the metadata fields. Click **Save and Preview**.

Preview

Sample Rate
required Maximum length: 25 characters

Bit Depth
required

Date Created
required

Compression
required Maximum length: 25 characters

11. When finished, click **Save**. You are redirected to the Metadata Profiles page.

Click **Edit** to modify your profile or **Delete** to remove it.

Applying Metadata Profile to Normal Packages

Metadata profiles require users to include additional information when sending a package. You must choose and apply a metadata profile to Faspex packages to include the fields in the metadata profile. For information about applying metadata profiles to dropboxes, see [Creating a Dropbox](#) on page 99.

1. Go to **Server > Metadata**.
2. Select a profile for normal packages from the Profile for normal packages drop-down menu.

Metadata Profiles [Add New Profile](#)

Profile for normal packages:

Save metadata to file: ☐

Name	
Audio Details	Edit Delete

The selected profile modifies the New Package Form. For more information, see [Sending a New Package](#) on page 82.

3. Select **Save metadata to file** to save the package metadata to its root directory as an XML file. You can use the XML data for post-processing and automation.

The metadata filename follows the format: **aspera-metadata-package_uuid.xml**. For example, a sample filename could be: **aspera-metadata-42dfda4c-ff05-4f61-8d82-f89c0523d799.xml**.

You can configure Faspex to include the metadata file in the package itself, instead of being placed at the root directory of the package. To enable this, set the **SaveMetadataInPackage** option to **true** in the **production** section of the **faspex.yml** configuration file. The **faspex.yml** file is located in the following directory:

/opt/aspera/faspex/config/faspex.yml

```
production:
  ...
  SaveMetadataInPackage: true
```

...

After saving changes in **faspex.yml**, restart Faspex.

```
asctl faspex:restart
```

Now, whenever you select **Save metadata to file**, Faspex inserts the metadata file in the package and users can view it in the package contents.

Backing Up and Restoring Faspex

Backing Up Faspex from the Application

Aspera strongly recommends backing up your IBM Aspera Faspex configuration and database as a precaution in case of system failure. You can also choose to restore Faspex on a completely new server on which you've installed Faspex.

- Go to **Server > Configuration > Save/Restore**.
- Click the **Download** button to save your current Faspex database in the format *.tar.gz.

Important: If you use the Safari web browser, you need to make sure the **Open "safe" files after downloading** option is unchecked in Safari's general settings, before downloading the backup file. Otherwise, the file is downloaded as a .tar file, rather than a .tar.gz file, and does not work when the user attempts to restore the server with this file.

- Back up the **secret.yml** file located at **/opt/aspera/faspex/configsecret.yml**. This file must be backed up and restored for the restored Faspex to correctly work with remote nodes.
- Back up your Faspex, Apache and MySQL application files.

Application	Location of Application Files	Files to Back Up
Faspex	/opt/aspera/faspex/	<ul style="list-style-type: none"> faspex.rb.yml config*.yml configmongrel_clustermongrel_cluster.yml configaspera.faspex.*.aspera-license libdaemons/npetckeystore.jks
Apache	/opt/aspera/faspex/ /opt/aspera/common/apache	<ul style="list-style-type: none"> apache.rb.yml conf*.key conf*.crt confextra/httpd-ssl_template.conf custom
MySQL	mysql	<ul style="list-style-type: none"> database.rb.yml

- If you configured SSL for Faspex, backup your SSL certificate files.
Locate and copy the **server.crt** and **server.key** files to a different location. The files can be found in the following locations:
 - apacheconfserver.crt
 - apacheconfserver.key

For instructions on restoring your Faspex configuration and database, see [Restoring your Faspex Database](#) on page 149.

Backing Up Faspex from the Command Line

Aspera strongly recommends backing up your IBM Aspera Faspex configuration and database as a precaution in case of system failure. You can also choose to restore Faspex on a completely new server on which you've installed Faspex.

1. Back up your Faspex MySQL database by running the following `asctl` command:

```
asctl faspex:backup_database
```

The `asctl` command uses `mysqldump` to backup Faspex's three MySQL databases to `/opt/aspera/faspex/backup/time_stamp-version_number.revision_number`

For example, the directory name may be **2016-04-15_140547-Faspex.4.0.0.100400**.

2. Back up the `secret.yml` file located at `/opt/aspera/faspex/configsecret.yml`. This file must be backed up and restored for the restored Faspex to correctly work with remote nodes.
3. Back up your Faspex, Apache and MySQL application files.

Application	Location of Application Files	Files to Back Up
Faspex	<code>/opt/aspera/faspex/</code>	<ul style="list-style-type: none"> • <code>faspex.rb.yml</code> • <code>config*.yml</code> • <code>configmongrel_clustermongrel_cluster.yml</code> • <code>configaspera.faspex.*.aspera-license</code> • <code>libdaemons/npetckeystore.jks</code>
Apache	<code>/opt/aspera/faspex/ /opt/aspera/common/apache</code>	<ul style="list-style-type: none"> • <code>apache.rb.yml</code> • <code>conf*.key</code> • <code>conf*.crt</code> • <code>confextra/httpd-ssl_template.conf</code> • <code>custom</code>
MySQL	<code>mysql</code>	<ul style="list-style-type: none"> • <code>database.rb.yml</code>

4. If you configured SSL for Faspex, backup your SSL certificate files.

Locate and copy the **server.crt** and **server.key** files to a different location. The files can be found in the following locations:

- `apacheconfserver.crt`
- `apacheconfserver.key`

For instructions on restoring your Faspex configuration and database, see [Restoring your Faspex Database](#) on page 149.

Restoring your Faspex Database

You can restore a backed up version of Faspex if you experience a system failure. You can also choose to restore Faspex on a completely new server on which you've installed Faspex. If you choose to restore Faspex on a separate

server, the restored version of Faspex must match the version of Faspex installed on the server. To restore Faspex, you need the following files:

- Faspex MySQL database files
- The `secret.yml` file
- Faspex, Apache, and MySQL application files

1. Copy the backup directory to the server and run the following `asctl` command:

```
asctl faspex:restore_database /path/to/backup_dir
```

2. Set the Faspex hostname to the hostname of the current server by running the following `asctl` command.

```
asctl apache:hostname hostname
```

3. Set the hostname or IP address in your `faspex.yml` file.

The `faspex.yml` file can be found at the following location:

```
/opt/aspera/faspex/config/faspex.yml
```

Change `Hostname:` and `BaseUrl:` to include the new hostname or IP address.

4. Update the `aspera.conf` file with the new hostname using the following `asconfigurator` command:

```
asconfigurator -x "set_server_data;server_name,hostname"
```

5. Create a node user on the server. Run the following command:

```
asnodeadmin -a -u node_user -p password -x faspex
```

6. If you backed up your SSL certificates and keys, copy them to the following locations on the server:

- `/opt/aspera/common/apache/conf/server.crt`
- `/opt/aspera/common/apache/conf/server.key`

Keep a backup of those files in that directory.


7. Copy the `secret.yml` file from your backup to `/opt/aspera/faspex/config/secret.yml`. Keep a backup of the original `secret.yml` file in the directory.

8. Restart Faspex.

```
asctl faspex:restart
```

9. Modify the localhost configuration.

Launch Faspex from a browser and log in using the Faspex admin account. Go to **Server > File Storage** and edit

the **localhost** node. (Select the  icon next to **localhost** and select **Edit**.) In the Basic Configuration section, enter the username and password you specified when you created the node admin user.

Note: Remote nodes should be accessible without changes.

10. If you experience issues, restart Aspera services.

Run the following commands to restart the `asperacentral`, `asperanoded`, the `asperahttpd` services:

```
# service asperacentral restart
# service asperanoded restart
# service asperahttpd restart
```

Note: If you created post-processing scripts, you must copy and restore them manually. For more information on post-processing scripts, see [Enabling Post-Processing Scripts](#) on page 35.

Each email template notification you have customized must be customized again from the application. For more information, see [Configuring Email Notification Templates](#) on page 138.

Configuring Faspex Using `faspex.yml`

The `faspex.yml` configuration file provides configuration options not available in the Faspex web UI. You can find the file at `/opt/aspera/faspex/config/faspex.yml`

Configuring Signed SAML Authentication Requests

Signed SAML authenticate requests must be configured in the `faspex.yml` configuration file. Make sure you have a valid SSL certificate and key to sign requests.

1. Edit the `faspex.yml` configuration file (`/opt/aspera/faspex/config/faspex.yml`).
2. Under the production section, add the following configurations:

```
production:
  EnableSignedAuthnRequests: true
  AuthnDigestMethod: XMLSecurity::Document::digest_method
  AuthnSignatureMethod: XMLSecurity::Document::signature_method
  AuthnCertificate: >
    -----BEGIN CERTIFICATE-----
    faspex_ssl_certificate
    -----END CERTIFICATE-----
  AuthnPrivateKey: >
    -----BEGIN RSA PRIVATE KEY-----
    faspex_ssl_private_key
    -----END RSA PRIVATE KEY-----
```

For example:

```
production:
  EnableSignedAuthnRequests: true
  AuthnDigestMethod: XMLSecurity::Document::SHA1
  AuthnSignatureMethod: XMLSecurity::Document::RSA_SHA256
  AuthnCertificate: >
    -----BEGIN CERTIFICATE-----
    MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJVUzER
    MA8GA1UEChMITmV0c2NhcGUxFTATBgNVBASDFN1cHJpeWEncyBDQTAeFw05NzEw
    MTgwMTM2MjVhFw05OTUwMTgwMTM2MjVhVMEgxCzAJBgNVBAYTAlVTREwDyYDVQQK
    EwhOZXRRZyY2FwZTENMAsgA1UECxmEUHViczEXMBUGA1UEAxMOU3Vwcml5YSB0
    dHkwZDZ8dQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRjgEjmKi
    qG7SdATYazBcABu1AVyD7chRkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1Askz
    Z8AW7LiQZBcrXpc0k4du+2Q6xJu2MPm/8WKuMonTuvzpo+SGXelmHVChEqooC
    wfdiZywyZNMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCGSAGG+EIBAQQE
    AwIAgDAfBgNVHSMEGDAWgBTy8gZzkBhHUfWJm1oxeuZc+zYmyTANBgkqhkiG9w
    0BAQQFAAOBgQBtI6/z07Z635DfzX4XbAFpj1Rl/AYwQzTSYx8GfcNAqCqCwa
    SDKvsuj/vwbf91o3j3UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uvi00m
    JYw8W2wUOsY0RC/a/IDy84hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfprqj
    d1A==
    -----END CERTIFICATE-----
  AuthnPrivateKey: >
    -----BEGIN RSA PRIVATE KEY-----
    MIICXAIBAAKBgQCVqGpH2S7F0CbEmQBgmBiDiOOGxhVwlg+yY/6OBQoPKcx4J
    v2hvLz7r54ngjaIqnqRNP71jKjFLp5zhnAu9GsdwXbgLPtrmMSB+MVFHTJvK
    jQ+eY9pdWA3NbQusM9uf8dArm+3VrZxNHQbVGXOIAPNHT008cZHMSqIDQ6Ov
    Lma7wIDAQABAoGAbxKPzsNh826JV2A253svdnAibesWBPgl7kBIrR8QWDctkH
    9fvqpVmHa+6pO55bShQyQSCkxa9f2jnBorKK4+0K412TBM/SG6Zjw+DsZd6
    Vuoz7P027mstTWQrMBxgHjgs7FSftj76HQ0OZxFeZ8BkIYq0w+7VQYAPBWEPS
    qCRQAECQQDv09M4PyRVWSQM S8Rmf/jBwMnY1gPPEOZD0iSWJqIBZUBznvOP
    OQSH6B+vee/q5edQA20IaDgNmn AurEtUaRAkEan7/65w+Tewr89mOM0RKMV
    PfpwNfGYA j3kT1mFEYDq+iNWdcSE6xE
```

```
2H0w3YEBdSsayxc36efFnmr//4ljt4iJfwJAalpOeicJhIracAaaa6dtG1/0AbOe
f3NibugwUxIGWkzlXmGnWbI3yyYoOta0cR9fvjhxV9QFomfTBcdwf40FgQJAH3MG
DBMO77w8DK2QfWBvbGN4NFTGYwWg52D1Bay68E759OPYVTMm4o/S3Oib0Q53gt/x
TAUq7IMYHtCHZwxkNQJBAORwE+6qViv/ZSP2tHLyf8DGOheEBJtQcVje7PfUjAbH5
lr++9qUfv0S13gXj5weio5dzgEXwWdX2YSL/asz5DhU=
-----END RSA PRIVATE KEY-----
```

3. Restart Faspex services

```
asctl faspex:restart
```

Handling Sender and Recipient Information in Tags

Faspex adds sender and recipient information to a transfer's `ascp` tags if the `UserFieldsInTags` setting is configured in `/opt/aspera/faspex/config/faspex.yml` and if the information does not exceed the `MaxTagsLength` field (also set in `faspex.yml`).

Faspex enforces a limit on tag length due to a limitation in `ascp`. If the tag length exceeds 4096, `ascp` does not start a transfer. To account for this limit, Faspex adds information to the tags on a best-effort basis. If at any point the total length of the tags exceeds the value in `MaxTagsLength`, Faspex removes the last added tag to keep the tag length below the limit and stops adding tags.

MaxTagsLength and Core Information in `ascp` Tags

The default `MaxTagsLength` value (1500) works with Faspex out of the box, but may not support your usage and use cases. The default value allows Faspex to generate tags with information core to Faspex features. In some cases, if metadata included in those tags grow too large, Faspex may try to generate tags with a length that exceeds the `MaxTagsLength` value. In that case, no tags are added. This causes some Faspex features, such as transfer relays, to not work.

If Faspex features are not working due to limited tag length, you may want to increase the value of `MaxTagsLength` (within the 4096-byte limit). This may bring other limitations and failures to downstream applications. For example, HTTP Gateway and Connect add information to the `ascp` tags and may also hit the 4096-byte, tag-length limit in `ascp`, resulting in failing transfers.

MaxTagsLength, UserFieldsInTags, and Sender/Recipient Information in `ascp` Tags

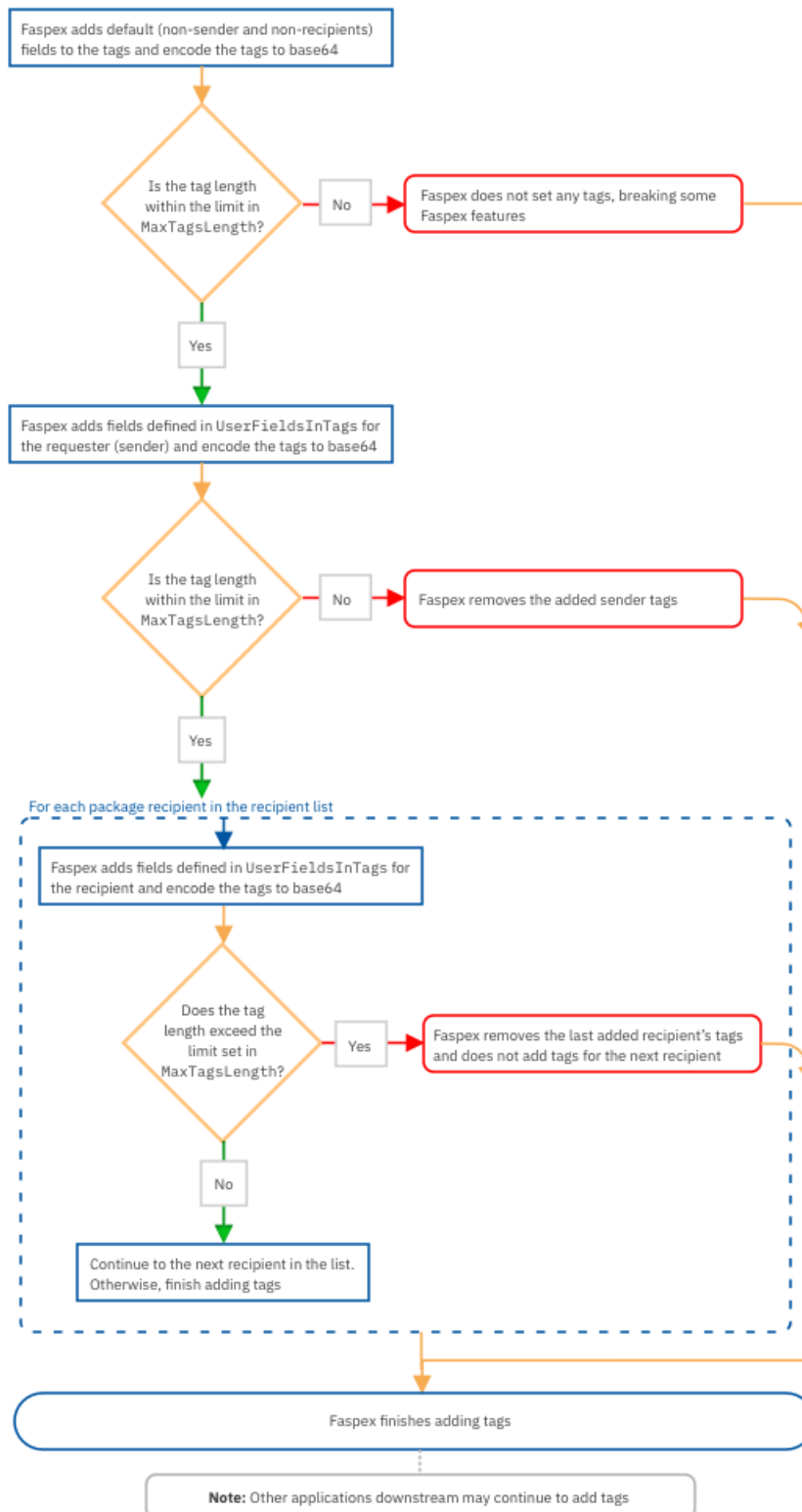
The default `UserFieldsInTags` list (`email, first_name, last_name, name`) works with Faspex out of the box, but may not support your use case, depending on what information you may need to provide to other applications. For example, if you have Console reporting on Faspex custom fields or the SAML `member_of` field, you must add those fields to the `UserFieldsInTags` list, or those Console reports will fail or will be inaccurate.

Depending on the number of recipients of a transfer, the limit set in `MaxTagsLength`, and the fields included in `UserFieldsInTags`, Faspex may end up reporting a limited set of recipients (or none at all). This may impact external applications that rely on information stored in `ascp` tags. For example, Console reports may not include the full list of recipients.

Note: If Console does not report the full list of recipients - length of the recipient list does not match the value reported in the `num_recipients` field in the `ascp` tags - use the Faspex [/packages/{package_delivery_id}](#) v4 API endpoint to retrieve all recipient information.

Tag Insertion Logic

Determine whether Faspex includes user fields in **ascp** tags used by Faspex features and other applications:



faspex.yml Configurations Reference

The `faspex.yml` configuration file provides configuration options not available in the Faspex web UI. You can find the file at `/opt/aspera/faspex/config/faspex.yml`.

Important:

- Modifying `faspex.yml` is for advanced administrative users only.
- Be sure to back up `faspex.yml` before modifying.

The following tables describe hidden options, along with their default values, that can be added to the `production` section of `faspex.yml`. For example, to require newly created users to reset their passwords the first time they log in, add `ForcePasswordResetForNewUsers: true` to the `production` section of `faspex.yml`.

```
production:
...
ForcePasswordResetForNewUsers: true
...
```

Note: Whenever you modify `faspex.yml`, restart Faspex for the new configuration to take effect:

```
asctl faspex:restart
```

Web Server Configuration

Option	Description	Default
<code>UseApachePortsForHttpFallback</code>	Forces Faspex to use its own Apache ports (usually 80/443) for the HTTP Fallback service.	false

Directory Services

Option	Description	Default
<code>CanonicalizeLdapGroupMembers</code>	Causes Faspex to strip spaces out of DNs during comparisons that can prevent Faspex from properly identifying DS users. You should only set this option to <code>true</code> if your LDAP server returns DNs with inconsistent spacing (for example, inserting or omitting spaces when user info is queried as part of an LDAP group vs. individually). Valid values: <code>true</code> , <code>false</code> .	false
<code>DsCheckPeriod</code>	Specifies check period for synchronization operations. It is during these checks that the <code>DsSyncPeriod</code> parameter is used to determine if synchronization is necessary.	600 (seconds) / 10 minutes
<code>DsSyncActiveState</code>	Determines whether to sync the active state. Valid values: <code>true</code> , <code>false</code> .	true

Option	Description	Default
DsSyncPeriod	Specifies how much time must pass since the last synchronization operation in order for a group or user to be judged in need of another.	3600 (seconds) / 1 hour
DsUsernameAttribute	Specifies the DS attribute to use as the Faspex username. The chosen attribute should be unique. Note: Set this option before importing any DS users. Do not change this option after importing users. Examples: mail, saml_account_name (Active Directory).	Depends on attributes returned by directory service
SearchPrimaryDNs	Use an alternative method to import AD users in a non-standard primary group (any group that is not called "Domain Users").	false

Security

Option	Description	Default
StrongPasswordRegex	A regular expression that can be used to customize strong password requirements. Changing this setting does not affect existing passwords, but any new password must match with this regular expression. Example: (?=.*[A-Z])(?=.*(\d W _)).{7,}	(?=.*\d)(?=.*([a-z] [A-Z]))(?=.*(\W _)).{6,}
StrongPasswordRequirements	An explanation of the strong password requirements defined by StrongPasswordRegex. Example: "Must be at least seven characters long, with at least one capital letter and one number or symbol."	"Must be at least six characters long, with at least one letter, one number, and one symbol."
ForcePasswordResetForNewUsers	Setting this option to true requires newly created users to reset their passwords the first time they log in.	false
SSLCAFile	Specify the path to the CA certificates to use to verify peer certificates (such as the certificates on a node when connecting to the Node API). false.	Path to the system's built-in certificates.

Self-Registered and External Users

Option	Description	Default
EnforceSelfRegisteredUserEmail	Prevents registering for an account using an email address that is already used by a full Faspex user (for example, not merely in use by an external email user record). Valid values: true, false.	false (not enforced)
SelfRegistrationUsesEmailAsLogin	Forces self-registering users to choose a login name that is in the format of an email address. This makes entering email address redundant but it is still required. Valid values: true, false.	false (not enforced)
RequireExternalRecipientsToSelfRegister	When a package is sent to an external email address, the recipient is required to self-register with that email address as the account name in order to access the package. Valid values: true, false. Important: You must enable self-registration or the recipient is redirected to "Page not Found". For more information, see Configuring Security Settings on page 47. Tip: You can require admin moderation for users creating new accounts with self-registration. For more information on self-registration settings, see Enabling Self-Registration on page 124.	false (not enforced)
HideSenderUsernameToExternalRecipients	When external users download a package, the Connect logs and Connect manifests do not show the sender's username.	false

Metadata

Option	Description	Default
SaveMetadataInPackage	Whenever this option is set to true and the Save metadata to file option is enabled on the Metadata Profiles page, the Create New Dropbox page, or the Edit Dropbox page, the metadata file is included inside packages, instead of being deposited in a package's root directory. Set the <code>SaveMetadataInPackage</code>	false

Option	Description	Default
	option in the "Production" section of the faspex.yml file. For more information, see Applying Metadata Profile to Normal Packages on page 147.	
ExcludeMetadataFromCookie	This setting excludes metadata from Faspex cookies. It also relaxes the length requirements on metadata from 2,000 characters per profile to 30,000 characters. Note: This option prevents IBM Aspera Console from reporting the metadata of Faspex transfers.	false
HideRelayInformation	This setting hides relay information on the Package Details page.	false


Timeouts


Option	Description	Default
PackageUploadTimeout	The timer starts when a user sends a new package. Even if queued, if a package does not start within the package upload timeout, Faspex marks the package as "Upload never started" and sends a failure notification to the Upload CC list. Extend the duration to account for transfers that may stay queued longer than the default duration.	60
LiveUpdateInterval	The interval sets the frequency in seconds that Faspex updates package or relay lists on these pages: <ul style="list-style-type: none"> • All Packages (Server > Packages) • Relays (Server > Packages > Relays) • Relay Details (Server > Packages > Relays > relay) • Received Packages • Received Packages History • Sent Packages • Sent Packages History • Pending Packages • Pending Packages History • Workgroup Packages By default, Faspex refreshes the lists every 5 seconds.	5

Accepted Hosts

Option	Description	Default
AcceptedHosts	The AcceptedHosts configuration defines a list of hostnames users can access Faspex through. If you try to log in to the web application from an unlisted hostname or perform a GET request with an unlisted hostname, Faspex returns the error, "Invalid hostname". To access Faspex from an alternate hostname, whitelist alternate hostnames by following the instructions in Configuring the Faspex Web Server on page 32.	No whitelist defined

Tags

Option	Description	Default
MaxTagsLength	<p>The MaxTagsLength field limits the total length (after base64 encoding) of Faspex-generated tags for the <code>ascp</code> command. The value cannot exceed 4096 chars (bytes) due to a limitation in <code>ascp</code>.</p> <p>Note: If you set a value higher than 4096, Faspex sets the value to 1500.</p> <p> Warning: Setting the MaxTagsLength value too low can result in Faspex features not working correctly, because some Faspex features rely on information in <code>ascp</code> tags. For more information, see Handling Sender and Recipient Information in Tags on page 152.</p>	1500
UserFieldsInTags	The UserFieldsInTags field determines what fields Faspex includes in sender and recipients fields in Faspex-generated tags for the <code>ascp</code> command. For example, setting <code>UserFieldsInTags: email, Company</code> includes the sender's and recipients' email addresses and their Company custom-field values in the tags.	<code>email, first_name, last_name, name</code>

Option	Description	Default
	<p>Note: The <code>member_of</code> SAML field is not included by default. If you are running Console reports based on the <code>member_of</code> field, add the field to the <code>UserFieldsInTags</code> field.</p> <p> Warning: If the <code>UserFieldsInTags</code> is cleared and left empty, Faspex does not add any sender and recipient information in the tags. Doing so may break Console reports that rely on that information.</p>	

Validating Packages and Files with IBM Aspera Validator

IBM Aspera Validator is service that validates files transferred to a local or remote IBM Aspera High-Speed Transfer Server. As soon as a client completes a transfer to the server, Validator runs a user-provided Lua script to validate transferred files. Use Validator to validate Faspex packages and files by either configuring Validator to monitor an existing HSTS node used as Faspex file storage, or by adding a Validator-monitored node to Faspex as file storage.

Installing and Configuring the Validator Service

Validator can validate files from multiple HST Server nodes. HST Servers used in Faspex as file storage must be added to Validator's `Servers` list for Faspex to validate packages and files. Validator requires access to the file storage on each HST Server node used as Faspex file storage where you want validation to take place.

Note: Validator is a standalone product that has separate documentation. For instructions on installing and configuring Validator, see the *IBM Aspera Validator Admin Guide*.

1. Go to **Server > Security** and enable the **Out-of-transfer file validation (otfv)** setting.

This setting enables Faspex reporting on file validation status. Since Validator performs validation directly with HSTS nodes, leaving this option disabled does not prevent Validator from performing file validation.



Warning: Enabling this option may cause performance issues for customers running millions of transfers, including slow UI and stats collector performance.

2. To prevent security breaches, disable downloads during transfer. Otherwise, users can download files from a package before the files pass validation.

Go to **Server > Transfer Options** and clear the **Enable downloads during transfers** option.

Monitoring Validation

When Faspex detects new package transfers, Faspex reports validation states for the related packages as validation happens.

Faspex uses the package statuses:

- `validating`

- completed
- validation failed

You can see the package validation statuses wherever you can see a package status in the UI.

If any file in the package fails validation, the entire package is flagged as `validation failed` and therefore cannot be downloaded as a whole package. For 30 days, Faspex shows the validation failure messages for the specific files that failed within the package. In those 30 days, you can download individual files in the package that passed validation and that are still available in the storage, but after 30 days, you cannot.

Note:

Faspex uses package-level information (package-transfer status and package-validation status) and file-level information (file-transfer status and file-validation status) to determine if packages and files are downloadable.

By default, Faspex retains file-level information for only 30 days. After 30 days, Faspex determines whether packages and files are downloadable using only package-level information. If the package validation status is `validation failed`, the entire package and its individual files are not downloadable.

You can configure the file-level information retention duration. For more information, see [Changing Stats Collector Purge Frequency](#) on page 163.

Validation and Relays

Faspex only supports validation happening on the direct-upload file storage, and does not support validation for any relay.

Possible scenarios include:

Scenario	Validation Performed	What does Validator work with?
Transfer a package with the default inbox.	Validator performs validation for packages transferred to the default inbox.	Default inbox file storage
Transfer a package to a workgroup or dropbox with a custom inbox.	Validator performs validation for packages transferred to the default inbox, but not for the relay to the custom inbox.	Default inbox file storage
Transfer a package to a workgroup or dropbox with a custom inbox and direct upload enabled.	Validator performs validation for packages transferred to the custom inbox.	Custom inbox file storage
Transfer a package to a workgroup or dropbox with relays.	Validator performs validation for packages transferred to the default inbox, but not for the relays to the relay destinations.	Default inbox file storage
Transfer a package that has metadata that define relays.	Validator performs validation for packages transferred to the default inbox, but not for the relays to the relay destinations.	Default inbox file storage

Troubleshooting Validation

Faspex relies on Validator for validating files. Troubleshooting the Validator servers should solve most validation issues. If packages and files are stuck in the `validating` state because of a Validator issue, Faspex cannot make them available.

For troubleshooting Validator issues, see *IBM Aspera Validator Admin Guide: Troubleshooting*.

Note:

If previously downloadable files in a package are no longer downloadable and files are still present on the file storage, check the package validation status and the package age. If the package failed validation and the package age is older than 30 days, Faspex has cleared file-level information and uses package-level information to determine if package files are downloadable.

For more information, see [Monitoring Validation](#) on page 159.

Troubleshooting Faspex

Common Errors in Faspex

Errors Displayed in IBM Aspera Connect

When uploading a file to Faspex, Faspex launches Connect to perform the transfer from your machine to the server. If the upload fails, Connect displays an error. See below for common error messages.

Error Code	Error Message	Issue	Solution
Code 44	Error: Failed to open TCP connection for SSH	Faspex uses port 33001 to connect to the node. If the node is running a Linux operating system, port 33001 may not be open.	<p>If your node is a Linux machine, open the sshd_config file (<code>/etc/ssh/sshd_config</code>) in text editor and add the line <code>Port 33001</code> to the configuration file to enable access to port 33001.</p> <p>Restart the service:</p> <pre># service sshd restart</pre>
Code 19	Error: Authentication failed	Faspex uses Connect key to authenticate an SSH connection with Connect. An authentication failure may mean a missing key.	<p>Copy the contents of the key (<code>/opt/aspera/var/aspera_id_dsa.pub</code>) into the authorized_keys file (<code>/home/faspex/.ssh/authorized_keys</code>).</p> <p>Note: Make sure the authorized_keys file has no file extension. Some text editors add a .txt extension to the filename automatically. Be sure to remove the extension if it was added to the filename.</p>

Package Creation Error on the New Package Page

When trying to create a new package (**New Package** or **New Package > Normal Package**), Faspex displays the `Package creation failed` error message.

Faspex may display this error message if HTTP Fallback is configured incorrectly. The fallback settings for the transfer server product (IBM Aspera High-Speed Transfer Server) must match the Faspex fallback settings. For more information, see [Configuring HTTP and HTTPS Fallback](#) on page 40.

Resetting Admin Password

To reset the Faspex admin password, execute the following command:

```
asctl faspex:admin_user name email
```

You can also enter the new admin password in the command:

```
asctl faspex:admin_user name email password
```

Troubleshooting File Storage Errors

If file storage is not properly configured for Faspex, Faspex displays the following error at the top of every page: "WARNING! Transfer server errors detected, transfers may not operate correctly"

You can test the file storage for errors by testing the connection between Faspex and the remote transfer node. Go to **Server > File Storage**, click the arrow next to the node, and select **Edit** from the drop-down menu. Select **Test Connection**. If the connection is successful, Faspex displays: "Connection succeeded!" Otherwise, Faspex displays an error.

See the following list of common errors and their possible solutions:

not pingable: SSL error

Faspex displays this error if you select **Verify SSL Certificate** but do not have a valid SSL certificate installed. Deselect **Verify SSL Certificate** or install a valid SSL certificate following the instructions in [Installing a Signed SSL Certificate Provided by Authorities](#) on page 55.

not pingable: Connection refused

Faspex may display this error if the Aspera NodeD service is down. To restart the Aspera NodeD service, on the node, run the following command

```
# service asperanoded restart
```

The connection may also be refused if the SSH port (port 22) is closed on the node. To check and open the port, follow the instructions below:

1. Open the `/etc/ssh/sshd_config` file in a text editor.
2. If `Port 22` is commented, uncommented the line. If `Port 22` is missing, add the line into the file.
3. Save the file.
4. Restart the SSH service:

```
service sshd restart
```

not pingable: Internal error

Node not configured correctly. For example, no valid license?

1. First, restart the Aspera NodeD service. It is possible that you made changes to `aspera.conf` or the license file without restarting Aspera NodeD. The service must be restarted for Faspex to recognize the changes. To restart the Aspera NodeD service, on the node, run the following command

```
# service asperanoded restart
```

2. If the issue is not resolved, make sure the node is fully configured for use with Faspex by reviewing the node setup instructions. For more information, see [Adding a Node to Faspex](#) on page 59.

not infoable: Not authorized

The Node API user credentials you entered do not match a valid Node API user on the transfer node.

1. Log into your transfer node and run the following command:

```
# /opt/aspera/bin/ asnodeadmin.exe -l
```

2. If your Node API user is not listed in the output or it is not associated with the **faspex** system user, use the correct user associated with the **faspex** system user or create a new Node API user and associate it with the system user. To create a new user, run the following command:

```
# /opt/aspera/bin/asnodeadmin -a -u node_username -p node_password -x
faspex
```

For example:

```
# /opt/aspera/bin/asnodeadmin -a -u faspex_node_user -p ***** -x
faspex
```

Changing Stats Collector Purge Frequency

The Stats Collector service holds file-level information in its database (in the `fasp_files` table), and purges that data 30 days (by default) after.

Customers making a large number of transfers may find their `fasp_files` table growing too fast. You can decrease the purge frequency by going to the `opt/aspera/faspex/lib/daemons/np/etc/stats-collector.properties` file and changing the value of the `purgestats.age` property. For example:

```
purgestats.age=7d
```

Important: IBM Aspera Validator reports file-level validation status in the `fasp_files` table. Lowering the `purgestats.age` value lowers the duration that Faspex has access to file-level validation status. For example, changing the value to `7d` means that, after 7 days, Faspex no longer has access to file-level information and must use package-level information to determine whether packages and files are downloadable. If the package validation status is `validation failed`, the entire package and its individual files are not downloadable.

Log Files

Faspex keeps most logs in the `/opt/aspera/faspex/` and `directories`.

Log File Locations

You can find log files for Faspex and its associated components in the following files and directories:

- **Faspex:** `/opt/aspera/faspex/log`
- **asctl:** `asctl`
- **MySQL:** `mysqldatamysqld_error.log`
- **Apache:** `apachelogs`

The `faspex/log` file includes the following log files:

- `faspex_background.log`
- `faspex_db_background.log`
- `faspex_ds_background.log`
- `faspex_email_background.log`
- `faspex_np_background_start.log`
- `mongrel.3xxx.log`

- `production.3xxx.log`
- `production.log`
- `statscollector.log`

Note: If you are encountering issues with updating transfer statuses in Faspex (for example, though a transfer has finished, Faspex still considers it to be uploading) the issue may be related to the stats collector.

Faspex Apache Logs

The Faspex Apache log folder contains the following files:

- `access_log`
- `error_log`
- `ssl_access_log`
- `ssl_error_log`
- `ssl_request_log`

Apache's log files are not automatically deleted. If you would like to remove old logs, it is recommended that you create a *cron job* to do so.

For example, to remove Apache log files that are 30 days or older, run the following command:

```
# find /opt/aspera/common/apache/logs -mtime +30 -exec rm {} \;
```

You can use the following commands to configure the Faspex Apache's log settings:

Setting	Command
Specify Apache log level (error level)	<code>asctl apache:log_level error</code>
Enable Apache log (set to notice)	<code>asctl apache:enable_logs</code>
Disable Apache log (set to emerg level)	<code>asctl apache:disable_logs</code>

Transfer logs are recorded into the system log file in the following location:

Platform	Path
RedHat	<code>/var/log/messages</code>
Debian	<code>/var/log/syslog</code>

Important: Older log files are saved as the same file name, with an incremental number attached (for example, `ascmd.0.log`).

Restarting Faspex and Common Aspera Services

Faspex Services

Restart Faspex services using the `asctl` command:

```
asctl faspex:restart
```

Restarting Aspera Services

If configuration changes you have made are not taking effect, or Faspex is otherwise not working as expected, the problem may stem from Aspera services not having been started or restarted. Examples:

- If you did not choose to start services such as Aspera Node Service (also known as Aspera NodeD) when prompted to do so during the Faspexsetup process, you may need to start them manually.
- Changes to `aspera.conf` may require you to restart Aspera Central (`asperacentral`) or Aspera NodeD (`asperanoded`). For example, any changes to the `<central_server>` section of `aspera.conf` (such as enabling `<persistent_store>`) require you to restart Aspera Central.
- If you see a notice about transfer server errors on the login page for Faspex, you need to install or update your IBM Aspera High-Speed Transfer Server license.

To check whether the Aspera node service or Aspera Central is running, you can use the **ps** command and **grep** for **aspera**, then look for **asperanoded** or **asperacentral**; for example:

```
# ps -e | grep aspera
```

To restart **asperanoded** or **asperacentral**:

```
# service asperacentral restart
# service asperanoded restart
```

Restarting Aspera Services

Aspera Central

If Aspera Central is stopped, or if you have modified the `<central_server>` or `<database>` sections in `aspera.conf`, then you need to restart the service.

Run the following command in a Terminal window to restart `asperacentral`:

```
# /etc/init.d/asperacentral restart
```

Aspera NodeD

Restart Aspera NodeD if you have modified any setting in `aspera.conf`.

Run the following commands to restart `asperanoded`:

```
# /etc/init.d/asperanoded restart
```

Aspera HTTPD

Restart Aspera HTTPD if you have modified any setting in `aspera.conf`.

Run the following commands to restart `asperahttpd`:

```
# /etc/init.d/asperahttpd restart
```

Appendix

High Availability Configuration

Introduction

IBM Aspera Faspex is a global person-to-person file delivery and collaboration platform for file-based collection, distribution, and collaboration among geographically dispersed teams. Faspex users can send and receive digital packages using a standard web browser, a desktop application, a mobile app or an add-in for Microsoft Outlook.

Leveraging IBM Aspera's patented *fasp* transport technology, Faspex delivers reliable, ultra-fast transfers, enterprise-grade security, and precise control over transfer settings and user permissions. Deployable on premise and on public, private or hybrid cloud platforms, Faspex is designed for extreme scalability and can seamlessly support thousands of concurrent transfers within a globe-spanning network of IBM Aspera transfer servers and clients.

Faspex can be deployed in a high availability (HA) environment. This document presents the Faspex HA Active/Active solution that leverages the Aspera Cluster Manager (ACM) software.

Intended Audience of This Document

This document requires that:

- You have background as a network engineer.
- You are knowledgeable about HA environments.
- You are familiar with the requirements of your use case.
- You are familiar with the Shares and High Speed Transfer Server products.
- You have expertise and experience configuring third-party systems, such as shared storage and load balancers.

How to Use This Document

This document is intended to be used as a basic guideline to inform and facilitate the customer's ability to craft a HA solution to match the requirements of the customer's particular use case. Each use case differs in requirements, including:

- Approved technology and software vendors
- Hardware sizing requirements
- Security requirements
- Type of shared storage
- Estimated traffic load and required bandwidth
- Budget to cover costs

Procedures for setting up third-party systems such as shared storage and load balancers are outside the scope of this document.

Note: Due to the complexity of any high-availability setup due to differing requirements for each customer, Aspera recommends customer engage with IBM professional services to do an HA install or upgrade of IBM Aspera products. This document primarily serves as a reference detailing basic considerations and requirements to operate IBM Shares in an HA configuration. You can engage professional services by contacting your sales representative.

Covered Use Case

The use case described in this guide is a dual, Shares instance cluster, where the traffic is balanced between two active nodes, providing a high-availability service with seamless automatic fail-over in the event that one node fails or becomes unavailable.

It is possible to have more than two nodes in an HA environment, but that configuration is outside the scope of this document.

It is also possible to separate the web application from the transfer server portion in order to run these services on different hosts. You can find instructions on separating these processes in the *IBM Aspera Shares Admin Guide*, but neither this document nor those instructions cover that procedure for HA environments.

Note: This HA solution supports Linux platforms only.

Architecture for High Availability Systems

Overview of HA Architecture

When implementing an active/active highly available environment for IBM Aspera Faspex, you can deploy two different types of architecture.

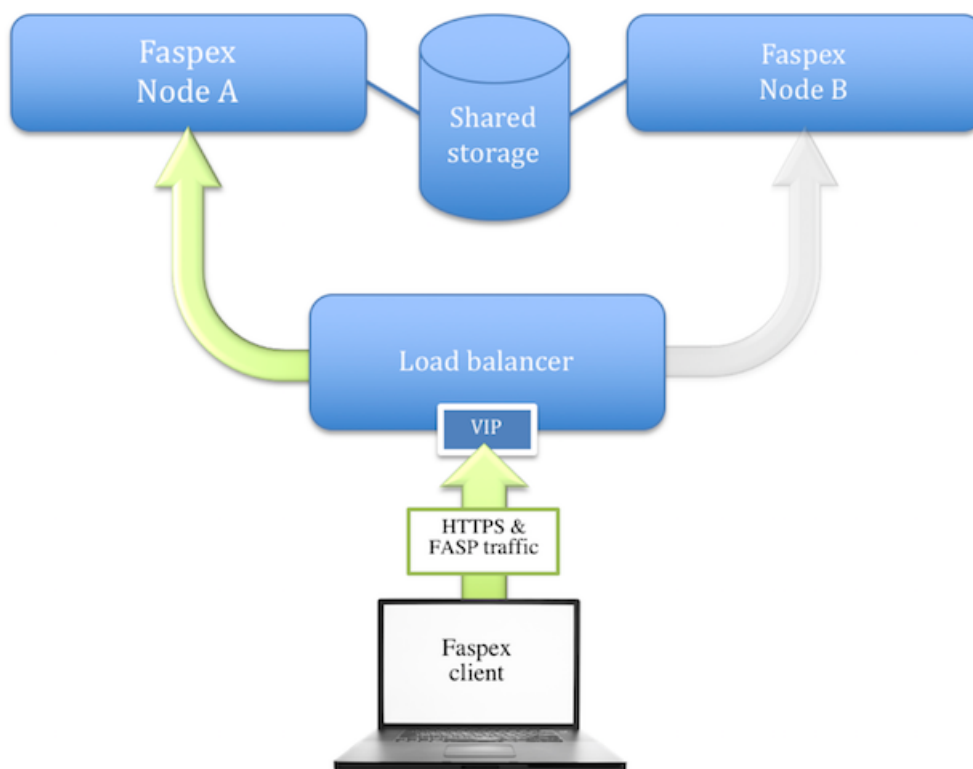
Both architectures implement a load balancer that monitors the health of each IBM Aspera Faspex node and redirects the traffic accordingly, balancing the load between all healthy nodes.

When the load balancer detects that an Shares node is unreachable, it automatically stops redirecting traffic to the unavailable node, and redirects all traffic to the remaining healthy nodes.

Once the faulty node can be reached, the load balancer automatically detects the presence of the new healthy node and includes it in the traffic-sharing function. The nodes share the load related to the web traffic and *fasp*-based transfers, utilizing all available servers.

Architecture Type 1: Redirect All Traffic

One form of load-balancing architecture provisions the load balancer with a virtual IP address (VIP) for user access; the load balancer then manages all the traffic related to the IBM Aspera Faspex service: the web requests (HTTPS/TCP traffic) as well as the FASP transfers (SSH/TCP and FASP/UDP traffic). A fully qualified domain name (FQDN) #typically `faspex.mydomain.com`#is used to access the Shares service and points to the VIP of the load balancer.

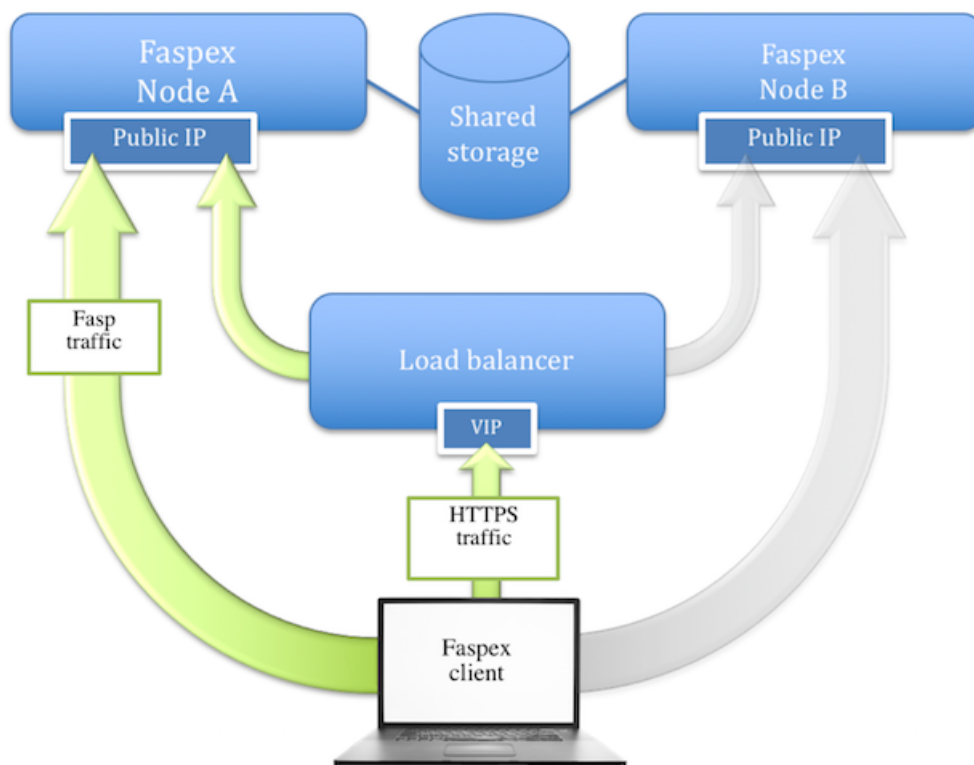


In this architecture, both Shares nodes can use private IP addresses. Only the VIP requires a public IP address, because it will be used by the clients to connect to the Shares service components.

Because the *fasp* transfers represent most of the total traffic generated by the Shares service, the load balancer must be powerful enough to handle the associated load. In some environments, this could mean a total bandwidth of up to several gigabits per second.

Architecture Type 2: Load Balancer Redirects Web Traffic Only

An alternative architecture requires the load balancer to handle the web traffic only. In most respects, the architecture for this environment is like the first model—it uses a load balancer with a virtual IP address (VIP), plus a FQDN that points to the VIP to let clients access the web application. However, in this architecture, the load balancer is used for redirecting web traffic only.



The traffic related to the FASP-based transfers takes place directly between the clients and the transfer services running on both nodes. In order to balance and fail-over the traffic in the event that the node is unavailable, Shares uses *another* FQDN (typically `faspex.mydomain.com`) which is resolved into a list containing the public IP addresses that point to the different nodes. The DNS in charge of resolving that domain name must provide a round-robin-type list, with the list entries presented in a different order every time a response to a new DNS query is sent. In this way, successive queries coming from different clients will see a different IP address on the top of the list. Because the High Speed Transfer Server clients only use the IP address at the top of the list to contact the transfer server (and this IP address is different each time), multiple clients connect to different transfer servers (nodes A and B).

Whenever a client is unable to connect successfully to a transfer server (because it is unavailable), it continues to resolve the FQDN and to make attempts to contact the IP address at the top of the new list. When the top IP address points to a healthy node, the client performs a successful transfer.

This process typically takes less than a minute. In order to keep the fail-over delay as short as possible, the Time-To-Live (TTL) value of the round-robin FQDN list must be kept as short as possible on the DNS server.

Shares Services Stack

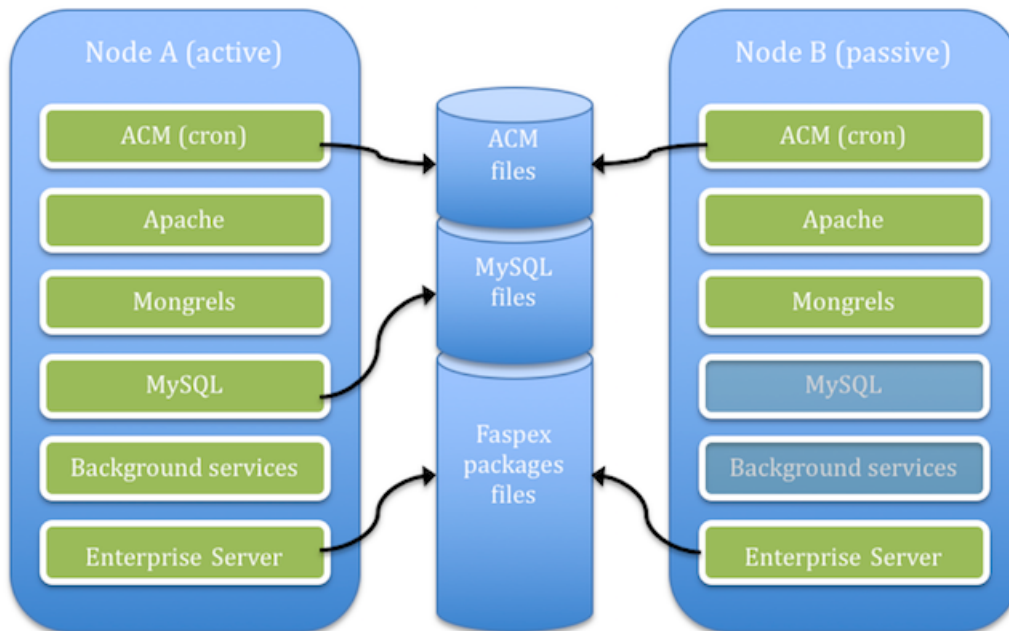
Regardless of which architecture is deployed, both IBM Aspera Faspex nodes are considered *active* because clients can contact any of them to access the web application portion or the transfer server portion. Nevertheless, not all of the IBM Aspera services run at the same time on both machines.

While some services are considered *active/active* and do run on both nodes, other services are considered *active/passive* and only run on one of the two nodes. The node that runs all the services is called the *active* node, and the node that only runs the *active/passive* services is called the *passive* node.

Shares Services Stack

Regardless of which architecture is deployed, both Faspex nodes are considered *active* because clients can contact any of them to access the web application portion or the transfer server portion. Nevertheless, not all of the IBM Aspera services run at the same time on both machines.

While some services are considered *active/active* and do run on both nodes, other services are considered *active/passive* and only run on one of the two nodes. The node that runs all the services is called the *active* node, and the node that only runs the *active/passive* services is called the *passive* node.



In the diagram above, the `mysql` service runs only on the active node. While both nodes can access the ACM files and the Shares packages simultaneously (read-write mode), the MySQL data files are accessed at a specific time by a single instance of the MySQL service running on the active node.

The following table lists each service and its location:

Service Name	Type	Location
<code>aspera_httpd</code>	<i>active/active</i>	Runs on both nodes
<code>aspera_mysql</code>	<i>active/passive</i>	Runs on the active node only
<code>aspera_faspex_mongrel</code>	<i>active/active</i>	Runs on both nodes
<code>aspera_faspex_background</code>	<i>active/passive</i>	Runs on the active node only
<code>aspera_faspex_np_background</code>	<i>active/passive</i>	Runs on the active node only
<code>aspera_faspex_ds_background</code>	<i>active/passive</i>	Runs on the active node only
<code>aspera_faspex_db_background</code>	<i>active/passive</i>	Runs on the active node only

Service Name	Type	Location
aspera_faspex_email_background	active/passive	Runs on the active node only
asperahttpd	active/active	Runs on both nodes
asperanoded	active/active	Runs on both nodes

Note: The last two services in the list belong to IBM Aspera High-Speed Transfer Server and are not managed by ACM. These services are started by the operating system at boot time, and they must always be running on both nodes.

IBM Aspera Cluster Manager (ACM) for IBM Aspera Faspex

ACM is the software module responsible for starting the right services on a node according to that node's current status (active or passive). It is also in charge of monitoring the active node to determine when to fail-over the active/passive services from the active to the passive (when the active node becomes unresponsive).

Note: ACM must run as `root`.

How does it work?

ACM is installed on both nodes; it is launched simultaneously on both nodes—every minute—by the `crond` daemon.

Both instances of ACM first determine the status of the node on which they are running by checking a common status file stored on the shared space dedicated to ACM. In order to avoid a race condition while accessing that common status file, a specific locking mechanism (`aslockfile`) is used to synchronize both instances.

Once the status of a node is determined, the ACM instance running on the active node verifies that all of the services are running, and it starts any service that is not running. Once this is done, the instance updates the status file in order to keep its last modification date current.

The ACM instance running on the passive node checks that the status file is *current*, meaning that its last modification date is not older than 2 minutes). If the file is current, ACM checks that the *active/passive* services are up and running; it then starts all the services that are not running currently but should be running. If the common status file is no longer current, then it is a fail-over scenario, and ACM takes over as the new active node by starting all of the services.

How long does a fail-over process take?

If the passive node fails, then ACM does nothing. It is up to the load balancer to detect that the passive node is unresponsive and redirect the traffic accordingly. In the scenario covered by this documentation, the process typically takes one minute or less.

If the active node fails, then ACM eventually detects that the status file is no longer current and it triggers a fail-over. Additionally, the load balancer detects that the active node is down and it redirects all traffic to the healthy node. This process typically takes up to 5 minutes.

Related information

[Expected Load Balancer Behavior](#) on page 170

A load balancer monitors the health of each Shares nodes and redirects the traffic accordingly, balancing the load between all healthy nodes.

Expected Load Balancer Behavior

A load balancer monitors the health of each Shares nodes and redirects the traffic accordingly, balancing the load between all healthy nodes.

This topic describes how the load balancer should function when handling HTTPS traffic and FASP transfers.

Note: This topic *does not* describe how to set up and configure a load balancer. For instructions on configuring a load balancer, refer to the documentation of your load balancer.

HTTPS Traffic

The load balancer must monitor the health of the HTTPS service running on each node. To do this, it can either use a method based on an HTTPS request, or simply check whether TCP port 443 is responding, that is, whether a SYN ACK packet is received after a SYN packet is sent by the monitoring service. If an RST packet is received instead, or if no packet is received at all, then the monitoring feature must consider the monitored service to be down and discard the related node (take it offline).

The load balancer can redirect any HTTPS request to any of the healthy nodes. Because the Shares web application uses a database shared by both nodes, any healthy node can respond to any request.

FASP Transfers

Once the FASP transfer is initiated by a successful SSH connection (typically using TCP/33001 on the server side), the FASP protocol uses UDP packets for data transfer (typically using a port range of 33001-33100).

When a client establishes a SSH connection, the load balancer has to choose which node will handle this connection. Once it has done so, and the SSH connection is established with one node, the load balancer must make sure that the following is true:

- The TCP connection related to the SSH session stays with the chosen node.
- Any subsequent UDP traffic coming from the same client is directed to the same node. This behavior is generally known as a *sticky/persistent session*, depending on the source IP address of the client.

In other words, if an SSH connection is established between a client with a particular IP address and node A, then all subsequent UDP packets sent from that IP address must be redirected to node A.

If a node is declared unavailable by the load balancer (by checking the HTTPS service or the SSH service), the load balancer needs to redirect all the traffic to the remaining healthy node.

The different types of traffic (SSH/TCP/33001 and FASP/UDP/33001-33100) may need to be joined together in a pool of services on the load balancer side. The exact settings vary depending on the load balancer model.

HTTP Redirection

The Shares application uses HTTPS by default, and it sets an automatic redirection from HTTP/TCP/80 to HTTPS/TCP/443 to force users to use a secure connection.

The load balancer can forward HTTP requests to the nodes, which then handle the redirection. Alternatively, the load balancer itself can handle the redirection; this prevents any insecure connections from being established with a node.

Installation

System Requirements

Use the requirements below to assess whether your resources and third-party systems meet the requirements to deploy a high availability environment.

Hardware	Normal HA operations require two servers. Virtual machines can be used as long as enough resources are allocated to them.
Operating Systems	<p>ACM only supports Linux platforms.</p> <ul style="list-style-type: none"> • RedHat 6 & 7 • CentOS 6 & 7 • SLES 11.4 & 12.3 <p>Note: Red Hat high-availability packages (such as <code>ricci</code>, <code>luci</code>, <code>rgmanager</code>, and <code>cman</code>) are <i>not</i> used, and therefore must not be installed or activated in the environment.</p> <p>The system clocks of all hosts in the HA environment must always be kept in sync in order for ACM to operate correctly. IBM Aspera typically</p>

	recommends using the <code>ntpd</code> daemon, but any time-synchronization mechanism should work fine.
Software	<p>IBM Aspera Faspex version 4.2.0 and higher.</p> <p>IBM Aspera High Speed Transfer Server 3.8.0 and higher.</p> <p>IBM Aspera Cluster Manager: ACM Package</p>
Shared Storage	<p>Shared storage is used for:</p> <ul style="list-style-type: none"> • Faspex packages • MySQL data files • ACM files <p>Important: The shared storage must be 100% reliable and accessible 100% of the time for ACM to secure highly available Shares operation and to prevent Shares data corruption.</p> <p>IBM Aspera recommends dedicating storage for ACM whenever possible, in order not to create I/O bottlenecks when large packages are being transferred to shared storage at very high speeds.</p> <p>ACM has been tested successfully on these shared file systems:</p> <ul style="list-style-type: none"> • NFS (<code>nfs</code> version 4 is required for MySQL data) • Quantum StorNext (<code>cvfs</code>) • Omneon MediaGrid (<code>omfs</code>) • Oracle Cluster File system 2 (<code>ocfs2</code>)
Load Balancer/VIP	<p>A load balancer that implements a VIP (Virtual IP) is required.</p> <p>For more information about what is expected from the load balancer, see Expected Load Balancer Behavior on page 170.</p>

Single point of failure

Aspera strongly encourages customers to consider SPOF (single point(s) of failure) in the environment and to recognize the risks of SPOF. Often, these are situations where all nodes are plugged into the same power strip or surge. It could also be that the shared storage or the load balancer are not HA.

Installing and Configuring the HA Environment

Install two stand-alone IBM Aspera Faspex servers and join them together into an HA environment.

This guide assumes that Shares is installed on two servers with IBM Aspera High-Speed Transfer Servers software installed and configured on each. The HSTS on each server behaves like any other node within the Faspex environment.

Note: All commands are run as root. (The examples in this section are for a CentOS 6.5 system.)

Before You Start

1. Review the [System Requirements](#) on page 171.
2. Check your network settings and names.

Confirm that your network settings are correctly configured and that each host has a unique hostname properly configured within the name resolution mechanism you use (DNS, hosts file, and so on). Each host must be able to resolve its own name, as well as the name of the other node.

Run the following command on both nodes. The resulting system output should make sense in your environment.

```
hostname
```

```
faspexnode1.mydomain.com
```

Securing Your System

Perform the following steps for both nodes.

1. Disable local firewalls.

No traffic filter should be put in place between the two nodes. If your nodes are located behind a corporate firewall (and thus appropriately protected), you should disable the Linux firewall components. Use `chkconfig` to prevent the firewall from becoming active when the system is rebooted:

On an OS running `systemctl`, instead of using `chkconfig`, disable services by running:

```
# systemctl disable iptables
# systemctl disable iptables off
```

Otherwise, run:

```
service iptables stop
iptables: Flushing firewall rules:          [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Unloading modules:                [ OK ]
service ip6tables stop
ip6tables: Flushing firewall rules:          [ OK ]
ip6tables: Setting chains to policy ACCEPT: filter [ OK ]
ip6tables: Unloading modules:                [ OK ]
chkconfig iptables off
chkconfig ip6tables off
```

Note: If the firewall is not disabled, make sure to configure the firewall to open the necessary ports for Aspera. See [TCP and UDP Ports Used in HA Environments](#) on page 195 for a list of ports used by the Faspex HA environment.

2. Disable SELinux.

SELinux must be disabled or set to permissive in the `/etc/selinux/config` file on each High Speed Transfer Server and each Faspex server system. You can confirm the SELinux current status by running the `sestatus` command.

```
sestatus
SELinux status: disabled
```

3. Configure SSH security on each High Speed Transfer Server.

See the *Securing your SSH Server* section in the *IBM Aspera Faspex Admin Guide* for additional information and guidance.

Make sure that public/private key authentication has been enabled on each server. Look for the following line in the `/etc/ssh/sshd_config` file and verify that it is uncommented.

```
PubkeyAuthentication yes
```

If you have modified the `sshd_config` file, you need to restart the `sshd` service:

```
service sshd restart
```

Install and Configure Faspex

1. Create user accounts and groups on each Faspex server.

The `mysql` and `faspex` user accounts and groups must be created manually on both systems before installing any Aspera packages to have consistent UID and GID across the HA environment.

Note: It is critical to ensure that the UID and GID for the `mysql` and `Faspex` user accounts are consistent across all `Faspex` servers.

You can use the following commands on each node to create the required users and groups:

```
groupadd -g 777 faspex && useradd -c "Aspera Faspex" -d /home/faspex -g
faspex -m -s /bin/aspshell -r -u 777 faspex
groupadd -g 778 mysql && useradd -c "Aspera Mysql" -d /home/mysql -g
mysql -m -s /bin/false -u 778 mysql
```

The UID and GID do not have to be 777 and 778, and you can use any value available. Just make sure you use the same values on both systems.

2. Install a standalone Faspex server on each system.

- Install High Speed Transfer Server. Follow the steps in the *IBM Aspera High Speed Transfer Server Admin Guide* to install your software and set up your license.
- Install Aspera Common.
- Install Faspex, answering any question as if you were installing a standalone server running its own transfer service locally.
- Log in to each Faspex server and install your Faspex license on each server.

You can find a detailed procedure in [Installing Faspex with a Local Node](#) on page 10.

3. On both servers, test that you can create, upload, and download new packages successfully.

Note: It is important that you can upload and download packages on each node before proceeding further. You will not have access to the Faspex GUI once you start the HA setup process. Test now so you do not end up having to undo the entire HA setup to troubleshoot the Faspex configuration.

Share Resources Between Nodes

- Choose one node to be the active node.
- On the active node, grant remote access to MySQL for both nodes.

Run the following commands and set the password. The password you choose must be the same for. The Aspera Cluster Manager (ACM) uses this password to access the database.

Tip: ACM uses "aspera" as a default password. You will provide the password you chose in a later step to ACM by editing the `acm` configuration file.

```
asctl mysql:grant_remote_access "local_server_ip_address"
New password: password
Confirm new password: password
asctl mysql:grant_remote_access "other_server_ip_address"
New password: password
Confirm new password: password
```

3. Configure the passive node to allow MySQL connections to the active node.

```
asctl mysql:grant_remote_access "active_node_ip_address"
New password: password
Confirm new password: password
```

Note: The password you choose must be the same as the password you provided in the previous step.

4. Stop and disable Faspex services.

ACM takes charge of starting the Faspex services. You must disable those services from the system boot-up process.

First, stop all Faspex services on both nodes:

```
asctl all:stop
```

Then disable the services on both nodes.

On an OS running `systemctl`, instead of using `chkconfig`, disable services by running:

```
systemctl disable aspera_mysqld; systemctl disable
aspera_httpd; systemctl disable aspera_faspex_np_background; systemctl
disable aspera_faspex_mongrel; systemctl disable
aspera_faspex_ds_background; systemctl disable
aspera_faspex_db_background; systemctl disable
aspera_faspex_background; systemctl disable
aspera_faspex_email_background
```

Otherwise, run:

```
chkconfig aspera_mysqld off; chkconfig aspera_httpd off; chkconfig
aspera_faspex_np_background off; chkconfig aspera_faspex_mongrel
off; chkconfig aspera_faspex_ds_background off; chkconfig
aspera_faspex_db_background off; chkconfig aspera_faspex_background
off; chkconfig aspera_faspex_email_background off
```

5. On both nodes, create a common nodeadmin user for the Node API:

a) Run the following `asnodeadmin` command:

```
/opt/aspera/bin/asnodeadmin -a -u nodeadmin -x faspex -p
```

b) Enter a password for this account when asked for one.

The `nodeadmin` account must be the same on both nodes (same username and password).

c) Verify that the account was created successfully:

```
/opt/aspera/bin/asnodeadmin -l
```

user	system/transfer user	acls
NaaJFJg39PFfTZ	faspex	
nodeadmin	faspex	

d) Delete the first account.

The first account in the list (in this case `NaaJFJg39PFfTZ`) was created with a random name and a random password by the Faspex setup program. It can now be deleted, as it won't be used. To delete it, run the following command:

```
/opt/aspera/bin/asnodeadmin -d -u user_name
```

Do this on *both* nodes.

6. Configure the same encryption key for the Faspex users.

Edit the `aspera.conf` file (`/opt/aspera/etc/aspera.conf`) folder on both nodes, and check that the settings for the user `faspex` are identical. In particular, check the value of the `encryption_key` tag. It must be the same on both nodes. If not, then choose one value and copy it to the other node:

```
<aaa>
  <realms>
    <realm>
      <users>
        <user>
          <name>faspex</name>
          <authorization>
            <token>
              <encryption_key>secret_encryption_key</encryption_key>
            </token>
```

```

    </authorization>
  </user>
</users>
</realm>
</realms>
</aaa>

```

7. Pick one node and copy its `secret.yml` file (`/opt/aspera/faspex/config/secret.yml`) into the same directory on the other node, preserving the same owner and permissions.
8. Copy the `keystore.jks` (`/opt/aspera/faspex/lib/daemons/np/etc/keystore.jks`) on one node to the other to make sure they are identical.

Mount Remote File Systems on Each Node

Faspex servers in HA environments must be configured with shared storage. There are three shared volumes that need to be available to each Faspex server. Mount the shared volumes if they are not already mounted.

The following are example mount points. Yours may be different.

Example Mount Point	Usage	User Permissions	Notes
<code>/mysql_data</code>	Used to store the MySQL data files	rwX for the mysql user	
<code>/faspex_packages</code>	Used to store the Faspex packages files	rwX for the faspex user	
<code>/acm_files</code>	Used to store the common ACM files	rwX for the root user	If using NFS, use the noac flag

Note: Make sure all the Faspex services are stopped on both nodes before continuing:

```
asctl all:stop
```

1. Move the MySQL data files into the shared volume.
 - a) Backup the MySQL data, create a symlink to the mount point, and change the owner and group.

```

cd /opt/aspera/common/mysql
mv ./data ./data.orig
ln -s mysql_mount_point ./data
chown -h mysql:mysql ./data

```

- b) Check the permissions.

```

ls -lah /opt/aspera/common/mysql
total 128K
drwxr-xr-x 11 mysql mysql 4.0K Jun 12 15:25 .
drwxr-xr-x  7 root root  4.0K Jan 28 13:58 ..
drwxr-x---  2 mysql mysql 4.0K Jan 18 16:13 bin
lrwxrwxrwx  1 mysql mysql  4 Jun 12 15:25 data -> mysql_mount_point
drwxr-x---  5 mysql mysql 4.0K Jan 18 16:26 data.orig
-rw-r----- 1 mysql mysql 14K Nov 28 2012 database_controller.rb
-rw-r----- 1 mysql mysql 14K Nov 28 2012 database.rb
-rw-----  1 mysql mysql 756 Jun 12 15:26 database.rb.yml
drwxr-x---  3 mysql mysql 4.0K Jan 18 16:13 include
drwxr-xr-x  3 mysql mysql 4.0K Jan 18 16:13 lib
drwxr-x---  2 mysql mysql 4.0K Jan 18 16:13 libexec
-rw-r----- 1 mysql mysql 1.3K Nov 28 2012 linux_database.rb
-rw-r--r--  1 mysql mysql 9.2K Jan 18 16:14 my.cnf
-rw-r--r--  1 mysql mysql 9.2K Jan 18 16:14 my.ini
-rw-r----- 1 mysql mysql 9.1K Nov 28 2012 my_template.ini
drwxr-x---  2 mysql mysql 4.0K Jan 18 16:13 sbin

```



```
drwxr-x--- 3 mysql mysql 4.0K Jan 18 16:13 share
drwxr-x--- 3 mysql mysql 4.0K Jan 18 16:13 var
-rw-r----- 1 mysql mysql 13 Nov 28 2012 version.txt
```

- c) On the first node, move the database file into the shared volume:

```
sudo mv -u /opt/aspera/common/mysql/data.orig/* /opt/aspera/common/
mysql/data/
```

- d) On the other node, verify that you can see the data files in the directory `/opt/aspera/common/mysql/data/`.

2. Move the Faspex packages files into the shared volume.

- a) Backup the Faspex data, create a symlink to the mount point, and change the owner and group.

```
cd /home/faspex
mv ./faspex_packages ./faspex_packages.orig
ln -s faspex_mount_point ./faspex_packages
chown -h faspex.faspex ./faspex_packages
```

- b) Check the permissions.

```
ls -lah /home/faspex
total 128K
drwxr-xr-x 11 faspex faspex 4.0K Jun 12 15:25 .
drwxr-xr-x 7 root root 4.0K Jan 28 13:58 ..
lrwxrwxrwx 1 faspex faspex 4 Jun 12 15:25 faspex_packages -
> faspex_mount_point
```

- c) On the first node, move the package folder into the shared volume:

```
sudo mv -u /home/faspex/faspex_packages.orig/ /home/faspex/
faspex_packages/*
```

- d) On the other node, verify that you can see the data files in the directory `home/faspex/faspex_packages`.

3. Download ACM here: <https://download.asperasoft.com/download/sw/acm/faspex/acm-faspex-1-98-20180316-tar.gz>

4. Extract it to the dedicated shared volume by running the following command:

```
cd acm_files_mount_point
tar xzvf /path/to/acm_package.tar.gz
```

Note: You only need to perform this task from one node as the `acm_files_mount_point` directory is shared by both Faspex servers.

Install and Configure ACM

You only need to perform the following tasks from one node as the `acm_files_mount_point` directory is shared by both Faspex servers.

1. Create the following symbolic links on both nodes:

```
ln -s /acm_files_mount_point/acm /opt/aspera/acm
cd /opt/aspera/faspex/config
mv database.yml database.yml.orig
ln -s /opt/aspera/acm/config/database.yml database.yml
chown -h faspex.faspex database.yml
```

2. You may need to edit the acm file (`/opt/aspera/acm/bin/acm`) to set correct values to these variables:

```
MYSQLPW="mysql_password"
SYSLOG_FACILITY=local2
```

```
LOG_TO_FILE=0
LOG_TO_SYSLOG=1
CHECK_DEVICE_ID=1
```

Note: The *mysql_password* is the password you configured when you granted the nodes remote access to the MySQL database.

Note: The *CHECK_DEVICE_ID* variable defines if ACM should verify the Device ID of the storage volume where ACM is located. Because that Device ID can change upon reboot with NFS volumes, you may want to set this variable to 0 in order to disable the verification, which could prevent ACM and Faspex from running correctly.

3. Install ACM in the crontab on both nodes so that the system launches ACM every minute.

```
crontab -e
* * * * * /opt/aspera/acm/bin/
acm local_ip_address device_number > /dev/null 2>&1
```

Two parameters are passed to the *acm* command. The first parameter is the local IP address of the host. You can use the following command to find out the list of IP addresses available on a system:

```
ip addr | grep "inet"
```

The second parameter is the device number of the partition where the ACM files are stored. You can determine the correct value by using this command:

```
stat -c "%d" /acm_files_mount_point/acm
```

For example:

```
crontab -e
* * * * * /opt/aspera/acm/bin/acm 10.0.0.0 21 /dev/null 2>&1
```

Once installed in the crontab, ACM starts running, elects an active node, and starts the services on the different nodes accordingly depending on their current status: active or passive.

4. Create a job on both nodes to backup Faspex database with the *acmctl* command.

Aspera recommends regularly backing up the database. In the example *cronjob* below, ACM performs a backup every day at 1:30 AM. Choose the interval depending on your requirements.

```
crontab -e
* * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
30 3 * * * /opt/aspera/acm/bin/acmctl -b > /dev/null 2>&1
```

5. Create a job on both nodes to reset *asctl* logs.

Each time the system launches ACM, ACM writes to the *asctl* logs. Since the *asctl* logs do not get rotated, the logs can start to cause performance issues if the files grow too large. In the example *cronjob* below, the system resets the *asctl* logs every 7 days at 3:45 AM. Choose the interval depending on your requirements.

```
crontab -e
* * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
30 3 * * * /opt/aspera/acm/bin/acmctl -b > /dev/null 2>&1
45 3 * * 7 echo -n "" > /opt/aspera/common/asctl/log/asctl.log > /dev/null
2>&1
```

6. Run the *acmctl* command on both nodes with the *-s* option nodes in order to verify some basic ACM prerequisites:

```
/opt/aspera/acm/bin/acmctl -s
ACM sanity check
-----
```

```

Checking if the database.yml symbolic link exists      OK
Checking if the database.yml symbolic link points to the right location
OK
Checking if an entry for ACM seems to exist in the crontab      OK
Checking that all the Faspex services are disabled in chkconfig      OK
Checking that SE Linux mode is not set to enforcing      OK
Checking that asctl uses the correct load_file procedure      OK

```

7. If the verification looks good, start ACM on all the nodes at once, using the `acmctl` command with the `-E` option:

```

/opt/aspera/acm/bin/acmctl -E
ACM is enabled globally

```

Within a few minutes, ACM selects an active node, starts all the Faspex services on it, and then starts the `active/active` services on the passive node.

Configure Faspex

If the load balancer is correctly configured, you should now be able to connect to the Faspex web application using the URL pointing to the VIP.

1. Log in to Faspex through the URL.
2. Go to **Server > File Storage** and edit the main transfer node (the one used for the Default Inbox).

Use the following table to set the different fields:

Field	Value
Host	<p>The host is the name pointing to a list of the IP addresses of each node in the cluster (typically something like <code>faspextransfer.mydomain.com</code>).</p> <p>This value is used by Faspex's Node Poller service (also called Stats Collector) to poll the transfer nodes to get the status of ongoing transfers.</p> <p>Both transfer nodes must be polled every few seconds.</p> <p>Note: If you don't have a valid FQDN resolving into a list of several IP addresses, it is also possible to use a name defined by several entries in the <code>/etc/hosts</code> file on both nodes (see Using /etc/hosts Entries to Poll Transfer Nodes on page 195).</p>
Port	Typically 9092
Username	nodeadmin
Password	The password you entered when you created the nodeadmin user (using the <code>asnodeadmin</code> command).
Primary transfer address or name (expand Advanced Configuration)	<p>If you chose to use Type 1 architecture, use the VIP or a FQDN pointing to the VIP (typically something like <code>faspex.mydomain.com</code>).</p> <p>If you chose to use Type 2 architecture, use the FQDN pointing to the list that includes the IP address of each node in the cluster (typically something like <code>faspextransfer.mydomain.com</code>).</p>

Basic Configuration

The configuration below must point to the server that hosts the Aspera Enterprise

Name:

Use SSL?: ☒

Verify SSL Certificate?: ☐

Host:

Port:

Username:

Password:

Storage type:

[Test Connection](#)

Advanced Configuration

The address below is what your users will need in order to start transfers. If you

Primary transfer address or name:

Enable secondary address: ☐

Secondary address or name:

Use if requester's address matches:

Use if browser hostname matches:

Figure 1: Type 1 Architecture Example

Basic Configuration

The configuration below must point to the server that hosts the Aspera Enterprise

Name:

Use SSL?: ☒

Verify SSL Certificate?: ☐

Host:

Port:

Username:

Password:

Storage type:

[Test Connection](#)

Advanced Configuration

The address below is what your users will need in order to start transfers. If you ha

Primary transfer address or name:

Enable secondary address: ☐

Secondary address or name:

Use if requester's address matches:

Use if browser hostname matches:

Figure 2: Type 2 Architecture Example

3. Verify the FQDN. The verification method depends on whether you used a valid FQDN or used the `/etc/hosts` file.

If you used a valid FQDN, use the `nslookup` command:

```
nslookup FQDN_url
```

For example:

```
# nslookup faspextransfer.mydomain.com
Server: 10.0.0.1
Address: 10.0.0.1#53

Name: faspextransfer.mydomain.com
Address: 10.0.115.102
Name: faspextransfer.mydomain.com
Address: 10.0.115.101
```

In this case, the `nslookup` command shows that the FQDN `faspextransfer.mydomain.com` points to a list of two IP addresses: 10.0.115.102 and 10.0.115.101.

If you used the `/etc/hosts` file, use the `getent` command:

```
# getent hosts transfer-nodes
10.0.115.101 transfer-nodes
10.0.115.102 transfer-nodes
```

Upgrading the Environment

Upgrading the HA Environment

To upgrade an IBM Aspera Faspex HA deployment, you must upgrade each Faspex node individually and then reconfigure them to run in an HA environment.

Stopping All Services for Upgrade

You need to stop Faspex and MySQL services before performing the upgrade.

1. Stop the cronjob on both the nodes by commenting out the job.

```
crontab -e
# * * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
# 30 3 * * * /opt/aspera/acm/bin/acmtl -b > /dev/null 2>&1
# 45 3 * * 7 echo -n "" > /opt/aspera/common/asctl/log/asctl.log > /dev/
null 2>&1
```

2. On the active node, back up the database:

```
asctl faspex:backup_database
```

3. Stop all Faspex services on the active node.

```
asctl all:stop
```

4. Start MySQL service on the passive node and back up the database.

```
asctl mysql:start
asctl faspex:backup_database
```

5. Stop MySQL and ensure all Faspex services are stopped on the passive node.

```
asctl mysql:stop
asctl all:stop
```

6. Download and run through the backup and upgrade process on your local or remote HSTS nodes. See the [IBM Aspera High-Speed Transfer Server Admin Guide](#).

Upgrade Faspex on the Active Node

1. Download and install the Common Components and Faspex packages.

```
rpm -Uvh ibm-aspera-common-version.rpm
rpm -Uvh ibm-aspera-faspex-version.rpm
```

2. Run the Faspex upgrade.

```
asctl faspex:upgrade
```

3. If you are running HSTS and Faspex on the same server, verify that the default shell of the faspex user is bin/aspshell. If it is not, change the default shell to bin/aspshell.

Note: As a security feature, asctl disables the faspex user by setting the default shell to /bin/false to prevent logins when HSTS is running on a different server. Depending on your HA configuration, in some cases you may need to change the default shell back to bin/aspshell.

4. Test the upgrade by logging in through the Faspex web UI.
5. Disable all Faspex services:

First, stop all Faspex services on both nodes:

```
asctl all:stop
```

Then disable the services on both nodes.

On an OS running systemctl, instead of using chkconfig, disable services by running:

```
for svc in $(systemctl -a | grep faspex | awk '{print $1}'); do systemctl is-enabled $svc && systemctl disable $svc; done
```

Otherwise, run:

```
chkconfig aspera_mysqld off; chkconfig aspera_httpd off; chkconfig
aspera_faspex_np_background off; chkconfig aspera_faspex_mongrel
off; chkconfig aspera_faspex_ds_background off; chkconfig
aspera_faspex_db_background off; chkconfig aspera_faspex_background
off; chkconfig aspera_faspex_email_background off
```

Upgrade Faspex on the Passive Node

1. Edit the database.yml configuration file (/opt/aspera/faspex/config/database.yml) and make sure the server IP address is 127.0.0.1.
2. Download and install the Common Components and Faspex packages.

```
rpm -Uvh ibm-aspera-common-version.rpm
rpm -Uvh ibm-aspera-faspex-version.rpm
```

3. Run the Faspex upgrade.

```
asctl faspex:upgrade
```

4. Test the upgrade by logging in through the Faspex web UI.
5. If you are running HSTS and Faspex on the same server, verify that the default shell of the faspex user is bin/aspshell. If it is not, change the default shell to bin/aspshell.

Note: As a security feature, `asctl` disables the `faspex` user by setting the default shell to `/bin/false` to prevent logins when HSTS is running on a different server. Depending on your HA configuration, in some cases you may need to change the default shell back to `bin/aspshell`.

6. Disable all Faspex services:

First, stop all Faspex services on both nodes:

```
asctl all:stop
```

Then disable the services on both nodes.

On an OS running `systemctl`, instead of using `chkconfig`, disable services by running:

```
for svc in $(systemctl -a | grep faspex | awk '{print $1}'); do systemctl is-enabled $svc && systemctl disable $svc; done
```

Otherwise, run:

```
chkconfig aspera_mysqld off; chkconfig aspera_httpd off; chkconfig aspera_faspex_np_background off; chkconfig aspera_faspex_mongrel off; chkconfig aspera_faspex_ds_background off; chkconfig aspera_faspex_db_background off; chkconfig aspera_faspex_background off; chkconfig aspera_faspex_email_background off
```

Restart the HA Environment

1. Copy the `keystore.jks` (`/opt/aspera/faspex/lib/daemons/np/etc/keystore.jks`) on one node to the other to make sure that they are identical.
2. Restart the cronjobs on both the nodes by uncommenting the jobs.

```
crontab -e
* * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
30 3 * * * /opt/aspera/acm/bin/acmtl -b > /dev/null 2>&1
45 3 * * 7 echo -n "" > /opt/aspera/common/asctl/log/asctl.log > /dev/null 2>&1
```

Upgrading the HA Environment From a Pre-4.2.0 Environment

To upgrade an IBM Aspera Faspex HA deployment, you must upgrade each Faspex node individually and then reconfigure them to run in an HA environment.

Stopping All Services for Upgrade

You need to stop Faspex and MySQL services before performing the upgrade.

1. Stop the cronjob on both the nodes by commenting out the job.

```
crontab -e
# * * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
# 30 3 * * * /opt/aspera/acm/bin/acmtl -b > /dev/null 2>&1
# 45 3 * * 7 echo -n "" > /opt/aspera/common/asctl/log/asctl.log > /dev/null 2>&1
```

2. On the active node, back up the database:

```
asctl faspex:backup_database
```

3. Stop all Faspex services on the active node.

```
asctl all:stop
```

4. Start MySQL service on the passive node and back up the database.

```
asctl mysql:start
asctl faspex:backup_database
```

5. Stop MySQL and ensure all Faspex services are stopped on the passive node.

```
asctl mysql:stop
asctl all:stop
```

6. Download and run through the backup and upgrade process on your local or remote HSTS nodes. See the [IBM Aspera High-Speed Transfer Server Admin Guide](#).

Upgrading Faspex



Warning: Faspex 4.2.0 and later uses a new version of MySQL included in the IBM Aspera Common Components. If you are upgrading from a version prior to 4.2.0, you must first back up and empty your MySQL database (/opt/aspera/common/mysql/data). You cannot upgrade the Common Components until you have backed up and emptied your database. When running the upgrade script, you are required to provide the path to a back up. For instructions on backing up, see [Backing Up Faspex from the Command Line](#) on page 149.

Note: Perform the following steps on both nodes, first on the active node, and then on the passive node.

1. Since the data folder points to the shared storage, remove the connection to the shared storage.

```
cd /opt/aspera/common/mysql
mv data data.old
mkdir data
chown mysql. data
chmod 750 data
```

2. Download and install the Common Components and Faspex packages.

```
rpm -Uvh ibm-aspera-common-version.rpm
rpm -Uvh ibm-aspera-faspex-version.rpm
```

3. Run the Faspex upgrade.

```
asctl faspex:upgrade
```

If prompted to enter the location of the database, provide the path to the database backup you made earlier:

```
Please provide the location of the Faspex database backup (e.g.
backup/20XX-XX-XX_XXXXXX-Faspex.4.1.1.XXXXXX):
```

4. Test the upgrade by logging in through the Faspex web UI.
5. Disable all Faspex services:

First, stop all Faspex services on both nodes:

```
asctl all:stop
```

Then disable the services on both nodes.

On an OS running `systemctl`, instead of using `chkconfig`, disable services by running:

```
for svc in $(systemctl -a | grep faspex | awk '{print $1}'); do systemctl
is-enabled $svc && systemctl disable $svc; done
```


Otherwise, run:

```
chkconfig aspera_mysqld off; chkconfig aspera_httpd off; chkconfig
aspera_faspex_np_background off; chkconfig aspera_faspex_mongrel
off; chkconfig aspera_faspex_ds_background off; chkconfig
aspera_faspex_db_background off; chkconfig aspera_faspex_background
off; chkconfig aspera_faspex_email_background off
```

6. Copy the `keystore.jks` (`/opt/aspera/faspex/lib/daemons/np/etc/keystore.jks`) on one node to the other to make sure that they are identical.
7. If you are running HSTS and Faspex on the same server, verify that the default shell of the faspex user is `bin/aspshell`. If it is not, change the default shell to `bin/aspshell`.

Note: As a security feature, `asctl` disables the faspex user by setting the default shell to `/bin/false` to prevent logins when HSTS is running on a different server. Depending on your HA configuration, in some cases you may need to change the default shell back to `bin/aspshell`.

Restarting the HA Environment

After upgrading, point the `/opt/aspera/common/mysql/data` back to the shared storage.

1. Run the following commands on both nodes to point the database to the shared storage:

```
cd /opt/aspera/common/mysql
mv ./data ./data.new
ln -s /mysql_data ./data
chown -h mysql:mysql ./data
rm data.old
```

Verify the data folder points to the `mysql_data` folder on the shared storage.

```
ls -lah /opt/aspera/common/mysql/data
lrwxrwxrwx 1 mysql mysql 11 Sep 19 19:00 /opt/aspera/common/mysql/data -
> /mysql_data
```

2. Replace the data on the shared storage with the upgraded data of one of the nodes:

```
rm -rf /opt/aspera/common/mysql/data/*
mv /opt/aspera/common/mysql/data.new/* /opt/aspera/common/mysql/data/
```

3. On one node, grant remote access to MySQL for both nodes:

Note: You must use the same password as the password set in the acm configuration file (`/opt/aspera/acm/bin/acm`). You can view the contents of the configuration file for the configured password or set a new password and change the configured password to the new password.

```
asctl mysql:start
asctl mysql:grant_remote_access "local_server_ip_address"
New password: password
Confirm new password: password
asctl mysql:grant_remote_access "other_server_ip_address"
New password: password
Confirm new password: password
asctl mysql:stop
```

4. After you complete all the previous steps on both nodes, restart the cronjobs on both the nodes by uncommenting the jobs.

```
crontab -e
* * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
30 3 * * * /opt/aspera/acm/bin/acmtl -b > /dev/null 2>&1
```

```
45 3 * * 7 echo -n "" > /opt/aspera/common/asctl/log/asctl.log > /dev/null
2>&1
```

Maintenance of the HA Environment

The ACM Control Command (`acmctl`)

You can use `acmctl` to diagnose and configure ACM.

Overview of the ACM Control Command (`acmctl`)

The `acmctl` command controls the ACM. Running it with the `-h` (Help) option displays the available command options:

```
# /opt/aspera/acm/bin/acmctl -h
Aspera Cluster Manager Control Command
Version: 1.97
Usage: acmctl {option}
List of options:
-i: Display the current state of ACM
-s: Perform a sanity check of ACM
-D: Disable ACM globally
-E: Enable ACM globally
-d: Disable ACM locally
-e: Enable ACM locally
-b: Back up the MySQL database (active node only)
-A: Display information about the version
```

Check that ACM works correctly

You can use the `#i` option to display the current status of ACM on a node output shown from the active node:

```
Aspera Cluster Manager status
-----
Local hostname:      faspex-ha2
Active node:         faspex-ha2 (me)
Status of this node: active
Status file:         current
Disabled globally:   no
Disabled on this node: no

Database configuration file
-----
Database host:       10.0.115.102

Faspex active/active services status
-----
Apache:              running
Faspex Mongrels:     running

Faspex active/passive services status
-----
MySQL:               running
Faspex Background:   running
Faspex NP Background: running
Faspex DS Background: running
Faspex DB Background: running
```

The following is an example of the `acmctl -i` output on the passive node:

```
Aspera Cluster Manager status
```

```

-----
Local hostname:      faspex-ha1
Active node:         faspex-ha2
Status of this node: passive
Status file:         current
Disabled globally:   no
Disabled on this node: no

Database configuration file
-----
Database host:       10.0.115.102

Faspex active/active services status
-----
Apache:              running
Faspex Mongrels:     running

Faspex active/passive services status
-----
MySQL:               stopped
Faspex Background:   stopped
Faspex NP Background: stopped
Faspex DS Background: stopped
Faspex DB Background: stopped

```

Data Provided by `acmctl -i`

On both the active and passive systems, the output of the `acmctl -i` command provides useful information about the status of the Faspex servers:

Output Element	Definition
Hostname	The name of the local system.
Active node	The name and IP address of the node that is currently the active node.
Status [of] file	Whether the common <code>status</code> file is current or has expired. A status of <code>expired</code> usually indicates a fail-over situation. The status file may not be available for a short period during fail-over, and the <code>Status</code> file may report as <code>Unable to find</code> .
Disabled globally	Answers the question: Is ACM disabled for all Faspex servers?
Disabled on this node	Answers the question: Is ACM disabled on this node?
Database host	The system that is currently managing the MySQL database files.
Faspex active/active service status	The <code>apache</code> and <code>crond</code> services should have a status of <code>running</code> on both the active and passive servers. The <code>MySQL</code> , <code>Faspex Background</code> , <code>Faspex NP Background</code> , <code>Faspex DS Background</code> , <code>Faspex DB Background</code> services should all be <code>running</code> on the active server and <code>stopped</code> on the passive server.

ACM Log Files

Use ACM logs to troubleshoot for errors.

Overview

ACM can write to two locations:

- Syslog (local2)
- The common acm.log file (/opt/aspera/acm/log/acm.log)

By default, only Syslog is enabled.

The following is an example of a typical log cycle when two instances of ACM are running (one on each node):

```
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): ACM START (1.97)
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): Lock acquired
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): Checking if this node is
active or passive
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): Status file found
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): From status file: active
host is faspex-ha2
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): This node is active
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): Updating file /opt/
aspera/acm/config/database.yml
2013-06-28 14:19:01 (-0700) acm faspex-ha1 (1750): ACM START (1.97)
2013-06-28 14:19:01 (-0700) acm faspex-ha2 (27080): Active processing BEGIN
2013-06-28 14:19:02 (-0700) acm faspex-ha2 (27080): Active processing END (1
seconds)
2013-06-28 14:19:03 (-0700) acm faspex-ha2 (27080): Updating status files
(hostname=faspex-ha2)
2013-06-28 14:19:03 (-0700) acm faspex-ha2 (27080): ACM STOP
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): Lock acquired
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): Checking if this node is
active or passive
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): Status file found
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): From status file: active
host is faspex-ha2
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): This node is passive
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): Checking if the status
file is current
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): Status file is current
(diff: 1)
2013-06-28 14:19:04 (-0700) acm faspex-ha1 (1750): Passive processing BEGIN
2013-06-28 14:19:07 (-0700) acm faspex-ha1 (1750): Passive processing END (3
seconds)
2013-06-28 14:19:07 (-0700) acm faspex-ha1 (1750): ACM STOP
```

Logging to a File

You can configure ACM to also write logs to a specific file by editing the acm file (/opt/aspera/acm/bin/acm) and setting LOG_TO_FILE=1. ACM writes logs to /opt/aspera/acm/log/acm.log.

Note: IBM Aspera recommends logging to a file only for debugging purposes. The acm.log file does not get rotated and can start to cause performance issues if the file grows too large.

Backing Up the Shares Database

Use the ACM Control Command (acmctl) to regularly make backups of the Shares HA database.

Note: Aspera strongly recommends performing a backup of the Shares database on regular basis. If the database is corrupted for any reason, restoring it from a healthy backup is the most (if not only) reliable solution.

Aspera also recommends that backup files be stored on dedicated media, (for example, tape or removable disk) stored at a secure location.

In order to back up the Shares database on a regular basis, you should use the `-b` option to the `acmctl` command (`/opt/aspera/acm/bin/acmctl`). This command performs a backup of the Shares database whenever it runs on the current active node (the node that runs the MySQL service).

Note: A backup is performed only if executed on the active node; running the command on a passive node does not create a backup.

```
# /opt/aspera/acm/bin/acmctl -b
Starting backup
Shares: Backup databases... Database backed up in /opt/aspera/acm4shares/
backup/2014-06-24_052222
done
Compressing SQL files
done
Looking for old backups to remove
Found 0 files(s) modified for the last time more than 15 day(s) ago
Backup procedure complete
```

When a backup is complete, the utility removes all backup files that are older than the default of 7 days. To modify this default value, edit the `/opt/aspera/acm/bin/acmctl` file and set the `BACKUP_MAX_AGE_IN_DAYS` variable to the desired number of days.

By default, backup files are created in a dedicated folder located on local storage: `/opt/aspera/acm4shares/backup`. You can change the default storage location by modifying the `BACKUP_DIR` variable in the `/opt/aspera/acm/bin/acmctl` file or by replacing the default backup directory with a symbolic link pointing to shared storage.

On both nodes, the command should be launched every day at a specific time from the crontab:

```
# crontab -e
* * * * * /opt/aspera/acm/bin/acm 10.0.71.21 20 > /dev/null 2>&1
30 2 * * 1-5 /opt/aspera/acm/bin/acmctl -b > /dev/null 2>&1
```

The example shown above runs a backup of the Shares database at 2:30 AM every weekday of every month.

Note: See the `crontab` man pages for details about the `crontab` file format.

Suspending ACM

Disabling and Re-enabling ACM on all Nodes

Use the ACM Control Command (`acmctl`) to disable and re-enable ACM on all nodes.

1. Run the `acmctl` command with the `-D` option on any of the nodes to disable ACM on all nodes:

```
# /opt/aspera/acm/bin/acmctl -D
ACM is disabled globally
```

2. Verify the status of ACM.

- a) Run the `acmctl -i` command to verify the status of ACM (the following example does not show the entire output).

```
# /opt/aspera/acm/bin/acmctl -i
Checking current ACM status...

Aspera Cluster Manager status
-----
Local hostname:      faspex-ha1
Active node:         faspex-ha2
Status of this node: passive
Status file:         current
Disabled globally:    yes
```

```

Disabled on this node:  no

Database configuration file
-----
Database host:          10.0.115.102

Faspex active/active services status
-----
Apache:                 running
Faspex Mongrels:        running

Faspex active/passive services status
-----
MySQL:                  stopped
Faspex Background:      stopped
Faspex NP Background:   stopped
Faspex DS Background:   stopped
Faspex DB Background:   stopped

```

- b) Check the logs at `/opt/aspera/acm/log/acm.log`.

```

# tail -f /opt/aspera/acm/log/acm.log
2013-07-11 15:57:01 (-0700) acm faspex-ha1 (7758): ACM is disabled
globally: aborting
2013-07-11 15:58:01 (-0700) acm faspex-ha2 (22432): ACM is disabled
globally: aborting
2013-07-11 15:58:01 (-0700) acm faspex-ha1 (7826): ACM is disabled
globally: aborting
2013-07-11 15:59:01 (-0700) acm faspex-ha2 (22560): ACM is disabled
globally: aborting
2013-07-11 15:59:01 (-0700) acm faspex-ha1 (7894): ACM is disabled
globally: aborting

```

Note: Disabling ACM only disables *new* instances of ACM launched by the `crond` daemon. Any running service launched before ACM was disabled runs normally until it has completed. This behavior does not pose a problem when ACM is disabled globally, as no other servers will attempt to become active.

3. Run the `acmctl` command with the `-E` option to re-enable ACM operation on all nodes:

```

# /opt/aspera/acm/bin/acmctl -E
ACM is enabled globally

```

One of the Faspex servers becomes the active node, with all associated services started, and the other will be passive, with only the `nginx` and `crond` services running.

Disabling and Re-enabling ACM on One Node

Use the ACM Control Command (`acmctl`) to disable and re-enable ACM on a single node.

If you disable ACM locally on the active node, another node running ACM eventually takes over, possibly generating conflicting access to some common files on the shared storage. You should always use this option with extreme caution, and stop all the Faspex services (`asctl all:stop`) on the active node immediately after you disabled ACM locally.

1. To disable ACM for one node only, run `acmctl` with the `-d` option on that node:

```

# /opt/aspera/acm/bin/acmctl -d
ACM is disabled locally

```

2. To verify ACM's status for a disabled node, run the `acmctl -i` command on that node:

```

# /opt/aspera/acm/bin/acmctl -i
Checking current ACM status...

```

```
Aspera Cluster Manager status
-----
Local hostname:      faspex-ha1
Active node:         faspex-ha2
Status of this node: passive
Status file:         current
Disabled globally:   no
Disabled on this node: yes
...
```

3. To re-enable ACM on a node, run the `acmctl` command with the `-e` option on the node:

```
# /opt/aspera/acm/bin/acmctl -e
ACM is enabled locally
```

Manually Failing-Over to the Passive Node

To force a passive node to assume the active role, disable ACM on the active node and stop all Faspex services on that node.

1. Determine the active node with the `acmctl` command.

```
# /opt/aspera/acm/bin/acmctl -i
Checking current ACM status...

Aspera Cluster Manager status
-----
Local hostname:      faspex-ha2
Active node:         faspex-ha2 (me)
Status of this node: active
...
```

2. Disable ACM locally.

```
# /opt/aspera/acm/bin/acmctl -d
ACM is disabled locally
```

3. Check to confirm that no ACM instances are running.

```
# ps aux | grep acm
root 1248 0.0  0.0  103252 824 pts/0  S+ 17:18 0:00 grep acm
```

4. Stop the Faspex services.

```
# asctl all:stop
Faspex Mongrels: Stop... done
Faspex Background: Stop... done
Faspex DS Background: Stop... done
Faspex DB Background: Stop... done
Faspex NP Background: Stop... done
MySQL: Stop... done
Apache: Stop... done
```

5. Run the `acmctl -i` command to verify that all Faspex services have been stopped.

```
# /opt/aspera/acm/bin/acmctl -i
Checking current ACM status...

...

Faspex active/active services status
-----
```

```

Apache:                stopped
Faspex Mongrels:       stopped
s
Faspex active/passive services status
-----
MySQL:                 stopped
Faspex Background:     stopped
Faspex NP Background:  stopped
Faspex DS Background:  stopped
Faspex DB Background:  stopped

```

6. Check the ACM logs to observe the other node taking over (this can take several minutes):

```

2013-07-11 18:16:01 (-0700) acm faspex-ha2 (28736): ACM is disabled
  locally on this host: aborting
2013-07-11 18:16:01 (-0700) acm faspex-ha1 (24404): ACM START (1.97)
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): Lock acquired
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): Checking if this node
  is active or passive
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): Status file found
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): From status file:
  active host is faspex-ha2
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): This node is passive
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): Checking if the status
  file is current
2013-07-11 18:16:06 (-0700) acm faspex-ha1 (24404): Status file acm.status
  is too old (diff: 123)
2013-07-11 18:16:07 (-0700) acm faspex-ha1 (24404): Status file acm.status
  is too old (diff: 124)
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Status file acm.status
  is too old (diff: 125)
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Failover scenario
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Stopping MySQL on this
  node (if running)
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Checking if MySQL is
  still active on the active node
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Trying to establish a
  connection to MySQL on host 10.0.115.102
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): The connection to
  mysql failed, testing TCP port 4406 on host 10.0.115.102
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Connection to
  10.0.115.102 on port TCP/4406 failed, MySQL is likely to be down
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Becoming the active
  node
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): ACM RESET
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Deleting status
  file...
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Status file deleted
2013-07-11 18:16:08 (-0700) acm faspex-ha1 (24404): Stopping Faspex
  services
2013-07-11 18:16:12 (-0700) acm faspex-ha1 (24404): Updating file /opt/
  aspera/acm/config/database.yml
2013-07-11 18:16:12 (-0700) acm faspex-ha1 (24404): Active processing
  BEGIN
2013-07-11 18:16:24 (-0700) acm faspex-ha1 (24404): Active processing END
  (12 seconds)
2013-07-11 18:16:29 (-0700) acm faspex-ha1 (24404): Updating status files
  (hostname=faspex-ha1)
2013-07-11 18:16:29 (-0700) acm faspex-ha1 (24404): ACM STOP

```

7. Check that the active node is no longer active.

```
# /opt/aspera/acm/bin/acmctl -i
```



```
Checking current ACM status...
```

```
Aspera Cluster Manager status
```

```
-----
Local hostname:      faspex-ha1
Active node:         faspex-ha2
Status of this node: passive
Status file:         current
Disabled globally:   no
Disabled on this node: yes
...
```

And check that the other node is now the active one:

```
# /opt/aspera/acm/bin/acmctl -i
Checking current ACM status...
```

```
Aspera Cluster Manager status
```

```
-----
Local hostname:      faspex-ha1
Active node:         faspex-ha1 (me)
Status of this node: active
Status file:         current
Disabled globally:   no
Disabled on this node: no
Database host:       10.0.143.6
```

```
IBM Aspera Faspex active/passive services status
```

```
-----
Apache:  running
MySQL:   running
IBM Aspera Faspex: running
```

```
...
```

Note: If the node does not become active, copy the `keystore.jks` (`/opt/aspera/faspex/lib/daemons/np/etc/keystore.jks`) on one node to the other to make sure they are identical.

8. Re-enable ACM on the node that recently became passive to let it start the active/active Faspex services.

```
# /opt/aspera/acm/bin/acmctl -e
ACM is enabled locally
```

9. After a several minutes, you can verify that the active/active services have started on the passive node:

```
# /opt/aspera/acm/bin/acmctl -i
Checking current ACM status...
```

```
Aspera Cluster Manager status
```

```
-----
Local hostname:      faspex-ha2
Active node:         faspex-ha1
Status of this node: passive
Status file:         current
Disabled globally:   no
Disabled on this node: no
```

```
Database configuration file
```

```
-----
Database host:       10.0.115.101
```

```
Faspex active/active services status
```

```
-----
Apache:                running
Faspex Mongrels:       running
...

```

Appendix

Shutting Down Shares HA

Completely shut down the Faspex HA environment.

1. Disable ACM globally.

```
# /opt/aspera/acm/bin/acmctl -D
ACM is disabled globally

```

2. Check to confirm that no ACM instances are running on either node. Run the following `ps aux` command on both nodes:

```
# ps aux | grep acm
root 1248 0.0 0.0 103252 824 pts/0 S+ 17:18 0:00 grep acm

```

3. Stop the Faspex services on both nodes with the `asctl` command:

```
# asctl all:stop

```

Once you have applied that procedure, it is then safe to reboot both nodes or shut them down for maintenance. After a reboot, re-enable ACM globally to start the Faspex services correctly:

```
# /opt/aspera/acm/bin/acmctl -E
ACM is enabled globally

```

List of System Commands Used by IBM Aspera Cluster Manager (ACM)

ACM uses many Linux system commands to perform its functions.

The following system commands must be available on any Linux system running ACM:

```
bash
date
sleep
usleep
sed
find
grep
hostname
tee
touch
readlink
crontab
expr
stat
let
logger
nc
ip
gzip
chkconfig
which
sestatus

```

TCP and UDP Ports Used in HA Environments

The Shares HA environment requires some ports to be open in order for the HA environment to operate correctly.

Port	Direction	Service
TCP-80	From web clients to the VIP of the load balancer	load balancer
TCP-80	From the load balancer to the Shares nodes <i>(if the load balancer does not take care of the HTTP to HTTPS redirection)</i>	asperahttpd
TCP-443	From web clients to the VIP of the load balancer	load balancer
TCP-443	From the load balancer to the Shares nodes	asperahttpd
TCP-33001	From the clients to the load balancer <i>(if using architecture Type 1)</i>	load balancer
TCP-33001	From the load balancer to the Shares nodes <i>(if using architecture type 1)</i>	sshd
UDP-33001	From the clients to the load balancer <i>(if using Architecture Type 1)</i>	load balancer
UDP-33001	From the load balancer to the Shares nodes <i>if using Architecture Type 1)</i>	ascp (FASP)
TCP-33001	From the clients to the Shares nodes <i>(if using Architecture Type 2)</i>	sshd
UDP-33001	From the clients to the Shares nodes <i>(if using Architecture Type 2)</i>	ascp (FASP)
TCP-9092	Between the nodes	asperanoded
TCP-4406	Between the nodes	mysqld

Note: You may have to open additional ports if the Shares nodes report to IBM Aspera IBM Aspera Faspex.

Using /etc/hosts Entries to Poll Transfer Nodes

If you cannot use a Fully Qualified Domain Name to point Faspex to the list of IP addresses referencing all the transfer nodes, then it is possible to use a name defined in the /etc/hosts file on each server in the Faspex cluster.

On each node of the cluster, add multiple host entries for a name like “transfer-nodes” to your /etc/hosts file. For example:

```
# cat /etc/hosts
... some other entries
10.0.115.101 transfer-nodes
10.0.115.102 transfer-nodes
```

Verify that the operating system has successfully taken those entries into consideration by running the following command:

```
# getent hosts transfer-nodes
10.0.115.101 transfer-nodes
10.0.115.102 transfer-nodes
```

You can then add the entries to your Faspex file storage by going to **Server > File Storage > Add New Node** and entering the name ("transfer-nodes") in the **Host** field. Configure the rest of the fields as normal.

Partitioning Mongrel Processes between Faspex and Cargo

Partition mongrels between handling Faspex UI requests and IBM Aspera Cargo requests to address performance issues.

When the number of Cargo clients attached to a Faspex cluster reaches a significant number, the performance of the Faspex Web UI can suffer due to resource contention with Cargo clients accessing the API.

To avoid this, tune the Apache configuration with separate sets of Mongrel processes dedicated to serving the Faspex web interface and API.

Note: The examples in the instructions below demonstrates Mongrel partitioning for 15 mongrel processes: 10 for Cargo and 5 for Faspex.

1. Run the following `asctl` command to set the proper total number of Mongrel processes:

```
asctl faspex:mongrel_count number+of_mongrels
```

Note: Running the `mongrel_count` command overwrites and removes any modifications to the `faspex.apache.linux.conf` configuration file, including the changes described in the following steps.

Choose not to restart Apache and Faspex.

2. Open the following Faspex Apache configuration file in a text editor: `/opt/aspera/faspex/config/faspex.apache.linux.conf` and make the following changes
 - a) Add the `<Proxy balancer://faspex_cargo_cluster>` section.

For example:

```
...
#Proxy balancer section (create one for each ruby app cluster)
<Proxy balancer://faspex_cargo_cluster>
</Proxy>
<Proxy balancer://faspex_cluster>
  BalancerMember http://127.0.0.1:3000
  BalancerMember http://127.0.0.1:3001
  BalancerMember http://127.0.0.1:3002
  BalancerMember http://127.0.0.1:3003
  BalancerMember http://127.0.0.1:3004
  BalancerMember http://127.0.0.1:3005
  BalancerMember http://127.0.0.1:3006
  BalancerMember http://127.0.0.1:3007
  BalancerMember http://127.0.0.1:3008
  BalancerMember http://127.0.0.1:3009
  BalancerMember http://127.0.0.1:3010
  BalancerMember http://127.0.0.1:3011
  BalancerMember http://127.0.0.1:3012
  BalancerMember http://127.0.0.1:3013
  BalancerMember http://127.0.0.1:3014
</Proxy>
...
```

- b) Distribute the `BalancerMember` entries under `<Proxy balancer://faspex_cluster>` between the two sections.

For example:

```
...
#Proxy balancer section (create one for each ruby app cluster)
<Proxy balancer://faspex_cargo_cluster>
  BalancerMember http://127.0.0.1:3000/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3001/aspera/faspex/inbox.atom
```

```

BalancerMember http://127.0.0.1:3002/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3003/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3004/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3005/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3006/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3007/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3008/aspera/faspex/inbox.atom
BalancerMember http://127.0.0.1:3009/aspera/faspex/inbox.atom
</Proxy>
<Proxy balancer://faspex_cluster>
  BalancerMember http://127.0.0.1:3010
  BalancerMember http://127.0.0.1:3011
  BalancerMember http://127.0.0.1:3012
  BalancerMember http://127.0.0.1:3013
  BalancerMember http://127.0.0.1:3014
</Proxy>
...

```

- c) Add `ProxyPass /aspera/faspex/inbox.atom balancer://faspex_cargo_cluster` to the proxy request section.

```

...
# send the proxy request
ProxyPass /aspera/faspex/inbox.atom balancer://faspex_cargo_cluster
ProxyPass /aspera/faspex balancer://faspex_cluster
...

```

3. Restart Apache and Faspex services.

```

asctl apache:restart
asctl faspex:restart

```

Sizing Guidelines and Suggestions

The sizing requirements differ for every high availability environment depending on the use case and security requirements of each environment. The guidelines in this article do not work for every set up, but are meant as a starting point for you to figure out the requirements for your particular set up.

There are two types of clients that can connect to a Shares HTTP endpoint: users and machines. Shares runs multiple Mongrel processes to handle requests, such as user interaction with the web application or a machine (such as IBM Aspera Cargo) calling the API to download the latest packages. To handle more requests, you need to configure Shares to run more Mongrel processes.

HTTP Connections from Users

Here are some sizing estimates to keep in mind:

- 1 CPU core supports 3 mongrel processes
- 1 mongrel process handles 3 concurrent, active users
- 1 mongrel process typically requires 500 MBs of memory

Tip: A mongrel process uses only 150-200MBs when first started, but usage goes up to the 500 MBs range as clients interact with the application.

In other words, the rule of thumb is:

```

1 CPU core ~ 3 mongrel processes * 3 concurrent active users ~ 10
concurrent, active users
1 CPU core ~ 3 mongrel processes * 500 MBs of memory ~ 1.5 GBs of memory

```

Sizing Example

Your environment needs to be able to support your worst case scenario: peak hours when you have the highest number of concurrent, active users.

Note: The maximum number of concurrent, active users determines the number of cores and memory needed for your HA environment. This is a metric you must figure out yourself.

In our example, we have 1,000 clients in our user pool, but the maximum number of concurrent, active users is 200. Apply the rule of thumb to that number:

```
200 concurrent, active users / 10 users per core = 20 cores
200 concurrent, active users / 3 users per mongrel * 500 MBs ~ 34GBs of
memory
```

Note: You should also allocate 4 GBs of memory for the OS and the MySQL database.

HTTP Connections from Machines

Tip: These guidelines use IBM Aspera Cargo as the client machine, since that is the primary use case.

The CPU core to client ratio is higher for Cargo clients since they connect more frequently (for example, every five minutes). Aspera recommends a conservative ration of one CPU core to 3 Cargo clients. Although Cargo clients take a up a more significant load, it's easier to determine and even control the peak number of connections if you control the machines running Cargo.

Make sure to spread out the schedules of Cargo machines so that they do not make calls to Shares all at the same time. Some situations can trigger a wave of connections that overloads the HA environment.

For example, a company performs a system-wide update of all Windows machines that requires a reboot. Each of those machines restarts at the same time, each Cargo application on those machines start at the same time, and the schedules of each Cargo application are now synchronized, triggering a massive spike in connections every 15 minutes.

You can ensure that Shares has enough mongrel processes to handle Cargo client connections by partitioning processes between Shares and Cargo. For more information, see [Partitioning Mongrel Processes between Faspex and Cargo](#) on page 196.

Network Storage

The network storage requirement applies mainly to the MySQL database, which needs to persist data. If using a standalone server, Aspera recommends using spinning disk drives with 10-15K RPMs or using SSD drives.

If using shared storage, use the same principles to keep latency low. In addition, the shared storage must be storage dedicated to Shares. At the least, you must make sure you have dedicated IO/sec for Shares. Sharing the storage with anything else will likely decrease performance.

Using the Health Check URL

Use the health check URL to check the Faspex server status without providing credentials to the server. You can pass on the response to other services like load balancers.

Using the Health Check for Load Balancers

Use the `health_check_lite` endpoint for load balancers. The endpoint returns simply whether the server is running.

```
$ curl -k https://server_address/aspera/faspex/health_check_lite
```

For example:

```
$ curl -k https://faspex.com/aspera/faspex/health_check_lite
```

```
{
  "message" : "Faspex is running"
}
```

Using the Detailed Health Check

The standard health check returns a JSON response with the validity of the server license and the statuses of the nodes on the server.

```
$ curl -k https://server_address/aspera/faspex/health_check
```

For example:

```
$ curl -k https://faspex.com/aspera/faspex/health_check
{
  "valid_license" : true,
  "nodes" : [
    {
      "id": 1,
      "status": "Active",
      "contains_default_share": true
    },
    {
      "id": 2,
      "status": "Error",
      "contains_default_share": false
    }
  ]
}
```

Important: The detailed health check is resource-intensive and should not be called too frequently as it may impact Faspex performance.

Detailed Health Response Codes

Code	Status
HTTP 200	Apache and Faspex services are healthy, the default node is healthy, and the Faspex license is valid.
HTTP 503	The Apache service is healthy, but the Faspex service is down.
HTTP 500	Apache and Faspex services are healthy, but either the default node is down or it has an invalid license. The JSON response reports the exact issue.

asctl Command Reference

You can use `asctl` commands in a Terminal window to display or modify IBM Aspera faspex Application component settings. Faspex configuration options that can be modified using `asctl` are listed below. If there are modifications that cannot be accomplished with `asctl`, notify Aspera Support.

Component	Description
Directory Service (DS)	Faspex Directory Service support.
Apache	Apache web server.

Component	Description
Background	Process new data from the MySQL database.
Faspex	Faspex main application.
Mongrel	Ruby's HTTP library.
MySQL	MySQL database.

All components commands

Important: The commands in this section control all Faspex components.

Task	Command	Description
Show config info	asctl all:info	Print info about all components.
Restart all components	asctl all:restart	Restart all components.
Setup status	asctl all:setup_status	Information about configuring all components.
Start	asctl all:start	Start all components.
Show status	asctl all:status	Display the status of each component.
Stop	asctl all:stop	Stop all components.
Show version	asctl all:version	Display the current version of each component.

Directory Service (DS)

Task	Command	Additional information
Start DS	asctl faspex:ds:start	
Stop DS	asctl faspex:ds:stop	
Restart DS	asctl faspex:ds:restart	
Show DS status	asctl faspex:ds:status	
Disable DS	asctl faspex:ds:disable	When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.

Apache

Task	Command	Additional Information
Create a setup file	asctl apache:create_setup_file <i>file</i>	Create a reusable file that contains answers to the setup questions. Replace <i>file</i> with a file name.
Disable Apache	asctl apache:disable	Disable the Aspera Apache server. When disabled, the service will not start when rebooting computer, does

Task	Command	Additional Information
		not print reminders or update its configurations.
Disable Apache logs	asctl apache:disable_logs	Set the Apache's log level to 'emerg'.
Enable Apache logs	asctl apache:enable_logs	Set the Apache's log level to 'notice'.
Re-generate conf	asctl apache:generate_config	Generate the component's configuration file using the current settings.
Display hostname	asctl apache:hostname	Display the hostname or IP address of the server.
Change hostname	asctl apache:hostname <i>host</i>	Change the hostname or IP address of the server. Replace <i>host</i> with a new hostname or IP address.
Display HTTP port	asctl apache:http_port	Display the HTTP port the web server listens to.
Change HTTP port	asctl apache:http_port <i>port</i>	Change the HTTP port the web server listens to. Replace <i>port</i> with a new port number.
Display HTTPS port	asctl apache:https_port	Display the HTTPS port the web server listens to.
Change HTTPS port	asctl apache:https_port <i>port</i>	Change the HTTPS port the web server listens to. Replace <i>port</i> with a new port number.
Show config info	asctl apache:info	Print configuration info about Apache.
Copy your SSL files into the Aspera default location (under default names)	asctl apache:install_ssl_cert <i>cert_file</i> <i>key_file</i> [<i>chain_file</i>]	After upgrading Faspex and Common, use this command to copy your original SSL certificate, key and optional chain file to /opt/aspera/common/apache/conf and give them Aspera-standard names. The httpd-ssl.conf file is also re-rendered and permissions/ownership is set for the cert files.
Set Apache log level	asctl apache:log_level <i>option</i>	Specify the Apache's log level. Replace <i>option</i> with crit , error , warn , notice , info or debug .
Create SSL certificate	asctl apache:make_ssl_cert <i>hostname</i>	Create a self-signed SSL certificate for the specified hostname. Replace <i>hostname</i> with your hostname.
Restart Apache	asctl apache:restart	
Configure Apache	asctl apache:setup	
Configure Apache using saved file	asctl apache:setup_from_file <i>filename</i>	Run setup using the answers from a file created using the "create_setup_file" command.

Task	Command	Additional Information
Start Apache	asctl apache:start	
Show Apache status	asctl apache:status	
Stop Apache	asctl apache:stop	
Upgrade Apache	asctl apache:upgrade	
Show Apache's version	asctl apache:version	

Background

Task	Command	Additional Information
Start Faspex background service	asctl faspex:background:start	
Stop Faspex background service	asctl faspex:background:stop	
Restart Faspex background service	asctl faspex:background:restart	
Show Faspex background service status	asctl faspex:background:status	
Disable Faspex background service	asctl faspex:background:disable	When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.

Faspex Database (DB) Background

Task	Command	Additional Information
Start Faspex DB background service	asctl faspex:db:start	
Stop Faspex DB background service	asctl faspex:db:stop	
Restart Faspex DB background service	asctl faspex:db:restart	
Show Faspex DB background service status	asctl faspex:db:status	

Faspex Node Poller (NP) Background

Task	Command	Additional Information
Start Faspex NP background service	asctl faspex:np:start	
Stop Faspex NP background service	asctl faspex:np:stop	
Restart Faspex NP background service	asctl faspex:np:restart	
Show Faspex NP background service status	asctl faspex:np:status	

Faspex

Task	Command	Description
Setup	asctl faspex:setup	Set up Faspex.
Setup status	asctl faspex:setup_status	Information about configuring this component.
Re-generate conf	asctl faspex:generate_config	Generate Faspex configuration file using the current settings.
Show package dir	asctl faspex:package_dir	Show current directory that Faspex uses to store packages.
Change package dir	asctl faspex:package_dir <i>dir</i>	Change directory that Faspex uses to store packages. Replace <i>dir</i> with the new path.
Upgrade	asctl faspex:upgrade	Upgrade Faspex from a previous version.
Show config info	asctl faspex:info	Print configuration info about Faspex.
Display URI namespace	asctl faspex:uri_namespace	Display the URI namespace.
Change URI namespace	asctl faspex:uri_namespace <i>namespace</i>	Change the URI namespace. Replace <i>namespace</i> with a new namespace.
Display mongrel number	asctl faspex:mongrel_count	Display the number of ports the web server listens to.
Change mongrel number	asctl faspex:mongrel_count <i>number</i>	Change the number of ports the web server listens to. Replace <i>number</i> with a number.
Display lowest mongrel port number	asctl faspex:base_port	Display the lowest port for the mongrel instances.
Change lowest mongrel port number	asctl faspex:base_port <i>number</i>	Change the lowest port for the mongrel instances. Replace <i>number</i> with a number.
Display HTTP Fallback port	asctl faspex:http_fallback_port	Display the port for HTTP Fallback.
Change HTTP Fallback port	asctl faspex:http_fallback_port <i>port</i>	Change the port for HTTP Fallback. Replace <i>port</i> with a new port number.
Backup Faspex database	asctl faspex:backup_database	Backup Faspex database and save the backup files to the path <i>/opt/aspera/faspex/db/backup</i> .
Migrate Faspex database	asctl faspex:migrate_database	Migrate Faspex MySQL database.
Restore Faspex database	asctl faspex:restore_database [dir]	Restore Faspex MySQL database. Note: [dir] is the directory containing the backup file. Note: To restore database, backup files must use default

Task	Command	Description
		name (central.sql, faspex.sql and user_service.sql).
Create or update admin	<code>asctl faspex:admin_user login email [password]</code>	Create a new admin, or update an existing admin account. Replace <i>login</i> with a login, <i>email</i> with its email. You can add the account's password in the command (<i>[password]</i>), or enter it when prompted. If the login you have entered exists, the account is updated with new email and password.
Create setup file	<code>asctl faspex:create_setup_file file</code>	Create a reusable file that contains answers to the setup questions. Replace <i>file</i> with a file name.
Setup from file	<code>asctl faspex:setup_from_file file</code>	Run setup using the answers from a file created using "create_setup_files". Replace <i>file</i> with a file name.
Rake command	<code>asctl faspex:rake arg</code>	Evoke a rake command.
Upload license	<code>asctl console:rake aspera:update_license</code>	Upload a license using a rake task. You must first set the <code>LICENSE_KEY</code> variable with your license key by running <code>export LICENSE_TEXT= 'license_key'</code> .
Show set up version	<code>asctl faspex:version</code>	Display the currently set up version.
Start Faspex	<code>asctl faspex:start</code>	Start Faspex application.
Stop Faspex	<code>asctl faspex:stop</code>	Stop Faspex application.
Restart Faspex	<code>asctl faspex:restart</code>	Restart Faspex application.
Show Faspex status	<code>asctl faspex:status</code>	Display Faspex application's status.
Disable Faspex	<code>asctl faspex:disable</code>	Disable Faspex application. When disabled, the service does start when rebooting computer, print reminders, or update its configurations.

Mongrel

Task	Command	Description
Start mongrel service	<code>asctl faspex:mongrel:start</code>	Start the Faspex mongrel service.
Stop mongrel service	<code>asctl faspex:mongrel:stop</code>	Stop the Faspex mongrel service.
Restart mongrel	<code>asctl faspex:mongrel:restart</code>	Restart the Faspex mongrel service.
Show mongrel status	<code>asctl faspex:mongrel:status</code>	Display the Faspex mongrel service status.
Disable mongrel	<code>asctl faspex:mongrel:disable</code>	Disable the Faspex mongrel service. When disabled, the service will not

Task	Command	Description
		start when rebooting computer, does not print reminders or update its configurations.

MySQL

Task	Command	Description
Create setup file	<code>asctl mysql:create_setup_file <i>file</i></code>	Create a reusable file that contains answers to the setup questions. Replace <i>file</i> with a file name.
Display database directory	<code>asctl mysql:data_dir</code>	Display the directory that the databases are kept in.
Disable MySQL	<code>asctl mysql:disable</code>	Disable the Aspera MySQL. When disabled, the service will not start when rebooting computer, does not print reminders or update its configurations.
Grant access on MySQL-only server	<code>asctl mysql:grant_remote_access <i>host mysql_user mysql_password</i></code>	If MySQL server is running on a different computer, use this command on the MySQL machine to allow access from the specified machine. Replace <i>host</i> , <i>mysql_user</i> and <i>mysql_password</i> with the server's hostname, MySQL's user name, and the user's password, respectively.
Show config info	<code>asctl mysql:info</code>	Print configuration info about MySQL.
Show port	<code>asctl mysql:port</code>	Display the port the MySQL server listens to.
Change port	<code>asctl mysql:port <i>port</i></code>	Change the port the MySQL server listens to. Replace <i>port</i> with a new port number.
Restart MySQL	<code>asctl mysql:restart</code>	Restart the Aspera MySQL.
Set root password	<code>asctl mysql:set_root_password</code>	Set the password for 'root' in MySQL.
Configure MySQL-only server	<code>asctl mysql:setup</code>	If MySQL server is running on a different computer, use this command on the MySQL machine to configure it.
Configure MySQL using saved file	<code>asctl mysql:setup_from_file <i>file</i></code>	Run setup using the answers from a file created using the "create_setup_file" command.
Start MySQL	<code>asctl mysql:start</code>	Start the Aspera MySQL.
Show MySQL status	<code>asctl mysql:status</code>	Display the Aspera MySQL status.

Task	Command	Description
Stop MySQL	asctl mysql:stop	Stop the Aspera MySQL.
Upgrade MySQL-only server	asctl mysql:upgrade	If MySQL server is running on a different computer, use this command on the MySQL machine to upgrade the database.
Show MySQL's version	asctl mysql:version	Display the currently set up version.

Faspex APIs

Overview

The Faspex Web API provides a set of RESTful web services to enable browsing, publishing, sending, and receiving Faspex packages. You can find documentation for the Faspex Rest APIs on the Aspera Developer Network at <https://developer.asperasoft.com/web/faspex/index>.

Note: You need login credentials for the Aspera Developer Network. If you do not have credentials, contact Aspera.

Faspex 4.0+ supports V4 Rest APIs in addition to V3 Rest APIs. For more information on the Faspex V3 Rest API, see the documentation at <https://developer.asperasoft.com/web/faspex/rest>. For more information on the Faspex V4 Rest API, see <https://developer.asperasoft.com/reference/whats-new/269-new-faspex-enhancements>.

Faspex V4 Rest API

Faspex V4 APIs provides additional/advanced feature set as below

- Follows REST API accepted standards (including response codes)
- All JSON payload and response
- HMAC Authentication
- User management APIs
- API's for setting download limits
- API's for "per-user" download statistics
- API's for editing email templates
- Ability to set override locations for package delivery. More than just mapping users to locations, this can override location priorities and essentially map packages to locations, not just users
- Increased metadata field length
- More information around packages and states, including download count, file count in packages, package creation date, package modification date, aggregate file size, and more
- More information around download stats, including username, downloader IP address, download date, and time

Note: The Faspex V4 REST API code is disabled by default. For instructions on enabling the V4 API, see [Enabling Faspex V4 APIs](#) on page 206.

Enabling Faspex V4 APIs

Faspex V4 REST API code is disabled by default. To enable the V4 Rest API, follow the instructions below.

1. Edit the **faspex.yml** file found at:
/opt/aspera/faspex/config/faspex.yml
2. Add the line below to the **production** section of **faspex.yml**.

```
EnableV4API: true
```

3. Restart Faspex services.

```
asctl faspex:restart
```

Available HTML Tags and Attributes in Faspex

Faspex supports the use of HTML tags and attributes in email notification templates and instructions for sending packages (see [Configuring Email Notification Templates](#) on page 138). For security purposes not all HTML tags and attributes are allowed in Faspex notification. Any tag not explicitly allowed is removed from your message. Here is a list of allowed HTML tags and attributes:

Allowed HTML Tags

```
del, dd, h3, address, big, sub, tt, a, ul, h4, cite, dfn, h5, small, kbd,
code, b, ins, img, h6, sup, pre, strong,
blockquote, acronym, dt, br, p, div, samp, li, ol, var, em, h1, i, abbr, h2,
span, hr
```

Allowed HTML Attributes

```
name, href, cite, class, title, src, xml:lang, height, datetime, alt, abbr,
width, style
```

Directory Service Group Permissions Reference

Directory Services (DS) must first be enabled. For more information, see [Adding a Directory Service to Faspex](#) on page 110.

To configure permissions for a DS, go to **Accounts > Directory Service Groups**. Click **New Group** and **Edit Additional Permissions** or click the name of a directory service and select **Group Import Policy**.

Permissions

Option	Description
Allowed to	<ul style="list-style-type: none"> • Uploads allowed: Select to allow users to send packages. • Downloads allowed: Select to allow users to download received packages. A user who does not have download permissions still receives packages, but cannot download the files. • Forwarding allowed: Select to allow users to forward received packages to other users. The package becomes available to the forwarded users in their Faspex accounts. • Can create from remote: Select to allow users to create a package from a remote source such as a remote server. Users allowed to access remote sources can access the Source drop-down menu when sending a new package. <p>You must first add remote sources to Faspex to see the Source drop-down menu. For more information on adding remote sources, see Adding a Node to Faspex on page 59.</p> <p>Note: This setting is disabled by default and must be set on a per-user basis (in other words, there is no global option).</p>

Option	Description
Allow inviting external senders	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable this user to invite users without Faspex accounts to upload a package to Faspex.</p>
Allow public submission URLs	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable users to send a Public URL to users without Faspex accounts. These external users can submit packages to registered Faspex users through this public URL. For more information about Public URLs, see Configuring Public URLs on page 91.</p> <p>Note: Even if the Public URL feature is enabled for registered Faspex users, they can override the feature for their own account by going to their user Account > Preferences > Misc and clearing Enable public URL.</p>
Can send to external email	<p>Select Allow to allow users to send packages to external email addresses.</p> <p>Faspex sends a download link through email. By default, this link expires after three days, but admins can change the duration or disable expiration by going to Server > Security. For more information, see Configuring Security Settings on page 47.</p>
Can send to all faspex users	<p>Select Allow to allow users to send packages to all Faspex users.</p> <p>If this feature is enabled, all existing Faspex users appear in the contact list. If disabled, users can, only send packages to members of workgroups they are part of.</p>
Keep user directory private	Select Yes to prevent users from being able to see the entire user directory, even if they have permissions to send to all Faspex users.
Can see global distribution lists.	Select Yes to give users access to global distribution lists. For more information on global distribution lists, see Creating a Global Distribution List on page 129.
Allowed IP addresses for login	Specify the IP addresses that a Faspex user can login from. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for download	Specify the IP addresses that a Faspex user can login from to download packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for upload	Specify the IP addresses that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Can send to external email	Allow or deny the user to send download links to external emails addresses (which are not Faspex users).
Can send to all faspex users	Enable to allow the user to send packages to all Faspex users (as opposed to only being able to send to the user's workgroup members).
Allowed IP addresses for login	Specify the IP addresses that an Faspex user can log in from to view his or her account. A wildcard (*) can be used in this option (for example, 198.51.100.* , which allows the user to login from 198.51.100.1 , 198.51.100.2 , etc.). Separate multiple email addresses with commas (,).

Option	Description
Allowed IP addresses for download	Specify the IP addresses that an Faspex user can login from to download packages. A wildcard (*) can be used in this option (for example, 198.51.100.*, which allows the user to login from 198.51.100.1, 198.51.100.2, etc.). Separate multiple email addresses with commas (,).
Allowed IP addresses for upload	Specify the IP addresses that an Faspex user can login from to upload packages. A wildcard (*) can be used in this option (for example, 198.51.100.*, which allows the user to login from 198.51.100.1, 198.51.100.2, etc.). Separate multiple email addresses with commas (,).

Package Deletion

Select from the following options to specify behavior after downloading a package:

Option	Description
After download	<p>You can override the server default by selecting Override system default. If you choose override, select one of the following policies:</p> <ul style="list-style-type: none"> • Do nothing: Do not auto-delete after the package is downloaded. • Delete files after any recipient downloads all files: Delete after <i>any</i> recipient downloads <i>all</i> files in the package once. <p>Important: When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option.</p> <ul style="list-style-type: none"> • Delete files after all recipients download all files: Delete if <i>all</i> files in the package have been downloaded by <i>all</i> recipients.
Allow user to set own delete setting on a package-by-package basis	Select Allow to allow this user to choose a package expiration policy when sending a new package.

Advanced Transfer Settings

By default, Faspex uses the transfer settings from the Aspera Central Server section. Select **Override default settings** to set user-specific transfer settings, which take precedence over the server-wide settings.

Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option Lock minimum rate and policy is checked, the user is not able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the maximum upload and download transfer rate for this user.

Configure User Settings

The following section describes the configurable settings for a Faspex user.

Account Details

Option	Description
Role	Select from one of the following roles for this user:

Option	Description
	<ul style="list-style-type: none"> • admin - Admins can access the Server tab to configure the Faspex server. They can create, edit, and delete every type of Faspex user (admins, managers, and regular users), and they can send packages (perform file transfers). Admins can also manage workgroups (create/edit/delete). • manager - The manager role enables Faspex server administration to be separate from Faspex user accounts administration. Managers can send packages, create/edit/delete workgroups, and create/edit/delete other managers and regular users. They can promote regular users to managers, and demote other Managers to regular users. However, they cannot, edit admin accounts or promote another user to admin. Managers do not have access to the Server tab, nor can they change the Faspex server configuration (a privilege limited to admins). • user - Regular users can send packages through Faspex. They typically do not manage other users or workgroups.
Account expires	<p>Select to set an expiration date for the user. The user becomes inactive on the specified date.</p> <p>Note: Admin accounts do not expire.</p>
Account activated	<p>Select to activate this account so that the user can log into Faspex. Clear to disable the account.</p> <p>Note: Admin accounts are always active.</p>
Custom password policy	<p>Select to override the global password policy for this user.</p> <p>Note: Admins cannot override their own password policies, but they can edit password policy settings for other admin accounts.</p>
Password expires	<p>You must enable Custom password policy to configure this option.</p> <p>Select to enable password expiration for the user password every specified number of days.</p>
Prevent password reuse	<p>You must enable Custom password policy to configure this option.</p> <p>Select to prevent users from reusing passwords. Enter the number of previous passwords users cannot reuse.</p>
Send copy of receipt email to these addresses	<p>Faspex sends a copy of every package receipt notification sent to this account to the Faspex users and email addresses listed in this field. Recipients listed in this field receive notifications for every package sent and received by this account. The CC Receipt field on the New Package page is auto-populated with the addresses listed in this field.</p> <p>If the sender has permission to Allow editing of receipt addresses on package creation, whatever the sender enters in the CC Receipt field on the New Package page overrides this setting. If the sender removes any of the original email addresses from the field, Faspex does not send a notification to that user.</p> <p>If the sender does not have permission to Allow editing of receipt addresses on package creation, then this field is honored.</p> <p>Note: If you are adding multiple email addresses, separate them with commas (,), semicolons (;), or white-spaces.</p>
Allow editing of receipt addresses on package creation	<p>Select to allow users to modify addresses to receive notification emails regarding a package sent by this user.</p>

An additional configuration option that can be set in **faspex.yml** allows admins to require that newly created users reset their passwords the first time they log in. For information on this setting and **faspex.yml**, see [faspex.yml Configurations Reference](#) on page 154.

Permissions

Option	Description
Allowed to	<ul style="list-style-type: none"> • Uploads allowed: Select to allow users to send packages. • Downloads allowed: Select to allow users to download received packages. A user who does not have download permissions still receives packages, but cannot download the files. • Forwarding allowed: Select to allow users to forward received packages to other users. The package becomes available to the forwarded users in their Faspex accounts. • Can create from remote: Select to allow users to create a package from a remote source such as a remote server. Users allowed to access remote sources can access the Source drop-down menu when sending a new package. <p>You must first add remote sources to Faspex to see the Source drop-down menu. For more information on adding remote sources, see Adding a Node to Faspex on page 59.</p> <p>Note: This setting is disabled by default and must be set on a per-user basis (in other words, there is no global option).</p>
Allow inviting external senders	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable this user to invite users without Faspex accounts to upload a package to Faspex.</p>
Allow public submission URLs	<p>You must enable this option globally to see this feature. For more information, see Configuring Security Settings on page 47.</p> <p>Select Allow to enable users to send a Public URL to users without Faspex accounts. These external users can submit packages to registered Faspex users through this public URL. For more information about Public URLs, see Configuring Public URLs on page 91.</p> <p>Note: Even if the Public URL feature is enabled for registered Faspex users, they can override the feature for their own account by going to their user Account > Preferences > Misc and clearing Enable public URL.</p>
Can send to external email	<p>Select Allow to allow users to send packages to external email addresses.</p> <p>Faspex sends a download link through email. By default, this link expires after three days, but admins can change the duration or disable expiration by going to Server > Security. For more information, see Configuring Security Settings on page 47.</p>
Can create normal packages	<p>Select Allow to allow users to create packages on the New Package page. Select Deny to prevent the user from accessing the New Packages site. In this case, the user can only create dropbox packages and only if they are a member of a dropbox. To change the server default, go to Server > Configuration > Security and edit the setting for Allow users to create normal packages.</p>
Can send to all faspex users	<p>Select Allow to allow users to send packages to all Faspex users.</p>

Option	Description
	If this feature is enabled, all existing Faspex users appear in the contact list. If disabled, users can, only send packages to members of workgroups they are part of.
Keep user directory private	Select Yes to prevent users from being able to see the entire user directory, even if they have permissions to send to all Faspex users.
Can see global distribution lists.	Select Yes to give users access to global distribution lists. For more information on global distribution lists, see Creating a Global Distribution List on page 129.
Allowed IP addresses for login	Specify the IP addresses that a Faspex user can login from. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for download	Specify the IP addresses that a Faspex user can login from to download packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).
Allowed IP addresses for upload	Specify the IP addresses that a Faspex user can login from to upload packages. A wildcard (*) can be used in this option. For example, specifying 198.51.100.* allows a user to login from 198.51.100.1 , 198.51.100.2 , 198.51.100.3 , and so on. Separate multiple IP addresses with commas (,).

Package Deletion

Select from the following options to specify behavior after downloading a package:

Option	Description
After download	<p>You can override the server default by selecting Override system default. If you choose override, select one of the following policies:</p> <ul style="list-style-type: none"> • Do nothing: Do not auto-delete after the package is downloaded. • Delete files after any recipient downloads all files: Delete after <i>any</i> recipient downloads <i>all</i> files in the package once. <p>Important: When this option is selected, a forwarded package can be potentially deleted before the original recipient has downloaded it. Thus, proceed with caution when selecting this option.</p> <ul style="list-style-type: none"> • Delete files after all recipients download all files: Delete if <i>all</i> files in the package have been downloaded by <i>all</i> recipients.
Allow user to set own delete setting on a package-by-package basis	Select Allow to allow this user to choose a package expiration policy when sending a new package.

Personal Details

If Faspex has custom user fields configured, they appear in this section in addition to the following default fields:

Option	Description
Last name	Enter the user's last name.
First name	Enter the user's first name.
email address	Enter the user's email address.

For more information about custom user fields, see [Configuring Custom User Fields](#) on page 74.

Advanced Transfer Settings

By default, Faspex uses the transfer settings from the Aspera Central Server section. Select **Override default settings** to set user-specific transfer settings, which take precedence over the server-wide settings.

Option	Description
Initial Transfer Rate	Specify the initial upload and download transfer rate. When the option Lock minimum rate and policy is checked, the user is not able to adjust transfer policy or minimum transfer rate.
Maximum Allowed Rate	Specify the maximum upload and download transfer rate for this user.

Welcome Email

Option	Description
Send a welcome message	Select this option to send a welcome email to the user.
Comments	Enter any comments to be added to the standard Faspex welcome email. These comments go to this user only.

Email Notification Template Types

The following table describes the available email templates in Faspex;

Email Template	Description
Welcome E-mail	Faspex sends this email to new users at account creation unless the Send welcome email to all new users (Server > Configuration > Security) option is disabled.
Forgot Password	Faspex sends this email when a user clicks the Forgot my password link on the local login page or when an admin manually resets a user account's password.
Package Received	Faspex sends this email to package recipients when Faspex successfully transfers a package to their inboxes.
Package Received CC	Faspex sends this email to cc'ed users when Faspex successfully transfers a package to the inboxes of the original recipients. CC'ed users are users that are included in the CC Receipt field when sending a new package.
Package Sent CC	Faspex sends this email to cc'ed users when Faspex initiates a package transfer. CC'ed users are users that are included in the CC Receipt field when sending a new package.
Package Downloaded	Faspex sends this email to users when a sent package has been downloaded.
Package Downloaded CC	Faspex sends this email to cc'ed users when a user in downloads a sent package. CC'ed users are users that are included in the CC Download field or the CC Receipt field when sending a new package.

Email Template	Description
Workgroup Package	Faspex sends this email to workgroup members when a package is sent to the workgroup.
Upload Result	Faspex sends this email to notify a package sender or dropbox submitter whether the package upload completed successfully.
Upload Result CC	Faspex sends this email to notify a cc'ed user the package upload completed successfully. CC'ed users are users that are included in the CC Upload field or the CC Receipt field when sending a new package.
Relay Started CC	Faspex sends this email to cc'ed users that arelay has started. CC'ed users are users that are included in the Relay Started CC field, set in workgroup or dropbox settings.
Relay Finished CC	Faspex sends this email to cc'ed users that a relay has finished. CC'ed users are users that are included in the Relay Finished CC field, set in workgroup or dropbox settings.
Relay Error CC	Faspex sends this email to cc'ed users that a relay has failed. CC'ed users are users that are included in the Relay Error CC field, set in workgroup or dropbox settings.
Dropbox Invitation	Faspex sends this email to external users when they are invited to submit a package to a dropbox.
Dropbox Submit	Faspex sends this email to external users when they submit a package to a dropbox.
Personal Invitation	Faspex sends this email to external users when a Faspex user invites them to submit a package.
Personal Submit	Faspex sends this email to external users when they submit a package to a Faspex user.
Account Approved	Faspex sends this email to account requesters when their self-registration applications are approved by an admin. They are instructed to activate the account by resetting the account password.
Account Denied	Faspex sends this email to account requesters when their self-registration applications are denied by an admin.
Package Validation Failed Sender	Faspex sends this email to a package sender if the package fails validation.
Package Validation Failed Recipient	Faspex sends this email to package recipients if the package fails validation.

Email Notification Template Text Strings

Welcome E-mail

String	Description
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
SERVER_ADDRESS	Name or ip of the Faspex server
LOGIN	Login name of the email recipient
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Forgot Password

String	Description
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
SERVER_ADDRESS	Name or ip of the Faspex server
LOGIN	Login name of the email recipient
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Package Received

String	Description
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL

String	Description
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
LINK_EXPIRATION_INFO	If the download link expires, a sentence describing when the link expires
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Package Received CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package

String	Description
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Package Sent CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Package Downloaded

String	Description
DOWNLOADER_NAME	Full name of the user who downloaded the package
DOWNLOADER_FIRST_NAME	First name of the user who downloaded the package
DOWNLOADER_LAST_NAME	Last name of the user who downloaded the package

String	Description
DOWNLOADER_EMAIL	Email of the user who downloaded the package
DOWNLOADER_LOGIN	Login name of user who downloaded the package
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Package Downloaded CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC
DOWNLOADER_NAME	Full name of the user who downloaded the package
DOWNLOADER_FIRST_NAME	First name of the user who downloaded the package
DOWNLOADER_LAST_NAME	Last name of the user who downloaded the package
DOWNLOADER_EMAIL	Email of the user who downloaded the package
DOWNLOADER_LOGIN	Login name of user who downloaded the package

String	Description
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Workgroup Package

String	Description
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
WORKGROUP_NAME	Name of the workgroup the package was sent to
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL

String	Description
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Upload Result

String	Description
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
UPLOAD_RESULT	The result of the package upload
STATUS_URL	URL to check package upload status (does not work in subject)
STATUS_LINK	Link to check package upload status (does not work in subject)
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package

String	Description
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Upload Result CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
UPLOAD_RESULT	The result of the package upload
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Relay Started CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC

String	Description
WORKGROUP_NAME	Name of the workgroup the package was sent to
DESTINATION_NODE	Storage node
DESTINATION_DIRECTORY	Docroot relative path to the destination directory on the storage node
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Relay Finished CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC
WORKGROUP_NAME	Name of the workgroup the package was sent to
DESTINATION_NODE	Storage node
DESTINATION_DIRECTORY	Docroot relative path to the destination directory on the storage node
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender

String	Description
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Relay Error CC

String	Description
CC_NAME	Full name of the user who received the CC
CC_EMAIL	Email of the user who received the CC
WORKGROUP_NAME	Name of the workgroup the package was sent to
DESTINATION_NODE	Storage node
DESTINATION_DIRECTORY	Docroot relative path to the destination directory on the storage node
SENDER_NAME	Full name of the sender of the package
SENDER_FIRST_NAME	First name of the sender of the package
SENDER_LAST_NAME	Last name of the sender of the package
SENDER_EMAIL	Email address of sender
SENDER_LOGIN	Login name of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package

String	Description
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
ALL_PUBLIC_RECIPIENTS	All recipients of the package
ALL_PUBLIC_RECIPIENTS_EMAIL	Email addresses of all recipients of the package
ALL_CC_RECIPIENTS	All contacts that were notified about the receipt of this package
ALL_CC_RECIPIENTS_EMAIL	Email addresses of all contacts that were notified about the receipt of this package
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Dropbox Invitation

String	Description
EMAIL	Email address of the invited outside email user
DROPBOX_NAME	Dropbox to which the outside email user was invited
DROPBOX_URL	The URL that the outside email user can use to send packages to the dropbox
DROPBOX_LINK	HTML link that the outside email user can use to send packages to the dropbox
LINK_EXPIRATION_INFO	If the download link expires, a sentence describing when the link expires
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Dropbox Submit

String	Description
DROPBOX_NAME	Dropbox to which the outside email user was invited
SENDER_EMAIL	Email address of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
STATUS_URL	URL to check package upload status (does not work in subject)
STATUS_LINK	Link to check package upload status (does not work in subject)

String	Description
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Personal Invitation

String	Description
EMAIL	Email address of the invited outside email user
RECIPIENT_NAME	Full name of the recipient who invited the outside email
RECIPIENT_FIRST_NAME	First name of the recipient who invited the outside email
RECIPIENT_LAST_NAME	Last name of the recipient who invited the outside email
SUBMISSION_URL	The URL that the outside email user can use to send a package
SUBMISSION_LINK	HTML link that the outside email user can use to send a package
LINK_EXPIRATION_INFO	If the download link expires, a sentence describing when the link expires
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Personal Submit

String	Description
RECIPIENT_NAME	Full name of the recipient who invited the outside email
RECIPIENT_FIRST_NAME	First name of the recipient who invited the outside email
RECIPIENT_LAST_NAME	Last name of the recipient who invited the outside email
SENDER_EMAIL	Email address of sender
PACKAGE_NAME	Name of the package sent to the e-mail recipient
PACKAGE_UUID	The UUID of the package
PACKAGE_URL	Package's download URL
PACKAGE_DATE	Package's sent date
PACKAGE_SIZE	Size of the data in the package
PACKAGE_FILES	Number of files in the package
PACKAGE_FILE_LIST_FIRST_10	The first 10 files or folders at the top level of the package
PACKAGE_NOTE	Message associated with the package
STATUS_URL	URL to check package upload status (does not work in subject)
STATUS_LINK	Link to check package upload status (does not work in subject)
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server
ALTERNATE_ADDRESS_#	The alternate hostname or IP Address of the Faspex server (if enabled)

Account Approved

String	Description
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
SERVER_ADDRESS	Name or ip of the Faspex server
LOGIN	Login name of the email recipient
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server

Account Denied

String	Description
USER_NAME	Full name of the email recipient
USER_FIRST_NAME	First name of the email recipient
USER_LAST_NAME	Last name of the email recipient
SERVER_ADDRESS	Name or ip of the Faspex server
LOGIN	Login name of the email recipient
PRIMARY_ADDRESS	The primary hostname or IP Address of the Faspex server

Partitioning Mongrel Processes between Faspex and Cargo

Partition mongrels between handling Faspex UI requests and IBM Aspera Cargo requests to address performance issues.

When the number of Cargo clients attached to a Faspex cluster reaches a significant number, the performance of the Faspex Web UI can suffer due to resource contention with Cargo clients accessing the API.

To avoid this, tune the Apache configuration with separate sets of Mongrel processes dedicated to serving the Faspex web interface and API.

Note: The examples in the instructions below demonstrates Mongrel partitioning for 15 mongrel processes: 10 for Cargo and 5 for Faspex.

1. Run the following `asctl` command to set the proper total number of Mongrel processes:

```
asctl faspex:mongrel_count number+of_mongrels
```

Note: Running the `mongrel_count` command overwrites and removes any modifications to the `faspex.apache.linux.conf` configuration file, including the changes described in the following steps.

Choose not to restart Apache and Faspex.

2. Open the following Faspex Apache configuration file in a text editor: `/opt/aspera/faspex/config/faspex.apache.linux.conf` and make the following changes

- a) Add the `<Proxy balancer://faspex_cargo_cluster>` section.

For example:

```
...
#Proxy balancer section (create one for each ruby app cluster)
<Proxy balancer://faspex_cargo_cluster>
```

```

</Proxy>
<Proxy balancer://faspex_cluster>
  BalancerMember http://127.0.0.1:3000
  BalancerMember http://127.0.0.1:3001
  BalancerMember http://127.0.0.1:3002
  BalancerMember http://127.0.0.1:3003
  BalancerMember http://127.0.0.1:3004
  BalancerMember http://127.0.0.1:3005
  BalancerMember http://127.0.0.1:3006
  BalancerMember http://127.0.0.1:3007
  BalancerMember http://127.0.0.1:3008
  BalancerMember http://127.0.0.1:3009
  BalancerMember http://127.0.0.1:3010
  BalancerMember http://127.0.0.1:3011
  BalancerMember http://127.0.0.1:3012
  BalancerMember http://127.0.0.1:3013
  BalancerMember http://127.0.0.1:3014
</Proxy>
...

```

- b) Distribute the BalancerMember entries under <Proxy balancer://faspex_cluster> between the two sections.

For example:

```

...
#Proxy balancer section (create one for each ruby app cluster)
<Proxy balancer://faspex_cargo_cluster>
  BalancerMember http://127.0.0.1:3000/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3001/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3002/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3003/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3004/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3005/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3006/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3007/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3008/aspera/faspex/inbox.atom
  BalancerMember http://127.0.0.1:3009/aspera/faspex/inbox.atom
</Proxy>
<Proxy balancer://faspex_cluster>
  BalancerMember http://127.0.0.1:3010
  BalancerMember http://127.0.0.1:3011
  BalancerMember http://127.0.0.1:3012
  BalancerMember http://127.0.0.1:3013
  BalancerMember http://127.0.0.1:3014
</Proxy>
...

```

- c) Add ProxyPass /aspera/faspex/inbox.atom balancer://faspex_cargo_cluster to the proxy request section.

```

...
# send the proxy request
ProxyPass /aspera/faspex/inbox.atom balancer://faspex_cargo_cluster
ProxyPass /aspera/faspex balancer://faspex_cluster
...

```

3. Restart Apache and Faspex services.

```

asctl apache:restart
asctl faspex:restart

```

Aspera Ecosystem Security Best Practices

Your Aspera applications can be configured to maximize system and content security. The following sections describe the recommended settings and practices that best protect your content when using IBM Aspera High-Speed Transfer Server and IBM aspera High-Speed Transfer Endpoint, IBM Aspera Faspex, IBM Aspera Shares, and IBM Aspera Console.

Contents

Securing the Systems that Run Aspera Software

Securing the Aspera Application

Securing Content in your Workflow

Securing the Systems that Run Aspera Software

The systems that run Aspera software can be secured by keeping them up to date, by applying security fixes, and by configuring them using the recommended settings.

Updates

Aspera continually improves the built-in security of its products, as do the producers of third-party components used by Aspera, such as Apache, Nginx, and OpenSSH. One of the first lines of defense is keeping your products up to date to ensure that you are using versions with the latest security upgrades:

- Keep your operating system up to date.
- Keep your Aspera products up to date.
- If using, keep OpenSSH up to date. The server security instructions require that OpenSSH 4.4 or newer (Aspera recommends 5.2 or newer) is installed on your system in order to use the `Match` directive. `Match` allows you to selectively override certain configuration options when specific criteria (based on user, group, hostname, or address) are met.
- If you are using the HSTS web UI, keep Apache server up to date.

Security Fixes

Rarely, security vulnerabilities are detected in the operating systems and third-party components that are used by Aspera. Aspera publishes security bulletins immediately that describe the affected products and recommended remediation steps.

Security Configuration

Recommended security settings vary depending on the products you are using and how they interact. See the following subsections for your Aspera products.

HSTS

1. Configure your SSH Server.

Aspera recommends that you:

- Open TCP/33001 and keep TCP/22 open until users are notified that they should switch to TCP/33001.
- Once users are notified, block TCP/22 and allow traffic only on TCP/33001.

The following steps open TCP/33001 and block TCP/22.

a) Open the SSH configuration file.

```
/etc/ssh/sshd_config
```

If you do not have an existing configuration for OpenSSH, or need to update an existing one, Aspera recommends the following reference: <https://wiki.mozilla.org/Security/Guidelines/OpenSSH>.

b) Change the SSH port from TCP/22 to TCP/33001.

Add TCP/33001 and comment out TCP/22 to match the following example:

```
#Port 22
Port 33001
```

HSTS admins must also update the `SshPort` value in the `<WEB...>` section of `aspera.conf`.

Once this setting takes effect:

- Aspera clients must set the TCP port to 33001 when creating connections in the GUI or specify `-P 33001` for command line transfers.
 - Server administrators should use `ssh -p 33001` to access the server through SSH.
- c) Disable non-admin SSH tunneling.

SSH tunneling can be used to circumvent firewalls and access sensitive areas of your company's network. Add the following lines to the end of `sshd_config` (or modify them if they already exist) to disable SSH tunneling:

```
AllowTcpForwarding no
Match Group root
AllowTcpForwarding yes
```

Depending on your `sshd_config` file, you might have additional instances of `AllowTCPForwarding` that are set to the default `Yes`. Review your `sshd_config` file for other instances and disable if necessary.

Disabling TCP forwarding does not improve security unless users are also denied shell access, because with shell access they can still install their own forwarders. Aspera recommends assigning users to `aspsell`, described in the following section.

- d) Disable password authentication and enable public key authentication.

Public key authentication provides a stronger authentication method than passwords, and can prevent brute-force SSH attacks if all password-based authentication methods are disabled.

Important: Before proceeding:

- Create a public key and associate it with a transfer user, otherwise clients have no way of connecting to the server.
- Configure at least one non-root, non-transfer user with a public key to use to manage the server. This is because in the following steps, root login is disabled and transfer users are restricted to `aspsell`, which does not allow interactive login. This user and public key is what you use to access and manage the server as an administrator.

Add or uncomment `PubkeyAuthentication yes` and comment out `PasswordAuthentication yes`:

```
PubkeyAuthentication yes
#PasswordAuthentication yes
PasswordAuthentication no
```

Note: If you choose to leave password authentication enabled, be sure to advise account creators to use strong passwords and set `PermitEmptyPasswords` to "no".

```
PermitEmptyPasswords no
```

- e) Disable root login.



CAUTION: This step disables root access. Make sure that you have at least one user account with `sudo` privileges before continuing, otherwise you may not have access to administer your server.

Comment out `PermitRootLogin yes` and add `PermitRootLogin No`:

```
#PermitRootLogin yes
PermitRootLogin no
```

- f) Restart the SSH server to apply new settings. Restarting your SSH server does not affect currently connected users.

```
# systemctl restart sshd.service
```

or for Linux systems that use `init.d`:

```
# service sshd restart
```

- g) Review your logs periodically for attacks.

For information on identifying attacks, see [IBM Aspera IBM Aspera High-Speed Transfer Server Admin Guide: Securing Your SSH Server](#).

2. Configure your server's firewall to permit inbound access to only Aspera-required ports.

Aspera requires inbound access on the following ports:

- For SSH connections that are used to set up connections, TCP/33001.
- For FASP transfers, UDP/33001.
- If you use HTTP and HTTPS fallback with HSTS, TCP/8080 and TCP/8443. If you only use HTTPS, only open TCP/8443.
- If your clients access the HSTS web UI, TCP/80 (for HTTP) or TCP/443 (for HTTPS).

3. For HSTS, require strong TLS connections to the web server.

TLS 1.0 and TLS 1.1 are vulnerable to attack. Run the following command to require that the client's SSL security protocol be TLS version 1.2 or higher:

```
asconfigurator -x "set_server_data;ssl_protocol,tls1.2"
```

4. If is exposed to internet traffic, run it behind a reverse proxy.

If your Aspera server must expose to the internet, such as when setting it up as a IBM Aspera on Cloud (AoC) node, Aspera strongly recommends protecting it with a reverse proxy. Normally, runs on port 9092, but nodes that are added to AoC must have run on port 443, the standard HTTPS port for secure browser access. Configuring a reverse proxy in front of provides additional protection (such as against DOS attacks) and resource handling for requests to the node's 443 port.

The following instructions describe how to set up Nginx as a reverse proxy and require that you have valid, CA-signed SSL certificates in .pem format for the server. Other reverse proxies might be supported on your server.

- Set up a system user with Node API credentials on your server.
- Download and install Nginx.
- Configure the HTTPS port for .

```
# asconfigurator -x "set_server_data;https_port,9092"
```

- d) Open the Nginx configuration file in a text editor.

Open `/etc/nginx/nginx.conf` and ensure the following `include` directive is present in the `http` section. If it is not present, add it to the file:

```
http {
...
include /etc/nginx/conf.d/*.conf;
}
```

- e) Create a file named `aspera_node_proxy.conf` and save it in the following location:

/etc/nginx/conf.d/aspera_node_proxy.conf

- f) Paste the following content into aspera_node_proxy.conf:

```
#
# Aspera configuration - reverse proxy for asperanoded
#
server {
    listen 443;
    server_name your.servername.com;
    ssl_certificate /opt/aspera/etc/aspera_server_cert.pem;
    ssl_certificate_key /opt/aspera/etc/aspera_server_key.pem;

    ssl on;
    ssl_session_cache builtin:1000 shared:SSL:10m;
    ssl_protocols TLSv1.2;
    ssl_ciphers EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH;
    ssl_prefer_server_ciphers on;

    access_log          /var/log/nginx/node-api.access.log;

    location / {
        proxy_pass https://127.0.0.1:9092;
        proxy_read_timeout 60;
        proxy_redirect https://127.0.0.1:9092 https://your.servername.com;

        proxy_set_header Host          $host:$server_port;
        proxy_set_header X-Real-IP      $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

Note: Configure SSL ciphers as required. The preceding sample is not configured for backwards compatibility, and the recommended list of secure ciphers might change. Aspera recommends reviewing and staying current with the list provided in <https://cipherli.st/>.

In this configuration, Nginx listens externally on port 443, not 9092. Replace *your.servername.com* with your server's domain name.

- g) Restart .

```
# systemctl restart asperanoded
```

or for Linux systems that use `init.d`:

```
# service asperanoded restart
```

- h) Restart Nginx.

```
# service nginx restart
```

5. Install Aspera FASP Proxy in a DMZ to isolate your HSTS from the Internet.

For more information, see [IBM Aspera FASP Proxy Admin Guide](#)

Faspex and Shares

1. Configure your Faspex or Shares server firewall to allow inbound access to TCP/443, the default HTTPS port.
2. Faspex and Shares transfer nodes should be configured as described for HSTS.

The transfer user that is used by Faspex and Shares (usually `xfer`) must be configured on the node to only allow transfers with a token:

```
asconfigurator -x
"set_user_data;user_name,xfer;authorization_transfer_in_value,token"
asconfigurator -x
"set_user_data;user_name,xfer;authorization_transfer_out_value,token"
```

Set the token encryption key to a string of at least 20 characters:

```
asconfigurator -x
"set_user_data;user_name,xfer;token_encryption_key,token_string"
```

Do not use UUIDs for this key because they might not be generated using cryptographically secure methods.

Console

Configure the firewall of the computer on which Console is installed to only allow Aspera-required connections to the following ports:

- For HTTP or HTTPS access for the web UI, inbound TCP/80 or TCP/443.
- For SSH connections, outbound TCP/33001 to managed nodes.
- For Node API connections, outbound TCP/9092 to managed nodes.
- For connections to legacy nodes (those running HSTS older than 3.4.6), outbound TCP/40001 and inbound TCP/4406. For security and reliability, Aspera strongly recommends upgrading all nodes to the latest version.

Securing the Aspera Applications

Your Aspera products can be configured to limit the extent to which users can connect and interact with the servers. The instructions for Shares 1.9.x and Shares 2.x are slightly different; see the section for your version.

HSTS

1. Restrict user permissions with `aspsshell`.

By default, all system users can establish a FASP connection and are only restricted by file permissions. Restrict the user's file operations by assigning them to use `aspsshell`, which permits only the following operations:

- Running Aspera uploads and downloads to or from this computer.
- Establishing connections between Aspera clients and servers.
- Browsing, listing, creating, renaming, or deleting contents.

These instructions explain one way to change a user account or active directory user account so that it uses the `aspsshell`; there may be other ways to do so on your system.

Run the following command to change the user login shell to `aspsshell`:

```
sudo usermod -s /bin/aspsshell username
```

Confirm that the user's shell updated by running the following command and looking for `/bin/aspsshell` at the end of the output:

```
grep username /etc/passwd
username:x:501:501:...:/home/username:/bin/aspshell
```

Note: If you use OpenSSH, sssd, and Active Directory for authentication: To make `aspsshell` the default shell for all domain users, first set up a local account for server administration because this change affects all domain users. Then open `/etc/sss/sss.conf` and change `default_shell` from `/bin/bash` to `/bin/aspsshell`.

2. Restrict Aspera transfer users to a limited part of the server's file system or bucket in object storage.

a) For on-premises servers, set a default docroot to an empty folder, then set a docroot for each user:

```
asconfigurator -x "set_node_data;absolute,docroot"
asconfigurator -x "set_user_data;user_name,username;absolute,docroot"
```

Replace *username* with the username and *docroot* with the directory path to which the user should have access.

- b) For cloud-based servers, set a default restriction to an empty folder, then set a restriction for each user:

```
asconfigurator -x "set_node_data;file_restriction,|storage_path"
asconfigurator -x
"set_user_data;user_name,username;file_restriction,|storage_path"
```

Replace *username* with the username and *storage_path* with the path to which the user has access. Restriction syntax is specific to the storage:

Storage Type	Format Example
local storage	file:///*
S3 and IBM Cloud Object Storage	s3:///*
Swift storage	swift:///*
Azure storage	azu:///*
Azure Files	azure-files:///*
Google Cloud Storage	gs:///*
Hadoop (HDFS)	hdfs:///*

The "|" is a delimiter, and you can add additional restrictions. For example, to restrict the system user *xfer* to `s3://s3.amazonaws.com/bucket_xyz/folder_a/*` and not allow access to key files, run the following command:

```
asconfigurator -x "set_user_data;user_name,xfer;file_restriction,|s3://
s3.amazonaws.com/bucket_xyz/folder_a/*|!*.key"
```

3. Restrict users' read, write, and browse permissions.

Users are given read, write, and browse permissions to their docroot by default. Change the global default to deny these permissions:

```
asconfigurator -x
"set_node_data;read_allowed,false;write_allowed,false;dir_allowed,false"
```

Run the following commands to enable permissions per user, as required:

```
asconfigurator -x "set_user_data;user_name,username;read_allowed,false"
asconfigurator -x "set_user_data;user_name,username;write_allowed,false"
asconfigurator -x "set_user_data;user_name,username;dir_allowed,false"
```

4. Limit transfer permissions to certain users.

Set the default transfer permissions for all users to deny:

```
asconfigurator -x "set_node_data;authorization_transfer_in_value,deny"
asconfigurator -x "set_node_data;authorization_transfer_out_value,deny"
```

Allow transfers for specific users by running the following commands for each user:

```
asconfigurator -x
"set_user_data;user_name,username;authorization_transfer_in_value,allow"
asconfigurator -x
"set_user_data;user_name,username;authorization_transfer_out_value,allow"
```

Note: For a user that is used by Shares or Faspex (usually *xfer*), allow transfers only with a token by setting `authorization_transfer_{in|out}_value` to `token`.

5. Encrypt transfer authorization tokens.

When a client requests a transfer from a server through an Aspera web application, an authorization token is generated. Set the encryption key of the token for each user or group on the server:

```
asconfigurator -x
"set_user_data;user_name,username;token_encryption_key,token_string"
asconfigurator -x
"set_group_data;group_name,groupname;token_encryption_key,token_string"
```

The token string should be at least 20 random characters.

Note: This is not used to encrypt transfer data, only the authorization token.

6. Require encryption of content in transit.

Your server can be configured to reject transfers that are not encrypted, or that are not encrypted with a strong enough cipher. Aspera recommends setting an encryption cipher of at least AES-128. AES-192 and AES-256 are also supported but result in slower transfers. Run the following command to require encryption:

```
asconfigurator -x
"set_node_data;transfer_encryption_allowed_cipher,aes-128"
```

By default, your server is configured to transfer (as a client) using AES-128 encryption. If you require higher encryption, change this value by running the following command:

```
asconfigurator -x "set_client_data;transport_cipher,value"
```

You can also specify the encryption level in the command line by using `-c cipher` with `ascp` and `async` transfers. `ascp4` transfers use AES-128 encryption.

7. Configure SSH fingerprinting for HSTS.

For transfers initiated by a web application (such as Faspex, Shares, or Console), the client browser sends the transfer request to the web application server over an HTTPS connection. The web application requests a transfer token from the target server. The transfer is executed over a UDP connection directly between the client and the target server and is authorized by the transfer token. Prior to initiating the transfer, the client can verify the server's authenticity to prevent server impersonation and man-in-the-middle (MITM) attacks.

To verify the authenticity of the transfer server, the web application passes the client a trusted SSH host key fingerprint of the transfer server. The client confirms the server's authenticity by comparing the server's fingerprint with the trusted fingerprint. In order to do this, the host key fingerprint or path must be set in the server's `aspera.conf`.

Note: Server SSL certificate validation (HTTPS) is enforced if a fingerprint is specified in `aspera.conf` and HTTP fallback is enabled. If the transfer "falls back" to HTTP and the server has a self-signed certificate, validation fails. The client requires a properly signed certificate.

If you set the host key path, the fingerprint is automatically extracted from the key file and you do not extract it manually.

Retrieving and setting the host key fingerprint:

- a) Retrieve the server's SHA-1 fingerprint.

```
cat /etc/ssh/ssh_host_rsa_key.pub | awk '{print $2}' | base64 -d |
shasum
```

- b) Set the SSH host key fingerprint in `aspera.conf`. (Go to the next step to set the host key path instead).

```
asconfigurator -x
"set_server_data;ssh_host_key_fingerprint,fingerprint"
```

This command creates a line similar to the following example of the <server> section of `aspera.conf`:

```
<ssh_host_key_fingerprint>7qdOwebGGeDeN7Wv+2dP3HmWfP3
</ssh_host_key_fingerprint>
```

- c) Restart the node service to activate your changes.

Run the following commands to restart `asperanoded`:

```
systemctl restart asperanoded
```

or for Linux systems that use `init.d`:

```
service asperanoded restart
```

Setting the host key path: To set the SSH host key path instead of the fingerprint, from which the fingerprint will be extracted automatically, run the following command:

```
# asconfigurator -x "set_server_data;ssh_host_key_path,ssh_key_filepath"
```

This command creates a line similar to the following in the <server> section of `aspera.conf`:

```
<ssh_host_key_path>/etc/ssh/ssh_host_rsa_key.pub
</ssh_host_key_path>
```

Restart the node service to activate your changes, as described for "Retreiving and setting the host key fingerprint".

8. Install properly signed SSL certificates.

Though your Aspera server automatically generates self-signed certificates, Aspera recommends installing valid, signed certificates. These are required for some applications.

Faspex

Many of the settings for Faspex are the same as for HSTS, including SSH server configuration, firewall settings, and signed SSL certificate installation. The following recommendations augment or are additional to the recommendations described for HSTS.

1. Restrict transfers by all users except "faspex".

If your system is a dedicated Faspex server - the HSTS installed as part of your Faspex installation is used only for Faspex transfers - prohibit transfers by all users except "faspex". If you have not already, deny transfers globally by default:

```
asconfigurator -x "set_node_data;authorization_transfer_in_value,deny"
asconfigurator -x "set_node_data;authorization_transfer_out_value,deny"
```

Allow transfers for "faspex" by running the following commands:

```
asconfigurator -x
"set_user_data;user_name,faspex;authorization_transfer_in_value,token"
asconfigurator -x
"set_user_data;user_name,faspex;authorization_transfer_out_value,token"
```

2. Configure the Nginx server to allow only strong TLS.

The default configuration of Faspex has TLS 1.0, 1.1 and 1.2 enabled. Older browsers require the older and less secure versions (TLS 1.0 and 1.1). You can disable support for older browsers by removing TLS 1.0 and TLS 1.1 from the configuration.

- a) Open the Nginx configuration file on the Shares server for editing:

```
/opt/aspera/common/apache/conf/extra/httpd-ssl.conf
```

- b) Locate the following line:

```
SSLProtocol ALL -SSLv2 -SSLv3
```

- c) Replace the line with the following and save your change:

```
SSLProtocol TLSv1.2
```

- d) Restart Apache to activate your change:

```
asctl apache:restart
```

3. Limit admin logins to those from known IP addresses.

Faspex admins have the ability to execute post-processing scripts on the server. If an admin account is compromised, this capability can be a serious threat to your server's security. You can add additional protection by allowing admin logins from only specific IP addresses.

- In the Faspex UI, go to **Accounts** and select the admin account.
- In the **Permissions** section, locate the **Allowed IP addresses for login** field and enter the IP addresses or IP address range to allow.
- Click **Save** to activate your changes.

4. Configure Faspex account security settings.

Go to **Server > Configuration > Security** and set the following global default configurations in the **Faspex accounts** section, then edit configurations for individual users, as needed:

- Set a non-zero session timeout.
- Lock users out after five failed login attempts within five minutes.
- Enable **Prevent concurrent login**.
- Set a password expiration interval of 30 days.
- Prevent reuse of the last three passwords and require strong passwords.
- Set **Keep user directory private** to **Yes**.
- Disable **Allow all users to send to all other Faspex users**.
- Disable **Users can see global distribution lists**.
- Disable **Ignore invalid recipients**.
- Disable **Allow users to change their email address**.

Stay in **Server > Configuration > Security** for the next step.

5. Configure Faspex account registration settings.

In **Server > Configuration > Security**, set the following configurations in the **Registrations** section:

- Set **Self-registration** to **None**.
When self-registration is enabled, it can be used to find out whether a certain account exists on the server. That is, if you attempt to self-register a duplicate account, you receive a prompt stating that the user already exists.
- Select **Require external users to register**.
By requiring external users to register, you can better track their Faspex activity.

Stay in **Server > Configuration > Security** for the next step.

6. Configure outside email address settings.

In **Server > Configuration > Security**, set the following global default configurations in the **Outside email addresses** section, then edit configurations for individual users, as needed:

- Disable **Allow inviting external senders**.
- Enable **Invitation link expires** and set an expiration policy.
- Disable **Allow public submission URLs**.
- Disable **Allow sending to external email addresses**.
- Set a package link expiration.
- Disable **Allow external packages to Faspex users**.

Stay in **Server > Configuration > Security** for the next step.

7. Configure Faspex encryption.

In **Server > Configuration > Security**, set the following configurations in the **Encryption** section:

- a) Enable **Encrypt transfers**.
- b) If possible in your work flow, set **Use encryption-at-rest** to **Always**.
See the next section, "Securing Content in your Workflow," for information about encryption at rest.
- c) Disable **Allow dropboxes to have their own encryption settings**.

8. Click **Update** when you have completed updating settings on the **Security** page to activate your changes.

9. Hide your server's IP address from email notifications.

If Faspex is configured to identify itself by IP address (rather than by domain name), then the URLs in your notification emails contain your IP address (for example, "https://10.0.0.1/aspera/faspex"). Configure an alternate IP address or domain name for users who are external to your organization.

- a) Go to **Server > Configuration > Web Server**.
- b) Select **Enable alternate address** then click **Add alternate address**.
- c) Enter the address name and description, and select **Show in emails**.
- d) Click **Update** to activate your change.
- e) Customize your email notification templates to use the alternate address.

Go to **Server > Notifications**.

Shares

The Shares server and its nodes should be secured as described for HSTS, including SSH server configuration, firewall settings, and valid, signed SSL certificate installation. You can also secure the Shares application and its network of nodes by restricting user permissions. Set the following settings globally, then edit the settings for specific users and groups.

1. Configure Shares security settings.

On the **Admin** page, click **User Security** and set the following:

- a) Set a non-zero session timeout.
- b) Require strong passwords.
- c) Set a password expiration interval of 30 days.
- d) Lock users out after five failed login attempts within five minutes.
- e) Do not allow self registration by setting **Self Registration** to **None**.

2. When setting up the email server (**Admin > SMTP**), select **Use TLS if available**.

3. Configure the Nginx server to allow only strong TLS.

The default configuration of Shares has TLS 1.0, 1.1 and 1.2 enabled. Older browsers require the older and less secure versions (TLS 1.0 and 1.1). You can disable support for older browsers by removing TLS 1.0 and TLS 1.1 from the configuration.

- a) Open the Nginx configuration file on the Shares server for editing:
`/opt/aspera/shares/etc/nginx/nginx.conf`
- b) Delete TLSv1 and TLSv1.1 from the following line:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

4. Configure secure transfer settings.

Go to **System Settings > Transfers** and set the following:

- a) Require a minimum Connect version of 3.6.1.
- b) For **Encryption**, select **AES-128**.
- c) If possible in your workflow, set **Encryption at Rest** to **Required**.

See the next section, "Securing Content in your Workflow," for information about encryption at rest.

5. Go to **System Settings > Web Server** and select **Enable SSL/TLS**.

This setting requires that the Shares server has a valid, signed SSL certificate.

6. When adding new users to Shares, disable **API Login** if users do not need to use the Shares API.
The Shares API is used by clients connecting through IBM Aspera Drive and IBM Aspera Command-Line Interface
7. When adding nodes to Shares, select **Use SSL** (required by Shares) and **Verify SSL** (requires that the node has a valid, signed SSL certificate).
8. When authorizing a user or group to a share (*share_name* > **Authorizations**), set the minimum permissions required based on their Shares use.

Shares 2.x

The Shares 2.x server and its nodes should be secured as described for HSTS, including configuring the SSH server, firewall settings, and installing valid, signed SSL certificates. You can also secure the Share application and its network of nodes by restricting user permissions. Set the following settings globally and then edit the settings for specific users, groups, and administrators.

1. Configure Shares security settings.

Go to **System Administration > Configuration > User Security** and set the following:

- a) Set a non-zero session timeout.
- b) Set an access token lifetime of 8 hours.
- c) Enable refreshing of expired access tokens, with a lifetime of 7 days.

Go to **System Administration > Configuration > Local User Security** and set the following:

- a) Require strong passwords.
- b) Set a password expiration interval of 30 days.
- c) Lock users out after five failed login attempts within five minutes.
- d) Prevent reuse of the last three passwords and require strong passwords.

2. When setting up the email server (**System Administration > Configuration > SMTP**), select **Use TLS if available**.
3. Configure secure transfer settings.

Go to **System Administration > Configuration > Transfers** and set the following:

- a) Require a minimum Connect version of 3.6.1.
- b) For **Encryption**, select **AES-128** (or higher, if needed).
- c) If possible in your workflow, set **Encryption at Rest** to **Yes**.

See the next section, "Securing Content in your Workflow," for information about encryption at rest.

4. Go to **System Administration > Configuration > Web Server** and select **Enable SSL/TLS**.

This setting requires that the Shares server has a valid, signed SSL certificate.

5. Configure the Nginx server to allow only strong TLS.

The default configuration of Shares has TLS 1.0, 1.1 and 1.2 enabled. Older browsers require the older and less secure versions (TLS 1.0 and 1.1). You can disable support for older browsers by removing TLS 1.0 and TLS 1.1 from the configuration.

- a) Open the Nginx configuration file on the Shares server for editing:

```
/opt/aspera/shares/etc/nginx/nginx.conf
```

- b) Delete TLSv1 and TLSv1.1 from the following line:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

6. When adding nodes to Shares, select **Use SSL** (required by Shares) and **Verify SSL** (requires that the node has a valid, signed SSL certificate).
7. When authorizing a user or group to a share, set the minimum permissions required based on their Shares use.

Console

Console nodes should be secured as described for HSTS, including SSH server configuration, firewall settings, and valid, signed SSL certificate installation. If possible for your workflow, limit Console and its nodes to your internal network.

You can also secure the Console application and its network of nodes by restricting user permissions:

1. Configure secure Console defaults.

Go to **Configuration > Defaults** and set the following:

- a) In the drop-down menu for **Default SSH encryption**, select a default SSH encryption algorithm of at least AES-128 for non-Console nodes.
- b) For **Transport Encryption**, select **AES-128**.
- c) Disable **Smart Transfer Sharing**.
- d) Set a non-zero session timeout.
- e) Lock users out after five failed login attempts within five minutes.
- f) Enable **Prevent concurrent login**.
- g) Enable **Suppress logging of transfer tokens** to prevent tokens from being written to the Console database.
- h) Set a password expiration interval of 30 days.
- i) Prevent reuse of the last three passwords and require strong passwords.

2. When setting up the email server (**Notifications > Email Server**), select **Use TLS if available**.

3. Restrict Console users' permissions.

- a) When creating a new user (**Accounts > Users > New User**), disable user login until their permissions are set by clearing **Active (allow user to log in)**. Click **permissions** and enable only the permissions that the user requires. Once permissions are configured, allow the user to login by going to **Accounts > Users**, clicking the user, and selecting **Active (allow user to log in)**.

- b) Assign users to Console Groups with only the required transfer paths and permissions allowed.

Create a group (**Accounts > Groups > New Group**) and restrict the group's transfers by clicking **Add Transfer Path**. Assign specific endpoints to the group's transfer path, rather than **Any**, which grants permission to transfer to all nodes. Limit the direction of the path, if the group's workflow allows.

4. When adding managed and unmanaged nodes, set the SSH port to 33001 and ensure SSH connections are encrypted with AES-128 or higher.

5. When adding a managed cluster, select **Use HTTPS to connect to node** and **Require signed SSL certificate**.

6. When adding SSH endpoints, use SSH public key authentication rather than password authentication.

The key file on the node should not be a shared key; it should be a "private" key in the specified user account.

Securing Content in your Workflow

1. If your workflow allows, enable server-side encryption-at-rest (EAR).

When files are uploaded from an Aspera client to the Aspera server, server-side encryption-at-rest (EAR) saves files on disk in an encrypted state. When downloaded from the server, server-side EAR first decrypts files automatically, and then the transferred files are written to the client's disk in an unencrypted state. Server-side EAR provides the following advantages:

- It protects files against attackers who might gain access to server-side storage. This is important primarily when using NAS storage or cloud storage, where the storage can be accessed directly (and not just through the computer running HSTS).
- It is especially suited for cases where the server is used as a temporary location, such as when one client uploads a file and another client downloads it.
- Server-side EAR can be used together with client-side EAR. When used together, content is doubly encrypted.
- Server-side EAR doesn't create an "envelope" as client-side EAR does. The transferred file stays the same size as the original file. The server stores the metadata necessary for server-side EAR separately in a file of the same name with the file extension `.aspera-meta`. By contrast, client-side EAR creates an envelope file

containing both the encrypted contents of the file and the encryption metadata, and it also changes the name of the file by adding the file extension `.aspera-env`.)

- It works with both regular transfers (FASP) and HTTP fallback transfers.

Limitations and Other Considerations

- Server-side EAR is not designed for cases where files need to move in an encrypted state between multiple computers. For that purpose, client-side EAR is more suitable: files are encrypted when they first leave the client, then stay encrypted as they move between other computers, and are decrypted when they reach the final destination and the passphrase is available. See Step 4 of this section for more information on client-side encryption.
- Do not mix server-side EAR and non-EAR files in transfers, which can happen if server-side EAR is enabled after the server is in use or if multiple users have access to the same area of the file system but have different EAR configurations. Doing so can cause problems for clients by overwriting files when downloading or uploading and corrupting metadata.
- Server-side EAR does not work with multi-session transfers (using `ascp -C` or node API `multi_session` set to greater than 1) or Watch Folders (versions prior to 3.8.0 that do not support URI docroots).

To enable server-side EAR:

- a) Set users' docroots in URI format (local docroots are prepended with `file:///`).

```
asconfigurator -x "set_user_data;user_name,username;absolute,file:///path"
```

- b) Set the server-side EAR password.

Set a different EAR password for each user:

```
asconfigurator -x "set_user_data;user_name,username;transfer_encryption_content_protection_secret,passphrase"
```

Important: If the EAR password is lost or `aspera.conf` is compromised, you cannot access the data on the server.

- c) Require content protection and strong passwords.

These settings cause server-side EAR to fail if a password is not given or if a password is not strong enough. For example, the following `asconfigurator` command adds both these options for all users (global):

```
asconfigurator -x "set_node_data;transfer_encryption_content_protection_required,true"
asconfigurator -x "set_node_data;transfer_encryption_content_protection_strong_pass_required,true"
```

2. Never use "shared" user accounts.

Configure each user as their own Aspera transfer user. Sharing Aspera transfer user account credentials with multiple users limits user accountability (you cannot determine which of the users sharing the account performed an action).

3. Use passphrase-protected private keys.

The `ssh-keygen` tool can protect an existing key or create a new key that is passphrase protected.

If you cannot use private key authentication and use password authentication, use strong passwords and change them periodically.

4. If your workflow allows, require client-side encryption-at-rest (EAR).

Aspera clients can set their transfers to encrypt content in transit and on the server, and the server can be configured to require client-side EAR. You can combine client-side and server-side EAR, in which case files are doubly encrypted on the server. Client-side encryption-at-rest is not supported for `ascp4` or `async` transfers.

Client configuration

The client specifies a password and the files are uploaded to the server with a `.aspera-env` extension. Anyone downloading these `.aspera-env` files must have the password to decrypt them. Users can enable client-side EAR in the GUI or on the `ascp` command line.

GUI: Go to **Connections > connection_name > Security**. Select **Encrypt uploaded files with a password** and set the password. Select **Decrypt password-protected files downloaded** and enter the password.

Ascp command line: Set the encryption and decryption password as the environment variable ASPERA_SCP_FILEPASS. For uploads (`--mode=send`), use `--file-crypt=encrypt`. For downloads (`--mode=recv`), use `--file-crypt=decrypt`.

Note: When a transfer to HSTS falls back to HTTP or HTTPS, client-side EAR is no longer supported. If HTTP fallback occurs while uploading, then the files are NOT encrypted. If HTTP fallback occurs while downloading, then the files remain encrypted.

Server configuration

To configure the server to require client-side EAR and to require strong content protection passwords, run the following commands:

```
asconfigurator -x "set_node_data;transfer_encryption_content_protection_required,true"
asconfigurator -x "set_node_data;transfer_encryption_content_protection_strong_pass_required,true"
```

Note: These commands set the global configuration. Depending on your work flow, you might want to require client-side EAR and strong passwords for only specific users.

5. For particularly sensitive content, do not store unencrypted content on any computer with network access.

HSTS, HSTE, and Desktop Client include the `asprotect` and `asunprotect` command-line tools that can be used to encrypt and decrypt files. Use an external drive to physically move encrypted files between a network-connected computer and an unconnected computer on which the files can be unencrypted.

- To encrypt a file before moving it to a computer with network access, run the following commands to set the encryption password and encrypt the file:

```
export ASPERA_SCP_FILEPASS=password
asprotect -o filename.aspera-env filename
```

- To download client-side-encrypted files without decrypting them immediately, run the transfer without decryption enabled (clear **Decrypt password-protected files downloaded** in the GUI or do not specify `--file-crypt=decrypt` on the `ascp` command line).
- To decrypt encrypted files, run the following commands to set the encryption password and decrypt the file:

```
export ASPERA_SCP_FILEPASS=password
asprotect -o filename filename.aspera-env
```

Patch Versions

A patched Faspex installation displays the current patch version in the page footer, defined by a patch-version file included in a patch. Upgrading Faspex removes the patch-version file.