Nava Certus

Version 1.1

2013

Product Installation

&

Administration Guide

http://www.navasolutions.com

Table of Contents

About This Document

This guide provides an introduction to Nava Certus and contains information about installing and configuring the product. You should read this document serially in order to gain maximum benefit from its content.

To install and configure Nava Certus, you should have working knowledge of the following:

- Windows administrative tasks
- Google Drive
- Amazon Simple Storage Service
- TCL scripting knowledge is a plus

What's in This Guide

Section	Description
Introduction	This section provides an overview of Nava Certus and introduces you to the general concepts behind it.
Installation	This section covers the installation procedure for Nava Certus. Issues such as hardware/software requirements and pre-installation tasks are explained.
Using Nava Certus	This section walks you through several scenarios of using Nava Certus.

Licensing

Purchase License

When first obtaining Nava Certus, you will have a 5 day trial license. You will be able to create and configure migration jobs and run them for a total limit of 1 GB. To download a free version of Nava Certus please visit our website.

Nava Certus is licensed per GBs of data migrated. In order to receive a license for the application you need to follow the steps below after downloading Nava Certus:

1. Evaluate the overall amount of data you are planning to migrate from each source.
2. Purchase amounts of GBs desired by either:
    - Visiting Nava Certus website
    - Nava Certus licensing GUI

    In a few minutes you will receive an Email with the license file -which is generated according to your order - attached.

License Nava Certus

In order to activate the application or add additional license you can either:

- Place the license file attached to the respective Email you received to the "licenses" folder located in Nava Certus installation directory.

- Open the Nava Certus GUI. Select **Enter License** from the Nava Certus license window which pops up. Enter the license key and click **Apply**. Note that this window only pops up when the license is in evaluation mode or is expired.

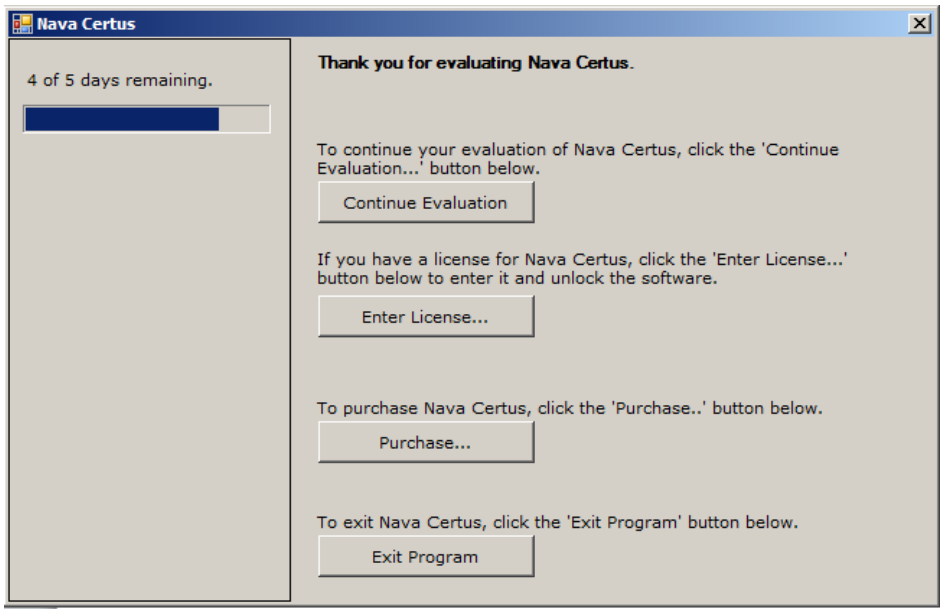


Figure 1 – License Nava Certus

After licensing Nava Certus you can view the license details by clicking the **About** button on the GUI.

You can add as many additional licenses to Nava Certus as you wish. Nava Certus license will be the cumulative of the licenses you have purchased over time.

Support

In order to get answers to questions that may arise while using Nava Certus in production, please send your question by Email to support@navasolutions.com.

To expedite troubleshooting a problem related to Nava Certus, please provide (if applicable) the following information in your e-mail:

- Detailed description of the problem along with steps to reproduce it.
- Nava Certus event logs and Nava Certus log files.
- Samples of specific problematic files (to be migrated).
- Your contact information (e-mail and telephone) along with the best time to reach you (please include time zone) in case further clarification is required.

Introduction

Overview of Nava Certus

Nava Certus is a data migration application. Nava Certus (NC) supports migration from various systems to various cloud platforms.

Nava Certus consists of a client service which performs the migration job and a client GUI which allows the user to configure the service and monitor the migration tasks. Each migration task is called a Job.

It is highly recommended to read and understand the properties of each of the sources and destinations you are planning to migrate from/to.

Sources

- *File system* source – Nava Certus will migrate files from the specified network storage, NTFS File System or local storage to the selected destination.
- *Google drive* source – Nava Certus will migrate files from the specified Google account to the selected destination.

Destinations

- *Google Drive (Centralized)* migration type will migrate the selected source to a centralized (single) Google drive account and will replicate the permissions that user/groups are granted on each file, at the destination. Using a preconfigured mapping file, NC will map the file permissions along with migrating the files to respective Google drives and we replicate the folder structure there.
- *Google Drive (Distributed)* migration type will migrate the selected source to one or more Google drives while distributing each file to its owner, and will replicate the permissions at the destination. Using a preconfigured mapping file, NC will migrate the file(s) only to the Google drive of the user who is the Owner of that file and will replicating the folder tree structure at the destination as well.
  Note that Distributed migration from Google Drive Source is not supported.
- *Amazon S3* migration type will migrate the source to a centralized (single) destination Amazon S3 bucket while migrating the permissions other users might have on the file as well. Using a preconfigured user mapping file, NC will migrate the file(s) and will replicate the folder tree structure at the destination.

Note: The Amazon S3 account Email address should be the primary Amazon account access. Otherwise the authentication will not pass and the migration will not take place.

Nava Certus Components

Client service

Client service is a windows service controlled over the network by HTTP calls. This service manages jobs and their statuses. There can be any number of jobs in various states controlled by the service. The service runs persistently on the client computer until the migration is over.

Client GUI

The graphical user interface allows the user to control the migration by starting/stopping migration jobs and adjusting configuration. In the Client GUI jobs are displayed in a grid on the right side of the NC window. User can manipulate migration jobs either by:

- Using the menu options or
- By the dockable NC Console window, located at the bottom of the screen with integrated TCL interpreter.

Authorization and Authentication

All requests to the destination APIs must be authorized by an authenticated user. Each migration job has its own authorization method. Authorization depends on the migration source and destination.

- Google Drive job - Before this migration type can be started, NC job should be authorized access. Google service accounts authorization is used in order to access multiple user's drives without direct interaction with the user.

Note: It is recommended for the account which will authorize the NC job to be the administrator of the organization's Google domain; otherwise Full Access permissions might not be set fully. It is recommended for all of the user accounts and the authorized account to be in the same domain for the Full Access permissions to be set fully.

- Google Drive (distributed) – Before this migration job can be started, the organization's Google domain administrator should authenticate the Nava Certus application using the OAuth key protocol.
  The following Client Name should be added as value to the **Client Name** field:

  - 274305349877-tuvj4n737f89plceeabd6sasvs52eti6.apps.googleusercontent.com

  The following API Scopes should be added to the **API Scopes** field:

    - https://www.googleapis.com/auth/drive
    - https://www.googleapis.com/auth/drive.file
    - https://www.googleapis.com/auth/drive.metadata.readonly
    - https://www.googleapis.com/auth/drive.readonly

- Amazon S3 – Before migration job can be started, Nava Certus job should be authorized access to the destination Amazon S3 bucket. The Amazon AWS Authentication mechanism is used to authorize the application. Target bucket's user needs to provide the Amazon "Access Key Id" and "Secret Key Access Id" when configuring the migration job.

Installation

Prerequisites

Hardware Prerequisites

Nava Certus does not require specific hardware specifications.

Software Prerequisites

Below are the software prerequisite and recommendation for Nava Certus:

- Microsoft .Net Framework 4.0 or higher

Pre-Installation Tasks

Service Account

In order for Nava Certus windows service to run, minimum rights required to run a windows service as a domain account should be granted to the user which will run the Nava Certus service.

It is recommended to authorize all migration jobs with the organization's Google domain account.

Create Folder Structure to House Nava Certus Files

Create a folder named NavaCertus and two subfolders named Log and Mapping such as:

- C:\ NavaCertus\Log
- C:\ NavaCertus\Mapping

Note that the naming of the folder structure can be arbitrary as long as the user understands which name corresponds with the appropriate folder containing the relevant files.

Installing Nava Certus

Obtain the executable installation file and save it to the computer where the component will run. Double-click the corresponding Setup.exe file to start the application wizard. You will be prompted to install the following prerequisite component, if you are missing it.

- Microsoft .Net Framework 4.0

Follow the installation steps. As soon as the components are installed, the corresponding Setup.msi will be run and Nava Certus installation will begin.

The steps to install Nava Certus are fairly simple. To do so:

1. Obtain the executable installation file and save it to the computer where Nava Certus will run. Double-click the file to start the application wizard.

2. On the first installation page that appears click **Next.**

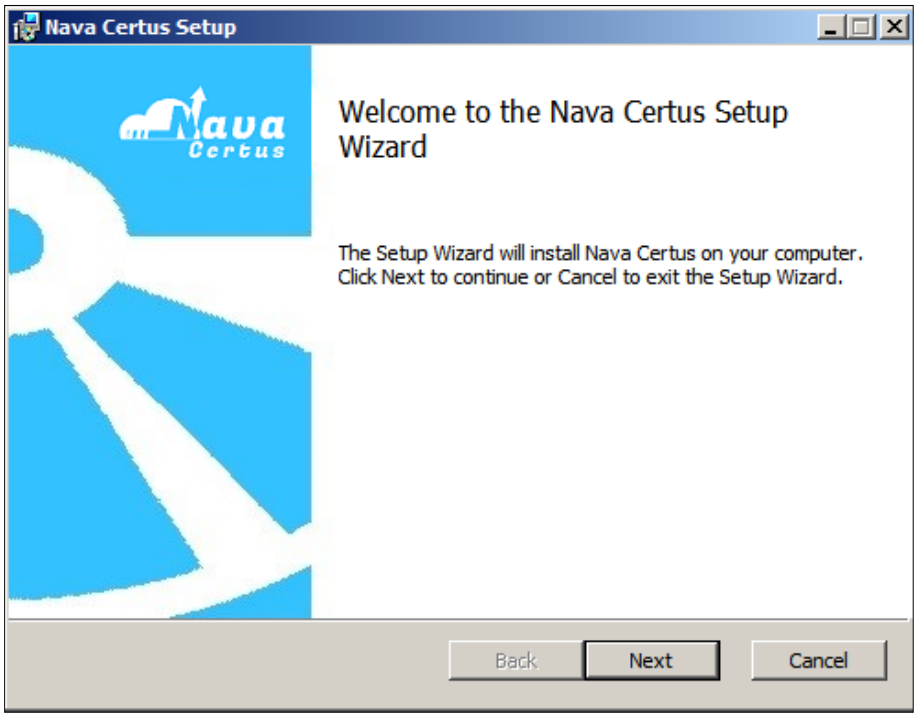


Figure 2 – Nava Certus Setup

3. In the **End-User License Agreement** page read the Nava Certus End User License Agreement carefully. Check "I accept the terms in the license agreement" checkbox if you agree to the terms; and then click **Next**.
4. From the feature-box, select the Enter "Entire feature will be installed on local hard drive" option.
5. Click **Disk Usage** in order to view the free space available on your hard drive.
6. Click **Browse** and change the location of the installation.
   The default folder location is C:\Program Files (x86)\Nava Solutions\Nava Certus\.
   To find another location, click **Change** and select another directory. Click **Next**.
7. On the **Ready to Install Nava Certus** window click **Install** in order to begin the installation.
   After a few moments the installation completion window will appear confirming the success of the installation. Click **Finish**.

You have successfully installed NC. As soon as the application is installed, the **Nava Certus** windows service will start automatically.

Using Nava Certus

Once Nava Certus is installed, open the client GUI by clicking **Start**, then point to **Programs**, **Nava Certus** and click **Nava Certus UI**. The Nava Certus user interface will appear. NC is also accessible through the **Nava Certus UI** desktop shortcut.

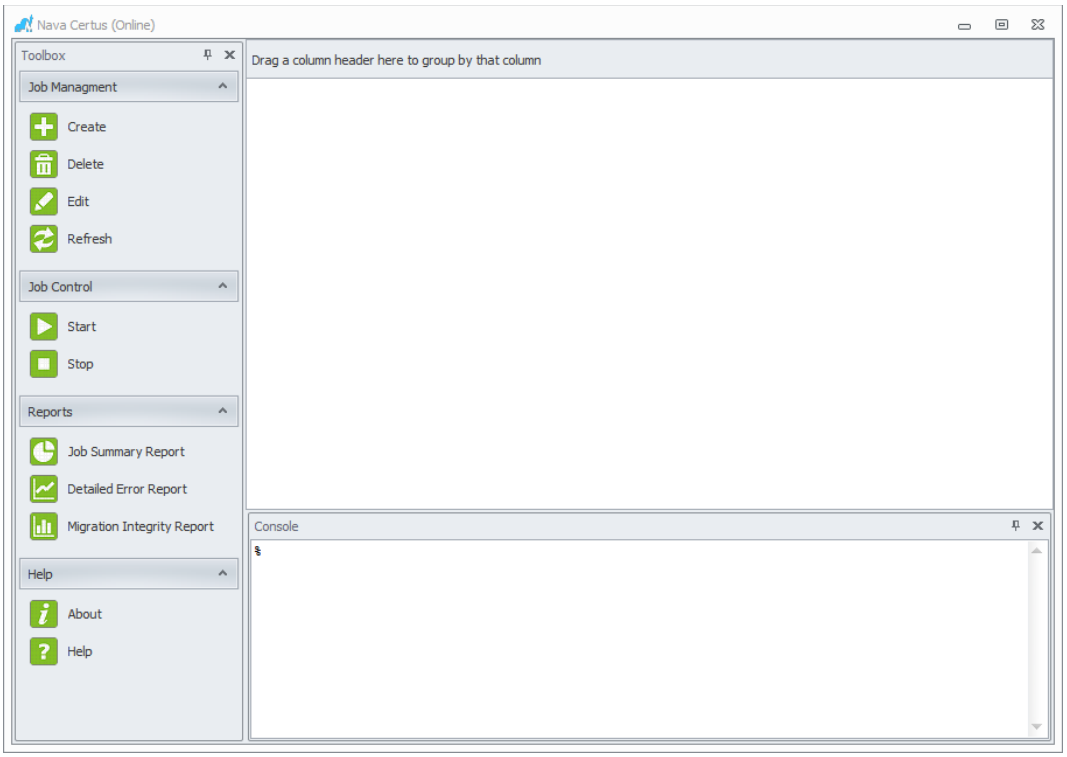


Figure 3 – Nava Certus Client GUI

File Migration Job

From the Nava Certus GUI you can do the following operations with jobs:

- *Create* – create a migration job.
- *Delete* – delete a migration job. Note that when deleting the job, the log file or mapping CSV file associated with the job file will not be deleted.
- *Edit* – edit the job and change job configurations. Note that if the job is stopped manually and is not finished yet, some features will not be editable.
- *Refresh* – refresh the GUI window where jobs reside.
- *Start/Stop* – start or stop a job.
- View different types of reports for each job.

Through GUI

In order to perform a migration job you first need to create and configure one. To do so you should click **Create** from the GUI. The **Job Configuration** window will open.

General tab

You can configure settings which are common to all job types.

Job Configuration – configure essential job settings:

- **Job name** - specify a unique job name.
- **Job description** (optional) - write a short text describing the job(not mandatory)
- **Thread Count** - Thread Count controls the number of items concurrently migrated per job. Each job will run Thread Count number of items in parallel, each with its own Source, DB and Destination. In addition, each Thread will require a certain amount of memory, dependent on the item size. As such, the Thread Count is perhaps the most important global configuration that may affect NC and the system at large.
- **Retry Count** – specify the number of times you want the application to retry migrating a failed item. If the item still cannot be migrated after the specified number of retries, it will be marked as failed.
- **Start Automatically** – set the value to **True**, if you want the job to start as soon as Nava Certus windows service is started.
  Note that the job will not start yet when you finish configuring the job in case you set the value to True.
  Set the value to **False**, if you do not want the job to begin simultaneously with the service start.
- **Reprocess Failures** –if set to True, failed items will be reprocessed.

Note: If the task status is "Failed" or "Finished", it will not start unless you set the reprocessing value to True.

Note: If the task status is "Finished" and reprocessing is set to True, the failed items will be reprocessed first and then the task will continue processing the new items.

Log Configuration – configure logging related settings:

- **Log File** – specify a location and a name for the job log file to be created.
- **Log Level** – from the drop-down list, select the level you wish to assign to the event log. Choose from **Error**, **Warning**, **Info** and **Debug**.

Email Configuration (optional) – using Email notification, user can be informed if there are long-term errors as no network connectivity, revocation of login token or if the migration performance is below a certain level (items/sec).

- **Email To** – A valid Email address which you want Email notifications to be send to in case there are continuous errors during migration or if the migration rate is low.
- **Failure Notification** – if True, an Email notification will be sent if any failures accrue during the migration. If false, then you would have to configure *Migration Rate* notification.
- **Migration Rate** (items/sec) – an Email notification will be sent if migration rate is below the specified rate.

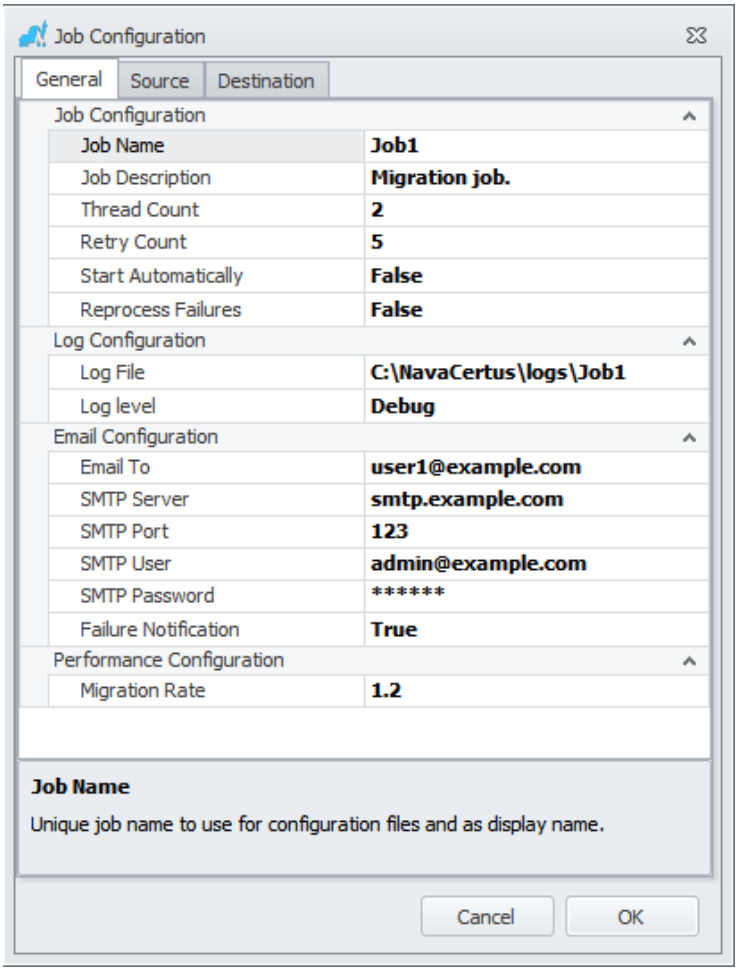


Figure 4 – General tab

Source Tab

You can select and configure all of the source types from this tab. Select the **Source Type** from the drop-down list.

- File System

  Select this source if you want to migrate files from a local or network location to any target.

  - **Root Folder** – select the root source folder that you want the application to migrate the files from. The application will go through sub-folders by default and will migrate the existing data. The folder structure will be replicated in the destination Google drive.

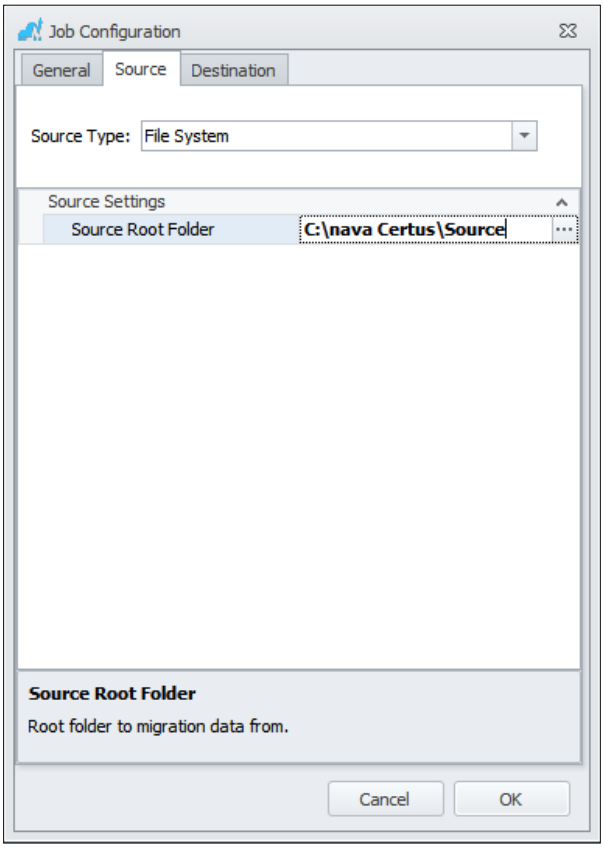


Figure 5 –Source tab – File System

Root folder can either be on the local computer, mapped drive or a network location. In order to migrate from mapped drives, provide the UNC path to the source file.

To be able to migrate the source located on a network or local computer, Nava Certus service account needs to be able to access the source folder:

- If the source folder is located on the local computer

Since the Local user account by default has sufficient permissions on the local folders and files, you do not need to do additional configurations.

- If the source folder is located on network or mapped drive

In case of migrating from network locations, the NC service account needs to be set to an account which has sufficient access to the source files.

A- To do so:

1. Stop all active Nava Certus jobs.
2. Close the NC GUI.
3. On Windows, open **Control Panel**, **Services**.
4. Find **Nava Certus** service and click **Stop**.
5. Right-click on **Nava Certus** service and select **Properties**.
6. Open the **Log On** tab.
7. Select **This Account** and specify a user account which you want to be able to access the source folder.
8. Provide the credentials and save the changes.
9. **Start** the service again.

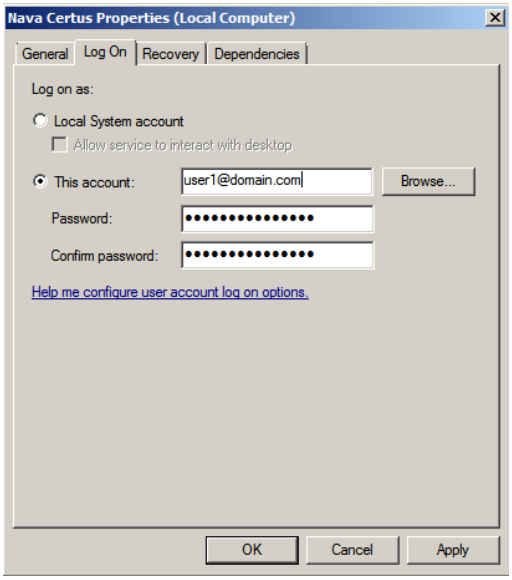


Figure 6 – Nava Certus Service - Properties

B- You granted a certain account sufficient permissions to run the Nava Certus service. You should now grant that same account sufficient permissions so that it will be able to access the source file.

1. Open the network location where the source folder is located.

2. Right-click on the source folder, select **Properties** and navigate to the **Security** tab.
3. Select **Edit** and add the user account you just specified to run the NC service.
4. Click OK to save the changes.
5. Grant **Read** permission to that user and save the changes.

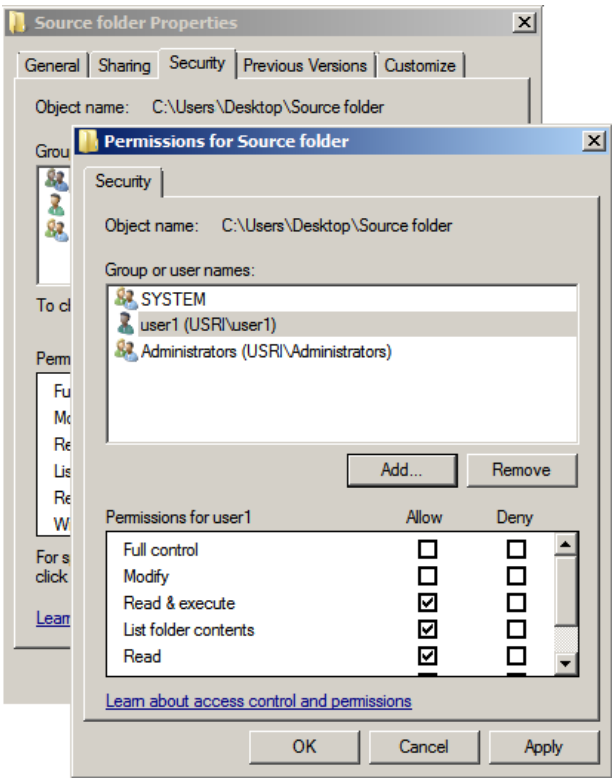


Figure 7 – Source folder – Security Tab

NC will now be able to access the source folder in order to run a migration.

Note: Minimum permissions the NC service account should have on the source folder are: *traverse folder/execute file*, *List folder/read data*, *Read attributes*, *Read extended attributes*, *Read permissions*.

- Google Drive
  - *Source Settings*
    - **Item Status** – from the drop-down menu select the category of items you want to migrate: **All**, **Owned**, **Starred**.

- *Google DOC Export Format*
  - Documents Export Format – select the format you want NC to migrate the Google document in.
  - Spreadsheets Export Format - select the format you want NC to migrate the Google Spreadsheets in.
  - Drawings Export Format - select the format you want NC to migrate the Google Drawings in.
  - Presentations Export Format - select the format you want NC to migrate the Google Presentations in.

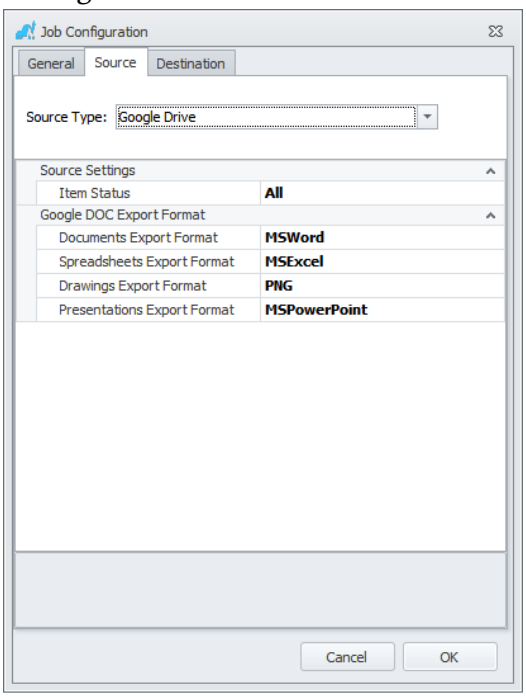


Figure 8 –Source tab – Google Drive

Destination tab

You can select and configure where you want to migrate the data to.

- Google Drive migrations
  - *Misc*
    - Specify a **Mapping File** - The CSV file is used to map the destination Google drive accounts to the existing domain users/groups or source user accounts, which have any type of permission on source files to be migrated. You can provide as many users as you desire in a mapping CSV file.
      - For File System source: The mapping CSV file should be in *"ComputerName/Usr-Name(or GroupName),EmailAddress"* format.

For example if you want to migrate a file on which windows User1or Group1 are granted a level of permission, the CSV file should be configured as follows:

PC-Name/User1,user1@gmail.com
PC-Name/Group1,Group1@gmail.com

- For Google Drive Source: The mapping CSV file should be in *"SourceEmailAddress, DestEmailAddress"* format.

Note: Currently the Special Permission type – Synchronize – mapping is not supported.

Note: You can map each source user to only one destination Email account.

- **Destination Root Folder** (optional) – you can either:
  - Provide a folder name - NC will create a folder with the specified name in the root Google drive and will migrate the source to that folder, while replicating the source folder structure in the newly created folder.
  - Do not provide a folder name – NC will create a default folder with the following format "Nava_Certus_YYYYMMDD-MMHH", and will migrate the source to that folder, while replicating the source folder structure in the newly created folder.

Note: Currently you cannot input an already existing Google drive folder path.

Note: If you provide a folder name which already exists in the Google drive root folder, NC will create another folder by the same name and the source will be migrated in the NC created folder.

- **Convert** – Convert files to corresponding Google DOC format while migrating the source.
- **Email Notification** – Set to **True** if you want to receive Email notifications from Google every time permission is set on a file (i.e. replicating file permissions at destination) by Nava Certus during migration. Set to **false** otherwise.
- **Preserve Modification Date** – If set to true, the "Modified" date of the source file will be migrated along with the item and will be visible at the destination Google Drive

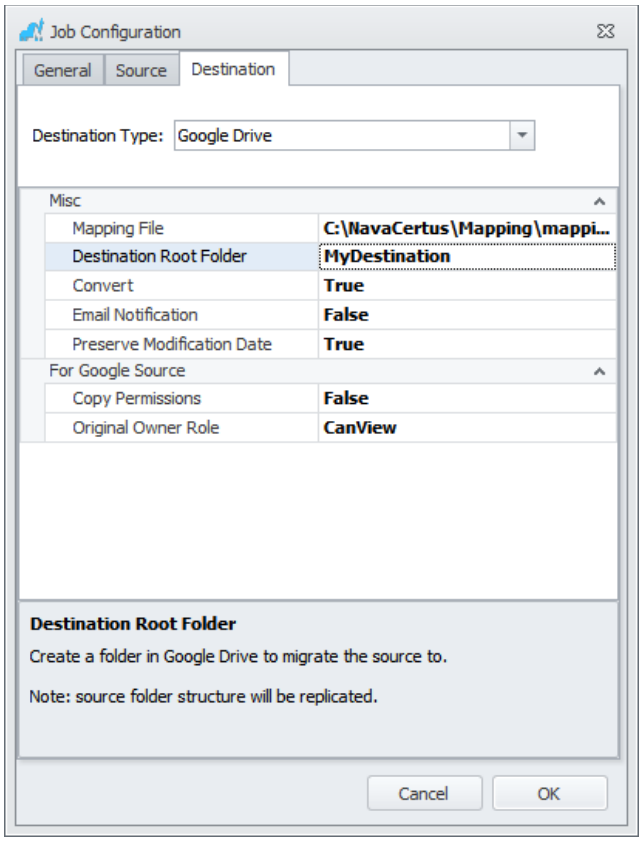


Figure 9 – Destination tab– Google Drive

- *For Google Source*
  - **Copy Permissions** – Copy the same permissions users have on source item to the destination. Note that this option is only useable for intra-domain migration.
  - **Original Owner Role** – The owner of the item in source will be assigned the selected permission at the destination.

After configuring the job, click **OK** to save your configuration. On the Nava Certus GUI the newly created job will appear in the list that is shown. In order to start the job, click **Start** button from the GUI.

In the window that pops-up provide the **Google Email** account of the user who is the owner of the files subjected to be migrated. Provide the **Google Password** of the account you specified above. Click **Allow Access** in order to authorize the job.

Note: If the source is **Google Drive**, two authorization windows will appear. Enter the credentials of the source Google drive in the first authorization window that pops up and enter the destination credentials in the second one.

Note: If the source and destination Google Apps domains are different, no permissions will be mapped.

Note: It is recommended to close all of the source files before starting the migration. Otherwise the opened files will fail to be migrated.

Note: Google drive does not have the same permission model for folder trees as the NTFS file system. If permissions are changed at some level in the folder tree within the drive, the child folders and files will inherit permissions from the parent folder.

Note: While setting user permissions at the destination, NC takes the *Inherit Permission* option into account.

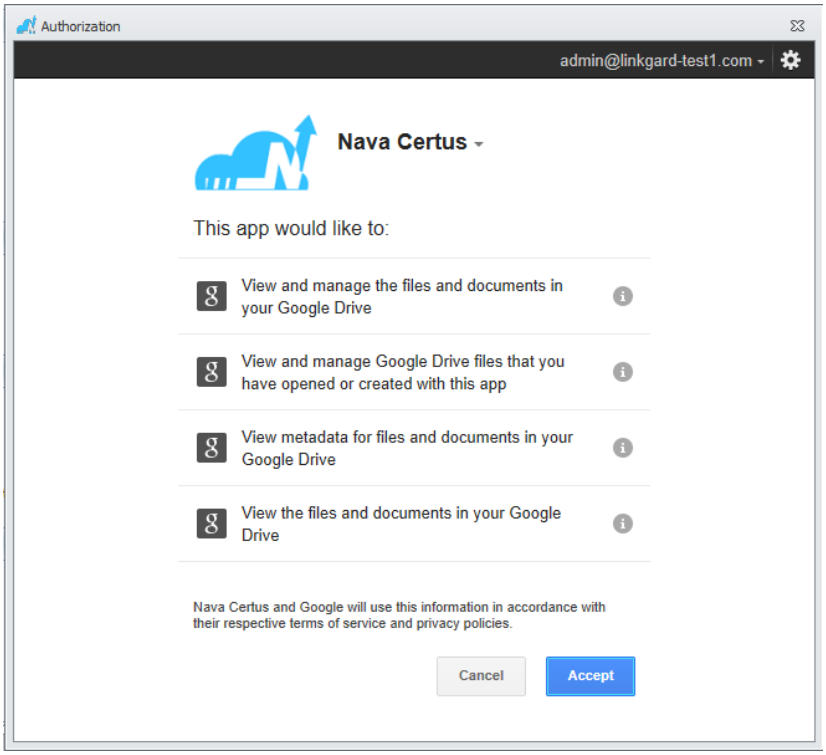


Figure 10 – Authorization

- Google Drive (distributed)
  - *Misc*
    - Provide a **Mapping File**.

Note: For the Distributed migration type, make sure to provide the users who are owners of files along with the users who have any type of permissions on those files. If you do not provide the file owner information in the mapping CSV, the subjected file will fail the migration

- Configure **Email Notification**.
- Configure the **Destination Root Folder**.
- **Default User** (optional) – Provide a valid Email address. If the owner of a file is not found in the user provided mapping CSV, the file will be migrated to the default user provided.
- Configure **Preserver Modification Date**.

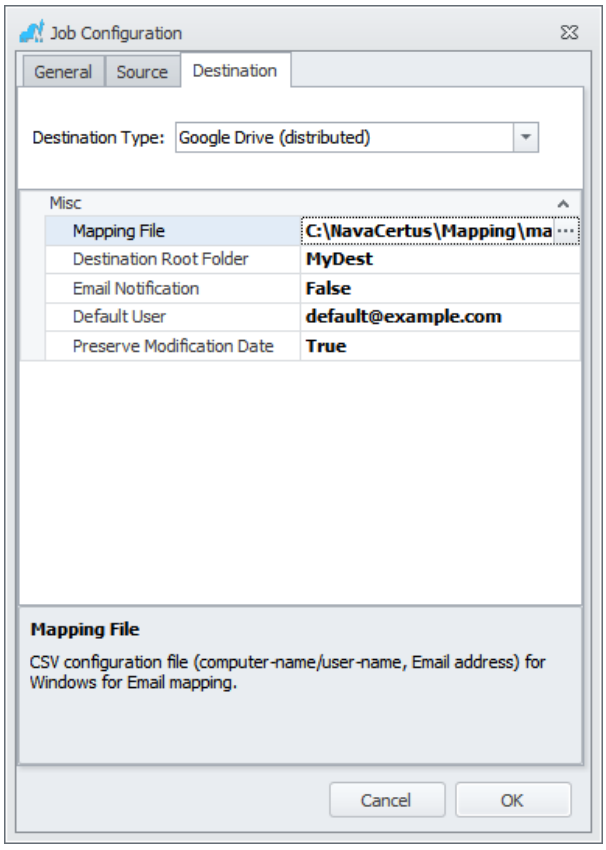


Figure 11 – Destination tab– Google Drive (distributed)

After configuring the job, click OK to save your configuration. On the Nava Certus GUI the newly created job will appear in the list that is shown.

NC will start redistributing the files to respective owners provided in the CSV.

Note: In the Distributed migration type, files with a windows group as the owner will fail to be migrated and will result in migration task failure.

- Amazon S3
  - *Authorization Settings*
    - **Access Key Id** – provide the Access Key Id assigned to your Amazon S3 account.
    - **Secret Key Access Id** – provide the Access Key Id assigned to your Amazon S3 account.
  - *Destination settings*
    - **Bucket Name** – after providing the authorization settings, click on the **Browse** button. In the **Select Bucket Name** window that appears, click **Connect** and from the drop-down list select the desired destination bucket.
  - *Misc*
    - Configure the **Mapping File**.
    - Configure the **Destination Root Folder**.

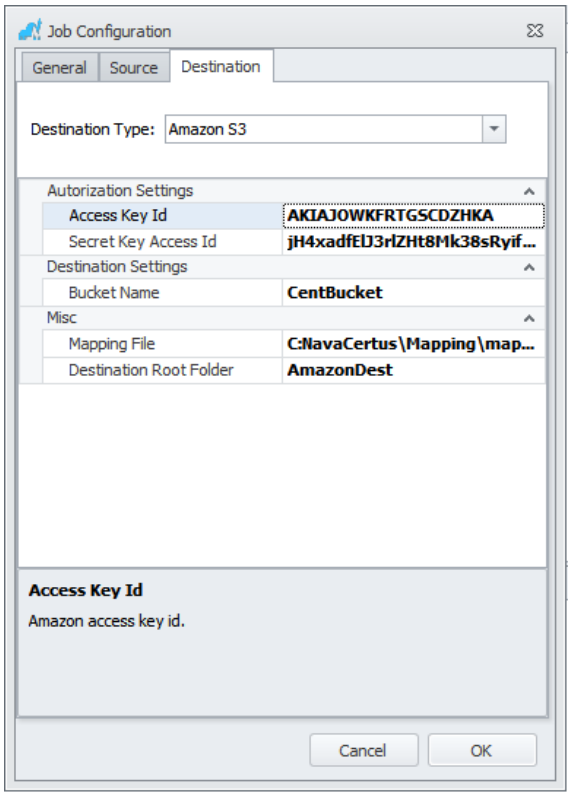


Figure 12 – Destination tab– Amazon S3

Through CLI

Currently you can do the following manipulations with the jobs through the command line:

- Create/Configure a job
- Start/Stop a job
- Get information about a specific job
- Download XML file of a particular task
- Upload modified XML file of a particular task
- List all or currently running jobs

For each job created (through CLI or GUI) an XML file is created which keeps the job configuration. This is done automatically by NC when a job is created from the GUI.

However if the user wants to create a job through CLI, he needs to create the XML file either manually or by copying the XML configuration file of an existing job and editing it. After the user has a valid XML file with the correct format, he is ready to create a job through CLI.

Note that after creating the job through CLI, it needs to be started from the GUI in order to pass the Google Authentication. This is because Google drive requires GUI authorization to be performed. However authentication needs to be done one time; once the job is authorized, you can stop or restart it from the CLI as desired.

Note: If you have already created the job from the GUI and have already provided Google Email and Password, you can run the job from the CLI freely.

In order to create a job from the CLI you can either:

- Perform a *config* operation in order to get an existing job's XML file, edit it and then set it as the new job's configuration file. Since the XML files vary for each job type, make sure you set the correct XML file for the respective job type. To do so:
    1. From the CLI, copy the existing job's configuration file:
       config get "Existing_Job_Name" "Destination_Path/New_Job_Name.xml"
       Example:
       config get "job 1" "C:/Program Files (x86)/Nava Solutions/Nava Certus/jobs/job 2.xml"

    2. Manually edit the configuration XML file; open it in a text editor and modify the settings; it is mandatory to change the *<Name>, <LogFile>* and clean the *<DestinationRootFolder>* entry (for Google Drive migration. You cannot specify a custom folder when creating a job using the CLI).

3. Go back to the CLI and type the following command in order to use the newly modified XML file for the new job:
   config set "New_Job_Name" "Job_XML_Path/Modified_XML_Name.xml"

   Example:

   config set "job 2" " C:/Program Files (x86)/Nava Solutions/Nava Certus/jobs/job 2.xml"

   The new job will appear in the GUI.

4. Go to the GUI and select the job you just created. Click **Start**.
5. In the window that pops up, enter the credentials of the user who is the owner of the files that are subjected to be migrated.
6. Click **Allow Access** in order to authorize the job.

- Manually create the configuration file:
  1. Open a text editor.
  2. Create an XML file with the correct format and save it as XML format.
  3. Go to the NC CLI and type the following command in order to use the newly created XML file for the new job:

     config set "NewJobName" "Job_XML_Path/XML_Name.xml"

     Example:

     config set "job 2" " C:/Program Files (x86)/Nava Solutions/Nava Certus/jobs/job 2.xml"

  4. Go to the GUI and select the job you just created. Click **Start**. Authorize the job if needed.

In order to do other operations with jobs from the CLI, use the following commands:

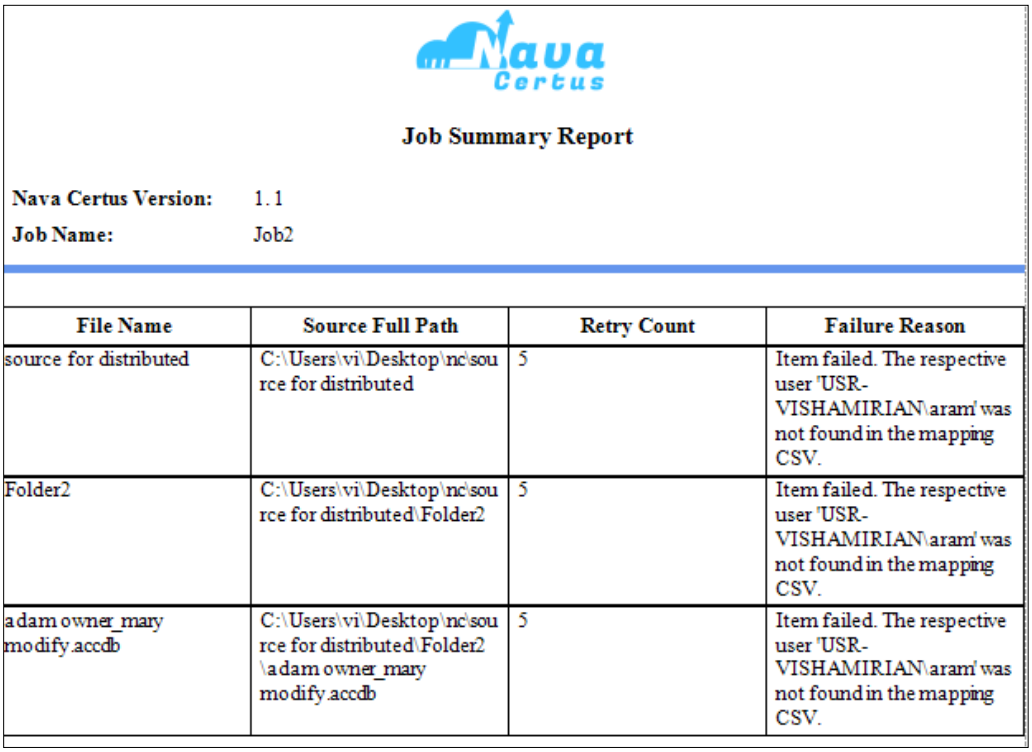
- Start - *job start "job name"*
- Stop - *job stop "job name"*
- List all of the jobs available - *job list*
- List the currently running jobs - *job list -running*

Reporting

There are three types of reporting available. In order to open any of them for a specific job, click on the job and select one of the following reports any time you wish.

Job Summary Report

This report contains a summary of the job in its current state.



Job Summary Report

Nava Certus Version: 1.1
Job Name: Job2

File Name	Source Full Path	Retry Count	Failure Reason
source for distributed	C:\Users\vi\Desktop\nc\source for distributed	5	Item failed. The respective user 'USR-VISHAMIRIAN\aram' was not found in the mapping CSV.
Folder2	C:\Users\vi\Desktop\nc\source for distributed\Folder2	5	Item failed. The respective user 'USR-VISHAMIRIAN\aram' was not found in the mapping CSV.
adam owner_mary modify.accdb	C:\Users\vi\Desktop\nc\source for distributed\Folder2\adam owner_mary modify.accdb	5	Item failed. The respective user 'USR-VISHAMIRIAN\aram' was not found in the mapping CSV.

Figure 13 – Job Summary Report

Error Detailed Report

Detailed Error Report shows the failed item and its location, along with failure reason and the number of times the failed item has been retried by NC to be migrated.

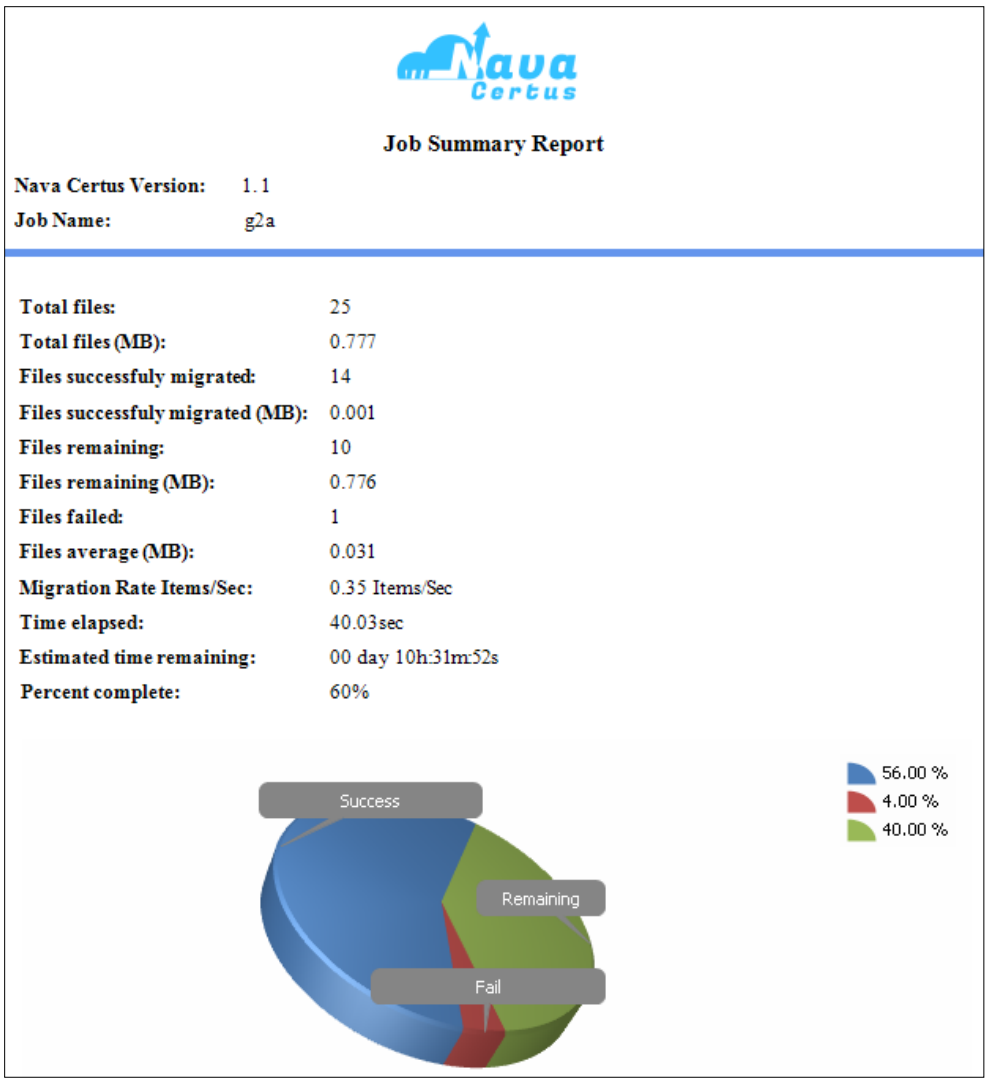


Figure 14 –Detailed Error Report

Migration Integrity Report

This report is not a graphical report. It contains information about source items along with the checksum calculated for each item at the source before migration by NC and the checksum returned by Google after an item resides at the destination drive. Note that this report is meant as a proof of the migration chain of custody.

When you select this report a pop-up window will appear. In the window enter the name and a location for the report to be exported to. The report will be exported in CSV format.