

Troubleshooting

Data Delivery System

Important note	3
Users: Unit Admin / Personnel / Researchers.....	4
A. Invitation link invalid.....	4
B. Too many authentication requests in one hour.....	4
C. Web: Invalid username or password.....	5
D. CLI: Failed to authenticate user: Missing or incorrect credentials.....	5
E. Not receiving emails	6
F. Documentation not accessible.....	6
G. Long error message (traceback).....	6
H. Token expires during delivery	6
I. Windows OS: Warning message "Storing the login information locally - please ensure no one else can access the file at ..."	7
J. Permission denied (authentication token) when using the DDS on a func account or similar	7
K. QuotaExceeded.....	7
L. Unrecoverable key error	8
M. ERROR: Internal Server Error	9
N. TooManyBuckets	9
O. Errors occurred during upload.....	9
P. Not possible to change project status (Deadlock).....	9
Data Centre.....	11
A. Invitation link invalid.....	11
B. Too many authentication requests in one hour.....	11
C. Web: Invalid username or password.....	11
D. CLI: Failed to authenticate user: Missing or incorrect credentials.....	12
E. Not receiving emails	12
F. Documentation not accessible.....	12
G. Long error message (traceback).....	13
H. Token expires during delivery	13
I. Windows OS: Warning message "Storing the login information locally - please ensure no one else can access the file at ..."	13
J. Permission denied (authentication token) when using the DDS on a func account or similar	13
K. QuotaExceeded.....	14
L. Unrecoverable key error	15
M. ERROR: Internal Server Error	16

N. TooManyBuckets	16
O. Errors occurred during upload.....	17
P. Not possible to change project status (Deadlock).....	18

Important note

Before contacting the Data Centre for support, **please:**

- **Verify that you have the latest CLI version installed** (if the issue is related to the CLI): <https://pypi.org/project/dds-cli/>
- Check the CLI documentation: https://scilifelabdatacentre.github.io/dds_cli/
- Read the sections in the technical overview relevant to your issue and check the topics below for possible solutions: [Data Delivery System: Technical Overview](#)

If the issue persists, contact datacentre@scilifelab.se and we will get back to you as quickly as possible.

Users: Unit Admin / Personnel / Researchers

If you experience any issues with the DDS, **please look through the sections below** for any similar issues and / or solutions.

If you cannot solve it with the information below, **please:**

1. Verify that you have the latest CLI version installed (if the issue is related to the CLI). Open a terminal window and run `dds --version` and compare the displayed version to the latest one. The latest version can be found at [PyPi](#).
2. Look through the CLI documentation [here](#).
3. Read through the sections in the technical overview relevant to your issue and check the topics below for possible solutions. The Technical Overview can be found on [GitHub](#) or downloaded as a [PDF](#).

If the issue persists, contact the [Data Centre](#) and provide the following information:

- Did the error occur in the web or CLI?
 - Web:
 - What did you attempt to do?
 - When did this message / error appear?
 - Screenshot of the web page with the error.
 - CLI
 - What command did you run? Please copy and paste the command so that we get the exact command.
 - Copy and paste the full output that the terminal displayed after you ran the command.

A. Invitation link invalid

1. Did you receive the invitation email more than 7 days ago?
 - **Yes:** An invitation is only valid for 7 days. Contact the SciLifeLab unit that sent the original invitation and ask them to invite you again.
 - **No:** Something else has gone wrong. This is something that has been reported previously and we are aware of it. We have not yet determined the cause and will look into it as soon as we can. Contact the SciLifeLab unit that sent the original invitation and ask them to:
 1. Remove the invitation with `dds user delete --is-invite`
 2. Invite you again
2. If the new invite still says that it's invalid, contact the Data Centre.

B. Too many authentication requests in one hour

If this message is displayed in the web interface or CLI, the user has attempted to log in or logged in and out more than 10 times within an hour. Please wait an hour and try again.

C. Web: Invalid username or password

Please verify the following:

1. Are you sure you are using the correct username?
 - **Yes:** Move on to step 2
 - **No:** It's currently not possible to reset / change a password. There are three options:
 - If your account has the role Unit Admin or Unit Personnel, ask a colleague to list the users within your unit (`dds user ls`) and check the table for the row with your name. Verify that the username matches the one you are using.
 - If your account has the role Researcher, contact the SciLifeLab unit that invited you to the DDS. A Unit Admin or Unit Personnel role can list the researchers in a specific project: `dds ls --project --users`. They can then check the table for the user and find the correct username.
 - If a Researcher is not yet connected to a project within the DDS, the Researcher should contact the SciLifeLab unit which invited them to the DDS, which should then contact datacentre@scilifelab.se.
2. Are you sure you are using the correct password?
 - **Yes:** Notify the Data Centre.
 - **No:** Try requesting a password reset in the web interface. **IMPORTANT:** If you have access to any projects before the password reset, notify an Unit Admin or Unit Personnel immediately that they need to run the following command: `dds project access fix`. The user running this command needs to have access to the projects in question. This can be seen in the "Access" column when a user does `dds ls` to list the projects.

If you still can not log in, contact the Data Centre and include all steps you have attempted and exactly what is happening and when.

D. CLI: Failed to authenticate user: Missing or incorrect credentials

Follow the same steps as in [C. Web: Invalid username or password](#) above.

E. Not receiving emails

KI seems to have a spam filter which makes receiving emails very slow in some cases. The email should show up at some point, but it may take some time.

If you have an email that you are certain does not go through the KI spam filter, first verify that you are checking the correct email address, and then contact the Data Centre.

F. Documentation not accessible

You can download the documentation as a PDF:

1. Go to: https://github.com/ScilifelabDataCentre/dds_cli/releases/latest
2. Scroll down to the “Assets” section
3. Click on the **dds_cli_user_manual.pdf** and the download should automatically start

Notify the Data Centre that the documentation page is down so that we can look into it.

G. Long error message (traceback)

If you get a long error message after running the CLI, report this to datacentre@scilifelab.se. Include the error message in the email. If the error is related to the DDS, an understandable message should always be displayed and it's therefore important that we get information so that we can change it.

H. Token expires during delivery

Unfortunately we cannot do anything about this at this time. Remember to authenticate yourself before every large delivery. Reauthenticate yourself and then upload or download again. We will look into this issue if and when it arises, but not before the beginning of autumn 2022.

I. Windows OS: Warning message "Storing the login information locally - please ensure no one else can access the file at ..."

Since the token file permissions check does not work on Windows OS, we are warning the users to be extra cautious in keeping this file secure. The dds client should be fully functional despite this warning.

J. Permission denied (authentication token) when using the DDS on a func account or similar

- The default setting is that the authenticated token generated by `dds auth login` has permission 600. This means read and write permissions for the specific unix user that is running the command.

Running the `dds auth login` command with the option `--allow-group` will allow users from the same unix group to use the resulting token file.

- The permissions of tokens cannot be changed after the tokens are established. If you began an authenticated session without the use of the `--allow-group` option, but want to use it in a new session, use `dds auth logout` to end the current session. Then use the `--allow-group` option and start a new session. This also applies to the reverse.
- Not recommended for users with role Researcher, use with care.
- If this does not work for some reason, we will not look into it before summer.

K. QuotaExceeded

The error could look something like this:

```
raise error_class(parsed_response, operation_name)
        botocore.exceptions.ClientError: An error occurred
(QuotaExceeded) when calling the UploadPart operation: Unknown
```

This indicates that the cloud storage location has a specific limit for your unit and that it has been exceeded. This should be an easy fix. Contact the Data Centre, inform them of the error (remember to include the full error message) and tell them the size of the data you are attempting to upload.

L. Unrecoverable key error

The most likely reason for a key related error is that you do not have access to the project you are trying to access. If you get an error message containing something similar to “Unrecoverable key error”, please go through the following steps:

1. Run `dds ls`

- Find the row of the project you were trying to access or use
- Check the “Access” column for that row - does it contain a red cross or a green check mark?
 - **Green check:** You have access to the project. This is not the issue.
 - Does the current project status allow for the action you are trying to perform? Please look at the technical overview and documentation. These are linked at the start of this document.
 - **Yes:** Go to step 2.
 - **No:** This is most likely the issue. Make sure the project status allows for the current action. Please report the error message, what you were trying to do, the exact command, what steps you have performed and any other information you may have, and we will look into this.
 - **Red cross:** You do not have access to the project. **Important note:** If no one else has access to the project, please note that the Data Centre cannot help you. As Super Admins in the DDS, we do not have access to any of your data and we cannot restore your access. **Please read the technical overview**, the link is displayed at delivery.scilifelab.se and also when running the CLI commands.
 - **Researcher:** You need to contact all SciLifeLab units responsible for the projects you are involved in in the DDS. They need to run `dds project access fix` for you. Try again after that is done.
 - **Unit Admin / Personnel:** You need to contact a colleague with access to the projects you are trying to use. They need to run `dds project access fix` for you. Try again after that is done.

2. If you have checked the project status, the project access, the access is fixed, or you have not been able to identify the issue, please contact the Data Centre and include the full error message, the exact command you are running.

M. ERROR: Internal Server Error

Contact datacentre@scilifelab.se and provide the information listed in the red box above.

N. TooManyBuckets

Safespring has a maximum number of buckets per unit, however this number is set quite high and therefore this should not happen. If it does happen, contact the Data Centre and we will fix this. You can also check the active projects and see if there is one that is an active project that can be archived, for example. Be careful with this and do not delete / archive (including abort) projects which you are not 100% sure that they are ready to be deleted / archived. This is not reversible.

O. Errors occurred during upload

When running **dds data put**, if there are issues, the following is a possible output:

```
Errors occurred during upload.
```

```
If you wish to retry the upload, re-run the `dds data put` command again,  
specifying the same options as you did now. To also overwrite the files that  
were uploaded, also add the `--overwrite` flag at the end of the command.
```

```
See /code/DataDelivery_2022-06-30_14-17-18/logs/dds_failed_delivery.json for  
more information.
```

In the future, the Data Centre will need this file to fix it, however, due to the reduced staff during July, we ask that you simply inform us of the issue and attempt the upload again.

P. Not possible to change project status (Deadlock)

A while back, someone commented that they were having issues with changing the status of a project. It turned out that the status had actually been changed, so before contacting the Data Centre, check the project status and see if it has changed despite the error.

Data Centre

If there are any issues that you are not able to solve, create a card in the Jira board, you should have access. Include the *exact* command that was run and any tracebacks etc. Provide a description if you have a guess (or know) to what is causing it.

A. Invitation link invalid

There have been reports that invited users are trying to use the invitation links that are sent via email and the web interface indicating that the link is invalid. The only thing we can do at this point is to ask them to follow the instructions in the **Invitation link invalid** section in the **User** part of this document, and / or run the following commands:

1. Delete the invite if it exists: `dds user delete --is-invite`
2. Invite them again. If this still does not work, try another email address.

In all cases so far, these two steps have worked. If it does not, create a card on the Jira board. We cannot do anything during summer aside from trying again and again. If you feel like it and have time, you can of course try to reproduce the error and figure out what's going on. Of course, do this with the local setups of the DDS repositories.

B. Too many authentication requests in one hour

If this message is displayed in the web interface or CLI, the user has attempted to log in or logged in and out more than 10 times within an hour. Ask the user to wait for an hour and try again later.

C. Web: Invalid username or password

If a user cannot log in to the web interface, ask them to follow the steps in Users: Unit Admin / Personnel / Researchers, subsection [C. Web: Invalid username or password](#). If they have already done this, check that they have provided a screenshot of the issue or an explanation of the message appearing. A possibility is that the web is not letting them in because they have attempted to log in more than 10 times in an hour. If that's the case, tell them to try again later. If it's not the case, there's not much you can do. Offer to delete their account and invite them again. It's better if a Unit Admin or Personnel handles the new invite, but if you do, remember that you

cannot invite Researchers to specific projects, only to the DDS in general and that you need to specify the unit public ID if you want to invite a Unit Personnel or Admin. However, if there are active projects in the unit, they will still not have access, so they still need to ask someone within their unit with access to the projects, for renewal of the project access.

D. CLI: Failed to authenticate user: Missing or incorrect credentials

Follow the same steps as in [C. Web: Invalid username or password](#) above. Make sure that they have provided the traceback if there is one. As in the above section, the CLI blocks authentication attempts after 10 times in an hour.

E. Not receiving emails

Check the information in the User section earlier in the document regarding this specific topic. If they contact us, the email is correct and it's not an email address connected to the KI spam filter, create a card in the Jira board and we'll get to it after summer. Also create an issue in the sysadmin repository so that they can check that it's not an issue on our cluster.

F. Documentation not accessible

1. Notify the users that they can download the documentation as a PDF. Instructions:
 - a. Go to: https://github.com/ScilifelabDataCentre/dds_cli/releases/latest
 - b. Scroll down to the "Assets" section
 - c. Click on the **dds_cli_user_manual.pdf** and the download should automatically start
2. Create an issue in the sysadmin repository. If you have time: Try to figure it out together with the sysadmins. If they are away and / or cannot help, or you just don't have time, then ignore this for now. They have access to the documentation via the latest release and it's not a huge priority.

G. Long error message (traceback)

1. Make sure they have upgraded the CLI to the latest version. If they have, or the upgrade does not help, move on to 2.
2. Make sure they have provided the traceback
3. Look through the traceback. There could be some uncaught error or similar in the CLI, most often this is not caused by the backend, and most likely this is not something that can wait. If that's the case, create a card in Jira - see [blue](#) box above.

H. Token expires during delivery

We cannot do anything about this. It's on the todo list. No need to add a card about this, but please add a comment that this has happened:

<https://scilifelab.atlassian.net/jira/software/projects/DDS/boards/13/backlog?selectedIssue=DDS-1173>

I. Windows OS: Warning message "Storing the login information locally - please ensure no one else can access the file at ..."

Since the token file permissions check does not work on Windows OS, we are warning the users to be extra cautious in keeping this file secure. The dds client should be fully functional despite this warning.

J. Permission denied (authentication token) when using the DDS on a func account or similar

Basic information:

- The default setting is that the authenticated token generated by `dds auth login` has permission 600. This means read and write permissions for the specific unix user that is running the command.
- Running the `dds auth login` command with the option `--allow-group` will allow users from the same unix group to use the resulting token file.

- The permissions of tokens cannot be changed after the tokens are established. If you began an authenticated session without the use of the `--allow-group` option, but want to use it in a new session, use `dds auth logout` to end the current session. Then use the `--allow-group` option and start a new session. This also applies to the reverse.
- Not recommended for users with role Researcher, use with care.
- If this does not work for some reason, we will not look into it before summer. As long as the `dds auth login` command works without the additional permissions option, that is what the users will have to work with for now.

Background / additional information:

Information from NGI and explanation to our (possibly temporary) solution: On Miarka, the deliveries are done through a web service which is run as a special user (func account) and the access for that user is heavily restricted. Usually the bioinformaticians that perform the data deliveries do not have access to that account and instead the delivery is done through API calls to the service. When starting the integration testing, their idea for the delivery with the DDS was that a user would generate an authentication token with their account on Miarka, place it in a folder that is accessible to both them and the func account, and then tell the DDS, run by the func account, to use that authentication token.

When performing the authentication, the DDS CLI originally collected the token from the API and saved that in a file with permission 600: `-rw-----` (only read and write for that specific user). Because of the issue mentioned above, there was a suggestion to change this to allow permission 660: `-rw-rw----` (read and write for specific user and group). In the end, we have now added the option `--allow-group` as a flag to the `dds auth login` command so that they can (should be able to but as of writing this it has not yet been tested) allow the func account to use the authenticated token for deliveries with the DDS. However, the permissions are now set to 640: `-rw-r-----` (read and write permissions for the user that is using the command and only read permission for a group). This is a conscious choice since the func account should only need to read the token file and should not be able to edit it, etc.

We have discussed the potential problems with this and we will look into it again when we can. For the time being we needed the DDS to be usable and therefore this is implemented. After summer we will look into this again at some point and it is possible that this will change in some way, we do not yet know if and in that case how.

K. QuotaExceeded

The error could end with something like this:

```
raise error_class(parsed_response, operation_name)
        botocore.exceptions.ClientError: An error occurred
(QuotaExceeded) when calling the UploadPart operation: Unknown
```

Hopefully we should be catching these and displaying something more user friendly, but if the error is not caught, then do the following:

1. Check with the user (if they have not already included the information in their email) which unit they have an account within and the size of the data that they are attempting to upload.
2. Contact safespring (will post the email to them and other important information in the dds-development channel on slack) and ask them to increase the quota for the specific project. It should currently be set to 300TB for SNP&SEQ and UGC and 500TB for NCI Stockholm. I have asked them if they will deliver more during the summer but it will be pilot deliveries so it should be fine. It doesn't matter which value you choose when you ask Safespring to increase it, it's just there as a precaution so that data is not uploaded without someone's knowledge. This is not something that we can affect, it's on Safesprings side.
3. When the quota has been changed, inform the users that they can try the upload again.

L. Unrecoverable key error

The most likely reason for a key related error is that the user does not have access to the project they are trying to access, and that there is an uncaught error somewhere. Add it as a card to the Jira board.

1. Ask the user to perform the steps in the section [Unrecoverable key error](#) in the **User** part earlier in this document. If they have done this, check if the user is active or not first: `dds user ls`. This should display all users and the right-most column ("Active") shows if they are active (green check mark) or not (red cross). If they are inactive, then that's the issue. There shouldn't be a possibility of this causing this type of error, report it as a bug in the Jira board. Inform the user that someone in their unit should activate them.
2. Ask them to run the commands as specified in the **Unrecoverable key error** section earlier in the document and for them to send you the output of those commands. Does the current project status allow for the command they are trying to run? Does it say that they have access to the project?
3. Ask them to create a new project and to do the same command with that one. If it works, the issue is with that specific project and this should be reported as a bug in the Jira board.

If, when running the `dds project access fix` commands, the users get error messages, it's most likely that the user does not have access to the projects. If no one else has access to the project either, we cannot help. This information is clearly explained in the technical overview: As Super Admins in the DDS, we do not have access to any of the data and we cannot restore any

access. They will need to create a completely new project and possibly perform the delivery a second time.

M. ERROR: Internal Server Error

The most likely reason for an Internal Server Error is an uncaught exception in the backend, often something database related. If someone contacts you regarding an Internal Server Error, begin with making sure they have provided the information mentioned in the **red box** in the beginning of the **Users** section. When they have done this, look through the traceback.

Most likely we cannot do anything about this during the summer and they will need to wait until August. If you cannot find the issue in the traceback, get the logs from the backend, either if you have access to the cluster and know how to handle it or create an issue in the sysadmin repository (<https://github.com/ScilifelabDataCentre/sysadmin/issues>) and ask for the log to be sent in slack to you. The log should not be posted in github just in case of the logs showing anything that shouldn't be public information (this shouldn't happen but it's a precaution).

When **creating an issue** in the sysadmin repository:

- Title: "DDS: get log from production instance"
- Leave a comment: Ask for the log in the DDS backend around the specific time point that the error occurred and write that the error code was a 500.
- Label: Help wanted

Try to figure out what's happening. If you cannot figure out what the issue is or if you know what the issue is but there is nothing you can do, create a card in the Jira backlog. Add an explanation if you know what the issue is and include the traceback. It will have to wait until August.

N. TooManyBuckets

Safespring has a maximum number of buckets per unit, however this number is set quite high and therefore this should not happen. If it does happen, it should only be possible when a user is creating a project. It's also possible that this is the cause of a failed project creation, so if a project cannot be created and there is a questionable error message displayed, check with the sysadmins for the log and see if the bucket could be created. To increase the number of allowed buckets, contact Safespring and ask them to increase the number of allowed buckets in the affected

safespring project, listed and pinned in the **dds-development** channel on Slack. After this, the users can attempt creating a project again.

O. Errors occurred during upload

The message from the CLI could be something like this:

```
Errors occurred during upload.
```

```
If you wish to retry the upload, re-run the `dds data put` command again,
specifying the same options as you did now. To also overwrite the files that
were uploaded, also add the `--overwrite` flag at the end of the command.
```

```
See /code/DataDelivery_2022-06-30_14-17-18/logs/dds_failed_delivery.json for
more information.
```

Note: Normally we would need to do the following, but as is noted in the section in the User part above, **they can simply perform the upload again during July**. This has also not happened yet apart from during the testing phase, but there's a first time for everything.

The json file does not contain any sensitive keys etc, but it does contain a file path which in itself may contain sensitive information. Therefore, we currently have 3 separate folders in nextcloud and I have shared the links and passwords to those DC members that should have access during summer.

If a user contacts us with a upload issue that has generated the above mentioned file, do the following:

1. Ask them to send the exact CLI command that they ran
2. Give them the nextcloud link and password corresponding to the unit that they are employed at; If someone at NGI Stockholm contacts you with this specific issue, send the link and password underneath the point in slack saying "NGI Stockholm", and so on.
3. Ask them to upload the json file to the folder that they can access with that link and password.
4. When they have done that, a sysadmin should also use the link and password
5. The sysadmin should download that file and run the following command in the cluster, in the DDS backend: `flask update-uploaded-file` while specifying the project that the user has used in the command emailed to us, and the path to the file as the options. This command goes through the file and checks if the file has been uploaded but has not been added to the database. If so, the backend adds the file information to the database which should mean that the project contents should now be accessible for download.
6. The sysadmin should delete the json file immediately after the command is done and the file should be removed from the nextcloud folder.

Make sure to do this as soon as possible since it's possible that the upload has in fact been successful but the information has not been added to the database. This means that the data is located in the cloud and will take up space there, but you cannot access it since it is not recorded in the database.

P. Not possible to change project status (Deadlock)

A while back, someone commented that they were having issues with changing the status of a project. It turned out that the status had actually been changed, but that there was a deadlock happening somewhere in the backend. This is already in the backlog and there's an ongoing draft PR to handle it. Ask the user to check the project status if they haven't already, it may be the status they were trying to change to. Otherwise, at this point the only thing we can do is ask them to wait for a bit and then try again, and tell them that we know this may happen and that we are looking into it.

Q. Lost access to 2FA Authenticator App

If you have configured the Two Factor Authentication of your DDS account to use an authenticator app, but you have lost access to it (e.g. due to a broken or lost device), the DataCentre can deactivate the configuration in order to let you authenticate using the default email option. After this you can choose to activate the authenticator app method again.

- **Researcher role:** Please contact a SciLifeLab unit responsible for one of your ongoing delivery projects and tell them you need a reset of the 2FA method.
- **Unit Admin / Personnel:** Please contact Data Centre and ask for a reset of the 2FA method. Inform them of the username and email address of the affected account.