T-MINUS 365

G SUITE TO OFFICE 365 MIGRATION PLAYBOOK

Table of Contents

This is a complete step-by-step guide for migrating from G Suite to Office 365 using BitTitan's migrationwiz. Mail, Calendar, and Contact items can be migrated over in the migration. Be aware, the following **cannot be migrated** over using this tool:

- Calendar Attachments
- Calendar Reminders
- Some calendar colors
- Tasks
- Chats and chat history
- Google Groups for Business, including forums and collaborative inboxes
- Google Categories (i.e., the Google category flags: Social, Promotions, Updates, Forums)
- Can only migrate items that are visible through IMAP
- Email attachments that are links to Google Drive

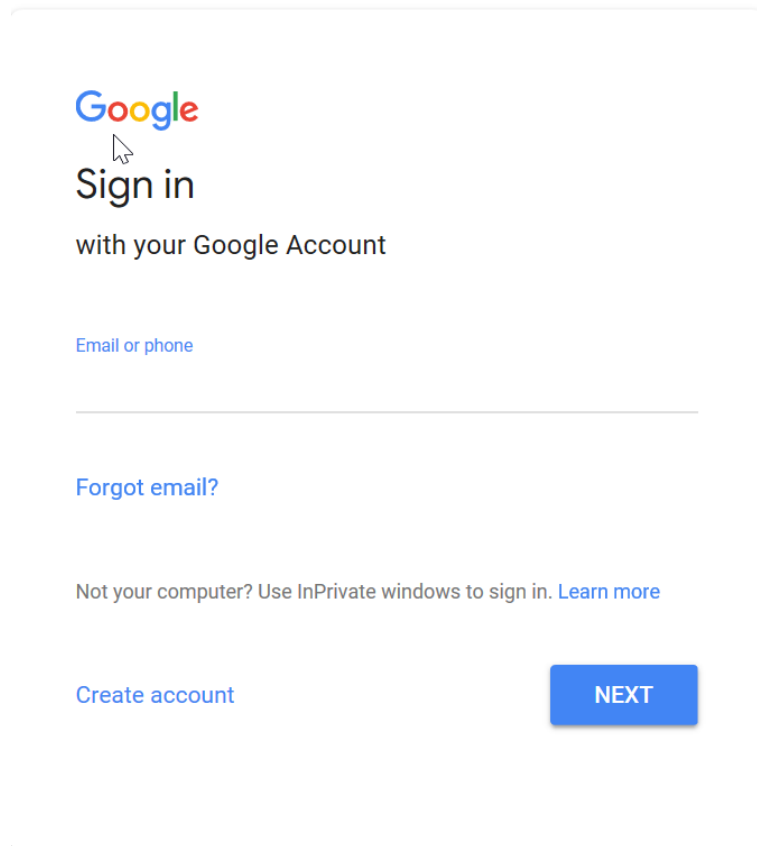*Planning Phase 1: Gather All the Necessary Credentials*

1. Credentials Checklist
   a. Office 365 Global Admin Credentials
   b. G Suite Admin Credentials
   c. BitTitan credentials
   d. DNS Login Credentials
   e. A list of users with Passwords (if not using AD Connect)

Note BitTitan comes with a tool called Deployment Pro which reconfigures Outlook profiles after the migration. This can be pushed out either through GPO or email. If you are going to be pushing this out via GPO you will additionally need:
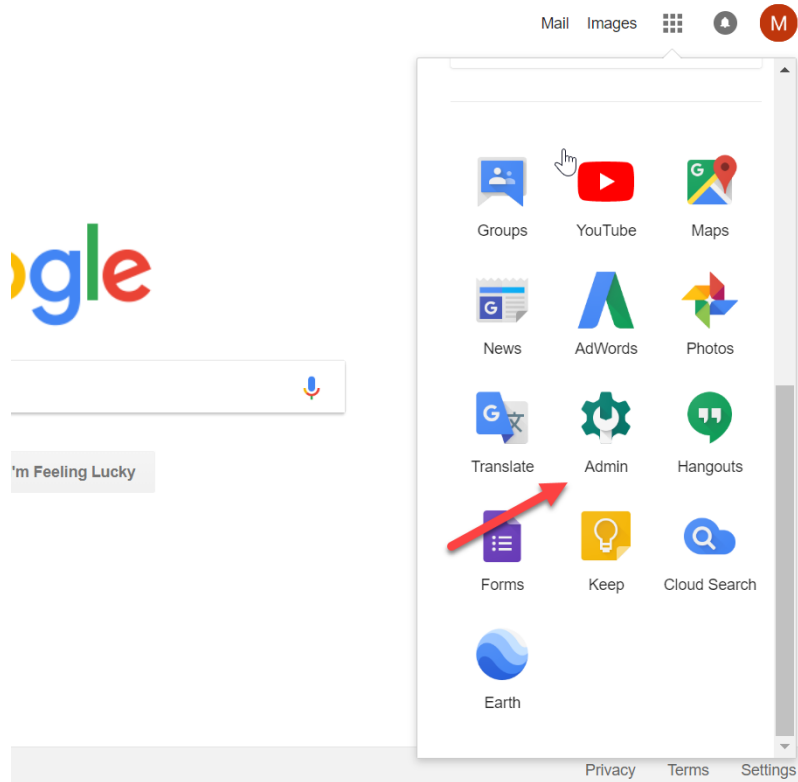
   e. Credentials remote into Primary DC (If applicable)
   f. Enterprise Admin Credentials for Primary DC

Prep Work Phase 1: Prepare G Suite Environment

1. The first step we need to take is to grant access to G Suite using OAuth 2.0. First, log in to google using the G Suite Admin Credentials:
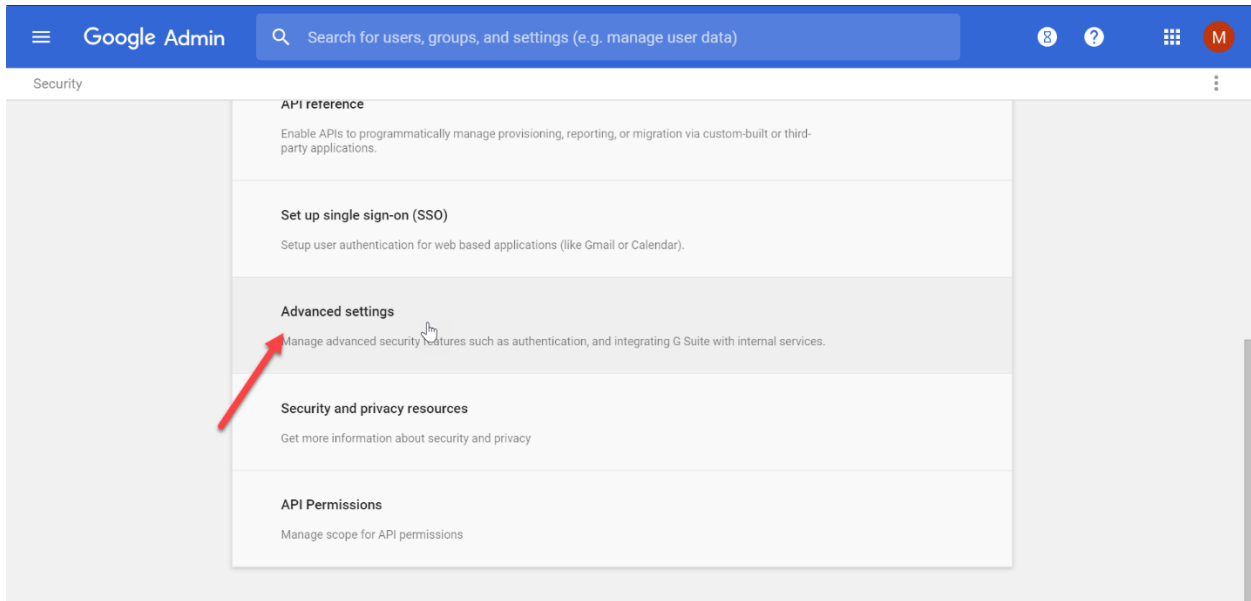
Google

Sign in

with your Google Account

Email or phone

Forgot email?

Not your computer? Use InPrivate windows to sign in. Learn more

Create account   NEXT

2. After you sign in, click the waffle icon in the top right corner and click on the Admin icon:
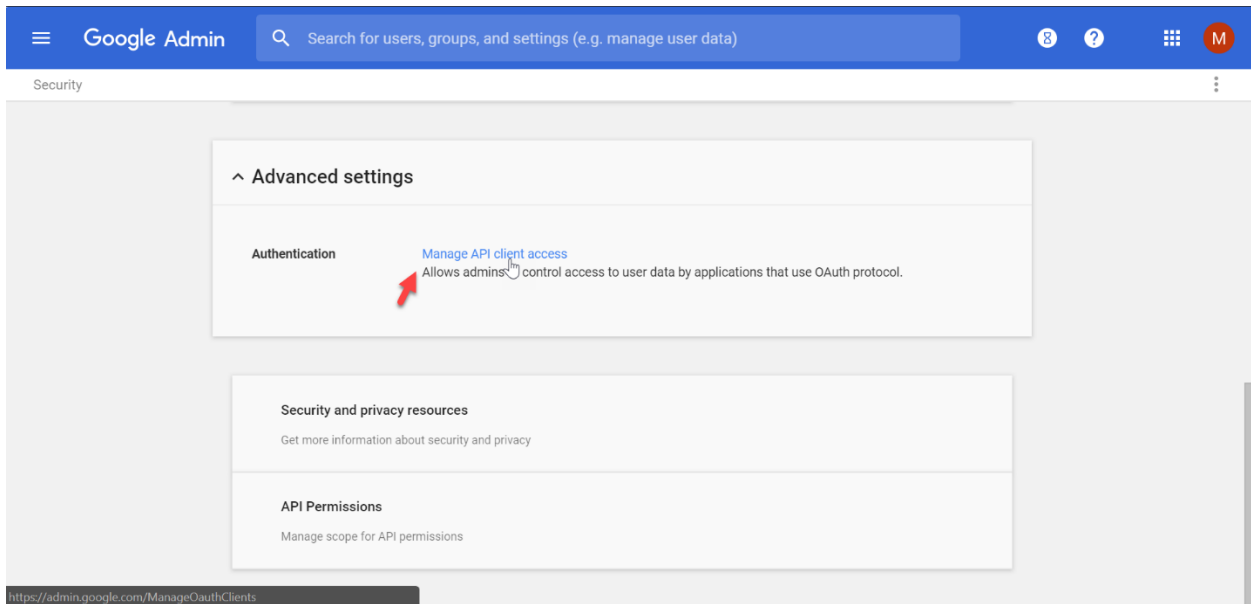

3. Next, go to Security:
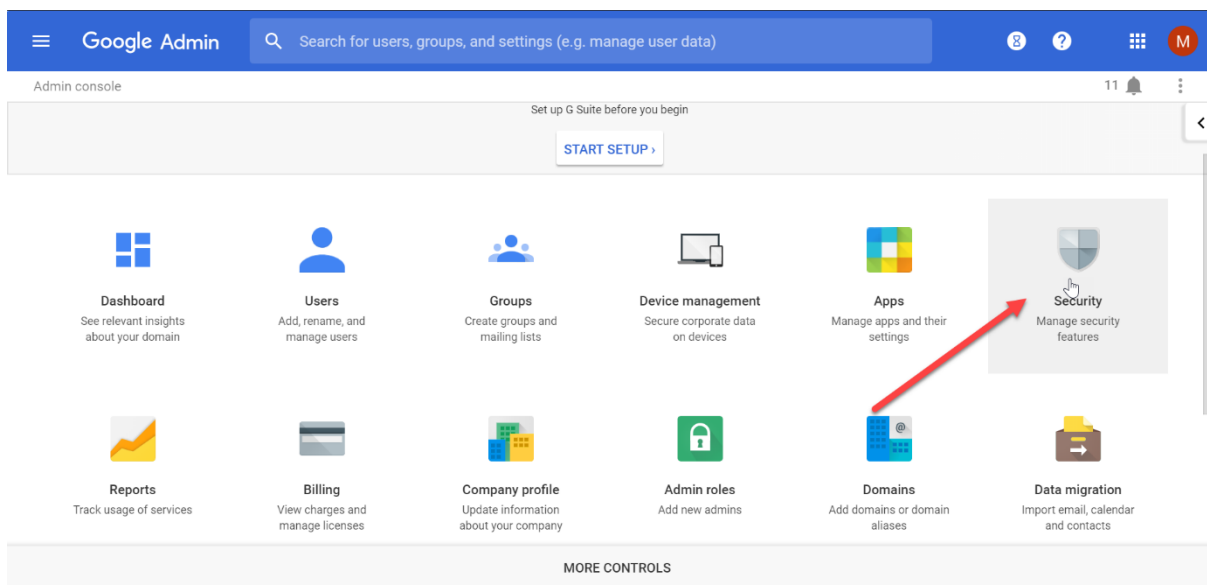
4. Scroll Down and Click on Advanced Settings:

5. Next Click "Mange API client access"

6. Type "113321175602709078332" into the "Client Name Field" *NOTE* This is granting MigrationWiz admin access to the account


7. Enter the following into the "One or More API Scopes" section and then click "Authorize":

https://mail.google.com/, https://www.google.com/m8/feeds,
https://www.googleapis.com/auth/contacts.readonly,
https://www.googleapis.com/auth/calendar.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
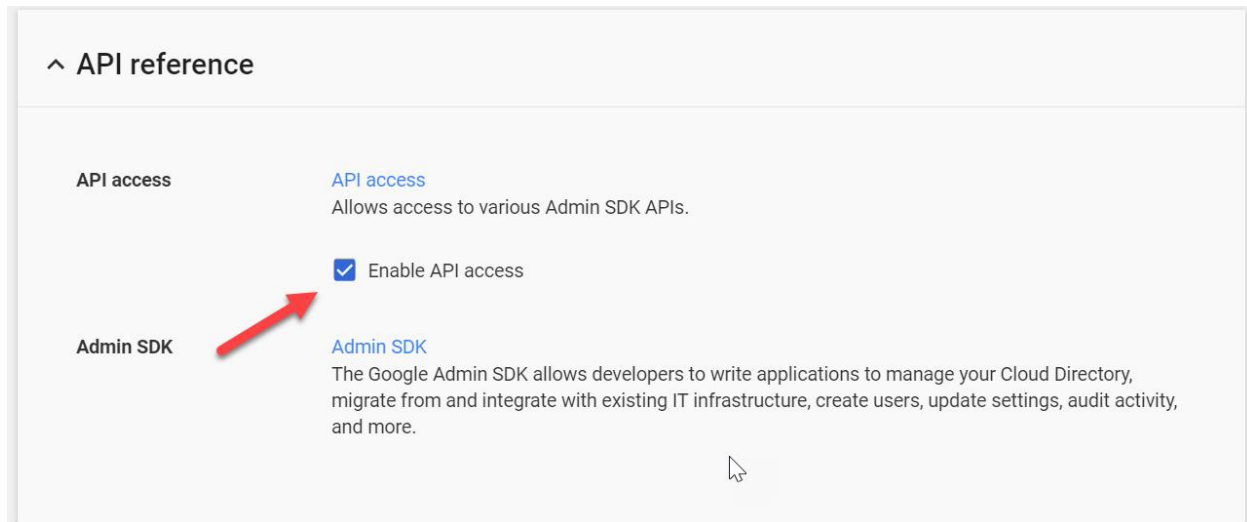https://www.googleapis.com/auth/drive, https://sites.google.com/feeds/

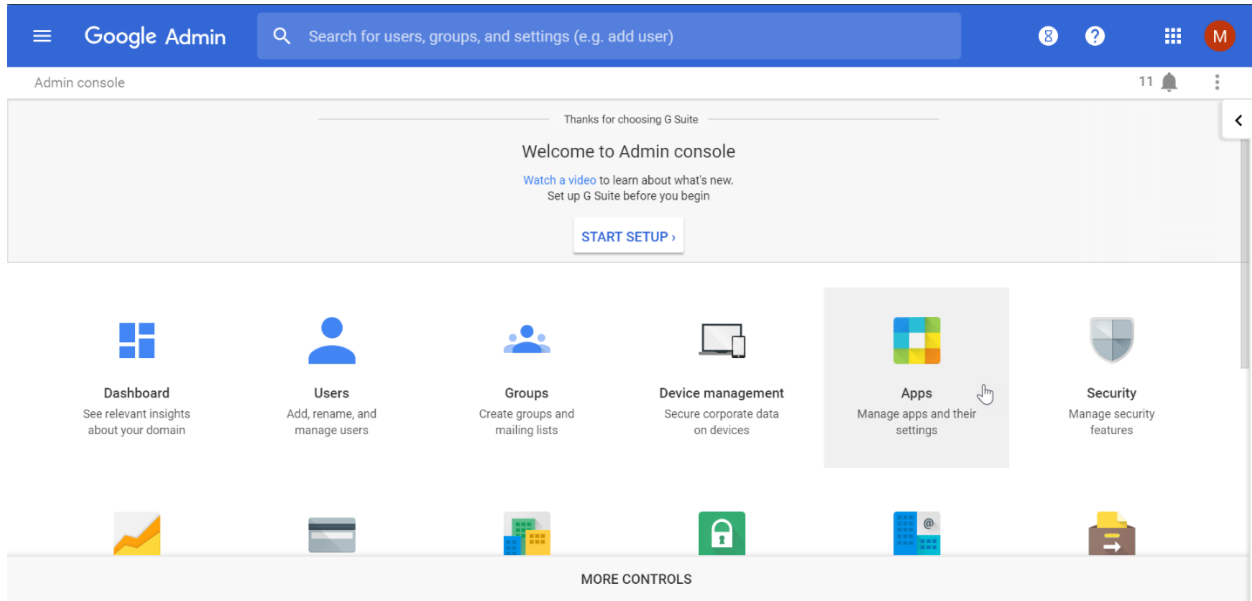8. Next, we will go back to the Security section under Admin:
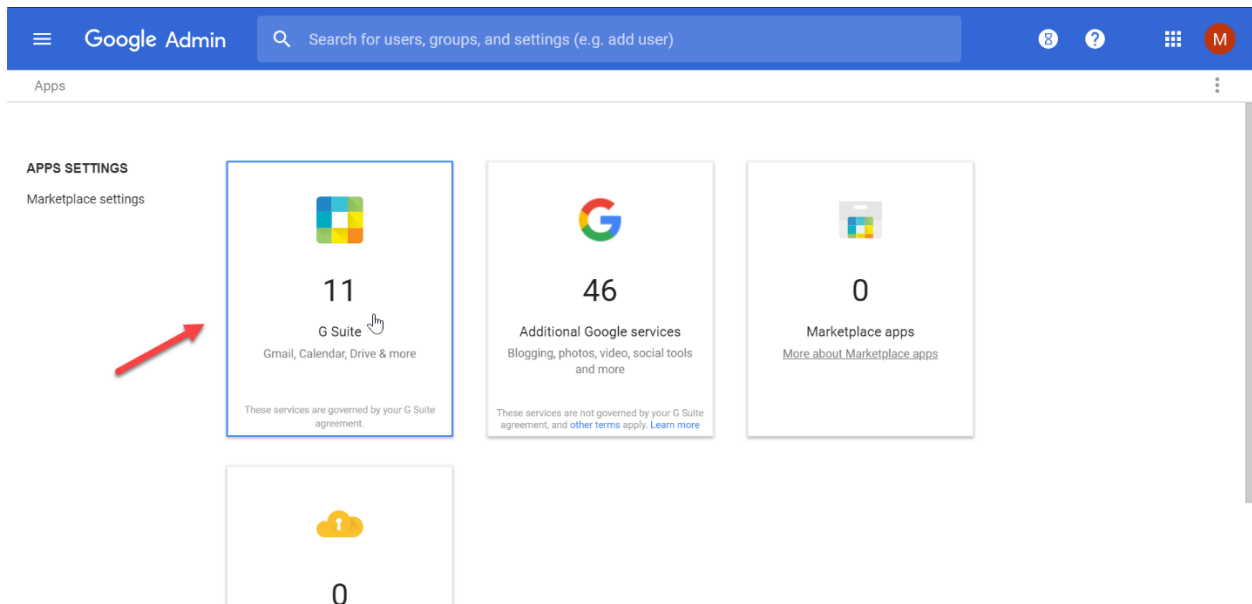
9. Click API reference
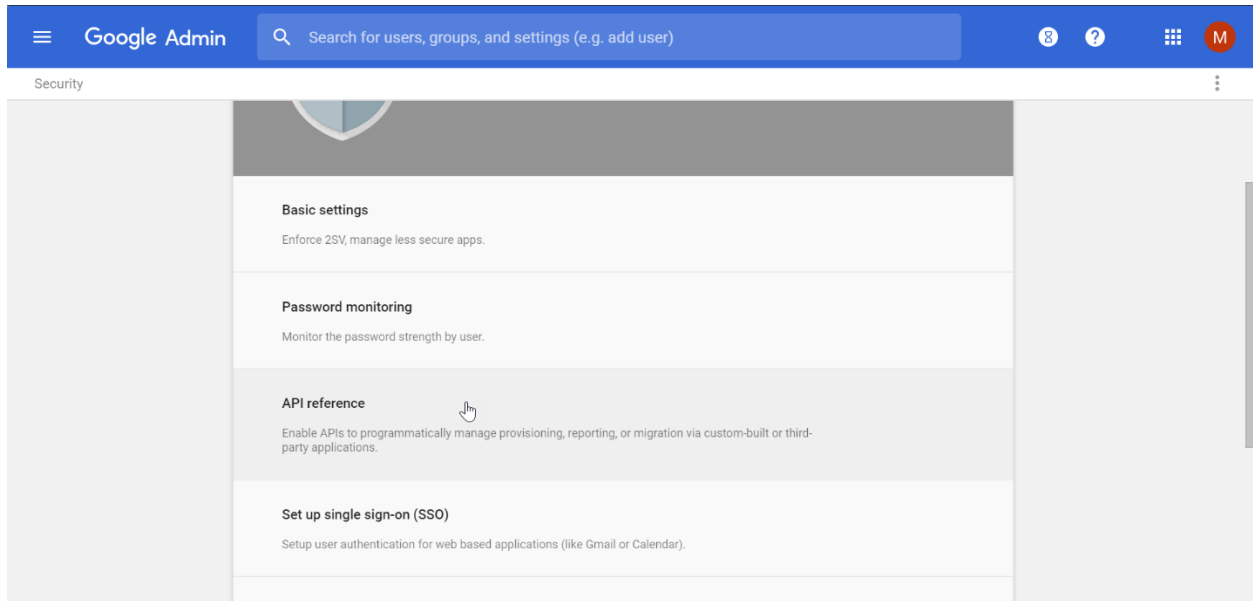
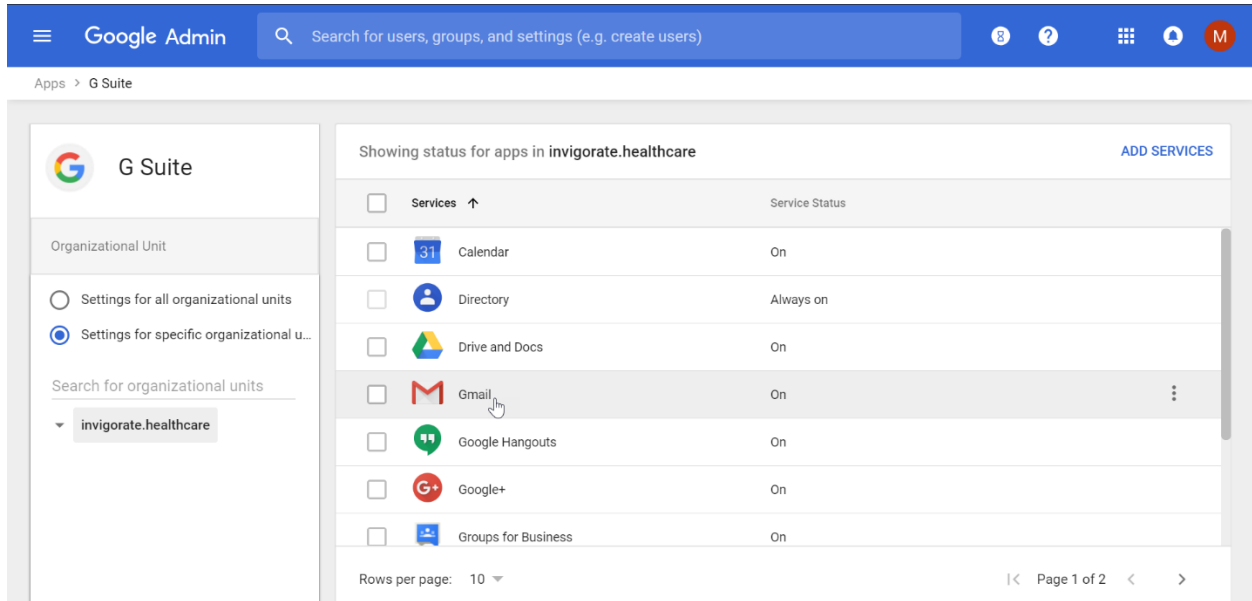10. Make sure that "Enable API Access" is selected

11. Once this is done, we need to make sure that IMAP access is enabled for all users. For this, we will go back to the Admin home page and select the "Apps" icon:
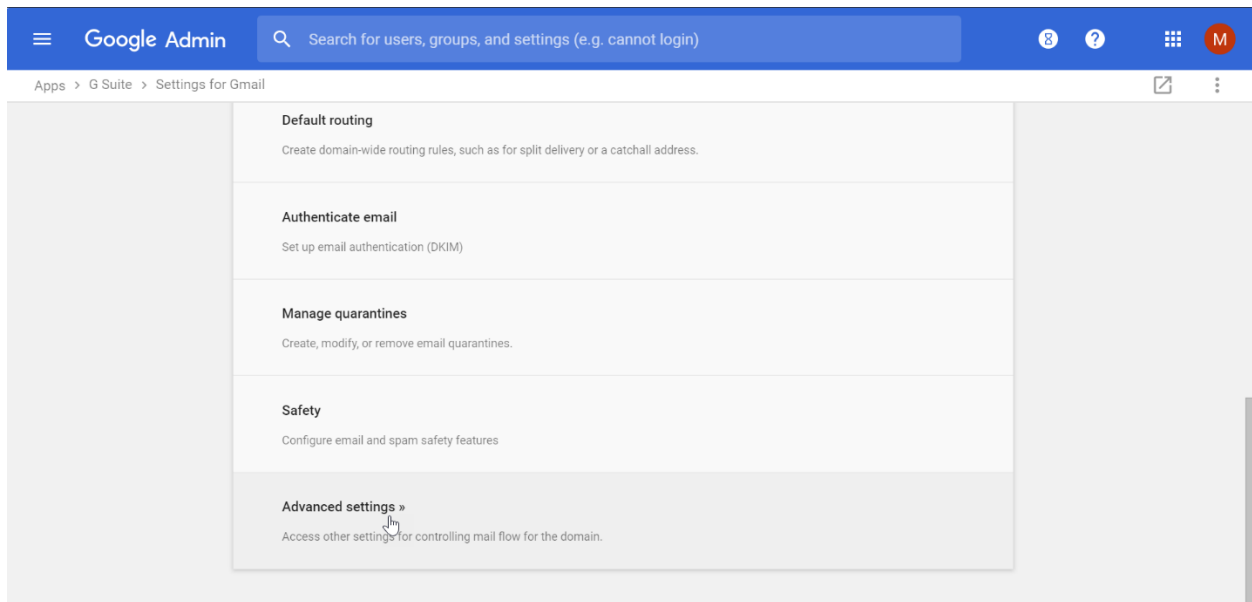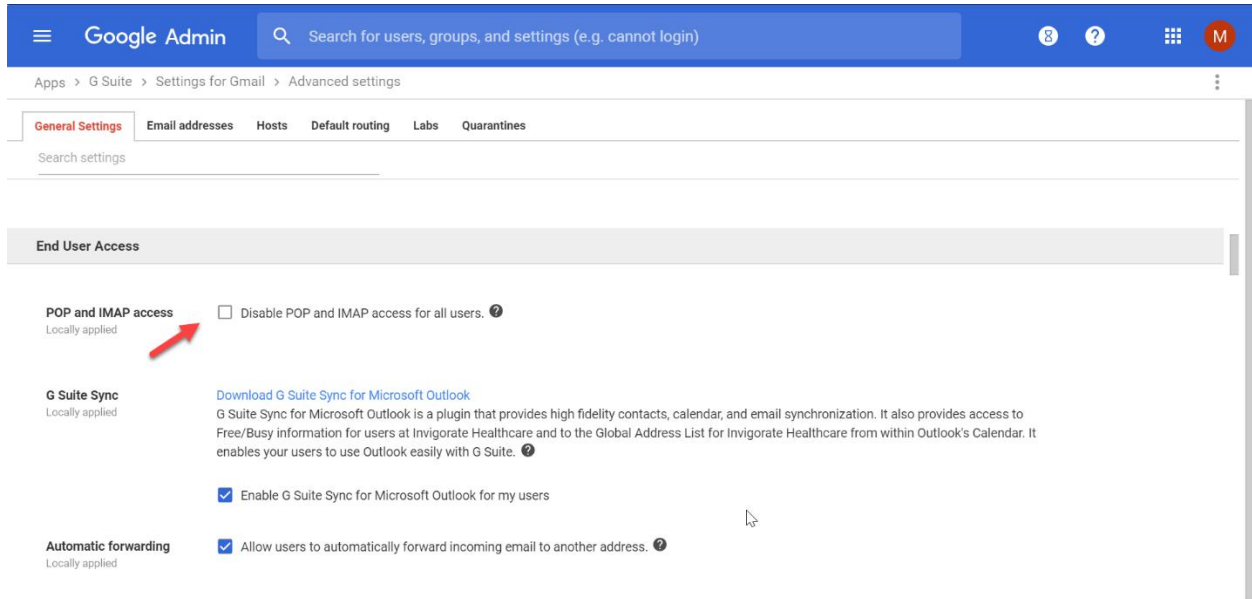

12. Next we will select G Suite:

13. Then, we will select Gmail:

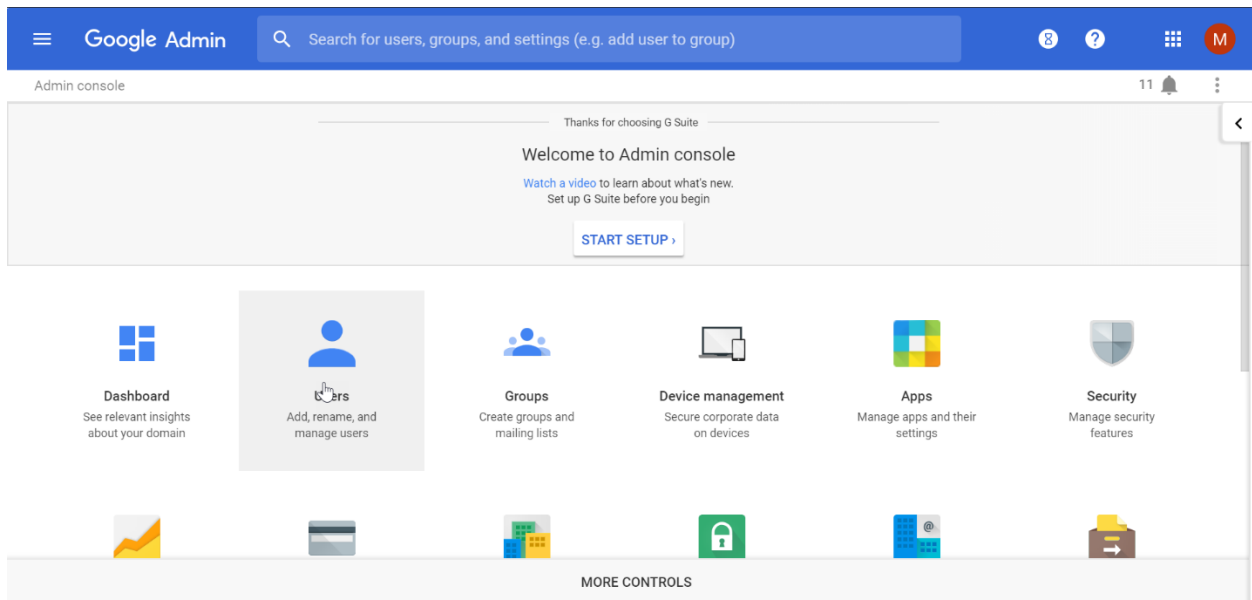14. Scroll Down to the bottom of the page and select "Advanced Settings"

15. From here, scroll down to the "End User Access" section and make sure the "Disable POP and IMAP access for all users" is **unchecked**

16. Last we will just want to export our userlist into CSV format. We will start back at the Admin Center and then go to the "Users" icon

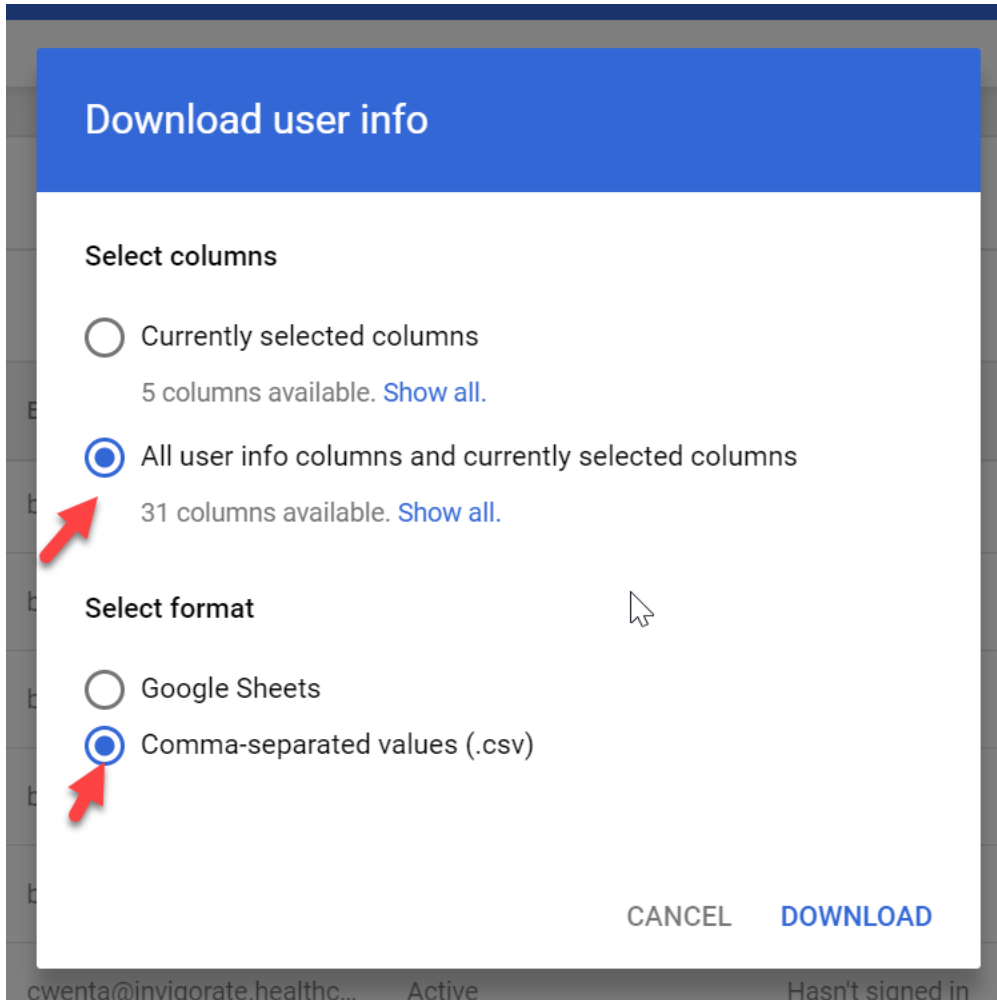17. In the top right corner, you will see the download icon:

18. Select "All user info columns" and "CSV" for the format:

NOTE You will want to audit this user list to make sure it does not have users not part of the migration. Clean up accordingly.

1. Create a net new office365 tenant, tenant will be spun up with the defaulted .onmicrosoft.com domain. This can be spun up direct with Microsoft or purchased through a CSP provider

2. Go to Setup>Domains>Add Domain

3. Verify Domain with TXT record provided

4. Select "I will manage DNS records myself" and checkmark the box "Skip this step" when it ask to place all the remaining DNS settings for you

5. Domain will say "possible service issues". This is ok. We will add the remaining records after we cut over MX Records

6. Add Users Manually, Bulk Upload with a Powershell Script or CSV, or with AD Connect

NOTE At this stage, if you are not using AD Connect, you will **need to decide** if you are collecting all user's passwords to upload into office365 or if you are providing passwords to users.

      a. Powershell Script

```
#Connecting to Exchange Online Account#

$credential = Get-Credential

Import-Module MsOnline
Connect-MsolService -Credential $credential

$exchangeSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
"https://outlook.office365.com/powershell-liveid/" -Credential $credential -Authentication
"Basic" -AllowRedirection
Import-PSSession $exchangeSession -DisableNameChecking
```

Create a CSV with the Following Headers:
- UserPrincipalName
- FirstName
- LastName
- DisplayName
- Password

```
#Bulk Import Users with Passwords#

Import-Csv -Path 'FilePath' | foreach {New-MsolUser -UserPrincipalName
$_.UserPrincipalName -FirstName $_.FirstName -LastName $_.LastName -DisplayName
$_.DisplayName -Password $_.Password -ForceChangePassword $False}
```

```
#Add Alias to Users#

$LiveCred = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -Connecti
dential $LiveCred -Authentication Basic -AllowRedirection
Import-PSSession $Session
$users = Get-Mailbox
foreach ($a in $users) {$a.emailaddresses.Add("$($a.alias)@domain.com")
$users | %{Set-Mailbox $_.Identity -EmailAddresses $_.EmailAddresses}
```

```
#Add Distribution Lists with Members#

Import-Csv -Path 'File Path.csv' | foreach {New-
Distributiongroup -Name $_.Name -PrimarySmtpAddress $_.Address
}

Import-Csv 'File Path.csv' | foreach {Add-
DistributionGroupMember
 -Identity $_.DL -Member $_.Alias}
```

b.AD Connect Setup: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-get-started-custom

1. Change Send/Receive size in office 365 to max of 150m: https://help.bittitan.com/hc/en-us/articles/115008108047

Note Make sure you are still connected to exchange online in powershell

```
#Change Send/Receive Size#

 Get-Mailbox | Set-Mailbox -MaxReceiveSize 150MB -MaxSendSize 150MB
```

2. Set Impersonation at Destination. This will allow you to use admin creds to impersonate all mailboxes. With this in place you will not need creds for all individual users

```
#Setting Impersonation#

Set-ExecutionPolicy Unrestricted

$LiveCred = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
https://ps.outlook.com/powershell/ -Credential $LiveCred -Authentication Basic -
AllowRedirection

Import-PSSession $Session

Enable-OrganizationCustomization

New-ManagementRoleAssignment -Role "ApplicationImpersonation" -User admin@domain.com
```

Prep Work Phase 4: Push out DMA agent

BitTitan comes with a deployment pro agent that automatically configures outlook profiles. This will bring over **autofill settings** and **signatures** for all users. There are two options to push this out:

      a. GPO
      b. Email

Note If we are deploying the agent via gpo, users will just receive a popup asking them to authenticate and will reopen outlook after cutover. If we are pushing the agent out via email, users will receive a message in which they will have to click on a link to install the agent on their device

1. Login to the BitTitan Portal and Click All Customers on the left-hand column

2. Click Add Customer>Fill out Customer Name and primary Domain>Click Save
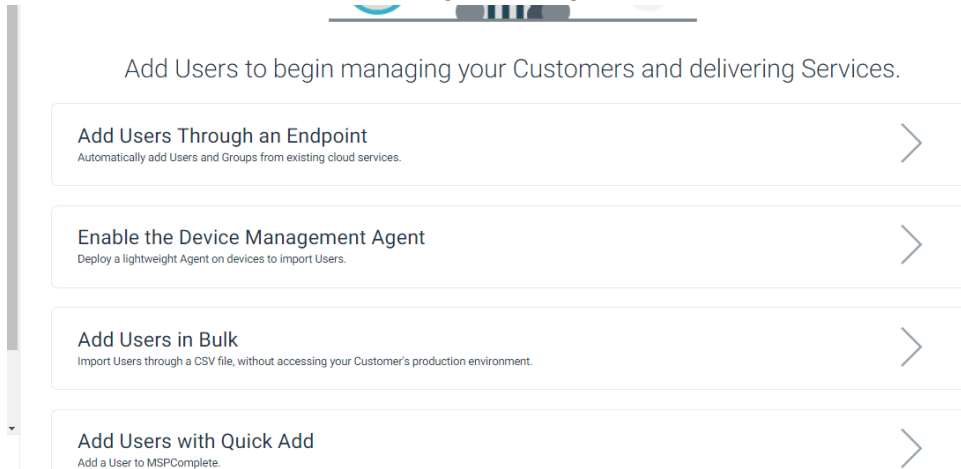
Follow Steps **3-14** if you are choosing to deploy the agent via **GPO**

3. Remote into Primary DC

4. Open Browser and Login to BiTitan.com

5. Go to All Customers>View Users on the Customer you created

6. Click "Enable the Device Management Agent"

7. Follow the steps from the following KB Article which walks you through setting up a new share, placing the exe in the share, creating the gpo, and scheduling it to run :https://help.bittitan.com/hc/en-us/articles/115008110847

8. Monitor users that successfully have the agent installed by going to Customers>Select customers>Manage>Device Management>Deployment pro

You will need to put in the destination domain and add the 365 endpoint

Once users start to login to their computers, their device will be registered and their primary upn will be listed "Primary Email Address" column

9. Users computers will be listed and will have a "heartbeat". Once a user signs into the device their email will be tied to the device in a one to one relationship.

Computer Name ↓	Number of Users	Agent Status
AR-004	1	✔
ARDEB	1	✔
AS400CONSOLE-PC	1	✔
BILLINGSARAH	1	✔
BROKERAGEJD-CR	1	✔

* If a status shows a ? symbol it most likely means the computer is shut down and the tool hasn't been able to find a heartbeat in over 4 hours*

CRDTAPP	2	✔
CRDT-AR-DLS	1	❓

11. Once all users have populated and have the DMA agent installed, Schedule the cutover date for the agent to run on their computer. (This is after you point MX records to office365)

Schedule DeploymentPro

Schedule for Profile Cutover

This is the date and time scheduled for DeploymentPro to run on your Users' machines. The module will install on their devices at the next heartbeat, and then run silently until:

Select a date.
May 11th, 2018 11:30am

The time specified is (America/Denver).

Subscribed Users (no license required): 1

License Consumption

Users	License per User	Total Licenses Required
1	1	0

User Destination Email

The Destination email address is the email address of the new profile after it has been configured.

Source Email	Destination User Principal Name	
		@crtrans.biz

Cancel   Schedule Cutover

Note If there are multiple domains involved you will have to go to "settings" in the deployment pro page and change the domain for the users who need the separate domain

12. Once the agent is scheduled successfully, all users should change to a status of "running"

13. If the status does not say "running" but remains in "scheduled" reschedule again until it moves into a **running status**

14. If users are not being picked up with the GPO, troubleshoot with one remote end user:

- Run Gpresult on their computer to see if the GPO is running
- If the GPO is running, try running the exe manually to see if it is blocked but a firewall setting
- If it is blocked, then create an exception to the firewall to allow the exe to run.
- If it is not being blocked check to see if there are any web proxy settings that may be blocking communication back to bittitan

15. *This completes the steps for setting up DMA via GPO. If you have completed this successfully then move on to the next section. If you are deploying the agent via email, follow steps 16-26.*
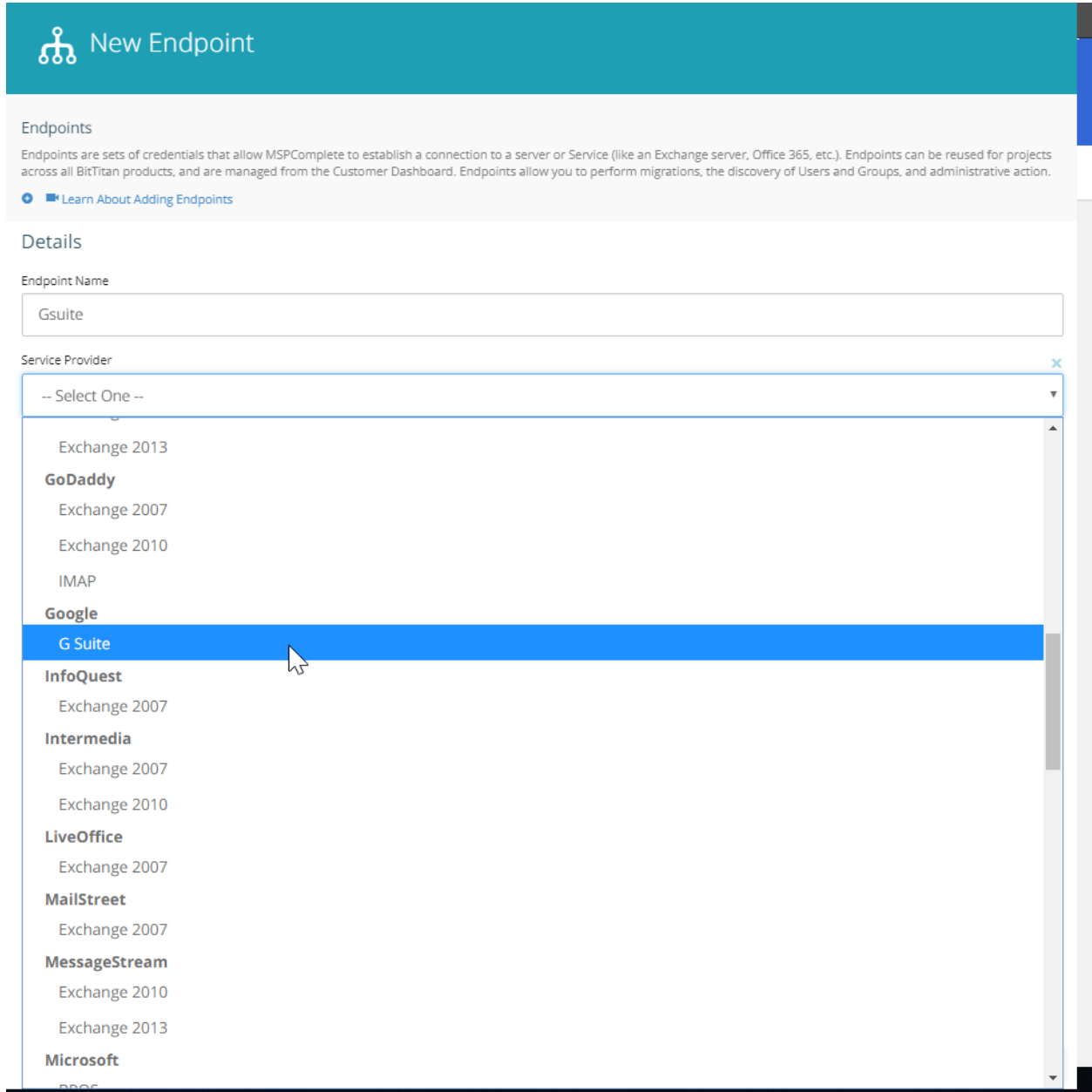
![T-MINUS 365 logo]

Deploying DMA via EMAIL

16. In the BitTitan portal, go to All Customers and select the customer you created

17. Click Add Users Through an Endpoint
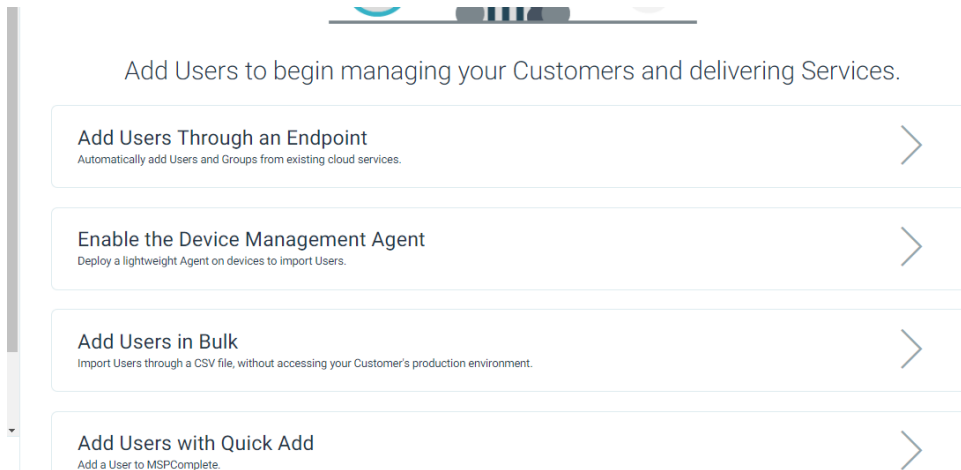
18. Click Manage Endpoint>Add Endpoint

19. Add the G Suite Endpoint and Provide the primary domain involved and Admin Email Address:

New Endpoint

Endpoints

Endpoints are sets of credentials that allow MSPComplete to establish a connection to a server or Service (like an Exchange server, Office 365, etc.). Endpoints can be reused for projects across all BitTitan products, and are managed from the Customer Dashboard. Endpoints allow you to perform migrations, the discovery of Users and Groups, and administrative action.

+ ◼ Learn About Adding Endpoints

Details

Endpoint Name

> Gsuite

Service Provider ✕

> G Suite ▼

From the drop-down menu, select a Service Provider. Based on your selection, we will complete the remaining fields for you.

Endpoint Type

> G Suite/Gmail ▼

◉ **Provide credentials**
Providing credentials at the endpoint level allows you to have a centralized set of credentials that can be used across BitTitan products.

◯ **Do not provide credentials.**
If credentials are not provided at the endpoint level, you will need to provide per-user credentials when using the endpoint as part of your projects.

Domains

> Enter a domain   🗑   +

Importing Users from a G Suite/Gmail endpoint requires an administrator email address.

Administrative Email Address (Optional)

> Enter administrator email address

Close   Add

Note This will autodiscover users from G Suite and populate them in the BitTitan portal

26

20. From here you can select users by checking the box next their name and selecting "Enable Device Management Through Email"

21. Enter a valid email in the "From" section of the template and click Send Email

Note You can white label this email specific to the content you want users to receive. This email is specific to the user and **cannot be forwarded** to another user for them to click on the link for the exe file. The User Simply clicks on a link to open a new page and clicks on one more link to download the exe file

22. Monitor users that successfully have the agent installed by going to Customers>Select customers>Manage>Device Management>Deployment pro

You will need to put in the destination domain and add the 365 endpoint

Once users start to login to their computers, their device will be registered and their primary upn will be listed "Primary Email Address" column

DeploymentPro

Home > Customers > Cardinal Transport > Device Management > DeploymentPro

DeploymentPro

Settings

Use BitTitan PowerShell to schedule DeploymentPro for a large number of mailboxes. Read more.

126	**80**	**1999059**
Total Users	Total Devices	Licenses Owned

▶ Schedule Cutover

Sort ▼

	Primary Email Address	Destination UPN	Module Status	Not Started	Scheduled	Running	Completed	Error
☐			Scheduled on Apr 9, 2018 11:30am	0	0	0	1	0
☐			Scheduled on Apr 7, 2018 12:15pm	0	0	0	1	0
☐			Scheduled on Apr 7, 2018 9:45am	0	0	0	1	0
☐			Not scheduled	5	0	0	0	0
☐			Not scheduled	1	0	0	0	0
☐			Not scheduled	1	0	0	0	0

23. Users computers will be listed and will have a "heartbeat". Once a user signs into the device their email will be tied to the device in a one to one relationship.

Home > Customers > Cardinal Transport > Device Management > **Computers**

Services	**Computers**

80 Computers

Computer Name ↓	Number of Users	Agent Status
AR-004	1	✔
ARDEB	1	✔
AS400CONSOLE-PC	1	✔
BILLINGSARAH	1	✔
BROKERAGEJD-CR	1	✔
BSCHAFFERZ	1	✔

* If a status shows a ? symbol it most likely means the computer is shutdown and the tool hasn't been able to find a heartbeat in over 4 hours*

CRDTAPP	2	✔
CRDT-AR-DLS	1	❓

29

24. Once all users have populated with a and have the DMA agent installed, Schedule the cutover date for the agent to run on their computer. (This is after you point MX records to office365)

Schedule DeploymentPro

Schedule for Profile Cutover

This is the date and time scheduled for DeploymentPro to run on your Users' machines. The module will install on their devices at the next heartbeat, and then run silently until:

Select a date.
May 11th, 2018 11:30am

The time specified is (America/Denver).

Subscribed Users (no license required): 1

License Consumption

Users	License per User	Total Licenses Required
1	1	0

User Destination Email

The Destination email address is the email address of the new profile after it has been configured.

Source Email	Destination User Principal Name		
▓▓▓▓▓▓	▓▓▓▓▓	🖉	@crtrans.biz

Cancel   **Schedule Cutover**

Note If there are multiple domains involved you will have to go to "settings" in the deployment pro page and change the domain for the users who need the separate domain

25. Once the agent is scheduled successfully, all users should change to a status of "running"

				Not Started	Scheduled	Running
Primary Email Address	Destination UPN	Module Status				
		Scheduled on Apr 30, 2018 9:15am		0	0	0
		Scheduled on Apr 30, 2018 4:00pm		0	0	0
		Scheduled on Apr 30, 2018 9:15am		1	0	1
		Scheduled on Apr 30, 2018 9:15am		0	0	1

26. If the status does not say "running" but remains in "scheduled" reschedule again until it moves into a running status

Prep Work Phase 5: Setup BitTitan Project

1. In BitTitan Portal, Open MigrationWiz by clicking on waffle icon at top of the page>Click Mailbox Migration

2. Click Create Project>Select 'Create a Mailbox Project'

3. Name the Project and select your customer from the dropdown>Click Next Step
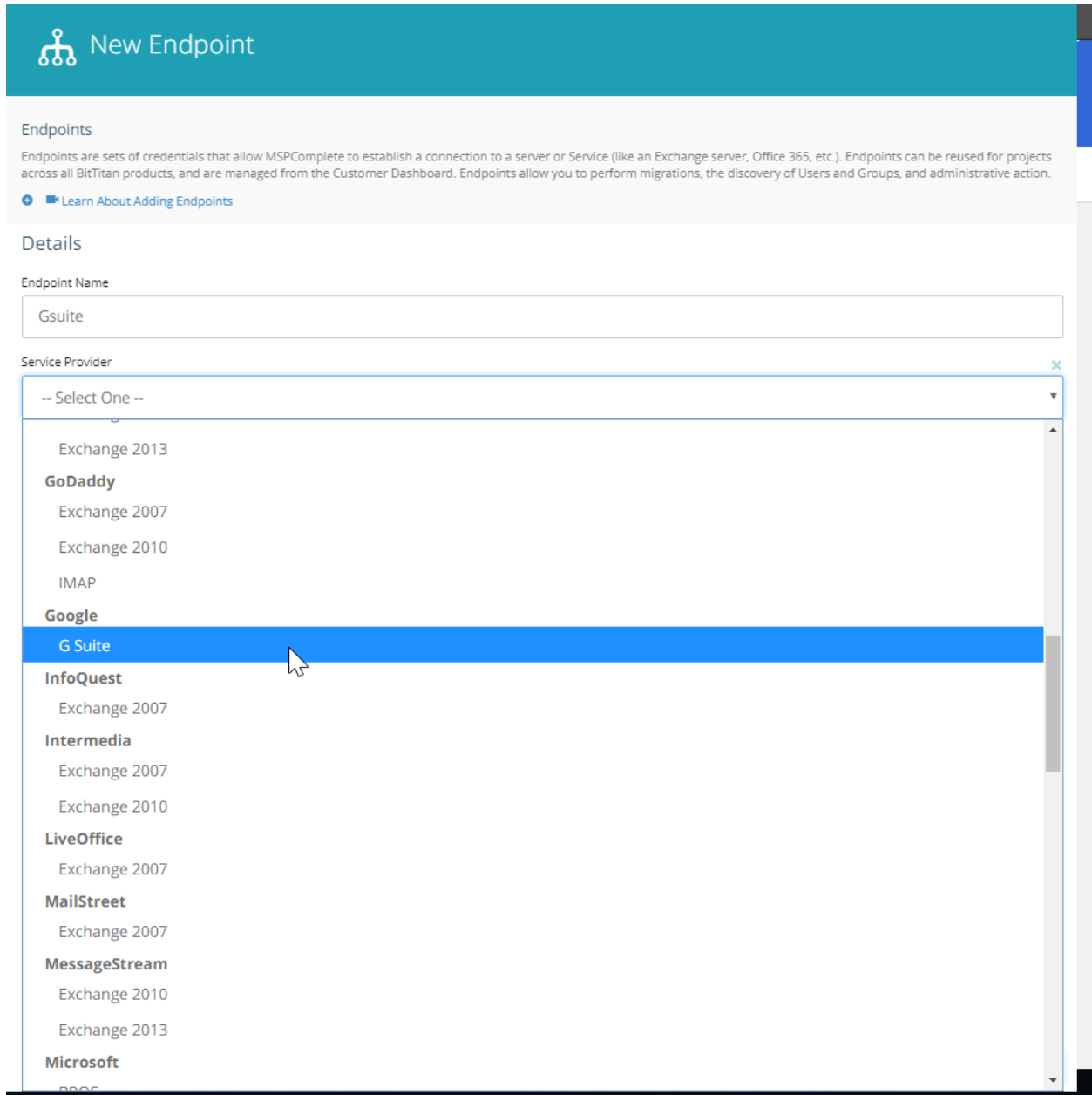
4. If you followed the steps for email deployment for the DMA agent you should be able to select your endpoint from the dropdown. If you did not, Select New and fill out the fields as shown below:

![T-MINUS 365]

New Endpoint

Endpoints

Endpoints are sets of credentials that allow MSPComplete to establish a connection to a server or Service (like an Exchange server, Office 365, etc.). Endpoints can be reused for projects across all BitTitan products, and are managed from the Customer Dashboard. Endpoints allow you to perform migrations, the discovery of Users and Groups, and administrative action.

⊕ ▪️ Learn About Adding Endpoints

Details

Endpoint Name

```
Gsuite
```

Service Provider   ✕

```
G Suite                                                                      ▾
```

From the drop-down menu, select a Service Provider. Based on your selection, we will complete the remaining fields for you.

Endpoint Type

```
G Suite/Gmail                                                                ▾
```
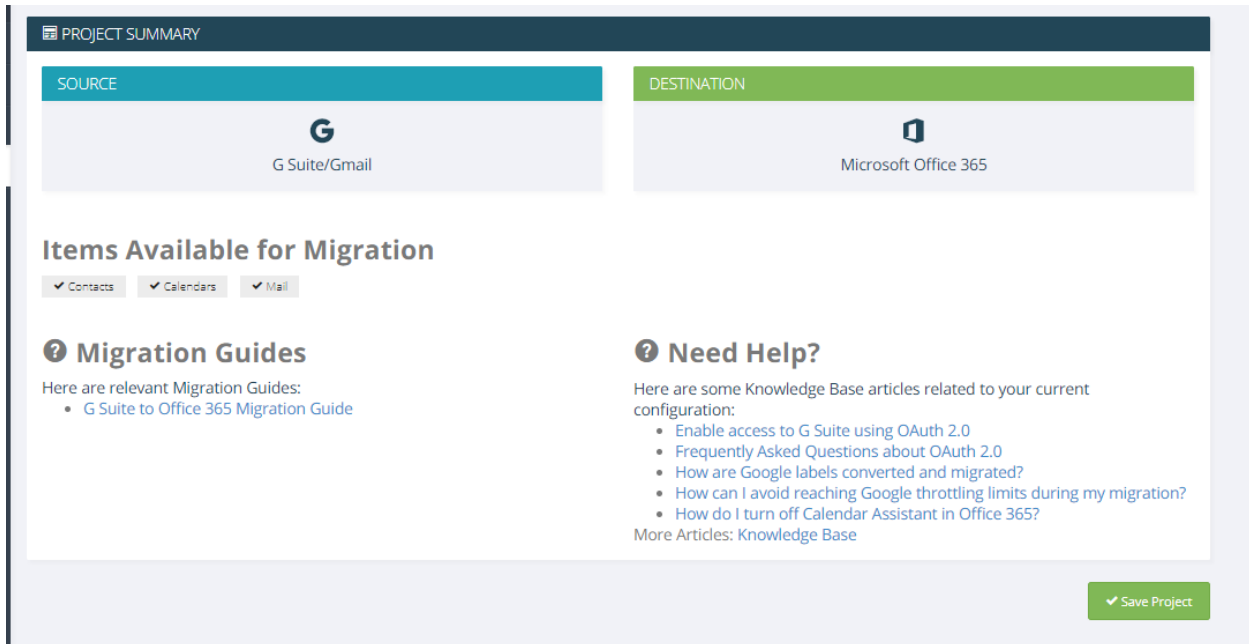
◉ **Provide credentials**
   Providing credentials at the endpoint level allows you to have a centralized set of credentials that can be used across BitTitan products.

○ **Do not provide credentials.**
   If credentials are not provided at the endpoint level, you will need to provide per-user credentials when using the endpoint as part of your projects.

Domains

```
Enter a domain                                              | 🗑 | + |
```

Importing Users from a G Suite/Gmail endpoint requires an administrator email address.

Administrative Email Address (Optional)

```
Enter administrator email address
```

[Close] [Add]

5. In the Destination Settings, Click New, and add the 365 endpoint. Providing the admin credentials

6. Click "Save and Go to Summary" This tells you what is eligible to move and gives you additional KB articles you can reference. Click 'Save Project' when you are ready to proceed

7. Add items to your project. If you already added users to the MSP complete portal either through GPO or an endpoint. You can select "Add from MSP Complete". If you have not yet, then you can select Autodiscover items to import users to the portal. Additionally, you could bulk upload users via CSV. (Great time saver is to use the CSV you pulled from Prep Work Phase 1 and copy/paste it into BitTitan's template)

8. Audit User names and Domains (Make sure they match 365). Clean up user-list. Verify the Source and Destination domains are correct.

9. Select All Users>Verify Credentials

10. There are numerous errors that could appear here. Most of the steps I made for prep work will make it so that you avoid most of these errors. Refer to BitTitans KB articles for most common errors and how to troubleshoot. https://help.bittitan.com/hc/en-us/sections/115003465187-Mailbox-Error-Lookup?page=2

Unsuccessful verification will show a "Failed" Message

You can click on the Failed icon to show a detailed message of what failed

Click on "Learn More" to access BitTitan's Relevant kb articles specific to the error:

Successful Verification will show a "Completed(Verification)" message

11. After all users have successfully completed verification, Select All users>Click on the Hamburger icon at the top of the toolbar> Click Subscribe Users
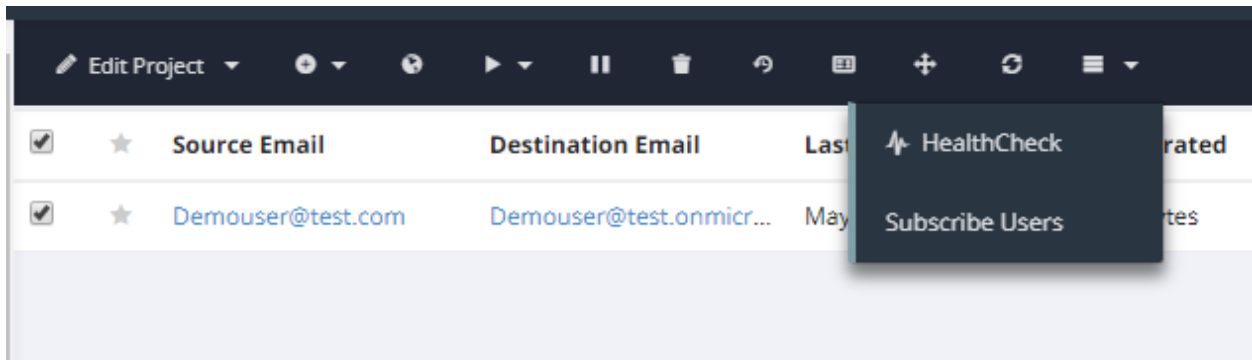
12. This will bring you back to the MSP complete portal. Select all users>Click Apply User Migration Bundle
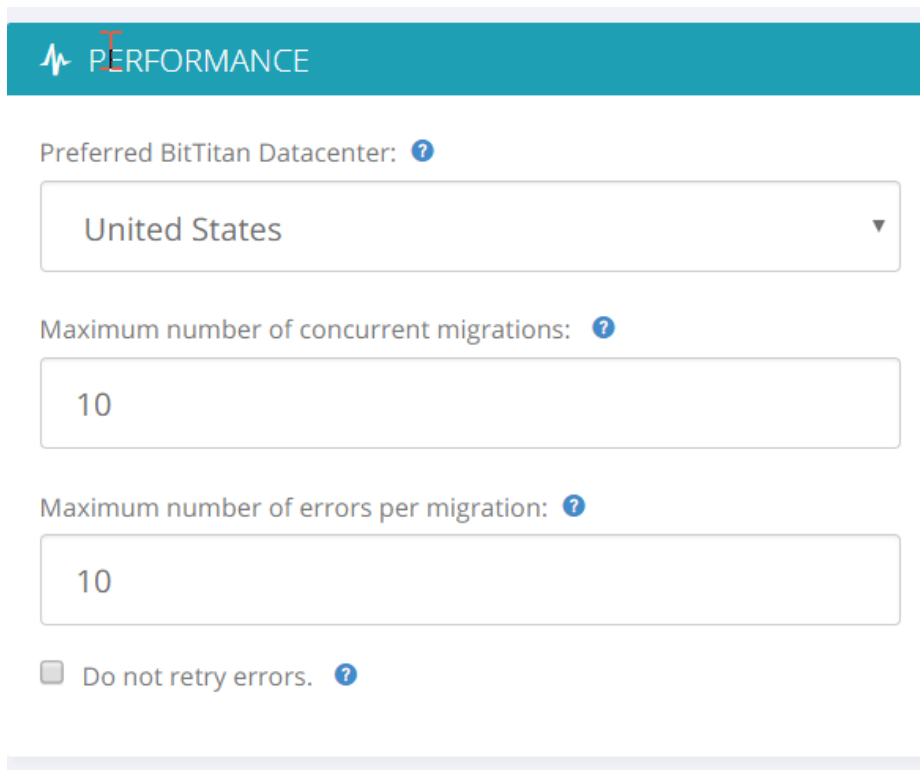

13. This takes a couple of minutes to propagate but after, in the migrationwiz portal the "User Migration Bundle" column will change from "No" to "Yes"

14. Go to Edit Project>Advanced Settings>Set Maximum # of Concurrent Migration (Guideline 3 per 1Mbps of Bandwith)>Save

NOTE This step isn't as important for G Suite migration because your uploads speeds will generally be very fast
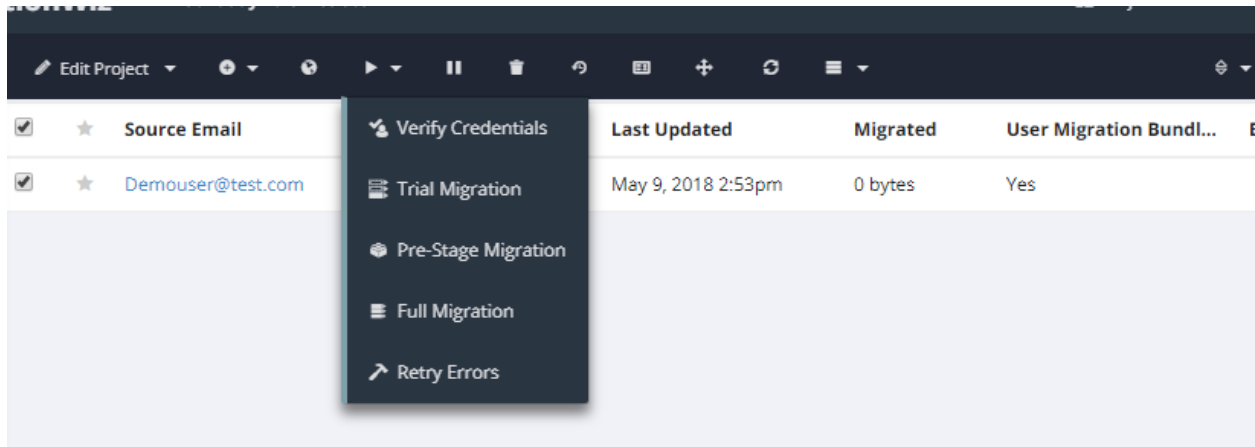

Migration Phase 1

---

1. Preferably start at beginning of the week to bring over a bulk of the mail, plan for domain cutover on Friday evening

Note During a pre-stage Pass BitTitan is simply making copies of mail in 365. The user will experience no loss of data during this time*

2. Select All Users>Click on the start button>Pre-stage Migration

3. Select a time range from the dropdown of prior to 90 days>Start Migration
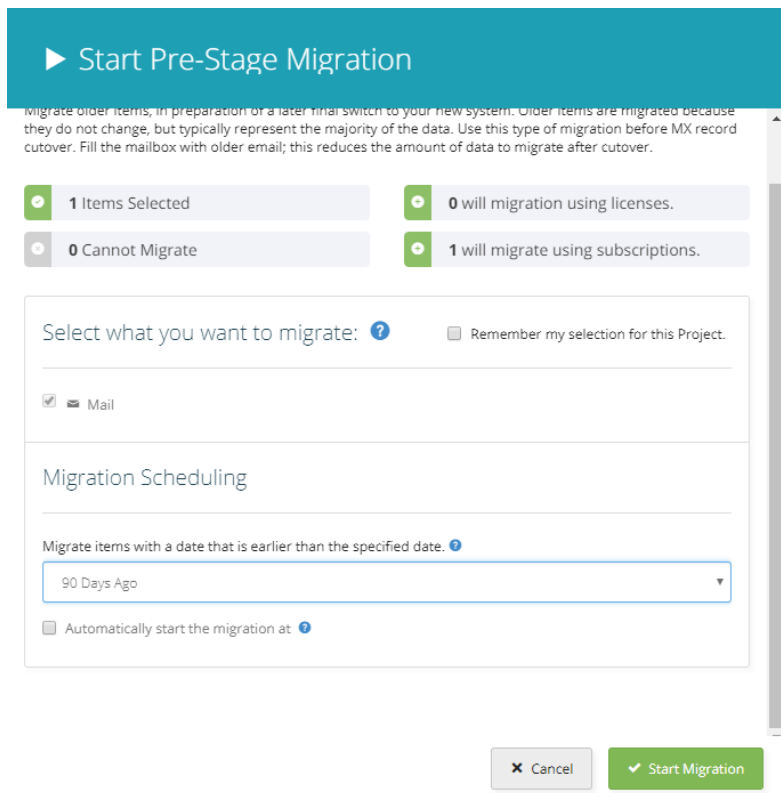
4. This will give you a status bar and show the amount of data moved over in the "bytes" column. If any users fail, it's usually do to server timeout. Simply rerun the pre-stage pass on these users to restart where it left off. If you click on any user's name, you can see metrics like upload speeds:

5. Once the pre-stage migration has run for all users and is in a "Completed" Status

6. Next we are going to perform a full migration to bring over copies of remaining mail plus calendars, contacts, notes, journals, rules. Select All users>Click on the start button>Full Migration

7. You can schedule this to start at a specific time if you would like:

8. Confirm all users go into a "Completed" Status

Migration Phase 2: MX Cutover

1. At Designated time, login to DNS provider and change you MX records to point to Office365
   a. You can find this in the 365 Admin Center by going to Setup>Domains
   b. Office365 MX record follow this format **Domain-com.mail.protection.outlook.com**

2. Run another Full Pass. This will perform a **delta sync** to pull over any residual data that may have been missed.

Migration Phase 3: Post Migration Cleanup

1. Audit Destination Environment Mailflow for Inbound/Outbound Mail

2. Login to BitTitan>Go to All customers>Select customer>Manage>Device Management>Deployment Pro

3. Make sure DMA status has moved into "Completed" status. If in "error" status it means the users failed authentication 3x. Reschedule the tool to run at the next time interval available

4. Reconfigure any mailbox permissions

5. Send out guides on reconfiguring mail on Iphone/Andriod:
    a. https://support.office.com/en-us/article/set-up-email-using-the-ios-mail-app-7e5b180f-bc8f-45cc-8da1-5cefc1e633d1
    b. https://support.office.com/en-us/article/set-up-email-in-android-email-app-71147974-7

6. Perform and account clean up that is required