Google Directory Integration Service (GDIS)

Administrator's Guide

DocuPhase version 6.2 and later

Last Revised: October 8, 2019

DISCLAIMER

These recommendations are only provided as a general point of reference for system installations, and may need to be adjusted to meet the demands of your specific situation.

DocuPhase has made every effort to ensure that this document is accurate; DocuPhase disclaims liability for any inaccuracies or omissions.

Information in this document is subject to change without notice and does not represent commitment on the part of DocuPhase.

If you find information in this document that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

Table of Contents

Revision History

Item #	Release #	Rev Date	Description	Tracking Notes
004	6.2 & later	10/08/19	Revised “Enabling the API for Google Access” section – reorganized it and deleted proprietary info (on page **Error! Bookmark not defined.**)	DNichitoae
003			Disclaimer statement added to cover.	kb
002		07/09/19	Added “Updating and Troubleshooting” (on page 7)	JiraTW25, EAllen
001			Updated to latest branding/format/styles	kb
000		05/07/18	Original	29685

Introduction and Purpose of this Guide

The DocuPhase GDIS integration was developed in order to synchronize Google users and groups with DocuPhase users and groups.

This Document is intended for the technical administrator who wants to understand the structure of the GDIS integration with the DocuPhase Platform. Conceptual and methodological, as well as important notices and warnings are provided. Additionally, information is provided with regard to enabling the API and IIS relay for Google email (gmail).

> ***IMPORTANT!***
> ***As of version 6.1, the name of the iSynergy platform was changed to DocuPhase. You may notice some updates and revised files paths have been updated to reflect this change.***
>
> ***Please review the 6.1 Release Notes (in online help or via the DocuPhase Learning Library: https://training.docuphase.com/lesson/docuphase-platform-6-1-release-notes) for more information about the name change.***

Assumptions

The following must be true in order to successfully configure and implement GDIS:

- ✓ Server Prerequisites have been installed.
- ✓ The DocuPhase platform is installed and successfully tested as http.
- ✓ An SSL certificate* has been purchased and configured for DocuPhase.
- ✓ Notepad ++ (run as an administrator) is to be used when editing config files.

> ***IMPORTANT!***
> - ***All access in GDIS is read-only.***
> - ***When referencing a "group" in Google, it may refer to "orgunits" or "distribution group". The current implementation of GDIS uses orgunits to map to DocuPhase Groups. However, it is possible that future client-integrations may require use of Google (distribution) groups.***

Enabling the API for Google Access/Google Suite (G-Suite)

In order to properly integrate and make settings between GDIS and DocuPhase, you must prepare the API for Google using the following process.

1) Login to the pertinent Google Admin account as a "super administrator" (https://support.google.com/a/answer/2405986#super_admin).
   - *Credentials do not end in "@gmail.com".*
2) Link the API to the account.
3) Create a service account for the API access.
4) Allow access by the service account to various parts of Google (known as "Scopes").
   - *Scopes allow access to user and orgunits in both read, and read/write modes.*

> ***NOTE***
> *For more information about enabling API Access: https://support.google.com/a/answer/60757?hl=en and/or contact Google directly (https://gsuite.google.com/support/).*

Go to https://en.wikipedia.org/wiki/Certificate_authority for more information about certificates and how to obtain them.

User and/or Group Synchronization

- Both Google orgunits and users have a non-changing, unique ID created in the following way:
  - DocuPhase makes an initial attempt to link with an established ID. However, If the ID does not yet exist, the user is associated via email; groups are associated by name.
  - Once one or both of associations (described above) are successful, a link is created using the ID stored within the DocuPhase Database.
- The link created using the ID is always used for synchronization.

NOTES

- *By using the ID, the user name and/or email can change without breaking the link synchronization is based on the ID rather than variable information. This is also true of links to group names.*
- *The IDs in Google are externally meaningless strings and compared in a case-insensitive manner.*
- *User and groups can be created in DocuPhase, and GDIS will ignore them. GDIS identifies users and groups it creates by CreatedBy = "DocuPhase Google Dir Sync".*

- When synchronizing begins between google users and groups, DocuPhase users and groups are compiled into lists in the GDIS service. Those lists are then used locally for user and group information vs fetching individual user groups: thus making the process more efficient.
- The Google API organizes groups of users to read a maximum of 500 at a time. DocuPhase reads Google users via in hard coded groups of 200; orgunits are not grouped.
- DocuPhase uses Attribute tables to create links between Google users and DocuPhase users, as well as for Google orgunits and DocuPhase groups. Each Attribute table has an ID to allow selection of only pertinent attributes.

IMPORTANT!
Throughout the remaining text in this Appendix, "Attribute" should be assumed to be scoped to GDIS.

- DocuPhase creates a list from all of current Google Users; it then looks at the UserAttribute table for a value matching the ID and the correct UserAttributeDefintionID. A similar list is created from the list of current Google Groups (i.e., orgunits).
- If we find a match in the UserAttribute table, it is synched with the DocuPhase user.

Users

New Users

- In the case of a new user, there is no match (as described above), DocuPhase searches for the new user by email.
- If an exact, case-insensitive match for the email is found, a UserAttribute record is created and linked to the existing DocuPhase user.
- If no match is found a new record is created in the UserAttribute table: creating a new DocuPhase user.

Updated Users

- If a Google user name or email has been changed, it is updated in (and synched with), DocuPhase via the ID (described previously).
- Any other changes to a user's Google account has no bearing on the link with DocuPhase.

> ***IMPORTANT!***
> ***Only DocuPhase users created by "DocuPhase Google Dir Sync" can be updated.***

Deleted Users

- In order to maintain referential integrity, as well as audit history, DocuPhase does not delete users from its database. However, Google directory services allows users to be deleted; therefore when users are deleted from Google directory services, DocuPhase "marks them for deletion" which means that the PasswordExpInterval for user records in DocuPhase are set to a value of "-99": indicateing that the user is no longer active in DocuPhase and unable to log into the system.
- Google Users can be suspended (and un-suspended) or deleted. Once a Google user is "deleted" he/she no longer appears in the list in Google.
- Users suspended, unsuspended, and/or deleted from Google are treated the same in DocuPhase; such users are designated as deleted ("-99") in DocuPhase.
- If a user is marked as deleted or suspended, DocuPhase uses the link to the ID in the UserAttribute table to locate the user record. IF a match is found, the user is marked as deleted.
- If the user is not found, then DocuPhase look for the user by email. If a match is made using the email, DocuPhase checks to see if the CreatedBy = "DocuPhase Google Dir Sync". Once this is verified, the user is marked as deleted, otherwise the record is ignored.
- Users who have been permanently (hard) deleted they no longer show up in the list of users from Google. At the end of the sync user routine DocuPhase matches the entire list of Google users against the entire list of DocuPhase users.
- Any user in the DocuPhase list and not in the Google list...
  - ✓ is a candidate for deletion...
  - ✓ and the user shows as CreatedBy = "DocuPhase Google Dir Sync" is designated by DocuPhase as deleted.

Orgunits/Groups

New Groups

NOTE

Only Google orgunits with users are added (i.e., "empty" groups are not added).

- As previously noted, DocuPhase creates a list of all orgunits from Google; orgunits become groups in DocuPhase.
- A Google user can be a member of only one Google orgunit; however, orgunits can be nested.
- Since hierarchical groups are supported in Google, but not in DocuPhase. Therefore, DocuPhase flattens the tree structure to convert the hierarchy in to equal groups.

> ☞ ***EXAMPLE***
>
> *A Google orgunit of "Accounting" with three sub-Organizations "payroll", "AR" and "AP" is converted into four groups in DocuPhase: "Accounting", "Accounting - payroll", "Accounting - AR" and "Accounting - AP".*

- Orgunits and sub-orgunits are separated by a space hyphen space or "X – Y".
- Once DocuPhase recognizes a list of all orgunits from Google, it looks for a UserGroupAttribute record with an AttributeValue that matches the orgunitID, along with the UserGroupAttributeDefintionID.
  - ✓ If a an ID match is not found, DocuPhase looks for an exact, case-insensitive match on the group name.
  - ✓ If an exact, case-insensitive match by group name is found, a UserGroupsAttribute record and set CreatedBy to "DocuPhase Google Dir Sync" is created.
  - ✓ If a matching group name is not found, a new DocuPhase group and UserGroupAttribute record are created.

New and Deleted Group Users

New Users

- New users in a Google orgunit are added to DocuPhase using the attribute table to get the DocuPhase UserID. DocuPhase users not already in the group are added.
- It is a safe assumption that if DocuPhase users are listed in the attribute table, they were created by GDIS; therefore, ***NO*** verification check is required as it is with individual users.

Deleted Users

- When users are removed from a Google orgunit, they are removed from the associated DocuPhase group.
- DocuPhase exclusively checks the attribute table for linking, but does not make a CreatedBy verification.

Deleted Groups

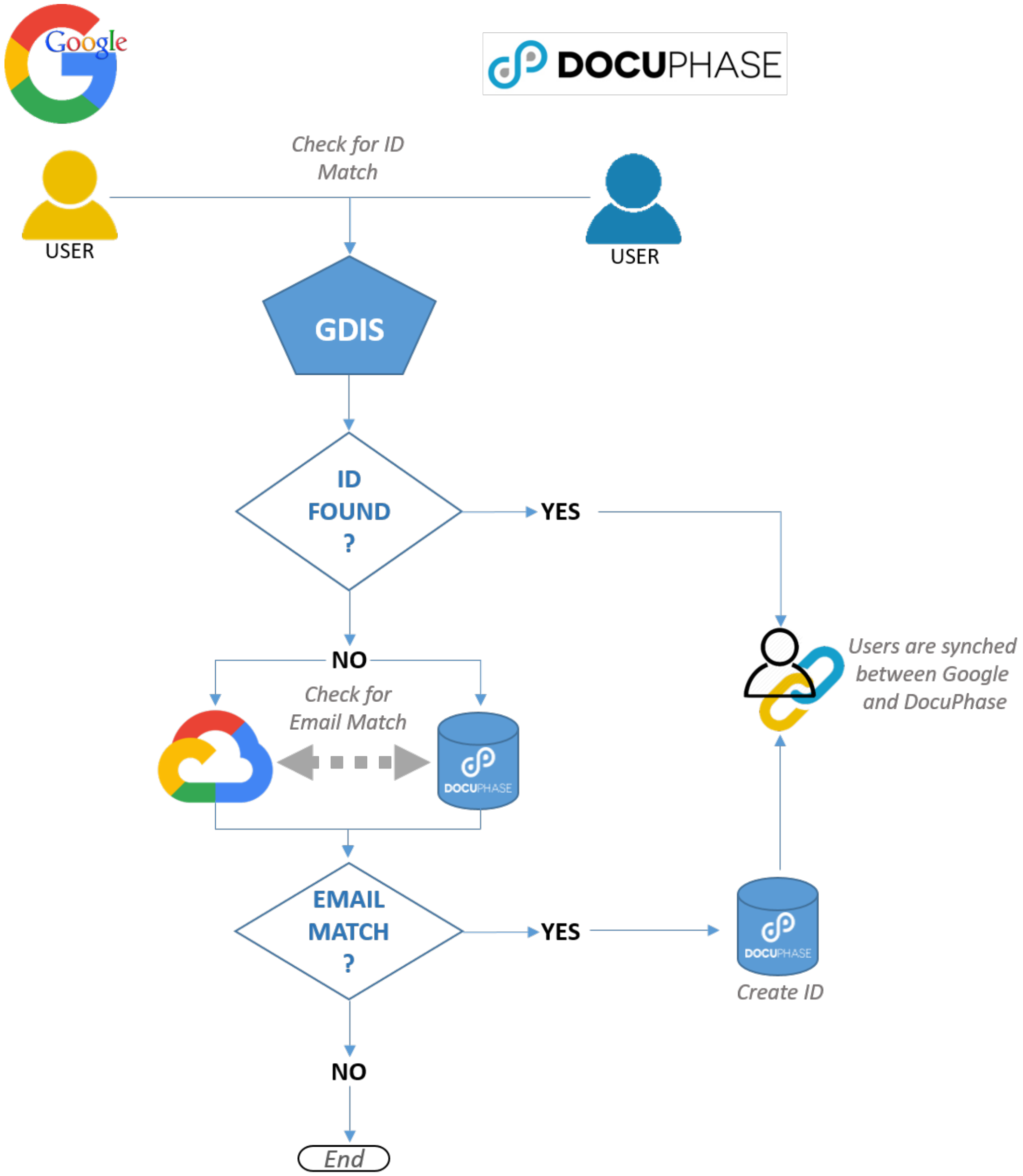
- Any DocuPhase group not in the list of Google orgunits is a candidate to be deleted.
- The list of candidates is checked, and only those with CreatedBy = "DocuPhase Google Dir Sync" are deleted.

Application Installation

- The application is installed as its own service; it is a 64 bit application and installed to \DocuPhase\programs\gdisservice.
- Frequently, client may want to run this service on their servers not ours. The service communicates with DocuPhase via web services; therefore, it can be deployed anywhere.
- Because of the size of DocuPhase services, GDIS Integration has its own service rather than being included in DocuPhase services.
- When clients want to install this service on their servers, DocuPhase provides them with a 100K install, rather than a 200M.
- The install requires an input of a user ID for running the service: use "LocalService", with no password.
- Once the User ID has been entered, the remainder of the settings must be set manually in the app.config, and are documented in \DocuPhase\programs\gdisservice\app.config

Diagrams of Synchronization Processes

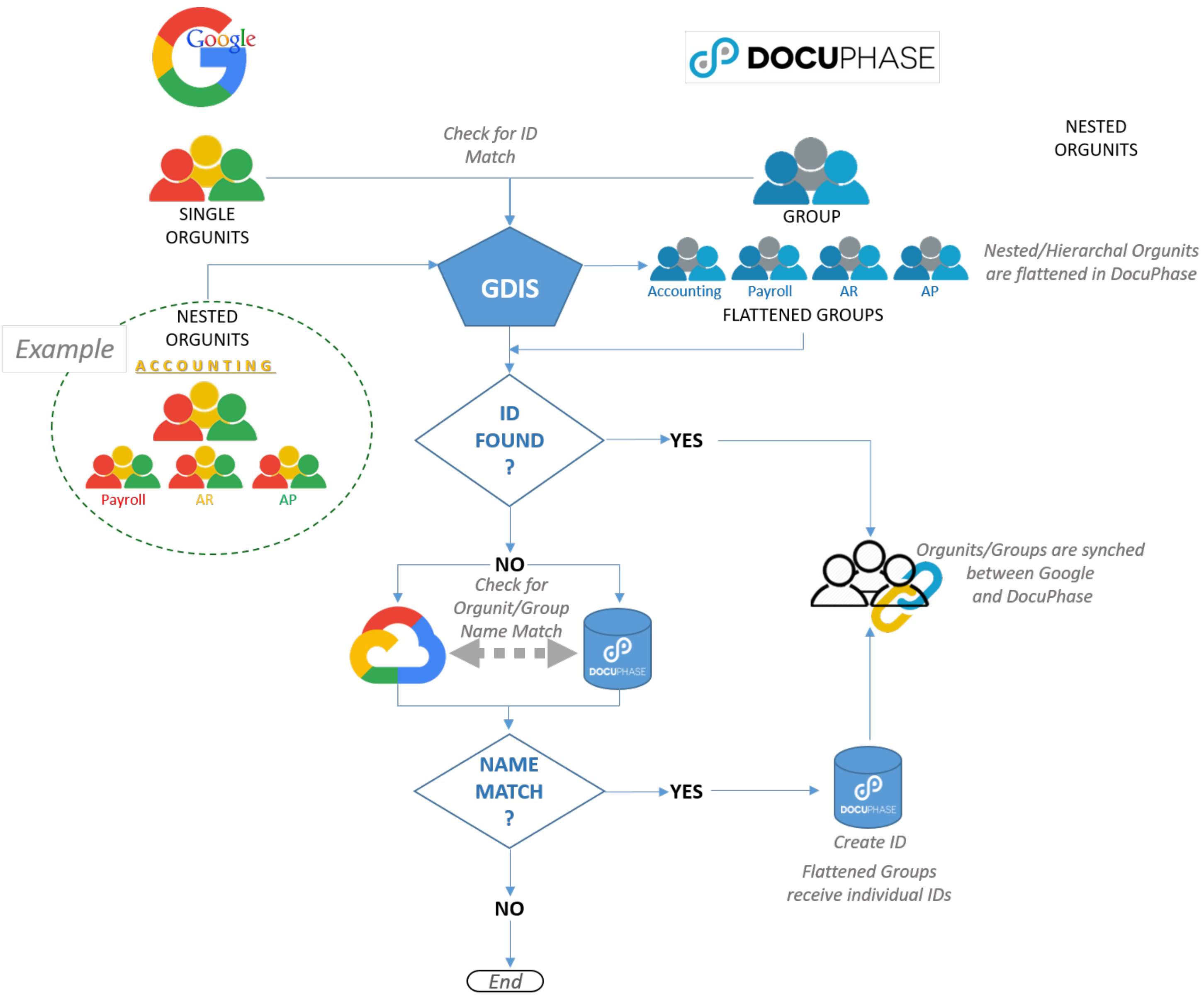
User Synchronization



Diagrams of Synchronization Processes (continued on next page)

Diagrams of Synchronization Processes (continued)

Orgunit/Group Synchronization



Updating and Troubleshooting

Some organizations choose to use Google integration service instead of ADIS for SSO. The GDIS integration performs differently than ADIS, in that once a user is linked, their Username, email, and other variables are updated and changed based on the information in Google.

In addition, organizations may also utilize an identity and access management provider (e.g., OneLogin, NetIQ, CrossMatch, etc) on each user's machine for single sign on functionality.

Updating GDIS

Task Scheduler can be configured (via PowerShell) to start the GDIS executable on any day(s), at any time. When this configuration is made PowerShell calls the executable program via console command to start up.

> ⚠ ***WARNING!***
> ***Updates may interfere with users' inability to log in (see Troubleshooting information below).***

> ***TIP***
> *Log data propagates to Program data, but can be set to logging level 3 for activity monitoring (i.e., Level 3 logging produces change log similar to ADIS activity log for review).*

Troubleshooting GDIS Log In Issues

Issue A: New User is unable to log in to DocuPhase

Use Task Manager to see if GDIS is running.

YES - it IS running, do the following:

- ✓ If multiple are running, stop the processes
- ✓ Check log for last activity
- ✓ Run GDIS task scheduler to kick off process & monitor log activity

OR

NO - it IS NOT running, do the following:

- ✓ Run GDIS if not running
- ✓ Check log for activity - users will be added

Issue B: Previously working user is no longer able to login to DocuPhase now

Does user exist in DocuPhase still?

Yes, but the user is disabled.

- ✓ Enable user if appropriate.

No, they were likely never there since users are not removed or deleted in this process:

- ✓ Add user if appropriate.

AND/OR

Check the GDIS trace logs for user activity or changes, and validate account settings in the Google Directory:

Is the account Enabled?

- ✓ If not, enable it.

Was an Alias used?

- ✓ If so, make the appropriate adjustment.