Release Notes: IBM Aspera Enterprise Server, Connect Server, Point-to-Point Client, and Desktop Client 3.8.0 for macOS

Product Release: February 26, 2018
Release Notes Updated: June 14, 2018

This release of IBM Aspera Enterprise Server, Connect Server, Point-to-Point Client, and Desktop Client provides the new features, fixes, and other changes listed below. In particular, the Breaking Changes section provides important information about modifications to the product that may require you to adjust your workflow, configuration, or usage. Additional sections cover system requirements and known problems.

Desktop Client users: Features and issues that are related to configuration, Watch Folders, and the Node API are not applicable to your product.

Note: Some Aspera product names are in a transition phase. During the transition, Enterprise Server and Connect Server might also be referred to as "IBM Aspera High-Speed Transfer Server", Point-to-Point Client might also be referred to as "IBM Aspera High-Speed Transfer Endpoint", and IBM Aspera Shares and IBM Aspera Faspex might also be referred to as the bundled product "IBM Aspera High-Speed Sharing Server."

NEW FEATURES

For more information about the new features in this release, see "New Features" in the guides:

Enterprise Server Admin Guide (macOS)
Connect Server Admin Guide (macOS)
Point-to-Point Client Admin Guide (macOS)
Desktop Client Admin Guide (macOS)

General

- Desktop Client no longer requires a license. For upgrades to 3.8.0, existing licenses are overwritten with the unlimited license after a successful upgrade.
- Updated Java Runtime Environment for improved GUI performance and security.
- The ALEE service is now available for macOS, enabling entitlement licensing for Aspera servers.
- Connections that are configured in the GUI and Hotfolders can now be set to encrypt data in transit with a specific encryption cipher: AES-128, AES-192, AES-256, or none. The default is AES-128.
- `ascp` and `ascp4` transfers to object storage can now include custom metadata if the object storage supports it (currently S3, Google, Azure, and Swift). Metadata is set using the `--tags` or `--tags64` option with a JSON payload argument. Metadata are applied per session, not per file. (CIM-723)
- A new command-line tool, `aclean`, is a fast method of deleting directories and files from local and object storage. Directories and files can be filtered based on their last modified times, and the tool supports doing a dry run to determine what content will be deleted.
- New traffic RTT predictor settings offer server configuration options that improve transfer rate stability and maximize FASP transfer performance.
- A new database mode for the Aspera Node Service, `acm_redis`, improves database cleanup and background job management for clusters of Aspera servers.
- A new post-transfer file validation process runs file validation once the transfer is complete, in contrast to existing inline validation methods. Out-of-tranfer validation is also applied to files transferred by HTTP(S) fallback, unlike inline validation. Files that are being processed are reported by Aspera Central (and Faspex and Console) as "validating", and then "complete" once the validation completes.
- Connection passwords can now be saved and restored when exporting and importing connections in the GUI.
- `ascp` and `ascp4` logging can now be configured in `aspera.conf`. (CIM-958)

Ascp

- Transfer sessions that fallback to HTTP now report file IDs in the management stream (as FaspFileID).
- Uploads with a `stdio-tar://` destination can now use transfer tokens for authorization.
- The `stdio-tar://` source file can now specify an offset parameter that indicates where in the destination file the inline raw data should be inserted to overwrite the existing data.
- When using `stdio-tar://` as the source for an `ascp` transfer, the value for "File:" can be a directory and the directory structure is preserved at the destination. Additionally, `stdio-tar://` can now be used as the destination.

Ascp 4

- The data-streaming capabilities of `ascp4` (powered by FASPStream technology) are now available for High-Speed Transfer Server and High-Speed Transfer Endpoint users. Features include:
  - Multiple multicast streams can now concurrently transfer to the same multicast IP address (as long as the multicast port varies) or concurrently transfer to the same multicast port (as long as the multicast IP address varies). (CIM-770)
  - TCP providers can be used as a source or destination I/O in command line.
  - UDP providers can be used as a source or destination I/O in command line.
  - A new parameter, `pktbatch`, can be used to control how UDP datagrams are read and written. By default,FASPStream now does a batch read and write of UDP datagrams. Disable the option to read and write one packet at a time.
- The encryption cipher can now be specified on the client command line using `-c` *`cipher`*. The server setting overrides the client if the server setting is stronger.
- A4 transfers can now use transfer token authorization. The transfer token must be created by using `astokengen` with the `--full-paths` option and passed to A4 with the `ASPERA_SCP_TOKEN` environment variable.
- Faster directory scanning on object storage.
- A4 now supports persistent sessions, using the new option `--keepalive`.
- Faster transfers to object storage, particularly for transfers that skip existing files (`-k 1`) or that use file lists.

Node API

- Access keys can now be backed up and restored by using new `asnodeadmin` options.
- POST requests to `/ops/transfers` can now use AES-192 and AES-256 ciphers for encryption of data in transit.
- When a file is deleted with `DELETE /files/{id}`, its preview file is now also deleted.
- The `files_cleanup_interval` setting in `aspera.conf` is now respected.
- Drastically faster response for `/files?sort=name` requests (files sorted by name); depending on the storage and number of files, browsing can be up to 20 times faster.
- Improved metadata rules for `ascp` decrease the load on the node database by only generating file IDs if `activity_event_logging` is enabled.
- `/files/delete` requests can now specify that folders that are not empty should not be deleted; otherwise, all folders are deleted by default.
- Improved Redis database performance by automatic expiration and removal of cached file metadata.
- Disabling `activity_logging` and `activity_event_logging` now turns off all event reporting, including transfer events, filelock events, and permission events.
- The Aspera Node daemon now locates `ascp` and `ascp4` relative to its own path, enabling the Aspera application to be installed in non-default location.
- POST requests to `/streams` can now specify more transfer parameters that are supported by A4, including compression, read and write threads, and minimum transfer rate.
- Filelocks and previews are now cached for faster directory listing and browsing.
- The `/streams` endpoint now accepts bearer token authorization.
- File statistics are now returned by the `/files/`*`file_id`* endpoint even if the user does not have list permission.
- Filelocks are now disabled when `ascp` is run without token authorization.
- Improved access level reporting by the `/permissions` endpoint.

- Filelocks can now be created and removed for files by pathname by using POST requests to `/files/filelock` and `/files/unfilelock`. These endpoints provide an alternative to sending POST, PUT, and DELETE requests to `/files/{id}/filelock`, which require that you specify the file by file ID.
- Transfer settings can now be configured at the access key level. The transfer capabilities are returned in response to calls to `/info`.
- Filelock and permissions operations are now reported by the `/events` endpoint.
- New permissions model allows user-specific permissions for file operations, grouped by access levels (edit, view, or none).
- Node-to-node transfer requests now respect the `xfer_retry` that is specified in the tags, and no longer accept a user-specified `xfer_id` (because Node generates its own `xfer_id` to ensure a unique identifier).
- The `/ops/transfers` endpoint now supports updating the maximum (target) transfer rate, minimum transfer rate, and rate policy.
- POST requests to the `/ops/transfers` endpoint now supports additional `ascp` options in the transfer specification, including excluding files older than or newer than the specified time, preserving timestamps, and moving or deleting files after transfer.

Watch Folders and Aspera Watch Service

- The Aspera Watch Service daemon now uses a single snapshot tree that represents the entire file system and monitors portions of the file system to which users subscribe. This system reduces memory requirements and simplifies watch configuration.

  A user subscribes for file system notifications on a directory, and the Aspera Watch daemon creates a watch for the directory and a subscription ID for the user. The user can unsubscribe from watches or renew a subscription (if it is nearing expiration) by using the subscription ID. If no users are subscribed to the watch, then the watch is automatically deleted, decreasing the load on the Redis database. The subscription system also allows the Redis database to delete snapshots that are no longer needed by any users, for additional database space savings.

  When upgrading to 3.8, existing Watch Folders are preserved with existing watches converted into subscriptions. For example, a Watch Folder with one watch becomes a Watch Folder with two subscriptions, one for the watch and one for the Watch Folder itself. See the guide for more information about the new subscription model and preparation for upgrading.
- Watch Folders and the Aspera Watch Service now support cloud storage and URI docroots. Object storage requires that a small scan period be set for the Watch Service subscription because cloud storage does not have a notification API.
- Watch Folders can now be created in "pull" mode, such that a folder on a remote host can be watched and automatically transfer files to the local computer. The remote host can be an Aspera server in object storage.

  The Watch Folder JSON configuration file syntax for the source and target now require that you specify the type of authentication, the port for authentication, and authentication credentials for the remote server (rather than in the `"target"` section). Post-processing is now specified for the source (rather than `"local"`). A new section for watchd configuration enables you to specify the remote watchd service.

  The previous version of the Watch Folder API and JSON configuration is still supported for push Watch Folders, but pull Watch Folders require that the remote server run version 3.8.0 or higher.
- Watches and Watch Folders can now be created, managed, and deleted in the application GUI.
- Watch Folders can now use IBM Aspera Shares version 1.9.11 (with patch) as a remote endpoint, authenticated by using Shares credentials.
- Snapshot differentials created through the Watch Service REST API can now be calculated asynchronously for more efficient processing of large differentials.
- Watch Folders can now use access keys for authentication to remote storage. Remote sources (for pull Watch Folders) must have an Aspera Watch Service running. Access key authentication can be used for push Watch Folders with destinations of Aspera Files, Aspera Transfer Service, or Aspera Transfer Cluster nodes.
- Watch Folders can be configured to use a specific Aspera Watch Service.
- Watch Folder-initiated transfers to object storage can now include custom metadata if the object storage supports it (currently S3, Google, Azure, and Swift). Metadata is set in the Watch Folder configuration under "aspera" in a "cloud-metadata" section. (CIM-723)

- The symbolic link handling policy can now be specified in the Watch Folder configuration when creating Watch Folders with `aswatchfolderadmin` or the Watch Folder API.
- The Watch Folder daemon now reports if a Watch Folder license is missing or expired; this information can be retrieved using the API, from the status file, or by running `asrun send -l`.
- Watch and Watch Folder services that are stopped can now be restarted by resending the configuration to the Node service. In the GUI, a stopped service can be reenabled in the **Services & Policies** dialog.
- The Aspera Watch Service and Watch Folder daemons are now gracefully shutdown by the Aspera Watch Services Manager (asrund), with improved reporting of daemon status.
- Watch Folders now supports AES-192 and AES-256 encryption.
- Faster drop statistics calculation by storing and updating statistics in the Redis database.
- GET calls to the `/drops` Watch Folder API endpoint now return the last error that occurred in the drop and the last error of a file in the drop. Additionally, a state filter can be specified in the query to limit the results to drops that match the state.
- A new Watch Folder API endpoint, `/schemas/watchfolders/configuration`, returns a JSON schema that provides the default value of each Watch Folder configuration field.
- The `/watchfolders` endpoints support concurrency for calls to the Redis database.

Sync

- Sync can now use multiple scanning threads on the local and remote computers to improve performance by decreasing the time required for directory scanning after the initial scan. Specify the number of threads by using the new command line options `--scan-threads` and `--remote-scan-threads`.
- Sync logging location, level, and size can be configured in `aspera.conf` using new logging settings. Command line options and `<async_log_dir>` take precedence over the new settings.
- Improved Sync logging when `<async_log_dir>` is set in `aspera.conf`, with all logging going to the specified directory.
- Sync sessions with object storage can now include custom metadata if the object storage supports it (currently S3, Google, Azure, and Swift). Metadata is set using the `--tags` or `--tags64` option with a JSON payload argument. (CIM-723)
- File metadata can now be preserved (using `-u -j -t`) when `--dedup=copy`. (File metadata are always preserved when `--dedup=hardlink` or `--dedup=inode`).
- Improved logging about Sync database (`snap.db`) loading.
- Sync can now use a cluster as an endpoint. Specify the remote host with the cluster DNS and provide a unique session name. Aspera recommends creating the session name with the UUID and a descriptive string, for example: `async -N cluster-sync-ba209999-0c6c-11d2-97cf-00c04f8eea45`.

Object Storage Support

- For transfers to object storage, the timeout for transfer requests to Trapd is now configurable in `aspera.conf` by setting `<cmd_timeout>` in the `<pvcl>` section. The default is now 10 minutes instead of 5 minutes. Increasing the timeout allows a transfer request to wait while Trapd handles long operations, such as removing folders that contain millions of files, rather than failing the transfer.
- Enhanced security through component updates. (CIM-930)
- Transfers to Azure Data Lake Storage are now supported.

Other Changes

- Mac OS X 10.8, 10.9, and 10.10 are no longer supported.

BREAKING CHANGES

If you are upgrading from a previous release, the following changes for this release may require you to adjust your workflow, configuration, or usage.

- Precalculating job size is no longer supported for persistent `ascp` sessions to avoid confusion when a transfer completes before the job size is calculated. (CIM-970)
- FASP transfers through IBM Aspera Forward Proxy Server now require that Proxy server self-signed SSL certificates include the hostname, otherwise transfers are refused. The self-signed certificates that are created upon

installation must be replaced. For instructions on creating a certificate with a hostname, see "Setting up SSL for your Nodes" in the IBM Aspera Connect Server Admin Guide for Linux.

- OpenSSH 7.0 and newer no longer supports DSA keys. If the client creates connections in version 3.7.3 or older of the GUI, HTTP/S-based connections (such as to Shares or ATS, or authenticated with Node API credentials) to Windows servers version 3.7.4 or newer, or with other OS servers that are using OpenSSH 7.0 or newer, fail to authenticate. Connections that provide a private SSH RSA key are not affected. **Workaround:** Upgrade the Aspera client to version 3.7.4 or newer.
- Performance enhancements to A4 required changes that make version 3.8.0 unable to transfer with versions 3.7.4 and earlier. **Workaround:** Upgrade your server and A4 clients to 3.8.0 to ensure compatibility.
- The `--delete-after` option is no longer supported by A4. Use `--delete-before` instead.
- The improvements to Watch Folders include several changes to the Watch Folder JSON configuration file syntax and to associated command line utilities:
  - The configuration settings for the Aspera Watch Service and Watch Folders services changed in order to simplify configuration. Individual watches are no longer configured in `aspera.conf`; watches are managed by subscriptions to Aspera Watch Services.
  - The command line option for the Aspera Watch Services Manager for returning information on services changed. A new option, `asrun send --list` (or `asrun send -l`) returns information for all services, equivalent to the behavior of `asrun send -g` or `asrun send --get` in versions 3.7.x. Users can now return information for a specific service using the modified `asrun send --get=`*`service_id`*; the service ID is now required for `asrun send --get` commands.
  - The options available for `aswatchadmin` changed. When subscribing to a Watch service, `--max-snapshots`, `--snapshot-min-interval`, and `--snapshot-min-changes` are no longer supported. The values for `snapshot-min-interval` and `snapshot-min-changes` are read from `aspera.conf`.
  - The use of PUT calls to `/v3/watchfolders/`*`watchfolder_id`*`/drops` has changed. PUT to `/v3/watchfolders/`*`watchfolder_id`*`/drops`, to restart all drops in a Watch Folder, is no longer supported. The drop ID must now be specified, as `/v3/watchfolders/`*`watchfolder_id`*`/drops/`*`drop_id`*`.`

ISSUES FIXED IN THIS RELEASE

Note: This release contains tickets that were created from different issue-tracking systems. For this reason, the list below uses two different formats for issue numbers.

ATT-556 - File and directory timestamps are not preserved (`-p` is not respected) when the docroot is specified in URI format, such as `file:///`. (CIM-1081)

ATT-550 - Vlink rules configured in the client `aspera.conf` are not respected if they include a fitness rule.

ATT-536 - Downloads of folders that use macOS custom icons stall because the icons contains a special character in the names that prevent canonicalizing the path. (CIM-1019)

ATT-522 - The documentation does not make clear that `asdelete` follows symbolic links when deleting files from the target directory. (CIM-957)

ATT-521 - When the upload target is a URI path, transfers that specify `--overwrite=always` overwrite files on the destination even if the server is configured to deny overwrite.

ATT-518 - A4 transfers report an error and abort if the destination path is a symbolic link.

ATT-510 - A4 transfers do not respect Vlink settings. (CIM-928)

ATT-506 - In version 3.7.4, Ascp does not properly release memory when transferring a large number of files. (CIM-920)

ATT-487 - In version 3.7.4, inline file validation with URI might fail due to a change in the tags structure in the JSON request. If you do not use tags in your validation, your validation is not affected. (CIM-876)

ATT-470 - Downloading and decrypting a file by using HTTP fallback can sometimes fail if the file was encrypted when it was uploaded by using HTTP fallback.

ATT-426 - To use SSH key authentication in A4, the full path to the private key must be specified as the argument for `-i` because A4 does not automatically look in the transfer user's home folder. This prevents Aspera Console from being able to use SSH keys if it is configured to use A4 instead of `ascp` because the full path cannot be specified in the Console UI.

ATT-424 - Filters that are configured in the client `aspera.conf` are not respected by A4 transfers to object storage. Filters that are specified on the command line are respected.

ATT-405 - When monitoring an `ascp` transfer, STATS messages report inconsistent WrittenBytes, FileBytes, and TransferredBytes.

ATT-189 - In rare cases, `ascp` keeps running after it encounters a disk read error. (CIM-233)

ATT-44 (#29613) - The timestamp of a parent directory that is transferred with `ascp4 -p` is not preserved, while the timestamps of the child files and directories are preserved.

ATT-30 and ATT-46 - `ascp4` transfer is slow when you upload many small files (for example, 1 million 4-byte files) to S3 storage.

ATT-27 - Direct-to-cloud `ascp4` transfers are skipped unless the full destination path is specified.

ES-728 - Advanced `ascp` options are listed as "Hidden" in the output of `ascp -hh`.

ES-623 - For files that are transferred to object storage and that have file names that contain spaces, as of version 3.6.2 Aspera Central stores the file names with the spaces URI encoded (as %20) rather than unencoded. (CIM-997)

ES-577 - Watch Folders cannot be created with a Shares source or destination if the share name contains a ".".

ES-447 - In the GUI, you cannot create a new folder when connected to a new AWS S3 region (Frankfurt, Ohio, or Korea) because Amazon's Signature Version 4 Signing Process is not automatically used.

ES-418 - Aspera clients version 2.7.4 cannot download from Aspera servers version 3.7.3 or 3.7.4, but can download from servers version 3.3.3. (CIM-808)

ES-416 - A4 transfers with object storage can hang if the Aspera Trapd service loses connection or otherwise errors.

ES-409 - Permissions assigned to IBM Aspera Shares users are not inherited by the Enterprise Server that hosts the share. For example, if a user is created in Shares and does not have delete permissions to a share, if the Shares user runs an `ascp` download directly from the server and uses `--remove-after-transfer` in the command line, the files are deleted from the source. (CIM-788)

ES-402 - Inconsistent error reporting by ascp4 to the source and destination can cause discrepancies in the transfer session logs. (CIM-767)

ES-367 - If a user's docroot contains a string variable, such as `/home/$(name)`, `ascp4` returns the error "No such file or directory (e=104)". (CIM-586)

ES-345 - Empty source directories are not deleted from Hot Folders even if the "Delete empty source directories" option is selected in the GUI. (CIM-614)

ES-312 - In the GUI, if the Default Target Rate under **Preferences** or **Global Preferences** is set to an alphanumeric value, such as "10 Gbps," then only the numeric values are retained. If an alphanumeric value is entered that starts with a letter, then the transfer rate resets to the last valid numeric value.

ES-281 - When several different users access a transfer server remotely, passwords might disappear from the GUI if the GUI is opened while simultaneously querying the SQLite database or the GUI is stopped abruptly and the database does not close gracefully. (CIM-487)

ES-280 - In the GUI, the upload and download rates that are configured for a connection (**Connection > Transfer > Speed**) cannot have different units.

ES-246 - When creating connections to Amazon S3 storage in the GUI, transfer authentication fails if the AWS Access Key or Secret Access Key contain a "+" or "/" character. (CIM-393)

ES-188 - Transfers through Aspera Forward Proxy are rejected if the node user password contains an @ symbol. (CIM-290)

ES-157 - On the **Security** tab of the **Connections Manager**, users must enter the decryption password twice.

ES-118 (#21517) - Folders that are created in the Connect Server web GUI can have permissions different from the permissions that are specified in `aspera.conf`.

ES-114 - The installer tries to install OpenSSH even for a custom installation with OpenSSH unselected.

ES-86 - After you reopen the GUI, Aspera cannot connect to a Microsoft SAS URL. (CIM-120)

ES-57 - After a fresh installation, initial values for **Limit Download Bandwidth** and **Limit Upload Bandwidth** in the GUI are not set to system defaults.

NODE-548 - The Aspera NodeD service does not respect the `activity_cleanup_interval` setting in `aspera.conf` for transfers that error.

NODE-451, 450 - The Aspera NodeD service starts database clean up as soon as it starts, even if the file system is not mounted, and can delete keys and file IDs from the database.

NODE-440 - The "Link" header that is returned for `/ops/transfers` requests is not part of the Access-Control-Expose-Headers and so it cannot be used with CORS requests. (CIM-842)

NODE-438 - `ascp` transfers fail when the destination path starts with two slashes ("//") and the docroot is a URI path. (CIM-858)

NODE-381 - The `/files/du` output incorrectly uses the size of a symbolic link's target when calculating disk usage, resulting in an overestimate.

NODE-345 - A POST request to `/ops/transfers` can trigger two transfer sessions for the same file and result in a corrupted file at the destination and a slower final transfer rate.

TRAP-86 - Folders cannot be created in an AWS S3 bucket from the Aspera GUI if the bucket's policy requires server-side encryption, even if server-side file encryption is specified for the connection. (CIM-714)

TRAP-71 - Multi-session transfers to object storage can stall if the number of files open for write in multi-session mode exceeds the default number of starting threads (64). **Workaround:** Open `/opt/aspera/etc/trapd/trap.properties` and set `aspera.session.max-starter-threads` to a larger value. If this setting is not in the file, add the following line with an appropriate value:

```
aspera.session.max-start-threads=1280
```

TRAP-28 - When downloading from cloud or object storage, `ascp` always takes the equivalent of 1 GB of buffers from Trapd. This can lock buffers in `ascp` queues for hours and may prevent other `ascp` transfers from transferring normally.

WAT-753 - Sync does not update file metadata when `--preserve-uid` and `--preserve-gid` are specified and the UID or GID does not exist on the destination. (CIM-1159)

WAT-702 - The UID and GID are not preserved for folders that are transferred by Watch Folders, they are only preserved for files. (CIM-986)

WAT-653 - Files might be marked as conflicted during a bidirectional Sync if they are modified on the client after being modified on the server and bidirectionally synchronized, with each Sync session preserving metadata.

WAT-642 - If a remote Redis database is configured in `aspera.conf`, the Node daemon tries to connect to `redis:localhost:31415` for queries to `/v3/watchfolders` rather than the remote Redis.

WAT-621 - [AIX] Watchfolder does not archive files if the system user is not the owner of the archive directory. (CIM-847)

WAT-571 - Sync deletes files from the destination if the files become inaccessible on the source, such as when permissions change. (CIM-729)

WAT-523 - Meta-attributes are not preserved in sync sessions that use the `--dedup=copy` option.

WAT-288 (#27311) - An `--apply-local-docroot` pull copies the local docroot path into the same path. For example, `/home/user1/sync` is copied into `/home/user1/sync`.

WAT-200 - Recently finished Watchfolder drops are not stored and are lost if asrund is restarted.

WAT-169 - If `top_level_dirs` drop detection is used with *x* top-level directories in Watchfolder, 7(*x*)+ drops are created. The drop count continually increases.

#32553 - When the FASP Session log source file list exceeds 500 bytes and contains multi-byte UTF-8 characters, the output is truncated in a manner that creates an invalid UTF-8 sequence.

SYSTEM REQUIREMENTS

Enterprise Server, Connect Server, Point-to-Point Client, and Desktop Client

- **Mac**: OS X 10.11, macOS 10.12 (Sierra), 10.13 (High Sierra)

Client Browsers for Connect Server Web UI

- **Windows:** Chrome 62-64, Microsoft Edge 39-41, Internet Explorer 11, Firefox 56-58, Firefox ESR 52
- **macOS:** Chrome 62-64, Firefox 56-58, Safari 11, Firefox ESR 52
- **Linux:** Chrome 62-64, Firefox 56-58, Firefox ESR 52

KNOWN ISSUES

Note: This release contains tickets that were created from different issue-tracking systems. For this reason, the list below uses two different formats for issue numbers.

General

ATT-580 - If a server has server-side encryption-at-rest enabled, when a file is uploaded to the server then modified at the source and uploaded again, that file cannot be downloaded from the server and returns error code 27 with the error "Other session error". (CIM-1209)

ATT-492 (#22998) - If the overwrite setting in the server's `aspera.conf` is "deny", a destination file with the same name as the source file is still overwritten.

ATT-325 - If the transfer rate exceeds the write capability of the storage and one endpoint is specified as a URI path, the transfer might stall for more than 5 minutes before erroring.

ATT-245 (#22726) - Successful transfers might log the error, `Failure Event: -34 - libssh2_channel_wait_closed() invoked when channel is not in EOF state`, particularly downloads in FIPS mode. The error can be safely ignored. (CIM-329)

ATT-107 - The file count that is reported in the GUI under session statistics is incorrect when the user has an exclude filter.

ATT-98 - If inline validation is configured on the server side, the server does not honor a session timeout if a transfer includes a skipped file.

ES-780 - Renaming files and directories on the server through the GUI errors with the message "Path outside docroot" if the transfer user has a docroot with the format `file:////dir_name`. (CIM-1258)

ES-770 - On Windows OS as of 3.7.4, updates to the Cygwin OpenSSH implementation that is used by High-Speed Transfer Server and High-Speed Transfer Endpoint cause transfers to error when:

- the OpenSSH service is run by an Active Directory domain user, and
- the transfer user is a different Active Directory domain user who has a docroot on a CIFS or SMB share.

In this case, the transfer user cannot use SSH key authentication for uploads or downloads because they do not get the proper credentials to access the mounted storage. (CIM-1239) **Workaround:** Open a command prompt as an administrator and run the following command:

```
> C:\Program Files\Aspera\Enterprise Server\bin\passwd.exe -
R domain\username
```

Where *domain* is the Active Directory domain and *username* is the transfer user's username. Then add the transfer user as a Remote Desktop user.

ES-742 - As of 3.8.0, some translated versions of the GUI have empty field names for configuration settings.

ES-675 - As of 3.7.4, in the rare case when a transfer fails with a "Session open failed" error, the status is not updated in the Aspera Central database from "running". As a result, Console continues to report the session as "RUNNING" until the entry in the central database is manually deleted or updated to "ERROR". (CIM-1072)

ES-664 - As of 3.7.4, `asconfigurator` no longer returns a warning to reload the Aspera Central service in order to activate a change in the server's configuration. (CIM-1037)

ES-610 - The Connect Server web UI displays duplicate headers and does not display symbolic link files if a symbolic link in the same directory is broken. **Workaround:** Correct the broken symbolic link and all files and symbolic links are shown correctly.

ES-526 - As of 3.8.0, some translated versions of the GUI have "!?!" in front of labels that are not translated from English.

ES-388 - If Connect Server and Faspex versions 4.1.0 or newer are installed on the same computer, they cannot use the same Apache.

ES-357 - If the user language is set to Spanish (`user.language=es` in `aspera.prop`) and global configuration settings are changed in the GUI (**Configuration > Global**), the GUI displays the default values after it is restarted even though the updated settings are saved in `aspera.conf`. (CIM-638)

ES-323 - When doing a dry run of an `asdelete` (by using the `-d` option), the log shows all the files that were scanned, not the files that would be deleted by the `asdelete` command. (CIM-558)

ES-249 - The aggressiveness setting is applied to Vlinks, rather than only the network rate controller. (CIM-399)

ES-248 - While an `ascp` or `ascp4` transfer of many files is in progress, skipped files are reported as complete. The counters are correct once the entire session is complete. (CIM-398)

ES-216 - If the Aspera Connect Plug-in is unable to connect to the server by SSH, a misleading error message, "Failed to authenticate," is reported rather than indicating that it is a connection problem. (CIM-72)

ES-215 - If Aspera Connect is unable to connect to the server by SSH, HTTP fallback is attempted but only after a 15 minute delay. (CIM-320)

ES-166 - To set a combination of symbolic links actions besides the default, `aspera.conf` must be manually edited. Selecting **any combination of the above delimited by commas** in the GUI sets that invalid text string as the value.

ES-98 (#34674) - When Japanese language is set in the GUI, the application doesn't respect `aspera.conf` settings; all docroot settings are set to false, and the other settings fail with attached Japanese errors.

ES-42 - When you retrieve the entitlement status by using `alee-admin status`, confusing error messages are returned even if the entitlement was registered successfully.

NODE-545 - Folder timestamps are not preserved when the source or destination is a URI path, even when `-p` is used.

#35952 - `asunprotect` cannot decrypt a re-protected file.

#34811 - You are unable to download encrypted files with an incorrect decryption passphrase when you are using HTTP fallback.

#32934 - If the Internet accountability software Covenant Eyes is installed, some HTTP fallback transfers appear to complete but then lose connection with the server and then attempt to retransfer. Covenant Eyes captures the entire HTTP transmission before forwarding it to the server. If the file is so large that this process takes longer than about 20 seconds, the server times out and cancels the session. **Workaround:** Reduce the probability of timeout by increasing

the server timeout length. Set `Session Activity Timeout` in `aspera.conf` by running the following command:

```
$> asconfigurator -x "http_server;session_activity_timeout,time_in_seconds"
```

#32517 - Retransfer requests are unencrypted when transfers are encrypted. This change in encryption can cause transfer failures in some scenarios, such as when a network device drops the retransfer request because it detects a bit sequence it considers malicious.

#31791 - Files with the file extension `.aspx` are not transferred. **Workaround:** Edit the `resume_suffix` setting in `aspera.conf` on the client.

#30690 - `ascp` fails with an inaccurate message—`Error: failed to authenticate`—when the server is configured to accept only unsupported ciphers.

#28679 - In some cases, the fallback server cannot accept additional connections, possibly due to too many 'incomplete' requests.

#27879 - [Mac] In Connect Server, `always_set_home` does not work if the user's home directory does not exist.

#27056 - `ascmd` does not respect server-side symlink configuration.

#21629 - Connect Server `aspera-dirlist.pl` does not accurately reflect file permissions for user actions.

Ascp

ATT-579 - Persistent `ascp` uploads to a server that is configured to skip symbolic links do not report when symbolic links are skipped.

ATT-537 - Downloads that use `ascp --overwrite=always` fail when they are authenticated using ASPERA_LOCAL_TOKEN that specifies a local storage path.

ATT-511 - When both `--overwrite=never` and `--remove-after-tranfer` are used, source files may be deleted even if no transfer occurred. (CIM-932)

ATT-435 - `save-before-overwrite` is not supported for URI

ATT-395 - When running a persistent `ascp` session, a FaspManager FILEERROR message truncates a filename that is longer than 128 characters to only the first 128 characters.

ATT-361 - `ascp` transfers to S3 fail when the `--symbolic-link=copy` or `--symbolic-link=copy +force` option is used.

ATT-360 - Directory timestamps are not always preserved on the destination during an `ascp` transfer that uses `-p`.

ATT-226 - If the docroot is a URL path, `ascp` reports incorrect bytes for the sessions that are involved in a multi-session transfer.

ATT-185 - `ascp` does not reconnect to Redis database when `asperanoded` is restarted.

ES-645 - The `ascp -@` option is not supported when the destination is `stdio://`.

ES-359 - `ascp` downloads from SoftLayer do not support `--move-after-transfer`.

ES-267 - Under rare conditions, `ascp` transfers to cloud object storage may be reported as successful even though Trapd reports an error and the content is not in the storage. (CIM-475)

ES-177 - The `range_low` value of a `-@` argument is not respected.

#35010 - If the source path in an `ascp` transfer is a file that is named \ (which is not supported by Aspera), the file is not transferred and an error is generated, but the folder then contains the file and all other files in that folder are transferred.

#32890 - During an `ascp` transfer that uses the `--preserve-xattrs= metafile --remote-preserve-xattrs=metafile` options, the metafile is not transferred.

#32680 - The option to create a directory (`ascp -d`) may create a directory at a destination before an expected session failure.

#30324 - During an `ascp` upload to cloud storage, if a mid-file read failure occurs on the sending computer (which is rare) it can cause the server-side `ascp` to crash and possibly fail to report transfer completion. This read failure can be caused when a source file is truncated during transfer, a drive or file system fails, or a transfer is canceled with `Ctrl+C` or other means.

#28939 - If command line `ascp` neglects to specify a destination host, then the failed transfer (error: "no remote host specified") gets recorded in `SQLite` with `client_node_id NULL`, instead of being populated with the `uuid` of the node. This database error causes an issue with Console.

#26281 - If you run approximately 100 (or a similarly high number) concurrent uploads to S3, intermittent transfer session failures can occur.

#26185 - During an upload to S3 storage, an error may result if `ascp` reports a successful file transfer before the transfer to S3 completes.

Ascp 4

ATT-583 - A4 does not automatically create a destination folder when the source is a file list and the destination does not exist. Instead, it writes all the files in the file list into one file. (CIM-1198)

ATT-582 - A4 sessions run with `-d` and a file list do not report an error if the destination already exists and is not a folder. (CIM-1199)

ATT-545 - A4 downloads all content from an AWS S3 docroot, rather than the specified content, if the docroot contains `?storage-class=REDUCED_REDUNDANCY`.

ATT-515 - When `ascp4` is used by the GUI and transfers are encrypted with AES-128, the GUI incorrectly shows that encryption is "none". (CIM-953)

ATT-485 - Persistent session A4 downloads from object storage do not report a STOP message to management after the transfer completes.

ATT-477 - When files are transferred to a server with an S3 docroot and quickly retransferred with the `--delete-before-transfer` enabled, some files are deleted from the destination.

ATT-473 - A4 uploads to object storage that specify `-k 1` (resume if file sizes match) are also sensitive to checksum, such that if a file transfer is resumed and the file has the same size but a different checksum then the entire file is retransferred, rather than resumed from the last successful chunk.

ATT-451 - A4 does not respect exclude filters if the file path is part of the command line.

ATT-438 - A4 downloads from object storage fail if the source filename contains special Unicode characters, such as Japanese font.

ATT-409 - If a file list contains an invalid path, no error is reported or logged.

ATT-338 - Parallel uploads of several large (>1 GB) files to object or HDFS storage may fail with the error "Peer aborted session" if the number of threads that are specified in the `ascp4` command exceeds the number of jobs that are allowed to run by Trapd. **Workaround:** Open `/opt/aspera/etc/trapd/trap.properties` and set the value for `aspera.session.upload.max-jobs` to one larger than the number of `ascp4` threads. For example,

```
# Number of jobs allowed to run in parallel for uploads.
# Default is 15
aspera.session.upload.max-jobs=50
```

ATT-29 - Files that are transferred to S3 storage with `ascp4` retain a `.partial` extension when viewed in the GUI.

ATT-2 (#32295) - The default minimum transfer rate set in `aspera.conf` is not respected.

ES-247 - Console-initiated `ascp4` transfers fail if the docroot on the source is a UNC path (for example, `\\localhost\SHARE`), returning the error `ERR Source base/path is not a valid directory/file (doesn't match any source path).` (CIM-397)

ES-151 - `ascp4` does not recognize the UNC-path docroot of a Console transfer user. (CIM-197)

Node API

ES-505 - If the Aspera Central database cannot be reached by a Reliable Query request to `/services/rest/transfers/v1/sessions`, the response only includes a 500 Internal Server error and does not describe the error. (CIM-895)

NODE-619 - The Node API does not clean up transfer session information if the session was submitted with an invalid SSH port. **Workaround:** Clean the jobs manually by running the following command on the server:

```
$> asnodeadmin --transfer-log-del transfer_id
```

NODE-492 - For transfers started by the Node API, the target directory is always created if it is not present, even when "`create_dir`" is set to false. (CIM-995)

NODE-481 - The Node service sometimes returns invalid JSON when Console polls `async` jobs. **Workaround:** Recreate the Redis database to resolve the issue. (CIM-988)

NODE-469 - When managing files with a request to `/files/{id}/files`, if the system user under whom the Node service runs does not have write permissions to the docroot, a 500 internal error is returned, even if the node user is attached to a system user who has write permissions.

NODE-466 - A POST request to `/ops/transfers` that contains an invalid hostname returns "waiting for 300 seconds" rather than an accurate error message.

NODE-463 - `ascp` transfers that use `--remove-after-transfer` do not report `file.deleted` events to the Node service.

NODE-460 - The Redis database grows large quickly when reporting Sync sessions to Console that frequently synchronize large directories. (CIM-936) **Workaround:** Reduce the number of files that are reported to Console or the retention time of data in the database.

NODE-442 - `/ops/transfers` can return a value of "null" for `files_failed`, which can prevent transfers from being displayed in Console. (CIM-864) **Workaround:** Enable the Console database to handle the "null" value by logging into the Console database and running the following command:

```
ALTER TABLE fasp_sessions CHANGE COLUMN files_failed files_failed INTEGER
 null;
```

NODE-437 - Transfers with object storage, particularly with buckets that contain a lot of data, become slow when `<files_filelock_enabled>` in `aspera.conf` is set to **true** (in order to enable the filelock feature in the Node API `/files` endpoint). The default setting is **false**.

NODE-433 - The value for `xfer_retry` that is submitted in a `POST` request to `/ops/transfers` is not respected. Transfers that retry but ultimately fail take a long time to be reported as inactive. (CIM-801)

NODE-405 - The `max_rate_kbps` in the output of a `/events` call is incorrectly reported as zero.

NODE-392 - PUT requests to `/access_keys/id/storage` cannot locate the specified access key. **Workaround:** Submit updated storage specifications as a PUT request to `/access_keys/id`.

NODE-257 - Reports sometimes fail if the Node API temporarily reports an impossibly large value for `bytes_transferred`.

NODE-236 - Transfers with a status of "waiting" cannot be canceled.

NODE-231 - When a node-to-node transfer fails due to a transfer authentication error, the `GET /ops/transfers` response does not provide error information.

NODE-139 - The `--token-key-length` option in `asnodeadmin` allows invalid token key lengths.

NODE-137 - A Node API `/ops/transfers` call reports the incorrect values for `files_completed` and `files_failed`.

#33206 - `/ops/transfers` might briefly report pending transfers as `failed` when transfers are retried.

#32669 - When a directory is symbolically linked from a subdirectory, it does not appear in the search result for a `/files/search` request in the Node API.

Watchfolder and Aspera Watch Service

AC-517 - Pull Watch Folders are not visible in IBM Aspera Console because it uses an older version of the Watch Folder API.

WAT-758 - The transfer token that is used for pull Watch Folders expires and is not automatically replaced, causing transfers to error. **Workaround:** Restart (disable and enable) the Aspera Watch Folder service (asperawatchfolderd) that is associated with the Watch Folder user.

WAT-567 - A Watch Folder configured for growing files reports a "Healthy" state and shows bytes are written at the destination despite having an invalid password and no transfer occurring.

WAT-559 - Watchd allows users to create a watch on the root folder, which can overload the Redis database and cause Watchd to coredump. (CIM-662)

WAT-554 - Due to changes in the way watches are managed as of 3.8.0, the entire watch hierarchy is retransferred after upgrade unless one of the following actions is taken to prepare your system:

1. Archive files in the source directory before upgrade. This prevents the Watch Folder Service from considering all files in the source as new files and retransferring them.
2. Update the configuration of existing Watch Folders to set `"overwrite"` to `NEVER`. After upgrade, Watch Folders only transfers files that do not exist at the target. Once the first drops after upgrade complete, you can reset `"overwrite"` to your preferred setting.

WAT-501 - Some `ascp` sessions started by a Watch Folder may not stop running after synchronization is complete when many (50) large (1000 files of 2 KB to 1 MB) Watchfolders are started at the same time.

WAT-314 - `asperawatchfolderd` must be running in order to delete a Watch Folder.

WAT-246 - [Mac OS X] Watches cannot be created on symlinked directories.

WAT-174 - Watch Folders uses excessive memory when it watches 10 million files.

WAT-159 - If one file in a Watch Folder transfer fails or a drop is aborted, the other files in the package are reported as aborted but `ascp` is not stopped and the transfer continues.

Sync

Async on AIX, Solaris, Mac OSX, does not support continuous PUSH or BIDI modes.

ES-455 - A continuous Sync session might log several error messages stating "add watch failed" because it tries to access the service when one is already in use. This issue does not affect file synchronization. (CIM-806)

WAT-759 - In continuous synchronization mode, the UID and GID are not preserved even when `--preserve-uid` and `--preserve-gid` are used.

WAT-742 - When filelocks are enabled on the server and a push or bidi Sync session is run with basic token authentication, a local file deletion is not propagated to the server.

WAT-737 - Sync can hang on a fatal error, such as if the disk with the Sync database runs out of space, rather than aborting the session. (CIM-1075)

WAT-715 - The initial synchronization of directories in object storage is very slow.

WAT-700/ES-92 - Sync reports incorrect counts for 'deleted_paths', 'deleted_bytes', and 'cumulative_deleted_bytes'.

WAT-644 - If the local directory to synchronize is a symlink, the Sync session succeeds the first time but then fails the second time with the error, "ERROR: Error reading from peer (disconnected)". **Workaround:** Replace the symlink with the full path. (CIM-897)

WAT-629 - When a remote docroot is a URL, including`file://`, then `async_db_dir` must be set in `aspera.conf`.

WAT-594 - During a Sync session, if `ascp` fails to transfer a file, Sync keeps the file as pending rather than as errored and the session does not stop. (CIM-814)

WAT-589 (#13645) - When a directory is renamed during transfer, Sync continues running and never completes.

WAT-557 - A continuous Sync push that is run with the `--scan-dir-rename` option does not synchronize files if the directory is created and then renamed after the Sync session has started.

WAT-550 (#29686) - A continuous Sync push to S3 storage does not update the object in S3 when the source file is renamed or deleted while it is transferred.

WAT-465 - Sync hangs following a TCP impairment that produces a libssh2 timeout or error.

WAT-362 (#24812) - If a file's size decreases during a continuous Sync push, the file remains pending and is never synced.

WAT-287 (#32064,#32883) - When syncing a directory in continuous bidi mode, Sync keeps running with one pending file rather than complete and go idle.

WAT-9 - When the `scan-file-rename` option is used with `asperawatchd`, moved files should be detected and renamed at the destination, not deleted and replaced by a transferred, renamed file.

#29038 - Using `overwrite=always` when you sync with cloud storage does not overwrite the file. The default checksum behavior with S3 (as with any cloud storage) is "none". An existing file on S3 is considered identical to the local file when their sizes are equal. Therefore, the file on S3 is not overwritten even when the content of S3 differs from the content of the local file.

#28817 - The Sync log entry for SYNCERROR_DELAY does not include information that describes the file name and path.

#27621 - Hidden, temporary, or transient files, such as temporary files created by Microsoft Office products, can cause Sync to report conflicts.

#25631 - When you transfer from Windows to Mac and use `preserve-acls=native` and `remote-preserve-acls=native`, ACL data are saved as `xattr`. **Workaround:** Do not use the `native` setting when you transfer or sync across platforms.

#20906 - `async` cannot create a watch on an unreadable directory; therefore, it does not get notified when permissions change. In addition, `async` treats an unreadable directory as "skip" rather than reporting an error or conflict.

#20767 - If you use the `-R log dir` from Linux to Windows and there are spaces in the directory path, the path is truncated at the first space in the path.

#19945 - `asyncadmin` creates SHM and WAL files for read-only operations. Once asyncadmin is run as the root, `async` run by the user does not have permission to access the existing SHM and WAL files and thus `async` fails. This issue is due to a bug in SQLite.

#16911 - Characters in the `async` session option that are not preceded by a "`-`" or "`--`" are ignored and no error message is reported. Any session options that are specified (such as `-l` or `-a`) after the string of characters that are not preceded by a "`-`" or "`--`" are also ignored. The session runs using the default values, and does not notify you that the command line settings were ignored.

#13826, #13827, #13833 - [Windows] Limited support for Unicode file names on Windows. If you create a directory with a name containing Unicode characters (for example, Japanese) and then create a file in that directory, the following errors may occur:

1. Running with an `-N` set to a string with non-English characters (such as Japanese) causes an error message.
2. After a sync, the UI displays an inaccurate directory name and path separator.
3. After syncing, using the `asyncadmin -M` option does not allow you to delete the file from the database.

#13761 - If file names contain "\" or new line, `async` transfer fails, causing the internal transfer queue to become full and the synchronization to stall.

Object Storage Support

ES-534 - ALEE licensing connections timeout after 10 seconds, which can disrupt upgrade installations of cloud-based installations of Enterprise Server or Aspera On Demand products (including Shares On Demand). **Workaround:** Edit the ALEE configuration to increase the timeout.

1. Open `/opt/aspera/alee/bin/asperalee-init.sh`.
2. Locate the line in which JVM_OPTIONS are declared, around line 656, and modify the line to read:

```
JVM_OPTIONS="-Xmx64M -Xms8M -Dhttp.connect_timeout=20000 -
Dhttp.socket_timeout=60000 -Dlocback.configurationFile=
```

   This sets the connect timeout to 20 seconds and the socket timeout to 60 seconds.
3. Restart ALEE:

```
$ /opt/aspera/bin/asperalee-init.sh restart
```

4. Restart the Aspera Node service (asperanoded):

```
 service asperanoded restart
```

TRAP-83 - Using the default configuration of the Java Heap size, Trapd might be unable to recover enough memory after a full garbage collection, resulting in an out-of-memory error. **Workaround:** Edit the configuration by opening `/opt/aspera/etc/init.d/asperatrapd_init.sh` and locating the following section:

```
trap_init_start()
{
...
    cdf_get_total_memory
    PROPS="$PROPS -Dsystem.total.memory="$TOTAL_MEMORY""

    MAX_JAVA_MEM=2000
    MIN_JAVA_MEM=512
    if [ $TOTAL_MEMORY -lt 2147483648 ]; then
...
```

Change the value of `MAX_JAVA_MEM` from 2000 to 6000.

TRAP-59 - If an incorrect DNS nameserver is set in `/etc/resolve.conf` and then corrected, TrapD must be restarted for the correct nameserver to be used by TrapD. If TrapD is not restarted, TrapD fails to connect and retries indefinitely. (CIM-469)

TRAP-57 - If a very large file (several TB) upload to AWS S3 is interrupted after more than 1 TB is transferred, resuming the transfer may take hours and the session may close before any data is transferred. (CIM-476)

TRAP-27 - In some cases, stopping Trapd while an `ascp` transfer is still running may cause a restart of Trapd to fail.

TRAP-26 - Sometimes when Trapd is being heavily loaded by many `ascp` transfers, Trap may return a 'No such file or directory' error.

#36067 - Deleting folders from a Limelight directory is slow.

#33214 - Transfers to and from cloud storage using authorization tokens with URIs that do not have a docroot specified are not supported.

PRODUCT SUPPORT

For online support resources for Aspera products, including raising new support tickets, please visit the Aspera Support Portal. Note that you may have an existing account if you contacted the Aspera support team in the past. Before creating a new account, first try setting a password for the email that you use to interact with us. You may also call one of our regional support centers.