

*IBM Aspera Shares 1.10*



---

# Contents

<b>Shares Admin Guide for Windows.....</b>	<b>1</b>
Introduction.....	1
Installing Shares.....	2
Installing Shares.....	2
Upgrading Shares.....	4
Securing an SSH Server.....	7
First Log In and Licensing.....	7
Configuring Shares Web Server and Transfer Policies.....	8
Uninstalling Shares.....	9
Configuring Shares Options.....	9
Configuring the Web Server.....	9
The Shares Home Page.....	9
Configure User Preferences.....	10
Configuring System Settings.....	11
Managing Home Shares.....	12
Enabling Home Shares.....	12
Disabling Home Shares.....	13
Changing the Home Shares Node.....	13
Configuring the Shares Time Zone and Time Format.....	13
Configuring Logging Settings.....	13
Configuring Transfer Settings.....	14
Configuring HTTP and HTTPS Fallback.....	15
Allowing Connections from More Hosts.....	16
Securing Shares.....	16
Configuring Shares Security.....	16
Configuring Manager Permissions.....	17
Moderate Self Registered Accounts.....	17
Installing a Signed SSL Certificate Provided by Authorities.....	17
Generating and Installing a New Self-Signed SSL Certificate.....	19
Generating New Diffie-Hellman Parameters.....	19
Configuring Email.....	20
Setting Up the SMTP Server.....	20
Updating Links in Email Notifications.....	20
Configure Email Settings.....	21
Creating Email Templates.....	21
Creating and Modifying Variables in Templates.....	23
Setting Up Transfer Nodes.....	23
Configuring Transfer Servers for Use with Shares.....	23
Setting Up a Linux Node.....	24
Setting Up a Windows Node.....	26
Setting Up a macOS Node.....	29
Managing Nodes.....	32
Adding Nodes.....	32
Modifying Nodes.....	35
Browsing Nodes.....	35
Searching Nodes and Shares.....	36
Managing User Accounts.....	36
Understanding User Roles and Share Authorization.....	36
Adding Local Users.....	37
Configure User Settings.....	38
Unlocking User Accounts and Changing Passwords.....	39

Disabling and Deleting User Accounts.....	39
Setting a User Account Expiration Date.....	40
Assigning Users the Manager Role.....	40
Disabling a User's Home Share.....	40
Searching Accounts.....	40
Managing Group Accounts.....	41
Adding Local Groups.....	41
Configure Local Group Settings.....	41
Configuring the Directory Service.....	42
Adding a Directory Service (DS).....	42
Importing Directory Service Users.....	43
Importing Directory Service Groups.....	43
Configure DS Users and Groups.....	44
Working with SAML.....	45
SAML and Shares.....	45
User Accounts Provisioned by Just-In-Time (JIT) Provisioning.....	45
Configuring Your Identity Provider (IdP).....	46
Configuring SAML for Shares.....	49
Creating SAML Groups.....	49
Customizing SAML Attribute Mapping.....	50
Importing a SAML User to Shares.....	50
Configuring Signed SAML Authentication Requests.....	51
Managing a Share.....	52
Creating a Share.....	52
Creating a Share from a Folder.....	54
Modifying a Share.....	55
Browsing a Share.....	56
Authorizing Users to a Share.....	57
Transferring Files.....	57
Uploading and Downloading Content.....	57
IBM Aspera Shares and the Connect Browser Plug-In.....	58
The Transfers Window.....	58
Monitoring Transfers.....	59
Serving Connect from a Local Location.....	60
Transferring Content Between Shares.....	61
Using Bookmarks.....	61
Monitoring Shares.....	62
Monitoring Shares Activity.....	62
Errors and Warnings.....	63
Configuring the Stats Collector.....	64
Adding Existing Nodes to Stats Collector.....	64
Configure Stats Collector Log Levels.....	64
Lowering Stats Collector Polling Frequency.....	64
Retrieving Stats Collector Version Number.....	65
Working with Rake Tasks.....	65
Configuring Users With Rake Tasks.....	65
Configure Groups With Rake Tasks.....	67
Configure a Share With Rake Tasks.....	69
Configure Nodes With Rake Tasks.....	71
Configure Server Settings With Rake Tasks.....	72
Configuring MySQL Server.....	73
Open a MySQL Prompt.....	73
Using an External MySQL Database.....	73
Backing Up and Restoring the Database.....	74
Backing Up Shares and the Database.....	74
Restoring Shares from a Backup.....	75
Troubleshooting Shares.....	76
Create a Shares Admin or Reset Admin Password.....	76

Restart Shares Services.....	76
Clearing Unresponsive Background Jobs.....	76
Gathering and Zipping All Logs for Support.....	77
Resetting the Stats Collector Database.....	77
Appendix.....	77
Updating the License.....	77
Checking for SSH Issues.....	78
Changing Nginx Ports.....	78
Disabling IPv6 Support in Shares.....	79
Shares API Permissions.....	79
Aspera Ecosystem Security Best Practices.....	80
Using the Health Check URL.....	94
Glossary.....	95

# Shares Admin Guide for Windows

## Introduction

IBM Aspera Shares is a web application that enables companies to share content in the form of files and directories of any size within their organization or with external customers and partners. Shares is powered by IBM Aspera High-Speed Transfer Server, which features the Aspera Node API, a daemon providing REST-enabled file operations and a transfer management API.

### Features

- Intuitive Shares web interface provides secure access to a consolidated, location independent view of all content to which a user is authorized.
- The administrator role has complete control over user, group, and directory service access to content and can define granular permission settings over all end-user operations such as browsing, uploading, downloading, making new directories, renaming or deleting files and directories
- Transfers initiated through the Shares web interface are managed by the Aspera Connect Plug-in – users do not need to have a native client application installed.
- Transfers are powered by Aspera's unique FASP protocol. Attachments are sent securely at high speed, regardless of file size, distance, or network.

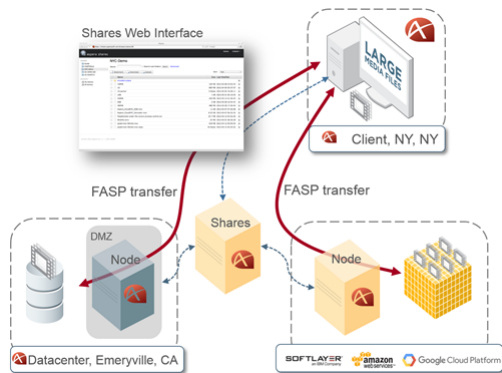
### Deployment

You can deploy Shares in the following ways:

- A single server solution that enables gathering or distributing content from a single content store and transfer node.



- A separate server that consolidates multiple content nodes – local, remote, or cloud-based file systems – into a single view and enables management of user access and file transfers across all nodes.



## Functionality

With Shares you can perform the following tasks:

- Use search, filtering, and sorting to find individual files or folders in content stores.
- Transfer single files, individual directories, or batches of files and directories of any size over any distance.
- Direct drag-and-drop transfers between shares to move files between globally dispersed nodes.
- Provide secure authenticated access with support for users, groups, and directory services.
- Manage access and visibility of nodes and directories.
- Manage user activities at the directory level.
- Set up a real-time activity feed that keeps track of user actions and operations such as creating, deleting, and renaming files and directories. Also keep track of all administration and management functions.
- Configure system logging levels.

## Installing Shares

---

### Installing Shares

#### Before You Begin...

Shares includes an Nginx web server listening on ports 80 and 443. For best results, Aspera recommends using a machine that does not run a web server. If you are using a web server, keep port 80 or 443 open, configure either that server or the Nginx server to use different ports. If you are installing an IBM Aspera High-Speed Transfer Server and Shares on the same host and configure a firewall, close all ports that are not required (see *IBM Aspera High-Speed Transfer Server: Configuring the Firewall*).

1. Review the system requirements section of the release notes.
2. Download the latest version of IBM Aspera Shares from <http://downloads.asperasoft.com/en/downloads/34>.
3. Verify that the **hosts** file has an entry for `127.0.0.1 localhost/`. You can find this file at `C:\WINDOWS\system32\drivers\etc\hosts`.

#### Install Shares

1. Run the Shares executable file and follow the onscreen instructions.

**Note:** On Windows 2008 with UAC (User Account Control) enabled, you must run the installer as an Administrator. To do so, right-click the executable file and click **Run as administrator**. You may be asked to enter the administrator's password to allow the installer to make changes to the computer.

2. Accept the license agreement.

3. Set up the Shares Administrator Account.

In the Shares Administrator Account Setup dialog, choose a name for a Shares administrator account and associate it with an existing email account:

4. Configure MySQL.

In the MySQL Setup dialog, enter the MySQL root account password. If this is a new installation, the root account for MySQL is automatically created and associated with the password you enter. Enter a name for the MySQL account that runs the Shares database.

5. Choose to generate new Diffie-Hellman parameters or use pre-generated parameters.

If you choose not to generate parameters now, you must generate new parameters at a later date to ensure the highest security standard for your Shares installation. For instructions on how to generate new parameters, see [“Generating New Diffie-Hellman Parameters”](#) on page 19.

6. Configure the Aspera Service Account.

In the **Aspera Service Account** dialog, enter the name of the user account to run Aspera services. By default, the user name is `svcAspera`. You may use a local or domain account, depending on your requirements:

- If the machine is not joined to a Windows domain, the Aspera Service account can be a local user, such as the default `svcAspera`. If the local account does not exist on the system, enter new credentials in the dialog and click **Next**. The Aspera Service account is created automatically. If the account already exists, enter the existing account password and click **Next**. You can use a domain account with local administrator privileges, but is not required.
- If the machine is configured to accept domain user login, use a domain account that has been added to the local administrator's group to run Aspera services. You must create this domain account on the domain controller before it can be configured as the Aspera Service Account.
- If you need to provision Active Directory accounts for users who want to transfer with your server are authenticated through Active Directory, use a domain account with local administrator privileges.
- If users who want to transfer with your server store their files and directories on a remote file system, such as an SMB file share, use a domain account with local administrator privileges. In some cases, additional actions are required to support this. For more information, see this [Aspera Knowledge Base article](#)

7. In the Choose Setup Type dialog, select **Typical**.

8. Complete the Shares installation.

In the Ready to Install dialog, you can click **Back** to change your installation settings, or **Install** to proceed with the installation. The installation process starts the MySQL service and the Aspera services.

9. If you forget to make a note of the administrator's password at installation time, you can reset it with a rake task.

The admin user account on the Shares server is used to configure Shares, including configuring users, security settings, and shares. Shares randomly generates a password that you can copy and paste to create the admin user, or you can create your own password.

```
> cd C:\shares\www
> rake aspera:admin NAME=username PASSWORD=password EMAIL=email_address
```

10. If Shares will be referenced as multiple IP addresses or hostnames (for example, as `localhost` or as `shares.example.com`), add those IP addresses or hostnames to the `AcceptedHosts` parameter in the Shares configuration file (`C:\Shares\www\config\shares.yml`).

The `AcceptedHosts` parameter lists the IP addresses or hostnames by which a user or client can reference the Shares server. Add multiple IP addresses and hostnames as a comma-separated list in the `AcceptedHosts` section in the `shares.yml` file. For example:

```
AcceptedHosts: [localhost, shares.example.com, 10.0.1.128] # 10.0.1.128 is the server IP address
```

## 11. Restart all Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to start and stop any of the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

Shares is now running and accessible from the IP address or domain name configured during installation. For more information about accessing Shares and logging in for the first time, see [“First Log In and Licensing”](#) on page 7.

## Upgrading Shares

**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.

**Note:** You can only upgrade to this release from an installation of 1.5 or higher.

1. Download IBM Aspera Shares.
2. Stop Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services**. Stop the following services:

- Aspera Nginx Services
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

### 3. Back up your system before performing an upgrade.

- a) Create a backup directory.

Run the following in a Command Prompt, where *C:\backups* is your backup directory:

```
> mkdir C:\backups
```

- b) Run the backup command.

```
> cd C:\shares\www
> bundle exec rake backup DIR=C:\backups
```

- c) Copy the files in *C:\backups* to the backup machine.
- d) Copy the following files to the backup machine:



- C:\shares\nginx\conf\cert.pem
  - C:\shares\nginx\conf\cert.key
  - C:\shares\www\config\database.yml
4. Install the new version of Shares by running the executable file and follow the onscreen instructions.
  5. If you are upgrading from a version of Shares prior to 1.9.6, choose to generate new Diffie-Hellman parameters or use pre-generated parameters..

If you choose not to generate parameters now, you must generate new parameters at a later date to ensure the highest security standard for your Shares installation. For instructions on how to generate new parameters, see [“Generating New Diffie-Hellman Parameters”](#) on page 19.

6. If the system is configured to serve Connect locally, point Shares to the new Connect SDK location.

**Note:** For more information on serving Connect locally, see [“Serving Connect from a Local Location”](#) on page 60.

To ensure the system continues to serve Connect locally after upgrade, go to the `_aspera_web_plugin_install.html.haml` file, located in the following location:

```
C:\Shares\www\app\views\node\shared\
```

Find the following line:

```
- connect_autoinstall_location = '//d3gcli72yxqn2z.cloudfront.net/connect/v4'
```

- To programmatically set the domain name of the server, change the line to the following:

```
- connect_autoinstall_location = "//#{ request.host_with_port }/connect/v4"
```

- To manually set the domain name of the server, change the line to the following, replacing `shares.example.com` with the Shares server domain.

```
- connect_autoinstall_location = '//shares.example.com/connect/v4'
```

Find the following line under function `loadConnectScript`:

```
var url = window.location.protocol + CONNECT_AUTOINSTALL_LOCATION + '/' + script +
'.min.js';
```

Replace it with the line below, deleting `.min`:

```
var url = window.location.protocol + CONNECT_AUTOINSTALL_LOCATION + '/' + script + '.js';
```

7. If Shares will be referenced as multiple IP addresses or hostnames (for example, as `localhost` or as `shares.example.com`), add those IP addresses or hostnames to the `AcceptedHosts` parameter in the Shares configuration file (`C:\Shares\www\config\shares.yml`).

The `AcceptedHosts` parameter lists the IP addresses or hostnames by which a user or client can reference the Shares server. Add multiple IP addresses and hostnames as a comma-separated list in the `AcceptedHosts` section in the `shares.yml` file. For example:

```
AcceptedHosts: [localhost, shares.example.com, 10.0.1.128] # 10.0.1.128 is the server IP
address
```

8. Restart all Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to start and stop any of the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

9. When upgrading from Shares 1.9.12, you must manually migrate the database.

**Important:** You must use the following workaround if your Shares server is running Shares 1.9.14.174845. The issues has already been fixed by the installer if your server is running a newer revision. You can find the revision number in the bottom-left of the footer in the Shares UI, or in the name of the Shares Windows installer.

The Stats Collector service installed with Shares 1.9.12 for Windows uses an improperly configured database schema (version 6). Shares 1.9.14 attempts to upgrade the schema to version 6, but cannot upgrade because the schema is already at version 6.

Follow the steps below to manually migrate the database.

- a) Open cmd . exe with the **Run as Administrator** option.
- b) Revert schema version to 5 using manual SQL statement:

```
> cd C:\Shares\www
> rails db -p
USE stats_collector;
UPDATE sc_version SET schema_version=5;
```

- c) Comment out the following line in the sc\_schema\_mig\_v5\_to\_v6.sql file located in the C:\Shares\statscollector\dbscripts\mysql folder:

```
ALTER TABLE `fasp_files` ADD COLUMN `bytes_processed` bigint;
```

For example:

```
/* ALTER TABLE `fasp_files` ADD COLUMN `bytes_processed` bigint; */
```

- d) Run the database migration command:

```
> C:\Shares\statscollector\bin\aspera-stats-collector.bat admin db-migrate
```

10. When upgrading from Shares 1.9.12, you must rename any SAML group that has special characters in its name.

Due to a security upgrade included in version 1.9.12 and later, Shares escapes special characters found in the SAML assertion, affecting SAML group IDs and names. Since the encoded version of the text does not match existing SAML group IDs or names, Shares creates new SAML groups. Shares escapes these special characters:

Special character	Encoded character
&	&amp;
<	&lt;
>	&gt;
"	&quot;
'	&#x27;
/	&#x2F;

Associate newly created groups with the existing SAML groups:

- a) If needed, remove any new group that was created with an escaped, special character in its name.
- b) Modify both the SAML IDs and names of existing SAML groups to use escaped, special characters.

Shares is now running and accessible from the IP address or domain name configured during installation.

**Note:** If after upgrading, Shares does not load in the browser, check to see if Nginx is running on the Shares machine. If Nginx is not running, and trying to restart the service manually results in the error

message below, follow the instructions in [“Disabling IPv6 Support in Shares”](#) on page 79 to disable Nginx from listening to IPv6 ports.

```
nginx: [emerg] socket() [::]:80 failed (97: Address family not supported by protocol)
```

## Securing an SSH Server

SSH servers listen for incoming connections on TCP port 22. Therefore, port 22 is subjected to unauthorized login attempts by hackers trying to access unsecured servers. To prevent unauthorized server access, you can turn off port 22 and run the service on a random port between 1024 and 65535.

The following task requires **Administrator** access privileges.

Aspera transfer products ship with OpenSSH listening on both TCP/22 and TCP/33001. Aspera recommends using TCP/33001 only and disabling TCP/22.

1. Use a text editor to open the SSH configuration file.

**Note:** Before changing the default port for SSH connection, verify with your network administrators that TCP/33001 is open. Notify users of the port change

2. Add the new SSH port

```
Port 22
Port 33001
```

**Note:** Before changing the default port for SSH connections, verify that TCP/33001 is open.

The OpenSSH suite included in the installer uses TCP/22 and TCP/33001 as the default ports for SSH connections. Aspera recommends disabling TCP/22 to prevent security breaches of your SSH server.

3. Disable TCP/22 by commenting it out in the `sshd_config` file.
4. In OpenSSH versions 4.4 and later, disable SSH tunneling to avoid potential attacks by adding the following lines at the end of the `sshd_config` file. As a result only *Administrator group* users are permitted to tunnel.

```
...
AllowTcpForwarding no
Match Group Administrators
AllowTcpForwarding yes
```

Depending on your `sshd_config` file, you may have additional instances of `AllowTCPForwarding` that are set to the default `Yes`. Review your `sshd_config` file for other instances and disable as appropriate.

5. Update authentication methods by adding or uncomment `PubkeyAuthentication yes` in the `sshd_config` file and comment out `PasswordAuthentication yes`.

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

6. Restart the SSH server to apply the new settings. Navigate to **Control Panel > Administrative Tools > Services**. Locate the OpenSSH Service and click **Restart**.

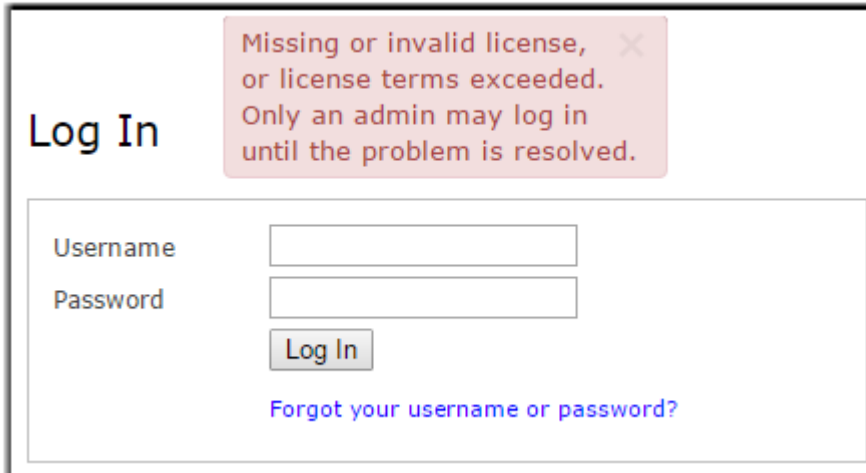
## First Log In and Licensing

**Important:** For purchasers of Aspera Enterprise, a license enabling Shares as part of Enterprise can be downloaded from [IBM Fix Central](#).

A Shares admin must log in and enter a valid license before other users can log into Shares. No other user interaction is permitted until a valid license is installed.

1. Open the Shares web application.

In a browser, go to `http://shares_ip_address`. The Shares login page appears with a warning related to the missing license file.



If Shares does not load in the browser, check to see if Nginx is running on the Shares machine. If Nginx is not running, and trying to restart the service manually results in the error message below, follow the instructions in [“Disabling IPv6 Support in Shares”](#) on page 79 to disable Nginx from listening to IPv6 ports.

```
nginx: [emerg] socket() [::]:80 failed (97: Address family not supported by protocol)
```

## 2. Log into Shares.

Log in using the Shares admin account username and password created during installation. If you don't remember your password, you can reset it by clicking **Forgot your username or password?** and following the on-screen instructions, or by running the following command on the Shares server:

```
> cd C:\Shares\www
> rake aspera:admin NAME=admin_username PASSWORD=password EMAIL=email_address
```

## 3. Enter your Shares license information.

Copy and paste the text from your license into the space in the license dialog. Click **Save**. If you need to update your license, see [“Updating the License”](#) on page 77.

After entering a valid license, Shares displays your Expiration Date and the Max Users and Max Nodes allowed by your license.

## Configuring Shares Web Server and Transfer Policies

After installing Shares for the first time, configure Shares to insert valid links in emails, and configure transfer policies for your use case.

### 1. Set the web server name to enable links in emails.

Setting	Description	Default
Host	Set the hostname or IP address of the server. The <b>Host</b> value is used in URLs generated in Shares notification emails.  For example, when an account is created for a user, Shares sends the user an email prompting the user to reset the password by clicking a URL. Shares uses the <b>Host</b> value to generate the URL.	example.com
Port	Set the HTTPS port on the server.	443
SSL/TLS	Enable or disable SSL/TLS.  For more information about SSL, see <a href="#">“Installing a Signed SSL Certificate Provided by Authorities”</a> on page 17.	Enabled

2. Set the transfer rates and transfer policies (**System Settings > Transfers**). If rates and policies are not set, Shares uses node defaults; if node defaults are not set, Shares uses **ascp** defaults.

Aspera recommends defining:

- a. **Upload target rate**
- b. **Starting policy**
- c. **Log policies**

For more information about transfer rates and transfer policy settings, see [“Configuring Transfer Settings”](#) on page 14.

## Uninstalling Shares

**Note:** If you wish to retain your data for future installations of IBM Aspera Shares, backup your system before performing an uninstall. See [“Backing Up Shares and the Database”](#) on page 74.

1. Stop Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services**, right-click the following services and select **Stop**:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

2. Uninstall Shares.

Go to **Start Menu > Control Panel > Programs and Features** or **Uninstall a program** (depending on your Control Panel view). Select Aspera Shares and click **Uninstall**.

## Configuring Shares Options

---

### Configuring the Web Server

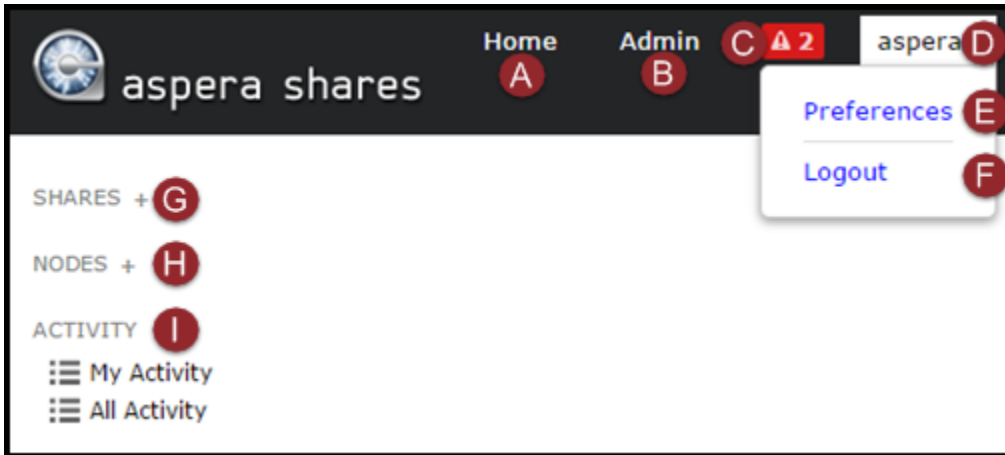
Configure the host, port, and SSL/TLS settings for Shares. Shares uses the host to create correct links in notification emails.

Enter the IP address of your Shares server in the Host field.

**Important:** If you are using a domain name, you must add that domain name to the `AcceptedHosts` parameter in the Shares configuration file (`C:\Shares\www\config\shares.yml`). For more information, see [“Allowing Connections from More Hosts”](#) on page 16.

### The Shares Home Page

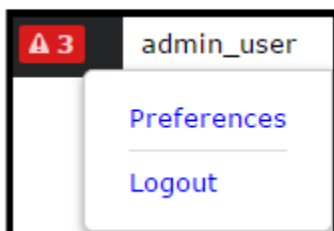
When you log into IBM Aspera Shares, you land on your Shares homepage.



Callout	Link	Action
A	Home	Goes to your Shares home page.
B	Admin	Goes to the admin page.
C	Errors and Warnings icon	Opens a pop-up window containing a summary of errors and warnings with links to individual errors and warnings as well as the <b>Errors and Warnings</b> page.
D	<i>username</i>	Opens a drop-down menu with links for <b>Preferences</b> and <b>Logout</b> .
E	Preferences	Goes to the <b>Preferences</b> page. For more information, see <a href="#">“Configure User Preferences”</a> on page 10.
F	Logout	Logs you out of Shares and goes to the Shares <b>Log In</b> window.
G	SHARES + <b>Note:</b> The + is visible only if you are authorized to create shares.	Your shares are listed below this heading. If you have authorization, click + to add a new share. For more information, see <a href="#">“Creating a Share”</a> on page 52. If Home Shares are enabled, your Home Share is listed above this heading. For more information, see <a href="#">“Managing Home Shares”</a> on page 12.
H	NODES +	Click + to add a new node. For more information, see <a href="#">“Adding Nodes”</a> on page 32. Once you have added nodes, they are listed below this heading.
I	ACTIVITY	Click <b>My Activity</b> to see and search your Shares activity. Click <b>All Activity</b> to see and search the activity of all users and all activities in nodes and shares.

## Configure User Preferences

To configure your user account settings, click your username in the top right corner of the browser window and click **Preferences**.



Click **Edit** next to the headers to change general settings such as your first and last name, your password, and your email address, as well as change your email notification options, configure your system display, and choose to suppress the Aspera Connect install dialog.

## Email Settings

**Note:** All notifications are enabled by default.

Setting	Description
Notify me when I am granted access to a new share	Receive an email whenever you are given access to a new share.
Notify me when a new transfer is completed to a share (and share notification is enabled)	Receive an email when new content has been added to your share. An admin must enable notifications for that share for you to receive an email.
Notify me when a user is authorized to a share	Receive an email whenever a user is given access to a share. <b>Note:</b> This option is available for admins only.
Notify me when a new user has requested an account	Receive an email whenever a new user requests an account when self-registration is enabled and set to <b>moderated</b> . <b>Note:</b> This option is available for admins only.

## Display

Setting	Description
Time Zone	The time zone for your system.
Date Order	The order that date, month, and year are displayed.
Date Delimiter	The punctuation used to separate the date, month, and year.
Time Format	Display a 12-hour time format or a 24-hour time format.
Number Delimiter	The punctuation used to denote the thousands place in a number. For example, if a comma ( , ) is chosen as the delimiter then one thousand is displayed as "1,000". <b>Note:</b> Number delimiter and separator cannot be the same.
Number Separator	The punctuation used to denote the decimal place in a number. For example, if a period ( . ) is chosen as the delimiter then ten and two-tenths is displayed as "10.2". <b>Note:</b> Number delimiter and separator cannot be the same.
Items Per Page	The number of items Shares will display per page. The default is 50.

## Connect Install Dialog

Each page of Shares checks for the presence of the Connect. If Connect is missing, Shares prompts you to download the plug-in. To suppress Shares from prompting users to install Connect on each page, set the value to **true**.

## Configuring System Settings

The following system configuration options are available under the **System Settings** menu on the **Admin** page.

Setting	Description
Background	Configure the frequency with which Shares monitors and updates the system. Also set the minimum allowable remaining space available on the Shares server, below which a warning notification is issued.
Home Shares	Enable or disable Home Shares. For more information on Home Shares, see <a href="#">“Managing Home Shares” on page 12</a> and <a href="#">“Enabling Home Shares” on page 12</a> .
License	View or change your Shares license. For more information on updating your license, see <a href="#">“Updating the License” on page 77</a> .
Localization	Configure your Shares server with your local timezone, date format, and time format. For more information on localization, see <a href="#">“Configuring the Shares Time Zone and Time Format” on page 13</a>
Logging	Configure the logging density. For more information on logging, see <a href="#">“Configuring Logging Settings” on page 13</a> .
Logos	Add, edit, or delete a custom logo for your Shares web application. Logo image files must be less than 500 kb. To make the new logo active, click <b>Select</b> . To delete a logo image file, click <b>Delete</b> .  <b>Note:</b> The logo's height must be equal to or greater than 58px.
Messages	Create messages that appear at the top of the log in page and the home page for all users.
Transfers	Configure settings for upload and download rates, transfer policies, and encryption. for more information on configuring transfers, see <a href="#">“Configuring Transfer Settings” on page 14</a> .
Web Server	Configure the web server settings, including the host, port, and whether SSL/TLS is enabled.

## Managing Home Shares

A Home Share is a private, empty share directory which is automatically created for new users when they first log into Shares (if Home Shares are enabled). Users can authorize other users to access their Home Share.

You can choose which node to use for Home Shares. A new directory is created on the node, and a share is added to the user's account. The user's username is used for both the directory and share name.

Home Shares are treated like regular shares by the application. Therefore, you can choose to authorize additional users to these shares or remove them individually after the initial creation.

When you log in, you can see all the Home Shares. For instructions on enabling Home Shares, see [“Enabling Home Shares” on page 12](#).

**Note:** If Home Share creation fails when a user first logs in, an error is logged to the activity log. The next time the user logs in, Shares tries to create the Home Share again.

## Enabling Home Shares

When Home Shares are enabled, Shares automatically creates and adds a private share directory for new users when they first log in to Shares. Home Shares are created for all new local users, directory users, and SAML users.

1. Go to **Admin > System Settings > Home Shares**.
2. To enable automatic creation of Home Shares, select **Enable Home Shares**.
3. From the **Node** drop-down list, select a node. You can also add a new node by clicking **New Node**. For details on how to add a node, see [“Adding Nodes” on page 32](#).



4. Select the default directory or click **Browse** to select a different directory for the Home Share.
5. Click **Save**.

## Disabling Home Shares

These instructions disable automatic Home Share creation for all new users. To disable a specific user's Home Share, see [“Disabling a User's Home Share” on page 40](#).

1. Go to **Admin > System Settings > Home Shares**.
2. Clear **Enable Home Shares**.
3. Click **Save**.

**Note:** When you disable home shares, Home Shares that already exist are not affected, and existing users can use their existing Home Shares. Home Shares for new users are no longer created.

## Changing the Home Shares Node

**Note:** When you modify the directory or node for Home Shares, existing Home Shares are not transferred. Only Home Shares of new users are created in the new destination.

1. Go to **Admin > System Settings > Home Shares**.
2. Select a different node from the **Node** drop-down list. You can also change to a new node by clicking **New Node**. For details on how to add a node, see [“Adding Nodes” on page 32](#).
3. Select the default directory or click **Browse** to select a different directory for the Home Share.
4. Click **Save**.

## Configuring the Shares Time Zone and Time Format

Localization settings allow you to set the time zone of the Shares server and configure date and time formats.

1. Click **Admin > System Settings > Localization**.
2. Configure the following settings.

Localization Setting	Description	Default
Time Zone	Set the time zone associated with the Shares server. All activity will be logged in the chosen time zone.	(GMT+00:00) UTC.
Us time zones priority	Select the box to show U.S. zones at the top of the Time Zone drop-down menu.	
Date order	Set the order of day, month, and year in the date.	YYYYMMDD
Date delimiter	Choose the date delimiter.	- (dash)
Time format	Set the time format.	24 Hour

3. Click **Save**.

Select the **Reset All Defaults** link to revert all changes.

## Configuring Logging Settings

Admins can configure the logging level in Shares based on the desired logging density and the tolerance for performance impacts under higher logging levels. Five logging levels are available: **debug**, **info**, **warn**, **error**, and **fatal**. Logging levels are set to **info** by default, which logs application events.

If you are troubleshooting Shares, you may want to increase the logging level to **debug**, which logs application events as well as more detailed information aimed at developers. Debug generates the most log entries, causing the logs to fill up and rotate faster, and incurs the greatest performance penalty. For

instructions on how to gather logs for support, see [“Gathering and Zipping All Logs for Support”](#) on page 77.

Errors and warnings are logged but may also be viewed in the Shares web application. For more information, see [“Errors and Warnings”](#) on page 63.

## Configuring Transfer Settings

To configure settings for upload and download rates, transfer policies, and encryption, click **System Settings > Transfers**.

Setting	Description
Min connect version	The minimum version of the Connect that can be used to transfer with Shares. The version must be in the form "X.Y.Z" for example, 0.0.0.
Upload target rate	Specify the target upload rate, such as 1.5 Gbps, 500Mbps, 10K, 3000. Once you click <b>Save</b> , the rate appears with standardized units. Leave the field blank to use the settings on the node.
Upload target rate cap	Specify a maximum upload rate. Leave the field blank to use the settings on the node. If a target rate cap is specified in Shares and on the node, the lesser of the two is used.
Download target rate	Specify the target download rate, such as 1.5 Gbps, 500Mbps, 10K, 3000. Once you click <b>Save</b> , the rate appears with standardized units. Leave the field blank to use the settings on the node.
Download target rate cap	Specify the maximum download rate to. Leave the field blank to use the settings on the node. If a target rate cap is specified in Shares and on the node, the lesser of the two is used.
Starting policy	Select the policy to be enforced when the transfer starts from the drop-down menu: <ul style="list-style-type: none"> <li>• <b>Fixed:</b> The transfer occurs at the target rate. This may impact the performance of other traffic present on the network.</li> <li>• <b>High:</b> The transfer uses available bandwidth up to the maximum rate.</li> <li>• <b>Fair:</b> The transfer attempts to run at the target rate. If the transfer is limited by network conditions, it occurs at a rate lower than the target rate, but not less than the minimum rate.</li> <li>• <b>Low:</b> 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 recedes.</li> </ul>
Allowed policy	Select which set of policies are available to the user during transfer. If you do not make a selection, settings are inherited from the node.
Encryption	Select <b>Optional</b> or <b>AES-128</b> . If you do not make a selection, settings are inherited from the node.
Encryption at rest	Select <b>Optional</b> or <b>Required</b> . Encryption at Rest (EAR) requires users, on upload, to enter a password to encrypt the files on the server. 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 Browser Plug-in.  If you do not make a selection, settings are inherited from the node.

## 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:

- 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 (the IBM Aspera HTTPD Service) 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. 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**.

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

Run the following commands:

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

```
$ /opt/aspera/bin/asuserdata -b -t
```

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

```
/opt/aspera/etc/aspera.confC:\Program Files\Aspera\etc\aspera.conf
```

2. After enabling HTTP fallback and setting a token encryption key, restart IBM Aspera Central, Aspera Node D, and the IBM Aspera HTTPD Service.

You can restart the Aspera Central from the Computer Management window. Go to **Control Panel > Administrative Tools > Computer Management > Services and Applications > Services**, click **Aspera Central**, and click **Restart**.

Go to **Control Panel > Administrative Tools > Computer Management > Services and Applications > Services**, click **Aspera NodeD**, and click **Restart**.

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

## Allowing Connections from More Hosts

To allow connections to the Shares UI beyond the server host IP address, you must add IP addresses and domain names to the `AcceptedHosts` parameter in the Shares configuration file (`C:\Shares\www\config\shares.yml`)

For example, if you want to access Shares from `localhost` and from `shares.example.com`, you need to add those to the `shares.yml` file:

```
AcceptedHosts: [localhost, shares.example.com, 10.0.1.128] # where 10.0.1.128 is the server host
```

## Securing Shares

### Configuring Shares Security

From the **Admin** page, configure Shares security by clicking **User Security** under the Security header.

Option	Description	Options
Session timeout	Log out users after this many minutes of inactivity.	1-480
Require strong passwords	Require passwords to be at least 8 characters and contain at least one uppercase letter, lowercase letter, number, and symbol.	
Password expiration interval	Number of days before a user must change the password. Leave the field blank to disable password expirations..	1-720
Failed login count	Number of failed logins within the Failed login interval before Shares locks the account .	1-20
Failed login interval	The interval in minutes within which hitting the Failed login count locks the account.	1-60
Self registration	Determines whether non-users can create or request user accounts. For more information on self-registered accounts, see <a href="#">“Moderate Self Registered Accounts”</a> on page 17.	<ul style="list-style-type: none"><li>• <b>None:</b> Not allowed.</li><li>• <b>Moderated:</b> An admin must approve the account before it is created. If you allow self-registration, the moderated setting is recommended for security.</li><li>• <b>Unmoderated:</b> After a user registers, the user’s account is automatically created.</li></ul>

### Removing Support for TLS 1.0 and 1.1

The default configuration of Shares has TLS 1.0, 1.1 and 1.2 enabled. Older browsers require the older and less secure version, TLS 1.0. You may disable support for these older browsers by removing TLS 1.0 from the configuration.

To remove TLS 1.0 from the configuration, edit the `nginx.conf` file located at `C:\Shares\nginx\conf\nginx.conf`. Delete `TLSv1` and `TLSv1.1` from the following line:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

## Configuring Manager Permissions

You can allow users with the Manager permission to manage every Shares user and group in Shares, not just users and groups that are part of the shares they manage.

Allow managers to manage every Shares user and group through the Shares UI, through the Shares API, or both:

- **Allow managers to administer users and groups through UI**
- **Allow managers to administer users and groups through API**

These options are disabled by default.

In a common use case, admins may decide that managers should administer users solely through the API and disable access to the Shares UI. For more information about users configured to use the API, see [“Shares API Permissions” on page 79](#).

For more information about managers and user roles in Shares, see [“Understanding User Roles and Share Authorization” on page 36](#) and [“Assigning Users the Manager Role” on page 40](#).

## Moderate Self Registered Accounts

Self registration allows users to request or create Shares user accounts. For more information on how to enable self registration, see [“Configuring System Settings” on page 11](#).

If self registration is enabled, the login page displays a **Request an Account** link that leads to a self registration form. When a user submits this form and self registration is moderated, **Self Registration** under the Accounts header on the **Admin** page turns red with the number of requests listed in parentheses and admins get an email notification.

By default, admins receive email notifications for new self registration request. Admins can configure whether they receive email notifications for new self registration request in their personal preferences (see [“Configure User Preferences” on page 10](#)). To change the global default setting, see [“Configure Email Settings” on page 21](#).

Click **Self Registration** to see the list of unprocessed requests. Select a user or all users in the list and click **Approve**, **Deny**, or **Delete**.

You can search accounts by their status by entering New, Approved, or Denied in the **Statuses** field.

## Installing a Signed SSL Certificate Provided by Authorities

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

1. Create a working directory

Go to **Start menu > All Programs > Accessories > Command Prompt** and create a new working directory:

```
> mkdir c:\ssl  
> cd c:\ssl
```

2. Copy **openssl.cnf** to your working directory.

Enter the following commands in your Command Prompt window:

OS Version	Commands
32-bit Windows	<pre>&gt; copy "c:\Program Files\Aspera\HSTS\etc\openssl.cnf" "c:\ssl\ &gt; cd c:\ssl</pre>
64-bit Windows	<pre>&gt; copy "c:\Program Files (x86)\Aspera\HSTS\etc\openssl.cnf" "c:\ssl\ &gt; cd c:\ssl</pre>

### 3. 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 -config "c:\ssl\openssl.cnf" -nodes -newkey rsa:2048 -keyout  
key_name.key -out csr_name.csr
```

**Note:** Windows does not, by default, have a C:\ssl\ directory. If the directory does not exist on your server, create the directory:

```
> mkdir c:\ssl  
> copy "C:\Program Files (x86)\Aspera\Enterprise Server\etc\openssl.cnf" "c:\ssl"
```

- 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.

### 4. 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.

5. Rename the certificate files provided with Shares.

Locate the original **cert.pem** and **cert.key** files in `C:\Shares\nginx\conf`. Rename them as follows:

- **cert.pem** to **cert.pem.orig**
- **cert.key** to **cert.key.orig**

You can also use the following commands in your command prompt window to rename the files:

```
# cd C:\Shares\nginx\conf
# move cert.pem cert.pem.orig
# move cert.key cert.key.orig
```

6. After receiving your signed certificate from your CA, if the CA requires a bundle or intermediate certificate, you need to concatenate the certificates for them to work with nginx. Bundle your intermediate certificate with your primary certificate.

```
> type your_domain_name.crt DigiCertCA.crt >> cert.pem
```

7. Copy your new SSL cert files to `C:\Shares\nginx\conf`. If the files are named differently, rename the cert file **cert.pem** and rename the key file **cert.key**.

8. Restart the web service.

Go to **Start > Administrative Tools > Services**. Right-click on the **nginx** service and select **Restart**.

## 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 Shares uses a generated, self-signed certificate as a placeholder until you can install a certificate signed by authorities.

You can find the installed certificate at: `C:\Program Files (x86)\Aspera\Enterprise Server\aspera_server_cert.pem`.

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
```

## Generating New Diffie-Hellman Parameters

Shares requires Diffie-Hellman parameters to enable SSL/TLS forward secrecy. If you chose to skip generating new Diffie-Hellman parameters when installing or upgrading Shares, you must generate new parameters to ensure the highest security standard on your Shares installation. Follow the instructions below to generate new parameters.

**Note:** Generating these parameters may take several minutes (more than 10 minutes on slow systems).

Run the following command:

```
> cd C:\Shares\nginx\objs\lib\openssl\openssl\bin
> openssl dhparam 2048 -out C:\Shares\nginx\conf\dhparam.pem
```

## Configuring Email

### Setting Up the SMTP Server

1. Select **Admin > SMTP** to configure the SMTP email server for Shares
2. To add a server's SMTP settings, select the **SMTP** option and complete the form, which requests the following information:

<b>Server</b>	SMTP server address
<b>Port</b>	SMTP port
<b>Domain</b>	Domain name
<b>Use TLS if available</b>	Aspera recommends turning TLS (Transport Layer Security) on to secure your email server.
<b>Timeout</b>	The timeout for connecting to SMTP servers. The default is 3 seconds.
<b>Username</b>	Email username
<b>Password</b>	Email password
<b>From</b>	The default sender email address and sender name that appear in email notifications when they receive an email notification.

3. To debug the SMTP server settings, click **Send Test Email**.

**Note:** If you get the error "Net::SMTPUnknownError: could not get 3xx (550)" when sending a test message, you might be blocked by your domain as a potential spammer. Aspera recommends that you set an SPF record for your domain to identify which mail servers are allowed to send email on behalf of your domain. For more information about SPF and how to create an SPF record, see <http://support.google.com/a/bin/answer.py?hl=en&answer=33786&topic=2759192&rd=1>

After you have configured the SMTP server, you can return to this page to view all Shares activity related to it in the **Activity** tab. Each reported activity event is accompanied by a tag. You can click the tag to find related activities.

You can also perform an activity event search by clicking **Search** and entering the requisite information.

### Updating Links in Email Notifications

IBM Aspera Shares generates links in email notifications using the hostname or IP address set in its **Web Server** settings. By default, it is set to example.com.

**Important:** If you change the hostname of the Shares machine, you must update the **Host** field with the new hostname or IP address.

1. Go to **Admin > System Settings > Web Server**.
2. Update **Host** with the IP address or hostname of the Shares machine.  
By default, the port is set to 443 and SSL/TLS is selected.



3. To save your changes, click **Save**.

## Configure Email Settings

Admins can set the default email notification settings for new IBM Aspera Shares users.

**Note:** Changing these preferences does not affect email settings for current users. Current users can update their own email settings. For more information see [“Configure User Preferences”](#) on page 10.

Go to **Admin > Email > Settings**. Select from the following options:

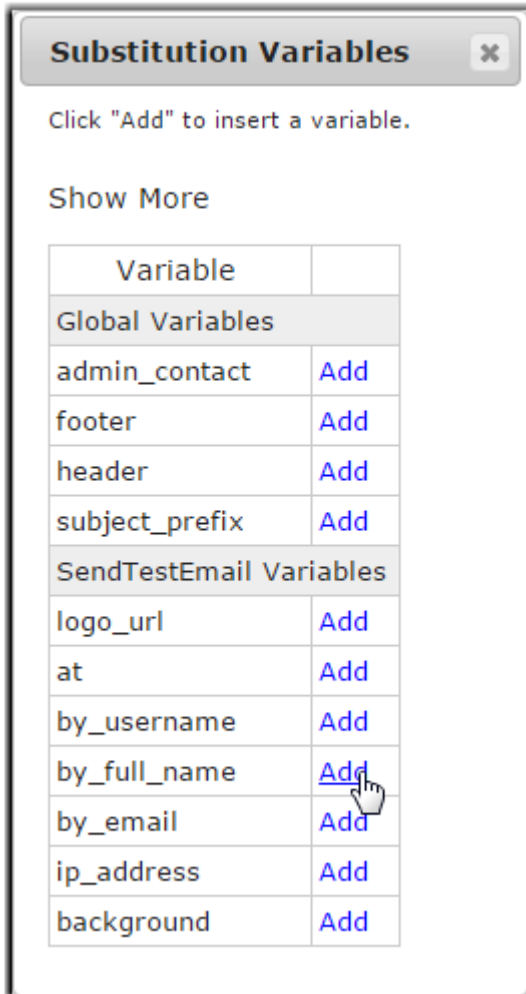
Option	Description
Notify users on share authorization.	Notify users when they are authorized to a new share.
Notify users on transfer complete.	Notify users when a new transfer is completed to a share (and share notification is enabled).
Notify admins on user share authorization.	Notify admins when a user is authorized to a share. <b>Note:</b> This option is available for admins only.
Notify admins on self registration request.	Notify admins when there is a new user self registration request and self registration is set to <b>moderated</b> . For more information, <a href="#">“Moderate Self Registered Accounts”</a> on page 17. <b>Note:</b> This option is available for admins only.

## Creating Email Templates

IBM Aspera Shares comes with preconfigured notification templates. The text of these templates can be customized to your specifications. Template substitution variables are useful for creating reusable boilerplate text that can be used across multiple email templates. To modify a template, create a new template by copying one of the preconfigured templates and editing it. You cannot modify or delete the preconfigured templates.

1. From the Admin page, click **Email > Templates**.
2. To view a template, click its name.  
To return to the list of templates, click your browser's back button or **Email > Templates**.
3. Click **Copy** to create a copy of the template you wish to modify.  
The copied template appears in the list with the name *template\_name 1* and is greyed out because it is not yet active.
4. Click the name of the new template to edit it.
5. To change the template name and subject line, click **Edit** next to **Details**.

The default subject line includes the Template Substitution Variable `{{subject_prefix}}`. To get more information about and use substitution variables, click **Template Substitution Variables** at the bottom of the page and click **Show More** in the pop-up window. (Make the pop-up window small again by clicking **Show Less**). To insert a substitution variable, put your cursor where you want the variable inserted in the text then click **Add** next to the variable in the Substitution Variables window.



To create new variables or modify existing ones, see [“Creating and Modifying Variables in Templates”](#) on page 23.

**Important:** You must click **Save** for your changes to be saved.

- To change the text of the email, click **Edit** next to **HTML Template** and **Plain Template**.

Email notifications always include the HTML and plain-text versions of the message. Aspera recommends editing the plain-text version first, then copying and pasting the edited text to the equivalent location in the HTML template. The editing interface for the two can be open simultaneously. You may add template substitution variables as described for editing template details.

**Important:** You must click **Save** under both editing boxes for your changes to be saved.

- Make the new template the default email notification.

Return to the **Templates** page and select **Active?** and **Default?**. When **Default?** is selected for the new template, it will automatically be cleared for the original template.

**Note:** To delete a modified template, select a different template for the default, clear **Active?**, then click **Delete**. Click **OK** in the pop up to confirm template deletion.

## Creating and Modifying Variables in Templates

Variables are useful for creating reusable boilerplate text that can be used across multiple email templates. You can create or modify variables for use in your IBM Aspera Shares notification templates. When editing a variable, you can configure both HTML and plain-text versions.

1. Click **Email > Variables** to open the **Notification Variables** page.

New Notification Variable					
Built In?	Name	Description	Plain Value	HTML Value	Actions
✓	admin_contact	Admin contact for your Shar...	your administrator		Edit
✓	footer	Boiler plate for the bottom...	This message and any attach...	<div style='font-size:small...	Edit
✓	header	Boiler plate for the top of...	This e-mail has been sent f...	<div style='font-size:small...	Edit
✓	subject_prefix	Prepended to email subject....	[Aspera Shares]		Edit

2. To modify a built-in Shares variable, click **Edit**.  
Edit the text and html then click **Update Notification Variable** to save your changes.
3. To create a new variable, click **New Notification Variable**.  
Edit the text and html then click **Create Notification Variable**. The new variable appears as a new entry in the **Notification Variables** list and is available in the **Substitution Variables** dialog for use in templates.

## Setting Up Transfer Nodes

### Configuring Transfer Servers for Use with Shares

#### What is a Node?

A *node* is a local, remote, or cloud server running an Aspera transfer server product (IBM Aspera High-Speed Transfer Server). Shares uses the Node API on the transfer server to configure the node and to perform transfers to and from the node.

#### Configuring a Node for Use with Shares

Nodes do not have to run on the same platform as the Shares server. To set up your machine to run as a node, follow the instructions pertinent to the platform of the workstation.

- **Windows:** [“Setting Up a Windows Node” on page 26](#)
- **Linux:** [“Setting Up a Linux Node” on page 24](#)

- **OS X:** [“Setting Up a macOS Node”](#) on page 29

## Setting Up a Linux Node

A *node* is a local, remote, or cloud server running an Aspera transfer server product (IBM Aspera High-Speed Transfer Server). Shares uses the Node API on the transfer server to configure the node and to perform transfers to and from the node.

**Note:** The following instructions require you to have administrative privileges.

1. Verify you have installed IBM Aspera High-Speed Transfer Server with a valid license on your transfer server. Shares requires that nodes use a Connect Server license.

Run the following command:

```
# ascp -A
```

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

2. Verify that the machine's **hosts** file has an entry for `127.0.0.1 localhost/`. You can find this file at `/etc/hosts`.
3. Disable SELinux.

SELinux must be set to "permissive" or "disabled", not "enforced". To check the status of SELinux, run the following:

```
# sestatus
```

If SELinux is set to "enforced", change the SELINUX value to disabled in the SELinux configuration file (`/etc/selinux/config`).

```
SELINUX=disabled
```

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

```
# setenforce 0
```

4. Create a system user account on the node.

Run the following command:

```
# useradd username
```

The examples in this topic use `xfer_user` as an example username.

The following steps use the **asconfigurator** utility to modify 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 Shares, 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,xfer_user;absolute,/project1"
```

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,token"
# asconfigurator -x
"set_user_data;user_name,username;authorization_transfer_out_value,token"
# 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,xfer_user;authorization_transfer_in_value,token"
# asconfigurator -x
"set_user_data;user_name,xfer_user;authorization_transfer_out_value,token"
# asconfigurator -x
"set_user_data;user_name,xfer_user;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. Verify persistent storage is enabled in `aspera.conf` for use with stats collector.

Run the following **asuserdata** command to verify that the `persistent_store` parameter is set to enable:

```
# /opt/aspera/bin/asuserdata -c
central server option set:
address: "127.0.0.1"
port: "40001"
backlog: "200"
schema_validation: "enable"
mgmt_backlog: "200"
mgmt_port: "0"
transfer_list_path: ""
persistent_store: "enable"
persistent_store_path: ""
persistent_store_max_age: "86400"
persistent_store_on_error: "ignore"
event_buffer_capacity: "1000"
event_buffer_overrun: "block"
compact_on_startup: "enable"
files_per_session: "1000000"
file_errors: "true"
ignore_empty_files: "true"
ignore_skipped_files: "true"
ignore_no_transfer_files: "true"
db_synchronous: "off"
db_journal: "wal"
```

If persistent storage is not enabled, run the following **asconfigurator** command to enable it:

```
$> asconfigurator -x "set_central_server_data;persistent_store,enable"
```

Restart the `asperacentral` service to update the node configuration:

```
service asperacentral restart
```

9. Set up a transfer user account with a Node API username and password.

Shares authenticates to the node machine using a Node API username and password. The following command creates a Node API user and password and associates it with the system user you created.

**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.

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

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

For example:

```
# /opt/aspera/bin/asnodeadmin -a -u node_user -p XF324cd28 -x xfer_user
```

**Note:** You need to escape special characters such as \$ to use them in a password. For example, to use XF324\$ as the password:

```
# /opt/aspera/bin/asnodeadmin -a -u node_user -x xfer -p XF324\$
```

- 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 **xfer\_user**, the result should be similar to the following example:

user	system/transfer user	acls
=====	=====	=====
node_user	xfer_user	

Adding, modifying, or deleting a node-user triggers automatic reloading of the user database and the node's configuration and license files.

## 10. Install the IBM Aspera Connect Browser Plug-In key.

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

```
# mkdir -p ~/.ssh
```

For example:

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

- b) Add the `aspera_id_rsa.pub` public key to the `authorized_keys` file by running the following command:

```
# cat /opt/aspera/var/aspera_tokenauth_id_rsa.pub.pub >> ~/.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 ~/.ssh
# chmod 600 /home/username/.ssh/authorized_keys
# chmod 700 /home/username
# chmod 700 /home/username/.ssh
```

The transfer node is now ready for connection to Shares.

For instructions on adding a node to Shares, see [“Adding Nodes”](#) on page 32.

## Setting Up a Windows Node

A *node* is a local, remote, or cloud server running an Aspera transfer server product (IBM Aspera High-Speed Transfer Server). Shares uses the Node API on the transfer server to configure the node and to perform transfers to and from the node.

**Note:** The following instructions require you to have administrative privileges.

1. Verify you have installed IBM Aspera High-Speed Transfer Server with a valid license on your transfer server. Shares requires that nodes use a Connect Server license.

Run the following command:

```
> ascp -A
```

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

When you install an Aspera transfer product, the installer automatically creates the Aspera service account (**svcAspera**, by default). Aspera recommends using this user as the transfer user. Otherwise, follow the instructions in the following step to create a new system account on the node.

The examples in this topic use **xfer\_user** as an example username.

2. Verify that the machine's **hosts** file has an entry for `127.0.0.1 localhost/`. You can find this file at `C:\WINDOWS\system32\drivers\etc\hosts`.
3. Create a new system account on the node.

Click **Control Panel > User Accounts** and add a new account. 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.

The following steps use the `asconfigurator` utility to modify the `aspera.conf` configuration file, located at:

```
C:\Program Files (x86)\Aspera\Enterprise Server\etc\aspera.conf
```

4. 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 Shares, 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,xfer_user;absolute,/project1"
```

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,token"  
> asconfigurator -x  
"set_user_data;user_name,username;authorization_transfer_out_value,token"  
> 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,xfer_user;authorization_transfer_in_value,token"  
> asconfigurator -x  
"set_user_data;user_name,xfer_user;authorization_transfer_out_value,token"  
> asconfigurator -x "set_user_data;user_name,xfer_user;token_encryption_key,encryption_key"
```

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. Verify persistent storage is enabled in `aspera.conf` for use with stats collector.

Run the following **asuserdata** command to verify that the `persistent_store` parameter is set to enable:

```
> asuserdata -c
central server option set:
address: "127.0.0.1"
port: "40001"
backlog: "200"
schema_validation: "enable"
mgmt_backlog: "200"
mgmt_port: "0"
transfer_list_path: ""
persistent_store: "enable"
persistent_store_path: ""
persistent_store_max_age: "86400"
persistent_store_on_error: "ignore"
event_buffer_capacity: "1000"
event_buffer_overrun: "block"
compact_on_startup: "enable"
files_per_session: "1000000"
file_errors: "true"
ignore_empty_files: "true"
ignore_skipped_files: "true"
ignore_no_transfer_files: "true"
db_synchronous: "off"
db_journal: "wal"
```

If persistent storage is not enabled, you must run the following `asconfigurator` command to enable it:

```
$> asconfigurator -x "set_central_server_data;persistent_store,enable"
```

Restart the Aspera Central service to update the node configuration:

Click **Start Menu > Control Panel > Administrative Tools > Services**. Right-click Aspera Central and select **Restart**.

8. Set up a transfer user account with a Node API username and password.

Shares authenticates to the node machine using a Node API username and password. The following command creates a Node API user and password and associates it with the system user you created.

**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.

- 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
```

```
> asnodeadmin -a -u node_user -p XF324cd28 -x xfer_user
```

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

```
> asnodeadmin -l
```

Given a node user named **node\_user** and a system user named **xfer\_user**, the result should be similar to the following example:

```
=====
      user          system/transfer user          acfs
=====
      node_user          xfer_user
```

Adding, modifying, or deleting a node-user triggers automatic reloading of the user database and the node's configuration and license files.

9. Install the IBM Aspera Connect Browser Plug-In key.

- 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\xfer_user"  
> 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.

10. Set up the transfer user account as a user in HSTS, if it is not already configured.

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

The transfer node is now ready for connection to Shares.

For instructions on adding a node to Shares, see [“Adding Nodes” on page 32](#).

## Setting Up a macOS Node

A *node* is a local, remote, or cloud server running an Aspera transfer server product (IBM Aspera High-Speed Transfer Server). Shares uses the Node API on the transfer server to configure the node and to perform transfers to and from the node.

**Note:** The following instructions require you to have administrative privileges.

1. Verify you have installed IBM Aspera High-Speed Transfer Server with a valid license on your transfer server. Shares requires that nodes use a Connect Server license.

Run the following command:

```
# ascp -A
```

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

2. Verify that the machine's **hosts** file has an entry for `127.0.0.1 localhost/`. You can find this file at `/etc/hosts`.
3. Create a 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) Select **Administrator** from the New Account drop-down menu.
  - e) Name the account.
  - f) Enter and verify a password for the account.
  - g) Click **Create User**.
  - h) Click **Login Options** in the users panel.
  - i) Click the **Join** button next to Network Account Server.
  - j) Click **Open Directory Utility**.
  - k) In the Directory Utility window, click the lock button and enter an administrator account and password to make changes.
  - l) From the menu bar, select **Edit # Enable Root User**.
  - m) Enter and verify the password.

n) Click **OK**.

The following examples use `xfer_user` as an example username.

The following steps use the `asconfigurator` utility to modify the `aspera.conf` configuration file, located at:

```
/Library/Aspera/etc/aspera.conf
```

#### 4. 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 Shares, 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,
```

For example:

```
# asconfigurator -x "set_user_data;user_name,xfer_user;absolute,/project1"
```

#### 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,token"
# asconfigurator -x
"set_user_data;user_name,username;authorization_transfer_out_value,token"
# 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,xfer_user;authorization_transfer_in_value,token"
# asconfigurator -x
"set_user_data;user_name,xfer_user;authorization_transfer_out_value,token"
# asconfigurator -x
"set_user_data;user_name,xfer_user;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. Verify persistent storage is enabled in `aspera.conf` for use with stats collector.

Run the following **asuserdata** command to verify that the `persistent_store` parameter is set to enable:

```
# /Library/Aspera/bin/asuserdata -c

central server option set:
address: "127.0.0.1"
port: "40001"
backlog: "200"
schema_validation: "enable"
mgmt_backlog: "200"
mgmt_port: "0"
transfer_list_path: ""
persistent_store: "enable"
persistent_store_path: ""
persistent_store_max_age: "86400"
persistent_store_on_error: "ignore"
event_buffer_capacity: "1000"
event_buffer_overrun: "block"
compact_on_startup: "enable"
files_per_session: "1000000"
file_errors: "true"
```

```
ignore_empty_files: "true"
ignore_skipped_files: "true"
ignore_no_transfer_files: "true"
db_synchronous: "off"
db_journal: "wal"
```

If persistent storage is not enabled, you must run the following `asconfigurator` command to enable it:

```
# asconfigurator -x "set_central_server_data;persistent_store,enable"
```

Restart the `asperacentral` service to update the node configuration:

```
# sudo launchctl stop com.aspera.asperacentral
# sudo launchctl start com.aspera.asperacentral
# sudo launchctl stop com.aspera.asperanoded
# sudo launchctl start com.aspera.asperanoded
```

## 8. Set up a transfer user account with a Node API username and password.

Shares authenticates to the node machine using a Node API username and password. The following command creates a Node API user and password and associates it with the system user you created.

**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.

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
```

```
# /Library/Aspera/bin/asnodeadmin -a -u node_user -p XF324cd28 -x xfer_user
```

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 **xfer\_user**, the result should be similar to the following example:

user	system/transfer user	acls
=====	=====	=====
node_user	xfer_user	

Adding, modifying, or deleting a node-user triggers automatic reloading of the user database and the node's configuration and license files.

## 9. Install the IBM Aspera Connect Browser Plug-In key.

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

```
# mkdir -p ~/.ssh
```

For example:

```
# mkdir -p ~/.ssh
```

b) Add the `aspera_id_rsa.pub` public key to the `authorized_keys` file by running the following command:

```
# cat /Library/Aspera/var/aspera_tokenauth_id_rsa.pub.pub >> ~/.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 ~/.ssh
# chmod 600 /home/username /.ssh/authorized_keys
# chmod 700 /home/username
# chmod 700 /home/username /.ssh
```

10. Set up the transfer user account as a user in HSTS, if it is not already configured.

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

The transfer node is now ready for connection to Shares.

For instructions on adding a node to Shares, see [“Adding Nodes” on page 32](#).

## Managing Nodes

---


### Adding Nodes

Transfer servers must be configured as nodes before they can be added to IBM Aspera Shares. For more information, see [“Configuring Transfer Servers for Use with Shares” on page 23](#). When adding a node, have the following information available:

- The node computer's hostname or IP address, the HTTPS port configured in its `aspera.conf` file, and path (if applicable, see below).
- The node API username and password that you created on the node machine.

**Important:** You must set up and configure a docroot for the transfer user on the node machine for Shares to successfully access the node.

**Note:** You can add one machine as a node multiple times to create nodes with different access credentials to different areas of the system defined by the node users' docroot settings.

1. From the Shares home page, click the  button next to **Nodes**.



2. Complete the **New Node** configuration form.

## New Node

Name

Host  :  /

API Username

API Password

HTTP Fallback Port   
*HTTP fallback port override*

Use SSL   
*Encrypt this connection*

Verify SSL Certificate   
*Cryptographically ensure the host is trusted*

Timeout   
*Number of seconds to wait for requests*

Open timeout   
*Number of seconds to wait for the connection to open*

Bytes free - warn   
*For example '10G', '50 MB', '3 terabytes'*

Percent free - warn

Bytes free - error   
*For example '10G', '50 MB', '3 terabytes'*

Percent free - error

Field	Description
Name	A description of the node.
Host	<p><b>Hostname or IP address:</b> The node's hostname or IP address. For remote nodes, use the IP address or resolvable host name. For a local host (Shares and Enterprise Server are installed on the same machine), the hostname is <b>localhost</b>.</p> <p><b>Note:</b> When adding a local node multiple times, you must ensure each node uses <b>localhost</b> as the host.</p> <p><b>Port:</b> The node's HTTPS port (as configured in <code>aspera.conf</code>). The port field represents the port on which the node service is running. The default is 9092.</p>

Field	Description
	<b>Path:</b> The path field is an advanced feature used for URL Proxy operations. In nearly all cases, you may leave this field blank.
API Username	The node API username associated with the transfer user on the node machine.
API Password	The node API password associated with the transfer user on the node machine.
Use SSL	<p><b>Note:</b> Aspera strongly encourages enabling SSL, if you do are not connecting through SSL, connect using port 9091. The node must accept HTTP connections on port 9091. On the node, run:</p> <pre>asconfigurator -x "set_server_data;enable_http,true" asconfigurator -x "set_server_data;http_port,9091"</pre> <p>Nodes may use an Aspera pre-installed and self-signed certificate (/opt/aspera/etc/aspera_server_cert.pem), or your own certificate. To generate a new certificate, see <i>IBM Aspera Enterprise Server Admin Guide: Installing SSL Certificates</i>.</p> <p><b>Note:</b> After generating a new certificate, you must create a cert.pem file that contains the private key and the certificate. To do so, copy and paste the entire body of the key and cert files into a single text file. Then save the file as <i>filename_cert.pem</i>.</p>
Verify SSL Certificate	<p>To verify the SSL certificate, select this checkbox.</p> <p>If the node's SSL certificate is not recognized by the Certificate Authority (CA), Shares displays the following error message at the top of the page when you try to add the node: "Status: Not pingable. Internal error. (Error-35)".</p> <p>If the node is using the default self-signed SSL certificate provided by Aspera, the certificate is not recognized by any CA. You must clear the <b>Verify SSL Certificate</b> option.</p>
Timeout	Sets the number of seconds Shares will wait for this node to respond to a request.
Open Timeout	Sets the number of seconds Shares will wait for the connection to this node to open.
Bytes free - warn	Issues a warning message when the node has equal to or less than a specified number of storage bytes free. You can enter the number as G, MB, terrabytes, and bytes.
Percent free - warn	Issues a warning message when the node has equal to or less than a specified percent of its storage free.
Bytes free - error	Issues an error message when the node has equal to or less than a specified number of storage bytes free. You can input the number as G, MB, terrabytes, and bytes.
Percent free - error	Issues an error message when the node has equal to or less than a specified percent of its storage free.

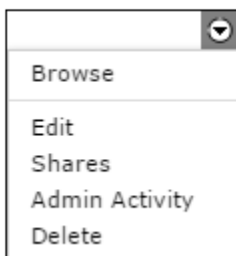
3. Click **Create Node** to create the node.

After the node is created, Shares redirects you to the node **Detail** page. A status message at the top of the page reads, "Stats collector issue. Node disabled. Configuration changes have not had time to propagate to the stats collector or node configuration incorrect." This is normal and indicates that the Shares server database has not yet been updated.

The node now appears on your Home page under **Nodes**

## Modifying Nodes

To modify a Shares node, go to **Home** and select **Edit** from the drop-down menu under NODES.



Action	Description
Browse	For more details, see <a href="#">“Browsing Nodes”</a> on page 35.
Edit	<p>Opens the node's <b>Detail</b> view.</p> <p>Check the node's status by clicking <b>Test</b>. If the node is functioning properly, a message below the node name will read "Status: OK. (Last checked X seconds ago.)"</p> <p>Change the values set during configuration in the fields and click <b>Update Node</b> to save your changes. For more details, see <a href="#">“Adding Nodes”</a> on page 32.</p> <p>To delete the node, click <b>Delete</b>.</p>
Shares	This is also accessible as a tab in the node's <b>Detail</b> view. View the name and directory of the node's shares. To edit a share, click <b>Edit</b> to go to the share's detail page appears. For more details, see <a href="#">“Creating a Share”</a> on page 52 and <a href="#">“Modifying a Share”</a> on page 55.
Admin Activity	This is also accessible in the <b>Activity</b> tab in the node's <b>Detail</b> view. View a list of all administrative activity that has occurred on the node. Click <b>Search</b> to search for activity based on tagged events or a date range.
Delete	Deletes the node from Shares.

## Browsing Nodes

You can browse a node by clicking **Browse** in the node's dropdown menu or by clicking the name of the node on the home page. This opens a page that displays all directories and files on that node.

Search for a directory name by entering a word or phrase in the **Name** field and clicking **Search**. Click **Advanced** to limit the search by size or date modified. For more information, see [“Searching Nodes and Shares”](#) on page 36.

The following buttons enable you to perform actions on a directory or directories.

Action	Description
Bookmark	Create a shortcut to the selected directory. If you do not select any directory, the bookmark is the node's root directory. Bookmarks appear in a list above the Shares list on your home page.
Download	Download the selected directory or directories using the Connect. For more information, see <a href="#">“Transferring Files”</a> on page 57.
Upload	Upload a file or folder from another machine to this node using the IBM Aspera Connect Browser Plug-In. For more information, see <a href="#">“Transferring Files”</a> on page 57.
Delete	Delete the selected directory or directories.
New Folder	Create a new directory on the node.

Action	Description
Rename	Rename a directory on the node.
Create Share	Create a share for the selected directory. You can only select one directory at a time. Click <b>Create Share</b> to open the <b>New Share</b> dialog. This dialog is pre-populated with the node and directory information. To complete the other fields, see “Adding Nodes” on page 32.
Sort	Sort the directories of a node by: <ul style="list-style-type: none"> <li>• Type</li> <li>• Size</li> <li>• Size Descending</li> <li>• Last Modified</li> <li>• Last Modified Descending</li> </ul>

## Searching Nodes and Shares

To search a share or node, select a share or node on your **Home** page. In the **Name** box, enter a keyword for your search. IBM Aspera Shares appends any keyword that you enter with \*, such that if you enter the keyword **Dec**, the search actually performs as **\*Dec\*** and Shares return any string that contains this word. To include sub-directories in the search, select **Search sub-folders**.

To limit the search results by size or date last modified, use **Advanced** search. For size values, include the unit of measure as bytes, MB, or GB. Select a date from the pop-up calendar.

## Managing User Accounts

### Understanding User Roles and Share Authorization

#### Overview:

User roles in Shares determine a user's permissions to access and perform actions on a share. There are three user roles for an account authorized to access a share: administrators, managers, and regular users. Admins have full permissions to view, modify, and remove all existing shares and users. Managers have permissions to view, modify, remove shares for which they have authorization to manage. Users have permissions depending on the authorizations given them by admins and managers. User, group, and directory service accounts must be authorized to access a share. If authorized, a user can perform the following actions on a share:

- Browse
- Upload
- Download
- Make directory
- Delete directory or file



- Rename

**Note:** If you do not have browse permissions but have all other permissions, you can still perform **Upload File** and **Upload Folder** operations in the user interface, though the contents of the share are not displayed.

## Authorization Precedence

- Authorizations can be granted to users, groups, and directory services.
- Authorization at the user level takes precedence over the user's group or directory service authorizations.
- In the absence of user level authorization, a user is granted the union of all authorizations for the groups and directory services to which the user belongs.

## Administrators

Users with the admin permission are authorized to create new shares and users, as well as to modify or remove any or all shares and users.

- Nodes are only visible to administrators.
- All administrators are authorized to create, edit, and delete any or all nodes and shares.
- Only administrators can create, edit, and delete top-level shares.

## Managers

Administrators can use the manager permission to delegate the creation of shares and users to another user without giving that account full administration privileges. Like administrators, managers can view, edit, and remove share authorizations but only for shares that they manage. Assigning a user to a share as its manager gives that user administrative privileges for that share and all inherited subdirectories. If a user creates a new share within a managed share, the manager of the share has administrative rights to the new share. For instructions on how to authorize manager permissions, see [“Assigning Users the Manager Role”](#) on page 40.

Though a user with manager permissions effectively becomes the admin for that share, the following restrictions apply:

- A manager cannot modify or delete the top-level share or any shares above it.
- A manager cannot create a share at the same level of the first share.
- For a manager to administer a group, the manager must have manager permissions for all of that group's shares.
- Managers cannot edit Admin user properties, but they can edit other managers in **Admin > Users**.
- A manager cannot authorize new users or groups for shares the manager does not manage.
- For a manager to change the password or email of a user, the manager must be a manager of all the shares that user is authorized to access.

## Users

Regular users can access any shares for which they have authorizations to access, but the actions they are allowed to take are set and managed by any user with administrative privileges for that share.

## Adding Local Users

Administrators can create local IBM Aspera Shares user accounts that are added to the local Shares database. For directory service users, see [“Importing Directory Service Users”](#) on page 43.

1. From the **Admin** page, click **Accounts > Users** and click **New**.
2. Enter the user's account information.

3. Set the user password. You can do so in one of two ways:

- Select **Send login link in welcome email** to send a login link through a welcome email that prompts the user to set a password.
- Select **Set password** to set a temporary password on the user's behalf. Enter the following information:

Option/Field	Description
Send welcome email	Send the new user an email with the new account's username and password.
Prompt to change password on first login	Force the new user to change the account password on first login.
Password / Password confirmation	Enter and confirm the user's password.

4. Click **Create User**.

After creating a user, Shares redirects you to the user's **Security** settings. From this page, you can also access the user's groups, shares, and transfer settings, the user's preferences, and the user's activity logs. For more information, see [“Configure User Settings” on page 38](#).

**Note:** A new user may only log in if the number of users active in the last hour is less than the max number of users allowed by your license.

## Configure User Settings

You can access a user's settings and activity logs by clicking **Edit** for the user you wish to configure. View a list of users by clicking **Accounts > Users** from the **Admin** page.

Tab	Description
Detail	Update the local user's name, username, and email address, or delete the local user from Shares.
Member of	<p>Add the user to a local group by selecting one from the drop-down list. Only local groups that have been added to Shares appear on this list.</p> <p>After adding a local user to a local group, click <b>Edit</b> to modify the group's settings or click <b>Remove</b> to delete the user from the group.</p> <p>Clicking <b>Edit</b> takes you to local group's configuration page. For details on modifying a local group's settings, see <a href="#">“Adding Local Groups” on page 41</a>.</p> <p><b>Note:</b> You cannot add local users to a directory service group, only to local groups. For instructions on configuring directory service users, see <a href="#">“Importing Directory Service Users” on page 43</a>.</p>
Security	<p>You can configure the following security settings:</p> <ul style="list-style-type: none"> <li>• Send the user a password reset link.</li> <li>• Disable the user's account. A disabled user cannot log into Aspera Shares even if the user belongs to a group that has group access permissions.</li> <li>• Allow the user to log into Shares.</li> <li>• Make the user an administrator.</li> <li>• Allow the user to log into the API. Users who do not have Browse permissions can log into the API and perform transfer and file operations through SSH. For more information, see <a href="#">“Shares API Permissions” on page 79</a>.</li> <li>• Set an account expiration date.</li> <li>• Set a temporary password.</li> </ul>

Tab	Description
Shares	<p>Displays all shares for which the user has authorization. For more information on authorizations, see <a href="#">“Authorizing Users to a Share”</a> on page 57. If this user belongs to a local group and the group has access to a share, that share is listed here because permission to access the share is inherited from the group. To edit these permissions or disallow the local user's access to a share, click <b>Edit</b>.</p> <p>To authorize new shares for the local user, click <b>Add Share</b>. A list of shares appears. Click <b>Authorize</b> to authorize a share.</p> <p>Select permissions that the local user has for the share. After modifying the settings, click <b>Update</b>. You may disallow access to a share by clicking <b>Delete</b>.</p> <p><b>Note:</b> Regular users are not automatically notified when given access to a share unless they have enabled it. For instructions on enabling these email notifications, see <a href="#">“Configure User Preferences”</a> on page 10.</p>
Preferences	Select a timezone and enter any comments.
Transfer Setting	The user's default transfer settings are those of the node where the share is located. To override these defaults, click <b>Override these settings</b> and configure the transfer settings. For more information, see <a href="#">“Configuring Transfer Settings”</a> on page 14.
Activity	View and search for Shares activities by this user.

## Unlocking User Accounts and Changing Passwords

If a user enters an incorrect password too many times, the user account is locked until the admin unlocks it and either resets the password for the user or sends a password reset link to the user.

1. Go to **Admin > Users**.
2. To unlock an account, click **Edit** for the locked user account.  
Click **Unlock** next to the username.
3. To reset the user account password, go to **Security**.  
The admin can either send a password reset link, or set a new password.
  - To send a password reset link, click **Send password reset link**.
  - To set a new password, select **Set password**. Enter the new password in the password fields. Select **Prompt to change password on next login** to require the user to update their password from the one assigned by the admin.

## Disabling and Deleting User Accounts

IBM Aspera Shares allows you to disable or delete user accounts.

Disabling an account removes all log in and transfer privileges, including logging into the API, but retains the account and its configuration settings. To reinstate access to the user, you can enable the account without adding them to Shares again.

Deleting an account removes all log in and transfer privileges, as well as the account and its configuration settings. To reinstate access to the user, you must add them again as a new user.

### Disabling a User Account

1. From the **Admin** page, click **Accounts > Users**
2. Click **Edit** next to the account you want to disable.
3. On the **Security** tab, select **Disabled**.
4. Click **Update Permissions** to save your change.

5. To restore a disabled user account, clear **Disabled** in the account security settings.

## Deleting a User Account

1. From the **Admin** page, click **Accounts > Users**.
2. Click **Edit** next to the account you want to delete.
3. On the **Detail** tab, click **Delete**.
4. Click **OK** in the pop-up window to confirm account deletion.

## Setting a User Account Expiration Date

If you want a user to have access to IBM Aspera Shares for a limited time, you can set an expiration date for the user account.

1. From the **Admin** page, click **Accounts > Users**  
The list of user accounts includes a column **Expiry Date** in which user account expiration dates are listed.
2. Click **Edit** next to the account for which you want to set an expiration date.
3. On the **Security** tab, click the box next to **Account expires on**.  
Click the desired expiration date in the pop-up calendar.
4. Click **Update Permissions** to save your change.  
If the user attempts to log in after the account expiration date, they receive an error message indicating that the account has expired.
5. To restore an expired user account, set a new expiration date or leave the field blank.

## Assigning Users the Manager Role

For more information on manager permissions, see [“Understanding User Roles and Share Authorization” on page 36](#).

1. Use the drop-down menu to the right of the share and click **Authorizations**.
2. Click **Authorize User**, **Authorize Group**, or **Authorize Directory**.
3. Search for the name of the user, group, or directory service you want to authorize. Click **Add**.
4. On the **Authorizations** page, select **manage** to enable management of the share.

The user, group, or directory service is now authorized to create and modify shares and users within the managed share.

## Disabling a User's Home Share

These instructions describe how to disable a specific user's Home Share. To disable automatic Home Share creation for all new users, see [“Disabling Home Shares” on page 13](#).

1. From the **Admin** page, click **Accounts > Users**.
2. Click **Edit** for the user.
3. Click the **Home Share** tab and select **Home Share disabled**.

## Searching Accounts

1. On the **Admin** page, click **Accounts > Groups** or **Accounts > Users**, depending on what account type you want to search for.
2. Click **Search** at the top of the page.
3. Enter at least two characters for your search query. You can search by username, first name, or last name.

### User Search

Search term must be at least two characters

**Note:** Shares does not support searching by full name. For example, if you are searching for a user "jd\_user1" with first name "John" and last name "Doe", searching "John" or "Doe" would both return "jd\_user1", but searching "John Doe" would not return the user.

## Managing Group Accounts

---

### Adding Local Groups

Administrators can create IBM Aspera Shares local groups, in which all users who belong to the group have the same Shares authorizations and belong to the local database, rather than to a directory service.

1. From the **Admin** page, click **Accounts > Groups > New**.
2. Name the new local group and click **Create Group**.
3. Optional: Select **Login** to enable all users in the group to log in to Shares and click **Update Permissions**.
4. Select **Admin** to authorize all users in the group as admins and click **Update Permissions**.

After creating a group, you are redirected to the group's **Security** settings. From this page, you can add users to the group, authorize shares, configure transfer settings, and view the group's activity logs. For more information, see [“Configure Local Group Settings”](#) on page 41.

### Configure Local Group Settings

You can access a group's settings and activity logs by clicking **Edit** for the group you wish to configure. You can view a list of groups by clicking **Accounts > Groups** from the **Admin** page.

Tab	Description
Detail	Update the group's name or delete the local group from Shares.
Members	<p>Add members to the group by selecting users from the drop-down list and clicking <b>Add</b>. You will only see local users who have been added to Aspera Shares.</p> <p><b>Note:</b> You cannot add directory service users to a local group. For more information on directory service groups, see <a href="#">“Importing Directory Service Groups”</a> on page 43..</p> <p>Manage existing users by clicking <b>Edit</b> to modify users' settings, or clicking <b>Remove</b> to delete them from the group.</p> <p>When you click <b>Edit</b>, the individual user's configuration page appears. See <a href="#">“Adding Local Users”</a> on page 37 for details on modifying a local user's settings.</p>
Security	<p>Configure group-specific security settings for all members.</p> <ul style="list-style-type: none"> <li>• Select <b>Login</b> to authorize all group members to log into Shares. If left clear, you may give individual users access to log in.</li> <li>• Select <b>Admin</b> to authorize all users with administrative permissions. If left clear, you may give individual users administrative access.</li> </ul> <p>To configure users' security settings from their individual account pages, see <a href="#">“Adding Local Users”</a> on page 37 for details.</p>

Tab	Description
Shares	<p>Click <b>Add Share</b> to authorize group access to specific shares. A list of nodes and shares that are currently configured in Shares appears. Click <b>Authorize</b> to authorize a share.</p> <p>Set the group's permissions for browsing, transferring, and performing file operations within the share. The default permission is browse. To edit these permissions or disallow the group's access to the share, click <b>edit</b>.</p> <p>Select permissions that group members have for the authorized share. Click <b>Update</b>. You can disallow access to this share by clicking <b>Delete</b>.</p>
Transfer Setting	<p>To override the default transfer settings for this group, click <b>Override these settings</b>. For more information, see <a href="#">“Configuring Transfer Settings” on page 14</a>.</p> <p>Click <b>Save</b> to keep the new settings or <b>Cancel</b> cancel setting changes. You may also click <b>Use Inherited Settings</b> to return to the application-wide transfer configuration.</p>
Activity	View and search for Shares activities by this group.

## Configuring the Directory Service

### Adding a Directory Service (DS)

IBM Aspera Shares supports the Lightweight Directory Access Protocol (LDAP) and can be configured to connect to a directory service. The following directory service databases are supported:

- Active Directory (AD)
- Apple Open Directory
- Fedora Directory Server
- Open LDAP

To add a directory service account:

1. From the **Admin** page, click **Accounts > Directories** and click **New**.
2. Complete the form.

Option	Description
Directory Type	<p>Select a directory service type from one of the following options:</p> <ul style="list-style-type: none"> <li>• Active Directory (AD)</li> <li>• Apple Open Directory</li> <li>• Fedora Directory Server</li> <li>• Open LDAP</li> </ul>
Name	Enter a name for this directory service.
Description	Enter a description for this directory service.
Host	<p>Enter the directory's IP address or hostname, and then enter the port number.</p> <p>By default, LDAP secured by simple TLS uses port 636, unsecured LDAP uses port 389, unsecured global catalog uses port 3268, and global catalog over SSL uses port 3269.</p>
Base DN	The search treebase, for example, <b>dc=myCompany,dc=com</b> for myCompany.com.

Option	Description
Authentication Credentials	<ul style="list-style-type: none"> <li>• Anonymous Bind</li> <li>• Simple Bind</li> </ul> <p>If Simple Bind is selected, you must type your directory service username and your directory service password. Your directory service name is typically your distinguished name or domain username.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• Distinguished name: CN=Administrator,CN=Users,DC=myCompany,DC=com</li> <li>• Domain username: DEV_Administrator_</li> </ul>
Encryption	<ul style="list-style-type: none"> <li>• Unencrypted (Default port 389)</li> <li>• Simple TLS (Default port 636)</li> </ul> <p><b>Note:</b> Aspera recommends using Simple TLS to secure your server. By default, LDAP traffic is transmitted unsecured but can be made confidential and secure by enabling TLS.</p>

3. Click **Create Ldap config**.

## Importing Directory Service Users

1. Find your directory service (DS) user. From the **Admin** page, you can search for your DS group from the **Accounts** page or from the **Directories** page:

- **Search by name:** Click **Accounts > Users > Search**. Type the username or at least two characters of the user name and click **Search**. A list of users that match the characters appears.
- **Select from a list:** Click **Directories** then click **Edit** for the corresponding directory. Go to the **Users** tab.

If the number of records exceeds the limit for displaying a list in Shares, Shares displays the following message: "This directory has too many users to show all at once." Enter a minimum of two characters in the search box to search for your user by name.

2. Click **Edit** to import the user and edit the user's profile.

For details on how to edit a user's profile, see ["Configure DS Users and Groups"](#) on page 44.

**Note:** A new user may only log in if the number of users active in the last hour is less than the max number of users allowed by your license.

## Importing Directory Service Groups

1. Find your directory service (DS) group.

From the **Admin** page, you can search for your DS group from the **Accounts** page or from the **Directories** page:

- **Search by name:** Click **Accounts > Groups > Search**. Type the group name or at least two characters of the group name and click **Search**. A list of groups that match the characters appears.
- **Select from a list:** Click **Directories**. Click **Edit** for the corresponding directory and click the **Groups** tabs.

**Note:** If the number of records exceeds the limit for displaying a list in Shares, Shares displays the following message: "This directory has too many groups to show all at once." Enter a minimum of two characters in the search box to search for your group by name.

2. Click **Edit** for the corresponding group to import the group and edit the group's profile. For details on how to edit a group's profile, see ["Configure DS Users and Groups"](#) on page 44.

## Configure DS Users and Groups

You can access and edit the settings and activity logs of directory service users and groups by selecting **Accounts > Users** or **Accounts > Groups** from the **Admin** page and clicking **Edit**.

Tab	Description
Detail	View the user or group name, modify the directory, or delete the user or group from Shares.
Member of	Displays all groups to which the DS user or group belongs. If the number of groups exceeds 100, a search facility is opened.  A group's <b>Edit</b> link takes you to a DS group's configuration page. For details on modifying DS group settings, see <a href="#">“Importing Directory Service Groups”</a> on page 43.
Members (groups only)	Displays the group's DS members and enables you to <b>edit</b> corresponding DS user settings. For details on editing DS user settings, see <a href="#">“Importing Directory Service Users”</a> on page 43.
Security	For users and groups: <ul style="list-style-type: none"> <li>• Allow the user or all users in the group to log into Shares.</li> <li>• Authorize the user or all users in the group with Administrator permissions.</li> </ul> For users: <ul style="list-style-type: none"> <li>• Disable the user's account. The user is unable to log into Shares even if the user belongs to a group or directory that has access permissions.</li> <li>• Allow the user to log into the API. Users who do not have Browse permissions, can still log into the API and perform transfer and file operations.</li> <li>• Set an account expiration date.</li> </ul>
Shares	Displays all shares for which the user or group has authorization. For more information on authorizations, see <a href="#">“Authorizing Users to a Share”</a> on page 57. If a user belongs to a DS group, and the group has access to a share, that share is listed because permission to access the share is inherited from the group. The same is true if the entire directory has access to this share. To edit these permissions or disallow the user or group access to a share, click <b>Edit</b> .  To authorize new shares for the DS user or group, click <b>Add Share</b> . A list of shares appears. Click <b>Authorize</b> to authorize a share.  Select permissions that the DS user or group has for the share. The default permission is browse. If browse is not selected, the DS user or group members are only able to access functions if they have been made API users. To edit these permissions or disallow the DS user or group access to the share, click <b>Edit</b> .  After modifying the settings, click <b>Update</b> . You may disallow access to this share by clicking <b>Delete</b> .
Preferences (users only)	Select a timezone and add any comments.
Transfer Settings	The user's default transfer settings are those of the node where the share is located. To override these defaults, click <b>Override these settings</b> and configure the transfer settings. For more information, see <a href="#">“Configuring Transfer Settings”</a> on page 14.
Activity	View and search for Shares activities by a specific user.



### SAML and Shares

Shares 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 Shares as a SAML *online service provider (SP)* that contacts a separate online *identity provider (IdP)* to authenticate users. Authenticated users can then use Shares to access secure content.

With SAML enabled, Shares 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 Shares, which grants the user access to Shares. When a SAML user logs in to Shares for the first time, Shares 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 Shares. For more information about user provisioning for SAML users, see [“User Accounts Provisioned by Just-In-Time \(JIT\) Provisioning”](#) on page 45.

### IdP Requirements

To use SAML with Shares, 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 Shares uses.
- Not configured to use pseudonyms.
- Can return assertions to Shares 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 Shares, make sure you configure your IdP to send a correct SAML response to Shares. For more information, see [“Configuring Your Identity Provider \(IdP\)”](#) on page 46.

For instructions on configuring SAML, see [“Configuring SAML for Shares”](#) on page 49.

**Note:** Shares users with SAML accounts are affected by Shares session timeouts configured on the User Security page (**Admin > Security > User Security**). After session timeout, SAML users are redirected to the local login page. To log in again, click **Log in using SAML Identity Provider**.

### SAML and Directory Services

Shares supports the use of both SAML and directory services. If you configure both services to Shares, ensure the services use different Active Directory domains. Aspera advises against configuring LDAP directly to Shares if the SAML IdP acts as a frontend for the same Active Directory domain.

### Bypassing the Default SAML IdP

Shares 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
```

### User Accounts Provisioned by Just-In-Time (JIT) Provisioning

When a SAML user logs in to IBM Aspera Shares for the first time, Shares 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 Shares, Shares 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 49.

## 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 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.

## Configuring Your Identity Provider (IdP)

### IdP Requirements

To use SAML with Shares, 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 Shares uses.
- Not configured to use pseudonyms.
- Can return assertions to Shares 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 Shares:

Tag	Format
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Entity ID	https://shares_ip/auth/saml/metadata/
Binding	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
Callback URL	https://shares_ip/auth/saml/callback

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 Shares configuration by going to `https://server_ip/auth/saml/metadata` and saving the XML as an XML file.

### SAML Assertion Requirements

Shares expects assertion from an IdP to contain these elements:

Default Attribute	Shares 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	
member_of	SAML group	Necessary for SAML groups

**Tip:** All attributes other than NameID or SAML\_SUBJECT can also use the urn:oasis:names:tc:SAML:2.0:attrname-format:basic format.

## SAML Assertion Example

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response Destination="https://aspera.ibm-sample.com/auth/saml/callback"
ID="_866852166a98ae2a855514761b870e64" InResponseTo="_6bba436a-54a6-4e4f-b109-97a6c6bd0349"
IssueInstant="2021-09-15T21:48:51.268Z" Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://shib-idp-01.dev.aspera.us/idp/
shibboleth</saml2:Issuer>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </saml2p:Status>
  <saml2:Assertion ID="a7d332169ef7ad5fd2967234ced2d736"
IssueInstant="2021-09-15T21:48:51.268Z" Version="2.0"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://shib-
idp-01.dev.aspera.us/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#_a7d332169ef7ad5fd2967234ced2d736">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            <ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-
exc-c14n#" />
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>2LMPPDFUKaQxIFK9JSoj3iMPWF0</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>a6ItMgcnDsqi8j8MMX2uaVMSoYGM2tbePomyFDn82a1HkucZLTHlGQSiXn1+36bCb11WbucZ9WYAt
Hw2hve8dBLMJj3s9SmVtFAoZl80HB4ZwuTHH730ykvXTmGL01MNkId1ry9uRW+1TIT9BqLHa0q1Ep/
SBLMJ+Ljzp8iT+9mi3DPBhP4uV8YPy/BYPQLdONPv9UBDz1FetBGov9BenaFwrbo5Y/NY0gEJ1+Mgj+98V/
gkJyotRTMDcX7tyIu2qXSSpIi5DiAv0/
UtKZtAm96SKWFqsCdyd662SUTSekPcXt9obXfvw76eV2vUf9nLebD3IvpIRXPZ7NFgjsjKA==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>MIIDUDCCAjgAwIBAgIVANKYV01LBB6MuViBihCDECq8XoAxMA0GCSqGSIb3DQEBBQUAMCQxIjAg
BgNVBAMTGXNoaW50eWwvLTAxLmRldi5hc3B1cmEudXMwHhcNMjMxMjMjIz0DAZWhcNMzMTA2
MjIz0DAZwJkMSIwIAYDVQQDExlzaG1lLWlkC0wMS5kZXZyYXNwZXJhLnVzMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAKk7e5vrtJpcmeQtbNQXlgbTgpeWkhhx+8t4zpeh4UbQr8sXh
so9gtDQjVhasWmfGPA0+Mlp112eXVvT8uQQMBh2Ce7qSx1axL4ZsJw+mPfuRf6xIZDk5sVNfY801
SxXbeVvPSGXN61TPV7/0/dd4s+IMieG6NfidfpFbYa4F2QaJD28ergf3KELzHkrBwti55NH8Np49
rk5Iq0fk56YR1KuETHI2pS3vvVIOJmWih0v0rsNxHu006oohFmLM5k+yHQqur1Lk0mV9GFZnwFQC
lwPcLkVJ6gTv8k4hUkIOfhWUVOENCleyyDc9acnMXCnM424ew4QnKE1H8u8x06DcwIDAQBo3kw
dzBWBgnVHREETzBNghlzaG1lLWlkC0wMS5kZXZyYXNwZXJhLnVzMIIBIjANBgkqhkiG9w0BAQ
wvLTAxLmRldi5hc3B1cmEudXMvaWRwL3NoaWJib2xldGgwHQYDVR00BBYEFPPzQ25rft0Wk+9WvL+Wl
+W+knKH2MA0GCSqGSIb3DQEBBQUAA4IBAQAHCICuAlKaLW1g1DVtp8YuYB3FZqbN0Y3ekt/OUXIU
uGwXDYhR8FDumXhGIgDUaP1QHd3MnZRIvougy7fS/Qyg8V/C8ALa5g7K/2sTOi/RtMjRQZK+v010
oxneqotk4BPGp3an+m1pdnxjJvphL4kX/ZPuCcvkyzoDnelv/c+dE/+Yz6Izml1j/drxRL8etPc
jPgGjIF4TDGTNDHle0yLP3yN2ANPqEpF/Y8W0Vhejrkux2YKwH6SQVKdSgodD6EVsUs13F1atvb
BRRwBwGg21FBnVR101r3LOjH0vtFK/Hms3V3L9jE7ucR+qdbWnDPEmVwBY2aHr0EQU/NscQ1/<
ds:X509Certificate>
```

```

    </ds:X509Data>
  </ds:KeyInfo>
</ds:Signature>
<saml2:Subject>
  <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://shib-idp-01.dev.aspera.us/idp/shibboleth" SPNameQualifier="https://
aspera.ibm-sample.com/auth/saml/metadata">asperauser1</saml2:NameID>
  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml2:SubjectConfirmationData Address="10.41.48.51" InResponseTo="_6bba436a-54a6-4e4f-
b109-97a6c6bd0349" NotOnOrAfter="2021-09-15T21:53:51.268Z" Recipient="https://aspera.ibm-
sample.com/auth/saml/callback"/></saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2021-09-15T21:48:51.268Z"
NotOnOrAfter="2021-09-15T21:53:51.268Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>https://aspera.ibm-sample.com/auth/saml/metadata</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2021-09-15T21:47:24.365Z"
SessionIndex="_4589689d46dd27161ff17e37c686db04"><saml2:SubjectLocality Address="10.41.48.51"/
><saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport</
saml2:AuthnContextClassRef></saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute FriendlyName="office" Name="office"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Emeryville</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="sn" Name="surname"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">user</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="company_name" Name="company_name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">Aspera SAML</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="email" Name="email"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">aspera-sample-user@ibm.com</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="entryDN" Name="id"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">CN=aspera-sample-user,OU=IBMASpera,OU=Users,OU=IBM,DC=aspera,DC=ibm-
sample,DC=com</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="givenName" Name="given_name"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">aspera</saml2:AttributeValue>
    </saml2:Attribute>
    <saml2:Attribute FriendlyName="memberOf" Name="member_of"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml2:AttributeValue xmlns:xsi="[*http://www.w3.org/2001/XMLSchema-instance*]"
xsi:type="xs:string">CN=SAML,OU=IBMASpera,OU=Users,OU=IBM,DC=aspera,DC=ibm-sample,DC=com</
saml2:AttributeValue>
      <saml2:AttributeValue xmlns:xsi="[*http://www.w3.org/2001/XMLSchema-instance*]"
xsi:type="xs:string">CN=SAML_group,OU=IBMASpera,OU=Users,OU=IBM,DC=aspera,DC=ibm-sample,DC=com</
saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
</saml2p:Response>

```

When passing in multiple attribute values (for example, `member_of`), make sure the SAML assertion follows this pattern pulled from the example above:

```

<saml2:Attribute FriendlyName="memberOf" Name="member_of"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue xmlns:xsi="[*http://www.w3.org/2001/XMLSchema-
instance*]" xsi:type="xs:string">CN=SAML,OU=IBMASpera,OU=Users,OU=IBM,DC=aspera,DC=ibm-
sample,DC=com</saml2:AttributeValue>
  <saml2:AttributeValue xmlns:xsi="[*http://www.w3.org/2001/XMLSchema-
instance*]" xsi:type="xs:string">CN=SAML_group,OU=IBMASpera,OU=Users,OU=IBM,DC=aspera,DC=ibm-

```

```
sample,DC=com</saml2:AttributeValue>
</saml2:Attribute>
```

## Configuring SAML for Shares

Before configuring SAML in Shares, make sure you have properly configured your SAML IdP (see “Configuring Your Identity Provider (IdP)” on page 46).

1. In IBM Aspera Shares, go to **Admin > Accounts > Directories**. Click **Edit** for the SAML Identity Provider.
2. For the SAML IdP entry, click **Edit**.
3. To enable SAML, select the check box Log in using the SAML Identity Provider.
4. Optional: Enable SAML login redirection.

If enabled, entering the default Shares URL will direct users to the SAML login page. If disabled, the Shares URL directs users to the local login page.

### Log In

The screenshot shows a login interface with two main sections. The top section is titled "Local" and contains a "Username" input field, a "Password" input field, a "Log In" button, and a link that says "Forgot your username or password?". The bottom section is titled "SAML" and contains a link that says "Log in using SAML Identity Provider".

5. Enter the SAML entry-point address provided by the IdP in the IdP Single Sign-On URL text box.
6. Enter the Identity Provider Certificate Fingerprint.
7. Enter the Identity Provider Certificate.
8. Click **Save**.

Your SAML configuration is now enabled for Shares. You can further configure security settings by going to the **Security** tab where you can restrict users from logging in through this configuration. If you allow users to log in, you can enable the **Restrict Login** feature so that only SAML users already imported from SAML can log into Shares.

## Creating SAML Groups

SAML groups are created in IBM Aspera Shares one of two ways:

- Creating a SAML group in Shares using the application and then logging in as a SAML user in the new group. The Shares 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 Shares using the web application.

1. When SAML is enabled, you can create SAML groups by navigating to **Admin > Groups**.
2. Click **New SAML Group** to create a SAML group.
3. Enter the group name, which is the distinguished name (DN).

4. Click **Create Group** to create the SAML group.

You can view and manage your SAML group in the **Groups** section under **Admin**.

## Customizing SAML Attribute Mapping

You can customize how Shares maps SAML attributes to Shares user fields.

There are two types of profile fields:

- **Default fields:** All SAML responses must provide these fields. You can edit the SAML name, but not the Shares field name.
- **Local fields:** You can map additional SAML fields to Shares users.

When there are enabled custom profile fields, a SAML user's details page shows values of those custom profile fields in the Custom Attributes tab.

To edit custom fields:

1. Add new SAML fields in your SAML identity provider. These fields must be correctly mapped to the SAML directory service.
2. Go to **Admin > Directories** and click **Edit** for SAML Identity Provider.
3. Go to the **Attribute Mapping** tab.
4. Click **Add Custom Profile Field** to add a new field:

Configuration Option	Description
Name	Enter the name of the field added to a Shares user.
SAML Name	Enter the name of the SAML field found in your IdP.  <b>Important:</b> The Shares <b>SAML Name</b> must be correctly mapped to your SAML fields in IdP. If the names are incorrectly mapped and the field is required, Shares rejects the user login.
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.

5. Click **Update user profile fields**.

## Importing a SAML User to Shares

You can pre-populate the SAML user record and set permissions for a user before the user logs in to Shares. You can import the user in one of two ways:

- Import the SAML user in the Shares UI
- Import the SAML user using a rake task

For more information about using a rake task, see [“Configuring Users With Rake Tasks” on page 65](#).

**Note:** You must first configure and enable SAML for Shares before you can create a SAML user. For more information, see [“Configuring SAML for Shares” on page 49.](#)

The instructions below describe how to import a SAML user in the Shares UI.

1. Go to **Admin > Users** and select **Import SAML User**.
2. Enter a value for each of the following fields for the SAML user.

Field	Description	Example
ID	The SAML user's full Distinguished Name (required)	<b>CN=saml doe,OU=AK,OU=Users,OU=Asperasoft,DC=dev,DC=aspera,DC=us</b>
Given_name	First name	<b>Sam</b>
Surname	Last name	<b>Doe</b>
Name ID	Username (required)	<b>saml_doe</b>
Email	Email address	<b>saml_doe@shares.example.com</b>

3. Click **Import User**.

For information about configuring the newly created user, see [“Configure User Settings” on page 38.](#)

## Configuring Signed SAML Authentication Requests

Signed SAML authenticate requests must be configured in the `saml.yml` configuration file. Make sure you have a valid SSL certificate and key to sign requests.

1. Edit the `saml.yml.sample` configuration file (`C:\Shares\www\config\saml.yml.sample`).
2. Under the `production` section, set `EnableSignedAuthnRequests` to `true` and add in your SSL certificate and SSL private key:

```
EnableSignedAuthnRequests: true
AuthnDigestMethod: XMLSecurity::Document::SHA1
AuthnSignatureMethod: XMLSecurity::Document::RSA_SHA256
AuthnCertificate: >
-----BEGIN CERTIFICATE-----
shares_ssl_certificate
-----END CERTIFICATE-----
AuthnPrivateKey: >
-----BEGIN RSA PRIVATE KEY-----
shares_ssl_private_key
-----END RSA PRIVATE KEY-----
```

For example:

```
EnableSignedAuthnRequests: true
AuthnDigestMethod: XMLSecurity::Document::SHA1
AuthnSignatureMethod: XMLSecurity::Document::RSA_SHA256
AuthnCertificate: >
-----BEGIN CERTIFICATE-----
MIICKzCCAZSgAwIBAgIBAZANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGEwJVUzER
MA8GA1UEChMlTmV0c2NhcGUxFTATBgNVBAsTDGF1c2NhcGUxFTATBgNVBAsTDGF1
c2NhcGUxFTATBgNVBAYTA1VTRREwDwYDVQQK
Ewh0ZXRzY2FwZTENMA5GA1UECxEUHVic2EXMBUGA1UEAxM0U3VWcm15YSB0aGV0
dHkwZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiPGfjX3uRjGEjmKiqG
7SdATYazBcAbu1AVyd7chRkiQ31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7L
iQZBcrXpc0k4du+2Q6xJu2MPm/8WKuM0nTuvzpo+SGXe1mHVChEqooCwfdiZywyZ
NMmrJgaoMa2MS6pUkfQVAgMBAAGjNjA0MBEGCWCWSAGG+EIBAQQEAwIAgDAfBgNV
HSMGDAWgBTy8gZzkBhHUfWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAA0BgQBT
I6/z07Z635DfzX4XbAFpjlR1/AYwQzTSYx8GfCNAqCqCwaSDKvsuj/vwbf9lo3j3
UkdGYpcd2cYRCgKi4MwqdWyltphuAH18hHZ5uvi00mJYw8W2wU0sY0RC/a/IDy84
hw3WwehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd1A==
-----END CERTIFICATE-----
AuthnPrivateKey: >
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCVqGpH2S7F0CbEmQBgmBiDi00GxhVw1G+yY/60BQoPKcx4Jv2h
vLz7i54ngjaIqnqRNP71jKjFLp5zhnAu9GsdwXbgLPtimMSB+MVFHTJvKjQ+eY9p
dWA3NbQusM9uf8dAim+3VrZxNHQbVGX0IAPNHT008cZHMSqIDQ60vLma7wIDAQAB
AoGAbxKPzsnh826JV2A253svdnAibeSWBPg17kBIrR8QWDCtkH9fvqpVmHa+6p05
5bShQyQSCkxa9f2jnBoiKK4+0K412TBM/SG6Zjw+DsZd6VuoZ7P027msTWQrMBxg
Hjgs7FSFtj76HQ00ZxFeZ8BkIYq0w+7VQYAPBWEPSqCRQAECQQDv09M4PyRVWSQM
S8Rmf/jBwmRnY1gPPE0ZD0iSWJqIBZUBznv0P00QSH6B+vee/q5edQA20IaDgNmN
AurEtUaRAKEAn7/65w+Tewr89m0M0RKMPFpwnfGyAj3kT1mFEYDq+iNwdcSE6xE
2H0w3YEbDsSayxc36efFnmr//41jt4iJfwJAa1p0eicJhIracAaaa6dtG1/0Ab0e
f3NibugwUxIGWkz1XmGnWbI3yyYo0ta0cR9fvjhXV9QFomfTBcdf40FgQJAH3MG
DBMO77w8DK2QfWBvbGN4NFTGYwWg52D1Bay68E7590PYVTMm4o/S30ib0Q53gt/x
TAUq7IMYHtCHZwxkNQJBA0RwE+6qVIv/ZSP2tHLYf8DG0hEBJtQcVjE7PfuJAbH5
lr++9qUfv0S13gXj5weio5dzgEXwWdX2YSL/asz5DhU=
-----END RSA PRIVATE KEY-----
```

3. Rename `saml.yml.sample` to `saml.yml`.
4. Restart Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to start and stop Shares services:


- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

## Managing a Share

---

### Creating a Share

You can create a share by using one of the following methods:

- On your **Home** page, click the  button next to the SHARES header.
- Browse a Node, Share, or Bookmark and select the directory to share, then click **Create Share**.
- Browse a Node, Share, or Bookmark, click the drop-down menu associated with the directory you want to share, and click **Share**.

Each of these goes to the **New Share** page.

**Note:** If you want to create a new share from a location on a specific share (for example, from an existing folder on a share), see [“Creating a Share from a Folder” on page 54](#).

1. Configure your new share.



## New Share

Name

Node  ▼

Directory

Bytes free - warn   
*For example '10G', '50 MB', '3 terabytes'*

Percent free - warn

Bytes free - error   
*For example '10G', '50 MB', '3 terabytes'*

Percent free - error

Field	Description
Name	The name of the share is only a description, which means that multiple shares can have the same name.
Node	Select a node from the drop-down list of all available nodes.  If you are creating this share by clicking <b>Create a share</b> for a directory selected while browsing a node or share, this field is automatically populated with the node containing the selected directory.
Directory	If you are creating this share from a directory selected while browsing a node or share, this field is automatically populated with the directory.  If you are creating a share using the SHARES <input type="button" value="+"/> button, click <b>Browse</b> to browse directories on the node. Select the directory that you want to share, then click <b>Select</b> .  <b>Note:</b> For Windows nodes, folders with names that do not follow the proper Windows folder naming convention do not open in the Shares web UI. For details on Windows folder naming conventions, see <a href="http://msdn.microsoft.com">http://msdn.microsoft.com</a> .
Bytes free - warn	Shares issues a warning message when the share has equal to or less than the specified number of bytes free. You can enter the number as G, MB, terrabytes, and bytes.
Percent free - warn	Shares issues a warning message when the share has equal to or less than the specified percent of its storage free.
Bytes free - error	Shares issues an error message when the share has equal to or less than the specified number of storage bytes free. You can enter the number as G, MB, terrabytes, and bytes.
Percent free - error	Shares issues an error message when the share has equal to or less than the specified percent of its storage free.

2. Click **Create Share** to save your entries.

The share appears under the **Shares** section on your **Home** page.

**Tip:** Only the first 100 shares are shown in the left sidebar. Clicking **See all** displays all shares. When you select a share that is not one of the first 100 shares, it appears under a new section in the left sidebar called "CURRENT SHARE".

To give a user permission to access a share, see [“Authorizing Users to a Share”](#) on page 57.

## Creating a Share from a Folder

When browsing a share, you can create a new share from a folder in the share.

1. Select the folder from which to create a share and click **Create Share**.

If you would like to create a share from a folder that does not exist, create a new folder with the **New Folder** button and select that folder.

2. Configure your new share.

**Note:** The **Name**, **Node**, and **Directory** fields are pre-populated with the name and location of the selected folder.

**New Share**

Name:

Node:  ▼

Directory:


Bytes free - warn:   
*For example '10G', '50 MB', '3 terabytes'*

Percent free - warn:

Bytes free - error:   
*For example '10G', '50 MB', '3 terabytes'*

Percent free - error:

Field	Description
Name	The name of the share is only a description, which means that multiple shares can have the same name.
Node	Select a node from the drop-down list of all available nodes. If you are creating this share by clicking <b>Create a share</b> for a directory selected while browsing a node or share, this field is automatically populated with the node containing the selected directory.
Directory	If you are creating this share from a directory selected while browsing a node or share, this field is automatically populated with the directory.

Field	Description
	<p>If you are creating a share using the SHARES  button, click <b>Browse</b> to browse directories on the node. Select the directory that you want to share, then click <b>Select</b>.</p> <p><b>Note:</b> For Windows nodes, folders with names that do not follow the proper Windows folder naming convention do not open in the Shares web UI. For details on Windows folder naming conventions, see <a href="http://msdn.microsoft.com">http://msdn.microsoft.com</a>.</p>
Bytes free - warn	Shares issues a warning message when the share has equal to or less than the specified number of bytes free. You can enter the number as G, MB, terrabytes, and bytes.
Percent free - warn	Shares issues a warning message when the share has equal to or less than the specified percent of its storage free.
Bytes free - error	Shares issues an error message when the share has equal to or less than the specified number of storage bytes free. You can enter the number as G, MB, terrabytes, and bytes.
Percent free - error	Shares issues an error message when the share has equal to or less than the specified percent of its storage free.

3. Click **Create Share** to save your entries.

The share appears under the **Shares** section on your **Home** page.

**Tip:** Only the first 100 shares are shown in the left sidebar. Clicking **See all** displays all shares. When you select a share that is not one of the first 100 shares, it appears under a new section in the left sidebar called "CURRENT SHARE".

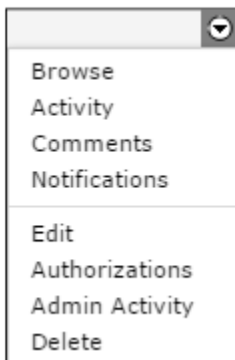
To give a user permission to access a share, see [“Authorizing Users to a Share”](#) on page 57.

## Modifying a Share

Shares are listed under the **SHARES** section of the Home page.

**Tip:** Only the first 100 shares are shown in the left sidebar. Clicking **See all** displays all shares. When you select a share that is not one of the first 100 shares, it appears under a new section in the left sidebar called "CURRENT SHARE".

Use the drop-down menu to the right of the share name to do the following on a share:



Action	Description
Browse	Explore directories and files within a share. For details, see <a href="#">“Browsing a Share”</a> on page 56.
Activity	A list of all activity that has occurred on the selected share appears. You can also search for activity based on tagged events or a date range.

Action	Description
Comments	A list of any comments that have been made about the share appears. You can also add your own comments.
Notifications	Set your preference for receiving notifications when new content has been added to your share.
Edit (Detail tab)	Open the share Detail view.  Check the status by clicking <b>Test</b> . If the share is functioning properly, a message below the share name reads, "Status: OK. (Last checked X seconds ago.)"  Change the values (set during configuration) in the fields and click <b>Update Share</b> to save your changes. For more details on the settings, see <a href="#">“Creating a Share” on page 52</a> .  To delete the share, click <b>Delete</b> .
Authorizations	Set authorization for browsing, file transfer, file operations, and notifications related to the share for existing users, groups, and directories. For more information on authorizations, see <a href="#">“Authorizing Users to a Share” on page 57</a>
Admin Activity	A list of all admin activity that has occurred on the share. You may also search for activity based on tagged events or a date range.
Delete	Deletes the share.

## Browsing a Share

When you browse a share, all files and directories within that share are displayed.

**Note:** Shares excludes files that match the `._*` pattern to hide MacOS extended attributes on file systems without native support for those attributes. File systems without native support prepend `._` to MacOS attribute names.

The search bar enables you to search for specific files or directories (for more information, see [“Searching Nodes and Shares” on page 36](#)). When you select a file or directory in the share, you can click one of the buttons (for example, Bookmark) to act on the share. **Total Count** displays the total number of entries (files and directories) in the current share.

The buttons perform the following functions:

Button	Function
Bookmark	Create a shortcut to the selected directory. If you do not select any directory, the bookmark is the node's root directory.
Download	Download the selected directory or directories using the IBM Aspera Connect Browser Plug-In. For more information, see <a href="#">“Transferring Files” on page 57</a> .
Upload File	Upload a file from another machine to this share using the Connect. For more information, see <a href="#">“Transferring Files” on page 57</a> .
Upload Folder	Upload a folder from another machine to this share using the Connect. Users do not need permission to create new folders to upload directories.
Delete	Delete the selected directory or directories.
New Folder	Create a new directory in the share.
Rename	Rename an existing directory in the share.
Create Share	Create a share for the selected directory. You must have admin or manager authorization to create a share. You can select only one directory at a time. Click <b>Create Share</b> to

Button	Function
	open the <b>New Share</b> dialog. The dialog is prepopulated with the node and directory information. To complete the other fields, see <a href="#">“Creating a Share” on page 52.</a>

## Authorizing Users to a Share

For an overview on user roles and authorizations, see [“Understanding User Roles and Share Authorization” on page 36.](#)

1. From your home page, click a share's drop-down menu, and select **Authorizations**.
2. Click **Authorize User**, **Authorize Group**, or **Authorize Directory**.
3. For users and groups, enter a user or group name and click **Search Users** or **Search Groups**.  
The search functions as it does for searching shares and nodes. For more information on searching, see [“Searching Nodes and Shares” on page 36.](#)
4. Click **Add** next to the user, group, or directory.
5. Select permissions for the user, group, or directory.

Permission	Description
Manage	Select <b>manage</b> to make the user a manager of the share. For more information about managers, see <a href="#">“Understanding User Roles and Share Authorization” on page 36.</a>
Browse	Select <b>browse</b> to give the user permission to browse the node.
Transfer	Select <b>download</b> and <b>upload</b> to give the user download and upload permissions. <b>Note:</b> Users with upload permissions can upload directories even if they are not permitted to create directories (mkdir is not selected).
File Operations	Select <b>mkdir</b> , <b>delete</b> , and <b>rename</b> to make changes to the files on the node.
Notifications	Select <b>content availability</b> for Shares to send email notifications to the user whenever new content is available.

The default permission is browse. If a user does not have the browse or upload permissions, the user can only access Shares functions if the user has been made an API user. For more information about API permissions, see [“Shares API Permissions” on page 79.](#)

6. Click **Update** to save your changes.
7. Remove all authorization for a user, group, or directory by clicking **Remove**.

## Transferring Files

### Uploading and Downloading Content

IBM Aspera Shares users may upload and download content to and from a share if they are authorized to do so by clicking the corresponding action buttons shown when browsing a share. Transfers are managed by Shares. For more information on the Connect Browser Plug-In, see [“IBM Aspera Shares and the Connect Browser Plug-In” on page 58.](#)

When initiating a transfer, Shares opens the transfer in the Connect Browser Plug-In transfer window. For more information on the Connect transfers window, see [“The Transfers Window” on page 58.](#)

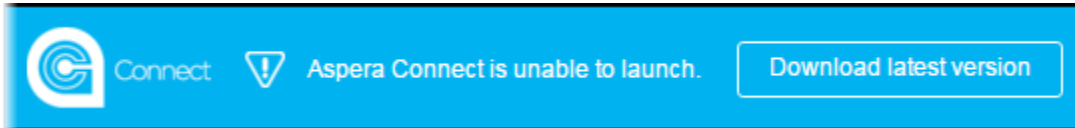
Users with sufficient permissions can adjust file transfer speed by opening the **Transfer Monitoring** window. For more information, see [“Monitoring Transfers” on page 59.](#)

## IBM Aspera Shares and the Connect Browser Plug-In

Transfers initiated in the IBM Aspera Shares 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, Shares checks if the Connect has been installed on their browser. If they have an outdated version or do not have the plug-in installed, Shares 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.

Each page of Shares checks for the presence of Connect. If Connect is missing, Shares prompts you to download the plug-in. To suppress Shares from prompting you to install Connect on each page, go to your **Preferences** page and set the value of **Suppress Connect Install Dialog** to **true**.

### Transfers with Connect

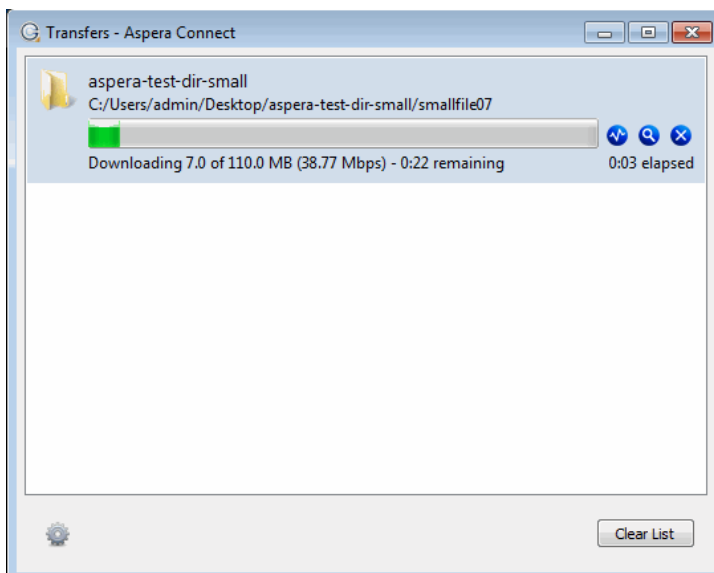
For more information on transferring content with Connect, see [“Uploading and Downloading Content”](#) on page 57.

### Serving Connect Locally






If you are operating within a closed system, you may want to host the IBM Aspera Connect installers and plugins 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 from a Local Location”](#) on page 60.

## The Transfers Window


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

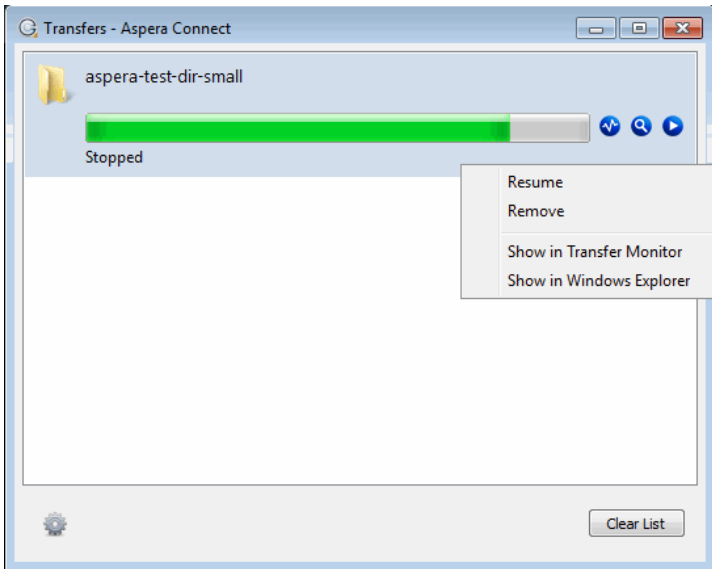


The **Transfers** window contains the following controls:


-  Open the Transfer Monitor. For more information on using this feature, see [Monitoring Transfers](#).
-  Open the folder on your computer that contains this content.
-  Stop the transfer session.
-  Resume transfer.
-  Retry a failed transfer.



When the queuing option is enabled, only a certain number of concurrent transfers are allowed. The additional transfers will be queued in the **Transfers** window and initiated when a transfer is finished.

You can manually start a queued transfer by clicking the  button. You can also right-click on a started or stopped transfer to access various controls. The example below shows the right-click options for a stopped transfer.



## Monitoring Transfers

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

Field	Value
Transfer progress bar	Adjust the file transfer speed by clicking and sliding the transfer progress bar.
	Click to view the destination folder of the transferred files.
	Click to stop the transfer session.
Transfer policy: <ul style="list-style-type: none"> <li>• Fixed</li> <li>• High</li> <li>• Fair</li> <li>• Low</li> </ul>	Select the transfer policy from the drop-down list: <ul style="list-style-type: none"> <li>• 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.</li> <li>• The transfer rate is adjusted to use the available bandwidth up to the maximum rate.</li> <li>• The transfer attempts to transmit data at a rate equal to the target rate. If network conditions do not permit that, it transfers at a rate lower than the target rate, but not less than the minimum rate.</li> </ul>

Field	Value
	<ul style="list-style-type: none"> <li>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.</li> </ul>

**Note:** You can only switch between High and Fair transfer policies if the host is IBM Aspera High-Speed Transfer Server version 3.0 or later.

## Serving Connect from a Local Location

If you need to host the IBM Aspera Connect Plug-in SDK installers locally, you can download the Connect SDK file and configure Shares to point to a local copy of the Connect SDK hosted at a non-standard location. In this way, users download Connect from a server of your choice.

1. Download the Connect SDK zip file from the Aspera Developer Network.
2. Create the directory, C:\Shares\connect-sdk, and extract the contents of the connect SDK into this directory.
3. Edit the connectinstaller-4.js file found at the following location:  
C:\Shares\connect\v4\connectinstaller-4.js  
Change the default SDK location to connectOptions.sdkLocation.

```
var updatesURL = connectOptions.sdkLocation;
```

4. Open the file at C:\Shares\nginx\conf\nginx.conf and ensure the directive below is included in the file:

```
http {
    server {
        include locations-enabled/*.conf;
    }
}
```

5. Create a file named "connect-sdk.conf" in the following location:  
C:\Shares\nginx\conf\locations-enabled\connect-sdk.conf. Paste the following content and save the file:

```
location /connect/ {
    alias C:/Shares/connect-sdk/;
    expires 1d;
}
```

6. Point Shares to the new Connect SDK location by editing the file at  
C:\Shares\www\app\views\node\shared\\_aspera\_web\_plugin\_install.html.haml.

Change the following line to one of two options:

```
- connect_autoinstall_location = '//d3gcli72yxqn2z.cloudfront.net/connect/v4'
```

- Programmatically set the domain name of the server.

```
- connect_autoinstall_location = "//#{ request.host_with_port }/connect/v4"
```

- Manually set the domain name of the server. Replace shares.example.com with the Shares server domain.

```
- connect_autoinstall_location = '//shares.example.com/connect/v4'
```

Find the following line under function loadConnectScript:

```
var url = window.location.protocol + CONNECT_AUTOINSTALL_LOCATION + '/' + script + '.min.js';
```

Replace it with the line below:



```
var url = window.location.protocol + CONNECT_AUTOINSTALL_LOCATION + '/' + script + '.js';
```

#### 7. Restart Shares and Nginx.

Go to **Start Menu > Control Panel > Administrative Tools > Services**. Right-click and select **Restart** for each of the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

Your Shares server is now hosting Connect and installers.

**Note:** You may need to clear your browser cache in order for these changes to take effect.

## Transferring Content Between Shares

**Note:** This feature is supported only by IBM Aspera High-Speed Transfer Server 3.4.5 or later.

You can transfer content from any share for which you have download permission to any share for which you have upload permission. Conversely, you can transfer content to any share for which you have upload permission from any share for which you have download permission.

1. Select one or more files or folders from a Share for which you have download permission.
2. Drag the files or folders to a Share for which you have upload permission, or to a bookmark.

When a transfer occurs, a transfer window opens showing the current status of each transfer that is being made.

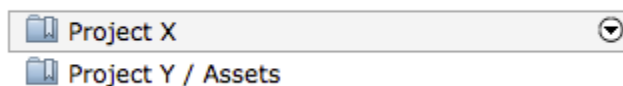
In the **Transfer** dialog, you can also perform the following actions:

Action	Description
Pause	Temporarily pause a transfer.
Resume	Resume a previously paused transfer.
Clear all	Clear transfers from the list.
Remove	Remove transfer from the list. (This will also cancel any paused transfers.)

## Using Bookmarks

Use bookmarks in Shares to save the location of a directory for quick and easy access. Saved bookmarks appear under the BOOKMARKS section in the left sidebar on the Home page. If you do not see BOOKMARKS, you do not have any saved bookmarks.

### BOOKMARKS



### Creating a Bookmark

To create a bookmark, browse the Node or Shares directory you want to bookmark. Select a directory and click the **Bookmark** button. If you do not select a directory, clicking the **Bookmark** button bookmarks the directory you are currently browsing.

**Note:** You can only bookmark directories. If you select a file and click **Bookmark**, Shares gives the following message: "Can only bookmark directories".

## Managing Bookmarks

You can edit or delete bookmarks from the left sidebar. Hovering over a bookmark reveals the drop-down arrow that allows you to perform the following actions:

Action	Description
<b>Browse</b>	Go to the directory saved by the bookmark.
<b>Edit</b>	Change the name of the bookmark. <b>Note:</b> You cannot change the bookmark directory. To change the directory, you must delete this bookmark and create a new bookmark from the desired directory.
<b>Delete</b>	Deletes the bookmark.

**Note:** If you lose permission to browse a directory, bookmarks of those directories are not automatically removed. You can still access the bookmark, though you can no longer browse the directory.

## Monitoring Shares

---

### Monitoring Shares Activity

Admins can view and search activity in IBM Aspera Shares, including user logins, share authorizations, and transfers, in the **Activity** page and in the **Activity** tab for users, groups, and directories.

#### Viewing Activity

**All activity:** On the **Admin** page, click **Activity** to go to a searchable list of all activity in Shares.

**Activity by user, group, or directory service:** On the **Admin** page, click **Users**, **Groups**, or **Directories**. Click **Edit** next to the user, group, or directory and go to the **Activity** tab where a searchable list of activity by that entity is displayed.

#### Searching Activity

Click **Search** to open a search dialog. Confine your search to a date range using the **From** and **To** fields. Search for specific events by typing in a keyword. Once you have entered one or more letters, Shares suggests a list of events containing the string. For example, typing **share** returns the following options:

- DirectoryCreatedOnShare
- FileRenamedOnShare
- FilesDeletedFromShare
- ShareAuthorizationCreated
- ShareCreated
- ShareDeleted
- ShareStatusChanged


## All Activity

Hide Search

Click **Search** to start your search.

In the search results, to view details of an event click **Show**. To see a list of all events of that type, click the event name.

## Errors and Warnings


You can review errors and warning associated with IBM Aspera Shares activity to identify problems. The **Errors and Warnings** page can be accessed by clicking **Monitor > Errors and Warnings** or the warning icon  in the upper right corner of Shares pages.



### Access from Monitor > Errors and Warnings

Click **Monitor > Errors and Warnings** to go to a table of all errors and warnings. The **Errors and Warnings** page provides the following options for viewing them.

- To search for specific errors or warnings, enter the object, such as Node or User, or the level (error or warning) in the search fields and click **Search**.
- To sort errors and warnings by level (warning or error) or object, click the dropdown menu next to Sort. The default sort is by level.
- If more information about an error or warning is available, go to it by clicking the Description link next to the error.
- To go to the error log, click the description link for the object "ErrorLog."

### Access from the Warning Icon

The warning icon shows the total number of errors and warnings. Click the icon  to open a pop-up window that displays a summary of errors (red icons) and warnings (orange icons). Buttons at the bottom of the window show the number of warning and errors. The pop-up window provides the following options for viewing errors and warnings:

- To go to a searchable list of all warnings, click .
- To go to a searchable list of all errors, click .
- If more information about an error or warning is available, go to it by clicking the error description.
- To go to the error log, click **Found number errors in error\_logs table**. If there are too many errors and warnings to fit in the pop-up window, click **+ number more**, which goes to the same page as **Monitor > Errors and Warnings**.

## Configuring the Stats Collector

---

### Adding Existing Nodes to Stats Collector

1. Go to the Shares shell.

```
> cd C:\Shares\www
```

2. Run the following rake task to add existing nodes to stats collector:

```
> rake aspera:stats_collector:add_all_nodes
```

### Configure Stats Collector Log Levels

Edit the stats collector logging configuration file, `logback.xml`, to view more detailed information in stats collector logs.

1. Open the `logback.xml` file.

Find it in:

```
C:\Shares\statscollector\etc\logback.xml
```

2. Edit the `statscollector.log.level` value.

Change `INFO` to `DEBUG`.

```
<root level="${statscollector.log.level:-INFO}">
  <appender-ref ref="FILE"/>
  <appender-ref ref="STDERR" />
</root>
```

3. Restart stats collector for the changes to take effect.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to view the list of the Shares services. Stop and start the **Aspera Stats Collector** service.

Stats collector logs should now show debugging information. To change log levels back to normal, open the `logback.xml` file and change `DEBUG` back to `INFO`.

### Lowering Stats Collector Polling Frequency

Lowering the frequency that stats collector polls nodes for statistics can free up memory and lower the load on your server. This is especially applicable to cases where the stats collectors of multiple machines are all polling a single node for statistics.

1. Open the `stats-collector.properties` file.

Find the file at:

```
C:\Shares\statscollector\etc\stats-collector.properties
```

2. Uncomment and specify the `polling.period` variable:

```
### The time period at which nodes are polled for new statistics.
### Default 1s
# polling.period=
```

For example, increase the polling period to 5s to lower the load on your server:

```
### The time period at which nodes are polled for new statistics.
### Default 1s
polling.period=5s
```

3. Restart stats collector for the changes to take effect.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to view the list of the Shares services. Stop and start the **Aspera Stats Collector** service.

## Retrieving Stats Collector Version Number

Run the following command:

```
> C:\Shares\statscollector\jre\bin\java -jar C:\Shares\statscollector\lib\stats-collector-admin.jar -A
```

## Working with Rake Tasks

---

### Configuring Users With Rake Tasks

Use rake tasks to create, modify, and delete users; to import SAML and LDAP users; and to export users to and import users from .csv files.

Rake tasks must be run from the Shares shell, as described in the following steps:

1. Go to the shares folder:

```
> cd C:\Shares\www
```

2. Test that your rake tasks are working correctly.

```
> bundle exec rake -T
```

#### Create User

```
> bundle exec rake data:user:create -- --username username --password password --email email_address --first_name first_name --last_name last_name
```

For example:

```
> bundle exec rake data:user:create -- --username johndoe --password ***** --email john@shares.example.com --first_name John --last_name Doe
```

By default, Shares requires a user to change their password when they first log in. You can disable that requirement by setting the `--set_password` option to `true`. For example:

```
> bundle exec rake data:user:create -- --username johndoe --password ***** --email john@shares.example.com --first_name John --last_name Doe --set_password true
```

#### Delete User

```
> bundle exec rake data:user:delete -- --username username
```

For example:

```
> bundle exec rake data:user:delete -- --username johndoe
```

#### Update User

```
> bundle exec rake data:user:update -- --username username --password password --email email --first_name first_name --last_name last_name
```

For example:

```
> bundle exec rake data:user:update -- --username johndoe --password ***** --email john@shares.example.com --first_name John --last_name Doe
```

## Export a List of Users

```
> bundle exec rake data:user:export -- --path \path\to\file
```

For example:

```
> bundle exec rake data:user:export -- --path C:\temp\projectgroups.txt
```

The export command writes the groups into a .txt file. For example, the `projectgroups.txt` file may read like below:

```
projectgroup1  
projectgroup2
```

## Import Users (from .csv)

**Note:** The .csv file must use the following format:

```
Username, Email, First Name, Last Name, Password
```

```
> bundle exec rake data:user:import -- --path \path\to\file
```

For example:

```
> bundle exec rake data:user:import -- --path C:\temp\users.csv
```

**Important:** By default, users created by this rake command are not allowed to log into Shares. A Shares admin can set login permissions for these users one by one by going to **Admin > Users**, selecting the user, clicking **Edit Security**, and selecting the **Login** permission. Users for whom no passwords are specified are assigned a random password and must click the **Forgot your username and password?** link to reset their password and log in.

## Import SAML User

```
> bundle exec rake data:user:saml:import -- --id full_distinguished_name --name_id  
shares_username [--option option_value]
```

**Note:** Delimit distinguished names containing spaces with quotes (").

When running the create and update tasks, you can add the following options to your command to set values for the Shares user's fields:

Option	Description
--given_name <i>given_name</i>	This value determines the Shares user's first name.
--surname <i>surname</i>	This value determines the Shares user's last name.
--email <i>email</i>	This value determines the Shares user's email address.

For example:

```
> bundle exec rake data:user:saml:import -- --id "CN=saml  
doe,OU=AK,OU=Users,OU=Asperasoft,DC=dev,DC=aspera,DC=us" --name_id samldoe --given_name Sam --  
surname Doe --email samldoe@shares.example.com
```

## Delete SAML User

```
> bundle exec rake data:user:saml:delete -- --username username
```

For example:

```
> bundle exec rake data:user:saml:delete -- --username samldoe
```

## Fetch User Details from LDAP

```
> bundle exec rake data:group:ldap:fetch -- --username username
```

For example:

```
> bundle exec rake data:group:ldap:fetch -- --username ldapdoe
```

## Delete LDAP User

```
> bundle exec rake data:user:ldap:delete -- --username username
```

For example:

```
> bundle exec rake data:user:ldap:delete -- --username ldapdoe
```

## Configure Groups With Rake Tasks

Use rake tasks to create, modify, and delete groups; to add users to groups; and to import SAML and LDAP groups.

Rake tasks must be run from the Shares shell, as described in the following steps:

1. Go to the shares folder:

```
> cd C:\Shares\www
```

2. Test that your rake tasks are working correctly.

```
> bundle exec rake -T
```

## Create Group

```
> bundle exec rake data:group:create -- --group_name group_name
```

For example:

```
> bundle exec rake data:group:create -- --group_name projectgroup1
```

## Delete Group

```
> bundle exec rake data:group:delete -- --group_name group_name
```

For example:

```
> bundle exec rake data:group:delete -- --group_name projectgroup1
```

## Add User to a Group

```
> bundle exec rake data:group:user:add -- --username username --group_name group_name
```

For example:

```
> bundle exec rake data:group:user:add -- --username johndoe --group_name projectgroup1
```

## Add LDAP User to a Group

```
> bundle exec rake data:group:authorizable:user:add -- --username ldap_username --group_name group_name
```

For example:

```
> bundle exec rake data:group:authorizable:user:add -- --username johnldap --group_name projectgroup1
```

## Remove User from a Group

```
> bundle exec rake data:group:user:remove -- --username username --group_name group_name
```

For example:

```
> bundle exec rake data:group:user:remove -- --username johndoe --group_name projectgroup1
```

## Export a List of Groups

```
> bundle exec rake data:group:export -- --path \path\to\file
```

For example:

```
> bundle exec rake data:user:export -- --path C:\temp\groupexport.txt
```

## Import Groups from a Text File

```
> bundle exec rake data:group:import -- --path \path\to\file
```

If the group already exists in Shares, the rake task does not add the group.

For example:

```
> bundle exec rake data:group:import -- --path C:\temp\projectgroups.txt
```

Where the `projectgroups.txt` file contains the following :

```
projectgroup1  
projectgroup2  
projectgroup3  
projectgroup4  
projectgroup5  
projectgroup6
```

## Create SAML Group

```
> bundle exec rake data:group:saml:create -- --group_name group_name
```

For example:

```
> bundle exec rake data:group:saml:create -- --group_name samlgroup1
```

## Fetch Group Details from LDAP

```
> bundle exec rake data:group:ldap:fetch -- --group_name group_name
```



For example:

```
> bundle exec rake data:group:ldap:fetch -- --group_name samlgroup1
```

## Delete LDAP Group

```
> bundle exec rake data:group:ldap:delete -- --group_name group_name
```

For example:

```
> bundle exec rake data:group:ldap:delete -- --group_name samlgroup1
```

## Configure a Share With Rake Tasks

Use rake tasks to create, modify, and delete shares, and to configure share permissions.

Rake tasks must be run from the Shares shell, as described in the following steps:

1. Go to the shares folder:

```
> cd C:\Shares\www
```

2. Test that your rake tasks are working correctly.

```
> bundle exec rake -T
```

**Tip:** Square brackets in usage statements denote optional arguments and do not need to be included when running the commands.

## Create Share

```
> bundle exec rake data:share:create -- --node_name node_name --share_name share_name --  
directory directory
```

For example:

```
> bundle exec rake data:share:create -- --node_name aspera --share_name share1 --directory /mnt
```

## Delete Share

```
> bundle exec rake data:share:delete -- --share_name share_name
```

For example:

```
> bundle exec rake data:share:delete -- --share_name share1
```

## Modify Share

**Note:** Uses the same syntax as create share. Change the values as needed to modify the attributes of the specified share.

```
> bundle exec rake data:share:create -- --node_name node_name --share_name share_name --  
directory directory
```

For example:

```
> bundle exec rake data:share:create -- --node_name aspera --share_name share1 --directory /mnt
```

## Manage User's Share Permissions

```
> bundle exec rake data:user:share_permissions -- --username username --share_name share_name
[--permission true/false...]
```

Where valid permissions are:

- `browse_permission`
- `download_permission`
- `upload_permission`
- `mkdir_permission`
- `delete_permission`
- `rename_permission`
- `content_availability_permission`
- `manage_permission`

For example:

```
> bundle exec rake data:user:share_permissions -- --username users --share_name share1
--upload_permission true --mkdir_permission true
```

## Manage Group's Share Permissions

```
> bundle exec rake data:group:share_permissions -- --group_name group_name --share_name
share_name
[--group-type active_directory/local/saml]
[--permission true/false...]
```

If `--group-type` is not specified, Shares assigns permissions to all groups with `group_name`.

Valid permissions are:

- `browse_permission`
- `download_permission`
- `upload_permission`
- `mkdir_permission`
- `delete_permission`
- `rename_permission`
- `content_availability_permission`
- `manage_permission`

For example:

```
> bundle exec rake data:group:share_permissions -- --group_name group1 --share_name share1
--upload_permission true --mkdir_permission true
```

## Export Share Name and Associated Directory

```
> bundle exec rake data:share:export -- --path path/to/file
```

For example:

```
> bundle exec rake data:share:export -- --path /tmp/share_export.txt
```

## Configure Nodes With Rake Tasks

Use rake tasks to create, modify, and delete nodes.

Rake tasks must be run from the Shares shell, as described in the following steps:

1. Go to the shares folder:

```
> cd C:\Shares\www
```

2. Test that your rake tasks are working correctly.

```
> bundle exec rake -T
```

### Options

When running the create and update tasks, you can add the following options to your command to set values different from the defaults:

Option	Default
<code>--port <i>port</i></code>	9092
<code>--ssl <i>true_or_false</i></code>	true
<code>--verify_ssl <i>true_or_false</i></code>	false
<code>--timeout <i>seconds</i></code>	30
<code>--open_timeout <i>seconds</i></code>	10

### Create Node

```
> bundle exec rake data:node:create -- --name name --host host --api_username api_username --  
api_password [--options value]  
api_password [--options]
```

For example:

```
> bundle exec rake data:node:create -- --name local_node --host localhost --api_username  
node_user --api_password ****
```

**Note:** You must create a node user and password to finish creating the new node. See *IBM Aspera Enterprise Server Admin Guide: Setting up Node Users* for instructions on how to create a node user.

### Modify Node

```
> bundle exec rake data:node:update -- --name name [--options]
```

For example:

```
> bundle exec rake data:node:update -- --name local_node
```

### Delete Node

```
> bundle exec rake data:node:delete -- --name name
```

For example:

```
> bundle exec rake data:node:delete -- --name local_node
```

## Configure Server Settings With Rake Tasks

Use rake tasks to add or configure LDAP settings, and to configure web server settings and SMTP server settings.

Rake tasks must be run from the Shares shell, as described in the following steps:

1. Go to the shares folder:

```
> cd C:\Shares\www
```

2. Test that your rake tasks are working correctly.

```
> bundle exec rake -T
```

**Tip:** Square brackets in usage statements denote optional arguments and do not need to be included when running the commands.

### Add or Configure LDAP

```
> bundle exec rake data:ldap_config -- --directory_type directory_type --name name [--  
description description]  
--host host --port port [--base_dn base_dn] --authentication_method authentication_method  
[--username username --password password --encryption encryption]
```

Where acceptable directory types are:

- ActiveDirectory
- OpenDirectory
- FedoraDirectoryServer
- OpenLdap

Where acceptable authentication methods are:

- anonymous
- simple (Simple bind requires a username and a password.)

Where acceptable encryption types are:

- unencrypted
- simple\_tls

**Note:** Encryption is, by default, set to unencrypted.

For example:

```
> bundle exec rake data:ldap_config -- --directory_type ActiveDirectory --name dest_dir  
--host ldap.aspera.us --port 1234 --base_dn OU=AsperaDirectory,DC=aspera,DC=asperasoft,DC=com  
--authentication_method simple --username johndoe --password ***** --encryption simple_tls
```

### Configure Manager UI and API Permissions

Admins can allow managers to administer users and groups through the Shares UI, through the Shares API, or both, using the following rake task:

```
> bundle exec rake data:manager_config -- --UI true/false --API true/false
```

For more information on manager permissions, see [“Configuring Manager Permissions” on page 17](#).

### Configure Host, Port, and TLS

```
> bundle exec rake data:web_server -- --host host --port port --tls tls
```

For example:

```
> bundle exec rake data:web_server -- --host shares.example.com --port 1234 --tls true
```

## Configure SMTP Server

```
> bundle exec rake data:smtp_server -- --server server --port port --domain domain --tls tls
--username
  username --password password --from from
```

For example:

```
> bundle exec rake data:smtp_server -- --server smtp2.example.com --port 25 --domain
example.com --tls 1 --username
  admin --password **** * --from server@shares.example.com
```

**Note:** The first time this task is run, the task creates requires an entry for all options. Afterward, running the task again only modifies the specified options, leaving non-specified fields the same.

## Configure Custom Logo

```
> bundle exec rake data:logo:set -- --path \path\to\file
```

For example:

```
> bundle exec rake data:logo:set -- --path /temp/aspera_logo.jpg
```

# Configuring MySQL Server

---

## Open a MySQL Prompt

To open a MySQL client prompt, run the following command:

```
> cd C:\Shares\www
> rails db -p
```

## Using an External MySQL Database

After installing Shares, you can choose to use a MySQL database on a remote system rather than the default local MySQL database. You need to have the MySQL credentials, port, and the hostname of the remote machine.

**Note:** You must configure Shares to use an external MySQL database is you are sharing the MySQL database among multiple Shares instances.

1. Dump the Shares and stats collector databases.

Run the following commands:

```
# mysqldump -u username -p web_production > sharesdb.sql
# mysqldump -u username -p stats_collector > statscollectordb.sql
```

The following step takes place on the remote system hosting the remote MySQL server.

2. Import the MySQL dumps into the MySQL on the remote system.

First log in to the MySQL command-line client and create the two needed databases if they do not exist:

```
mysql> create database web_production;
mysql> create database stats_collector;
```

Exit the MySQL client then import the dumps. You can do this with commands like the following:

```
# mysql -u username -p web_production < sharesdb.sql
# mysql -u username -p stats_collector < statscollectordb.sql
```

The following steps return to the system with Shares installed.

3. Back on the system with Shares, update the Shares application configuration file, which can be found at the following location:

```
C:\Shares\www\config\database.yml
```

Add in the *remote\_host*, *remote\_username*, *remote\_password* and *port* for your remote MySQL in the *production* and *production\_stats\_collector* sections:

```
production:
  database: web_production
  username: "remote_user"
  password: "remote_password"
  host: remote_host
  port: remote_port
  encoding: utf8
  reconnect: false
  pool: 5
```

```
production_stats_collector:
  database: stats_collector
  username: "remote_user"
  password: "remote_password"
  host: remote_host
  port: remote_port
  encoding: utf8
  reconnect: false
  pool: 5
```

4. Update the stats collector configuration file, which can be found at the following location:

```
C:\Shares\statscollector\etc\persistence.xml
```

Add in the *remote\_host*, *remote\_username* and *remote\_password* for the remote MySQL server under the connection URL header:

```
<!-- connection URL: jdbc:mysql://HOST:PORT/DATABASE -->
<property name="hibernate.connection.url" value="jdbc:mysql://remote_host/
stats_collector"/>
<property name="hibernate.connection.username" value="remote_user"/>
<property name="hibernate.connection.password" value="remote_password"/>
```

5. Restart Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to start and stop any of the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

6. If you are sharing the MySQL database with multiple Shares instances, make sure the following Shares files are identical on every Shares instance:

```
C:\Shares\statscollector\etc\keystore.jks
C:\Shares\statscollector\etc\persistence.xml
C:\Shares\www\config\aspera\secret.rb
C:\Shares\www\config\database.yml
C:\Shares\www\config\initializers\secret_token.rb
```

## Backing Up and Restoring the Database

### Backing Up Shares and the Database

Aspera recommends backing up Shares and the MySQL database before any major changes to your Shares installation, such as installing a patch or upgrading to a newer version of Shares.

**Note:** The Shares web application and the nginx service are still available when performing a backup.

1. Create a backup directory.

Run the following in a Command Prompt, where `C:\backups` is your backup directory:

```
> mkdir C:\backups
```

2. Stop Shares services.

Click **Start > Control Panel > Administrative Tools > Services** and stop the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

3. Run the backup command.

```
> cd C:\shares\www
> bundle exec rake backup DIR=C:\backups
```

4. Copy the files in `C:\backups` to the backup machine.

5. Copy the following files to the backup machine:

- `C:\shares\nginx\conf\cert.pem`
- `C:\shares\nginx\conf\cert.key`
- `C:\shares\www\config\database.yml`

6. Restart Shares services.

Click **Start > Control Panel > Administrative Tools > Services** and start the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

For instructions on how to restore a backup of Shares, see [“Restoring Shares from a Backup” on page 75](#).

## Restoring Shares from a Backup

The following instructions assume you have a Shares backup. For instructions on backing up Shares, see [“Backing Up Shares and the Database” on page 74](#).

**Note:** If you are restoring Shares on a new installation, make sure your MySQL password on the new installation matches the password of the backed up MySQL database.

1. Stop Shares services.

Click **Start > Control Panel > Administrative Tools > Services** and stop the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

2. Update `database.yml`, `cert.pem`, and `cert.key` files.

Replace following files with the backup versions:

```
C:\shares\nginx\conf\cert.pem
C:\shares\nginx\conf\cert.key
C:\shares\www\config\database.yml
```

**Important:** If you are restoring the backed up Shares onto a new installation of Shares, do not restore the database .yml file. Changing the database .yml file may force Shares to use a MySQL password different from the one used during the fresh install.

3. Run the restore command.

Open Command Prompt as an administrator and run the following commands. In the example below, *E:\aspera-shares-restore* is the directory where the backup files are stored on the new server.

```
> cd C:\shares\www
> bundle exec rake restore DIR=E:\aspera-shares-restore
> bundle exec rake db:migrate
> bundle exec rake init
> bundle exec rake aspera:stats_collector:add_all_nodes
```

4. Start Shares services.

Click **Start > Control Panel > Administrative Tools > Services** and stop the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

## Troubleshooting Shares

---

### Create a Shares Admin or Reset Admin Password

To create a Shares admin or reset the password of an existing Shares admin, run the following command as a system administrator.

```
> cd C:\shares\www
> rake aspera:admin NAME=username PASSWORD=password EMAIL=email_address
```

### Restart Shares Services

Some troubleshooting fixes may require that you stop, start, or restart one or more Shares services.

Go to **Start Menu > Control Panel > Administrative Tools > Services** to start and stop any of the following services:

- Aspera Nginx Service
- Aspera Delayed Job Service
- Aspera Web Services
- Aspera Stats Collector

### Clearing Unresponsive Background Jobs

If IBM Aspera Shares background jobs are not responding, they can be cleared using the command line.

1. To open a MySQL client prompt, run the following command:

```
> cd C:\Shares\www
> rails db -p
```

2. Clear background jobs in MySQL.

```
DELETE FROM delayed_jobs;
```

3. Restart Aspera background jobs.

Click **Start Menu > Control Panel > Administrative Tools > Services** to view the list of the Shares services. Stop, then start the **Aspera Delayed Job Service**.



## Gathering and Zipping All Logs for Support

Aspera Technical Support often requires system logs to help troubleshoot errors. The following instructions describe how to gather the logs created by IBM Aspera Shares, background processes, and stats collector into a .zip file that can be sent to IBM Aspera Support:

1. Create a folder in which to gather all your Shares logs.  
For example, go to C:\tmp and create the folder `aspera_logs`.
2. Go to C:\Shares\www\log and copy all the logs starting with "production-job-" and "production-web-" to your folder.
3. Go to C:\Shares\statscollector\logs and copy the file "statscollector-admin.log" to your folder.
4. To compress your folder into a zip file, right-click the folder and select **Send to > Compressed (zipped) folder**.

## Resetting the Stats Collector Database

Stats Collector is responsible for keeping track of transfer status and statistics, which can thus affect things such as notifications and reporting. When there are issues with the Stats Collector database for Shares, such as tables not being updated, corrupted entries or other database-specific errors, reset the database to get the system running again.

1. Stop the Stats Collector.  
Go to **Services** and stop **IBM Aspera Stats Collector**.

2. Back up the Shares database:

```
> cd C:\shares\www
> bundle exec rake backup DIR=backup_dir
```

3. Re-create the Stats Collector database.

```
> C:\Shares\statscollector\bin\aspera-stats-collector.bat admin db-recreate --quiet
```

4. Restart the Stats Collector database.

Go to **Services** and start **IBM Aspera Stats Collector**.

5. Regenerate the keys and wait for the public key to be added to the database:

```
> C:\Shares\statscollector\bin\aspera-stats-collector.bat admin regenerate-keys
```

6. Reset the iteration sequence number to 0 for re-polling all transfers and re-add all nodes:

```
> cd C:\Shares\www
> bundle exec rake aspera:stats_collector:add_all_nodes
> bundle exec rails db -p
mysql > update web_production.transfer_reporters set sequence_number = 0;
mysql > exit
```

## Appendix

---

### Updating the License

1. Select **Admin > Other > License**.
2. Select **Change license**. Paste your license key and click **Save**.  
After entering a valid license, Shares displays your Expiration Date and the Max Users allowed by your license.

**Note:** A new user may only log in if the number of users active in the last hour is less than the max number of users.

## Checking for SSH Issues

Aspera recommends that you review your SSH log periodically for signs of a potential attack. Launch **Control Panel > Administrative Tools > Event Viewer**. To see only SSH Server events, select **View > Filter** to show the filter settings. In the **Application Properties > Filter tab**, select **sshd** in the Event source menu to display only SSH Server events. You may also apply other conditions when needed.

With a filter applied, you can review the logs in the Event Viewer main window, or select **Action > Save Log File As...** to export a log file using .txt or .csv format.

Look for invalid users in the log, especially a series of login attempts with common user names from the same address, usually in alphabetical order. For example:

```
...
Mar 10 18:48:02 sku sshd[1496]: Failed password for invalid user alex from 1.2.3.4 port 1585
ssh2
...
Mar 14 23:25:52 sku sshd[1496]: Failed password for invalid user alice from 1.2.3.4 port 1585
ssh2
...
```

If you have identified attacks:

- Check the SSH security settings.
- Report attackers to your ISP's abuse email, for example, abuse@your-isp.

## Changing Nginx Ports

1. Edit the IBM Aspera Shares `nginx.config` file.

```
C:\\Shares\\nginx\\conf\\nginx.conf.
```

2. Update the HTTP and HTTPS server blocks with your desired ports.

These are the default settings for the two server blocks:

```
server {
    listen      80;
    rewrite ^ https://$host$request_uri? permanent;
}

server {
    listen      443;
    root        ../www/public;

    [...]
}
```

Update the values of the `listen` and `rewrite` directives with the desired ports (for example, 9080 and 9443).

```
server {
    listen      9080;
    rewrite ^ https://$host:9443$request_uri? permanent;
}

server {
    listen      9443;
    root        ../www/public;

    [...]
}
```

3. Reload the `nginx.config` file with the following command:

```
> cd C:\\Shares\\nginx
> nginx -s reload
```

## Disabling IPv6 Support in Shares

By default, the Nginx web server in Shares is configured to listen on IPv6 ports in addition to the standard IPv4 ports. If your operating system does not support IPv6, Nginx is unable to start and Shares fails to load for your users. To disable IPv6 support in Shares, you must edit the `nginx.conf` configuration file.

1. Edit the `nginx.conf` configuration file, located at:

```
C:\Shares\nginx\conf\nginx.conf
```

2. In the `server` sections, comment out the following lines:

```
listen [::]:80;
```

```
listen [::]:443 ssl;
```

After making the changes, your `nginx.conf` `server` sections may look like the following example:

```
server {
    listen 80;
    # listen [::]:80;

    return ^ 301 https://$host$request_uri;
}

server {
    listen 443 ssl;
    # listen [::]:443 ssl;

    [...]
}
```

3. Save your changes.
4. Reload the `nginx.conf` file with the following command:

```
> cd C:\Shares\nginx
> nginx -s reload
```

5. Test your changes. Try to access Shares by entering an IPv6 address in the browser.

## Shares API Permissions

Aspera products such as Drive and HSTS have integrated capabilities for working with IBM Aspera Shares. Such products interact with Shares using the API. To allow the API to correctly access users shares, configure permissions as described below.

1. Allow API login.

For each Shares user, ensure that the **API Login** check box is checked under the **Security** tab. This permission is enabled by default whenever new users are created.

2. Create shares and authorize users for each share.

The table below describes the mapping between API permissions and Shares permissions.

API Permission	Shares Permissions that should be Enabled
View	<b>browse</b> and <b>download</b>
Edit	<b>upload</b> , <b>rename</b> , <b>mkdir</b>
Delete	<b>delete</b>

**Note:** Folders with names that do not follow the proper Windows folder naming convention do not open in Shares. For details on Windows folder naming conventions, see <http://msdn.microsoft.com>.

# 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 serverIIS 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.

```
C:\Program Files\Aspera\etc\sshd_config
```

```
/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 Administrators
AllowTcpForwarding yes
```

```
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.

Click **Start > Control Panel > Administrative Tools > Services**. Locate the `OpenSSH Service` and click **Restart**.

```
# 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. For Aspera servers on Windows in an Active Directory Domain, create the Active Directory user account to use as the Aspera service account before installing your Aspera server software. This ensures that the correct security settings are applied to the user. If you create the Active Directory service account user after installation, see the following knowledge base article for instructions on how to configure security policies for the account.

<https://support.asperasoft.com/hc/en-us/articles/216125388-OpenSSH-in-Active-Directory-Environments>

3. 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 (or a range, see below).
- 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).

4. 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:

```
> /opt/aspera/bin/asconfigurator -x "set_server_data;ssl_protocol,tls1.2"
```

5. If Aspera Node D is exposed to internet traffic, run it behind a reverse proxy.

If your Aspera server must expose Aspera Node D 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, Aspera Node D runs on port 9092, but nodes that are added to AoC must have Aspera Node D run on port 443, the standard HTTPS port for secure browser access. Configuring a reverse proxy in front of Aspera Node D 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.

- a) Set up a system user with Node API credentials on your server.

- b) Download and install Nginx.
- c) Configure the HTTPS port for Aspera Node D.

```
# asconfigurator -x "set_server_data;https_port,9092"
```

- d) Open the Nginx configuration file in a text editor.

Open `C:\nginx\conf\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/*.confC:\nginx\*.conf;
}
```

- e) Create a file named `aspera_node_proxy.conf` and save it in the following location:

`C:\nginx\conf\sites-enabled\aspera_node_proxy.conf`

Create the `sites-enabled` folder if it does not exist.

- 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 "C:/Program Files/Aspera/Enterprise Server/etc/
aspera_server_cert.pem";
    ssl_certificate_key "C:/Program Files/Aspera/Enterprise Server/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          C:\Logs\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 Aspera Node D.

```
# systemctl restart asperanoded
```

or for Linux systems that use **init.d**:

```
# service asperanoded restart
```

```
> net stop asperanoded
> net start asperanoded
```

- h) Restart Nginx.

```
> nginx -s reload
```

i) Run Nginx as a Windows service.

When you install Nginx on a Windows OS, it is installed as an application that runs only when the user who installed the application is logged in. However, for HSTS nodes that are added to AoC, Aspera recommends running Nginx as a service so that its function is not tied to a specific user.

For instructions, see <https://ibm.ibmaspera.com/helpcenter/admin/nodes/configuring-an-aspera-transfer-server-as-a-node-for-aspera-on-cloud>.

6. 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 **aspshe11**.

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 **aspshe11**, 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.

Windows users are assigned to **aspsshell** automatically when you configure the user in the GUI and specify a non-empty docroot. If you do not specify a docroot or configure users from the command line, you must manually set the users' shell as **aspsshell.exe** in C:\Program Files\Aspera\etc\passwd.

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/aspsshell
```

**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:///.*file:///c%3A/Documents/*
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 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 - | sha1sum
```

On the server, run a local **ascp** transfer. The transfer does not need to complete successfully in order for the remote host-key fingerprint to appear in the log.

```
> ascp source_file username@localhost:destination
```

Open `C:\Program Files\Aspera\var\log\aspera-scp-transfer.log`. Search for "remote host-key fingerprint". The line appears similar to the following, in which `19f7cf4d495234ng4342ha062f5d98b5a9d665` is the SHA-1 fingerprint:

```
2017-12-08 12:04:53.024 [1888-0000264c] LOG [asssh] remote host-key fingerprint
19f7cf4d495234ng4342ha062f5d98b5a9d665
```

- b) Set the SSH host key fingerprint in `aspera.conf`.

```
> 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>7qd0webGGeDeN7Wv+2dP3HmWfP3
</ssh_host_key_fingerprint>
```

- c) Restart the node service to activate your changes.

Go to **Control Panel > Administrative Tools > Services**, click **Aspera NodeD**, and click **Restart**. 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 "Retrieving 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:

```
C:\Program Files\Common Files\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.

#### a) In the Faspex UI, go to **Accounts** and select the admin account.

#### b) In the **Permissions** section, locate the **Allowed IP addresses for login** field and enter the IP addresses or IP address range to allow.

#### c) 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:

#### a) Set a non-zero session timeout.

#### b) Lock users out after five failed login attempts within five minutes.

#### c) Enable **Prevent concurrent login**.

#### d) Set a password expiration interval of 30 days.

#### e) Prevent reuse of the last three passwords and require strong passwords.

#### f) Set **Keep user directory private** to **Yes**.

#### g) Disable **Allow all users to send to all other Faspex users**.

- h) Disable **Users can see global distribution lists**.
  - i) Disable **Ignore invalid recipients**.
  - j) 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:
- a) 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.
  - b) 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:
- a) Disable **Allow inviting external senders**.
  - b) Enable **Invitation link expires** and set an expiration policy.
  - c) Disable **Allow public submission URLs**.
  - d) Disable **Allow sending to external email addresses**.
  - e) Set a package link expiration.
  - f) 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:  
C:\Shares\nginx\conf\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:
      - C:\Shares\nginx\conf\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 a 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:

```
> setexport ASPERA_SCP_FILEPASS=password  
> /opt/aspera/bin/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:

```
> setexport ASPERA_SCP_FILEPASS=password  
> /opt/aspera/bin/asprotect -o filename filename.aspera-env
```

## Using the Health Check URL

Use the health check URL to check the Shares server status without providing credentials to the server. You can pass on the response to other services like load balancers.

### Using the Health Check URL

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/health_check
```

For example:

```
$ curl -k https://10.0.0.1/health_check  
{  
  "valid_license" : true,  
  "nodes" : [  
    {  
      "id": 1,  
      "status": "Active",  
    },  
    {  
      "id": 2,  
      "status": "Error",  
    },  
    {  
      "id": 3,  
      "status": "Disabled",  
    }  
  ]  
}
```

### Response Codes

Code	Status
HTTP 200	Shares nodes are healthy and the Shares license is valid.
HTTP 500	Either Shares has an invalid license, or one of the Share nodes are down. The JSON response reports the exact issue.

## Glossary

---

### **Admin user**

An admin account on the Shares server that can be used in the Shares web app to add and configure users, groups, directory services, nodes, and shares.

### **Aspera Service Account**

In Windows, an admin account that Shares uses to run Aspera services. Admins never need to log in using the Aspera Service account unless it is assigned to an existing account during installation.

### **Node**

A transfer server that has been configured to support the IBM Aspera Node API, enabling transfers through Aspera web applications including Shares, Files, and Faspex.

### **Node API**

A daemon that provides a single REST-inspired interface for file browsing, management, and transfers.

### **Node API username and password**

Credentials used by the Aspera web application to authenticate to a remote node and generate token authorization for transfers between the Aspera web application user's machine and the remote node.

### **Share**

A file or directory with which users, groups, and directories have conditional authorization to interact (browse, upload to, download from, rename).

### **Shares**

An IBM Aspera web application that enables companies to conditionally view and share files and directories of any size within their organization or with external customers and partners.

### **Shares user account**

The account with which a user logs into the Shares web application.

### **System user account**

On a node, a designated account (not belonging to a Shares user) that can be configured as a transfer user.

### **Transfer server**

Any machine running Aspera transfer server software, such as Enterprise or Connect Server.

### **Transfer user account**

On a node, a system account that is configured with a Node API username and password, and that is set up as a user in the transfer application. This account is used to authorize and manage transfers initiated by Aspera web application users between their machines and the node.

