BAE SILVERSKY TO OFFICE 365 MIGRATION PLAYBOOK

PROPERTY OF T-MINUS 365. ALL RIGHTS RESERVED.

Table of Contents

Planning Phase 1: Gather All the Necessary Credentials 3

Planning Phase 2: Gather and Audit all Users part of the Migration 3

Prep Work Phase 1: Prepare Office 365 4

Prep Work Phase 2: Prepare Source/Destination for BitTitan 8

Prep Work Phase 3: Push out DMA agent 11

- Push out DMA agent via GPO 13
- Push out DMA agent via Email 18

Prep Work Phase 4: Setup BitTitan Project 26

Migration Phase 1 34

Migration Phase 2: MX Cutover 38

Migration Phase 3: Post Migration Clean Up 38

Introduction

There are many customers looking to migrate off of BAE/Silverskys hosted exchange platform. Migrating from this platform is fairly simple and upload speeds are far quicker than your typical exchange environment. This is a step-by-step guide for migrating to Office 365 using the tools from BitTitan

Planning Phase 1: Gather All the Necessary Credentials

1. Credentials Checklist
    a. Office 365 Global Admin Credentials
    b. Provisor Admin Credentials
    c. BitTitan credentials
    d. DNS Login Credentials

Note BitTitan comes with a tool called Deployment Pro which configures 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 to Remote to Primary DC (RDP, TeamViewer, LogMeIn, Splashtop, etc)
f. Enterprise Admin Credentials for Primary DC

Planning Phase 2: Gather and audit all Users part of the Migration

1. Gather Users List in CSV format, Export from the Provisor

2. If using AD Connect with password sync users will have the same password as their on prem active directory. However, if not using AD Connect then you will need to get a list of passwords from BAE users or notify them of what their password will be in 365

3. Gather Distribution List with members of Distribution list in CSV format

4. Verify Organizational Units in Active Directory that will be a part of the GPO/AD Sync

5. Take note of any 3rd partner connectors for email filtering: Symantec, Barracuda, etc. Look up necessary steps for creating connectors in 365

6. Define MX Cutover Time (Typically recommend Friday Evening)

Prep Work Phase 1: Prepare Office 365

---

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 Office 365 Admin Center>Setup Domains>Add Domain

3. Verify Domain with TXT record provided to DNS provider

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 fine. We will add the remaining DNS records after the MX cutover

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

    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:

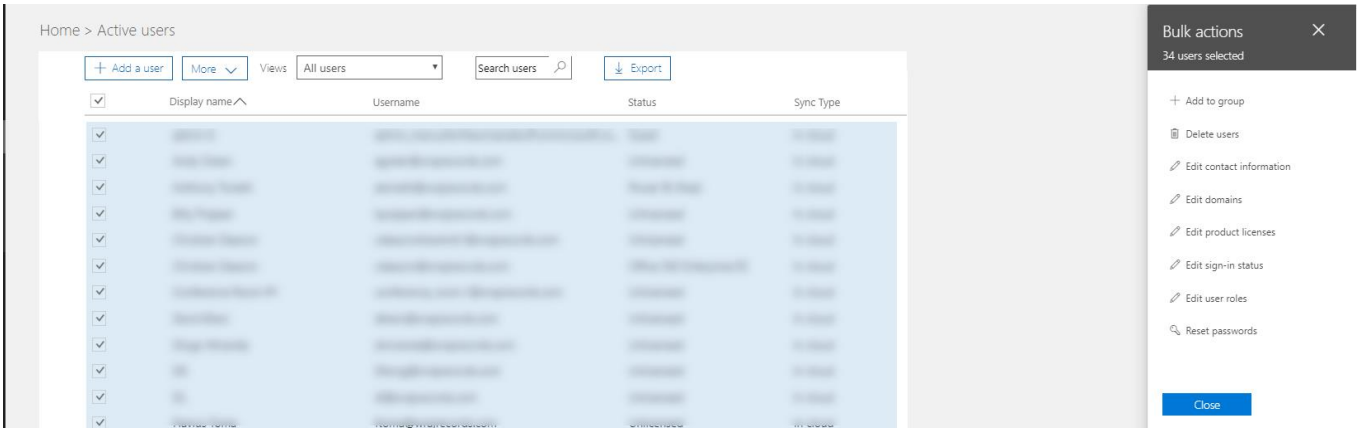
- UserPrincipalName
- FirstName
- LastName
- DisplayName
- Password

#Bulk Import Users with Passwords#

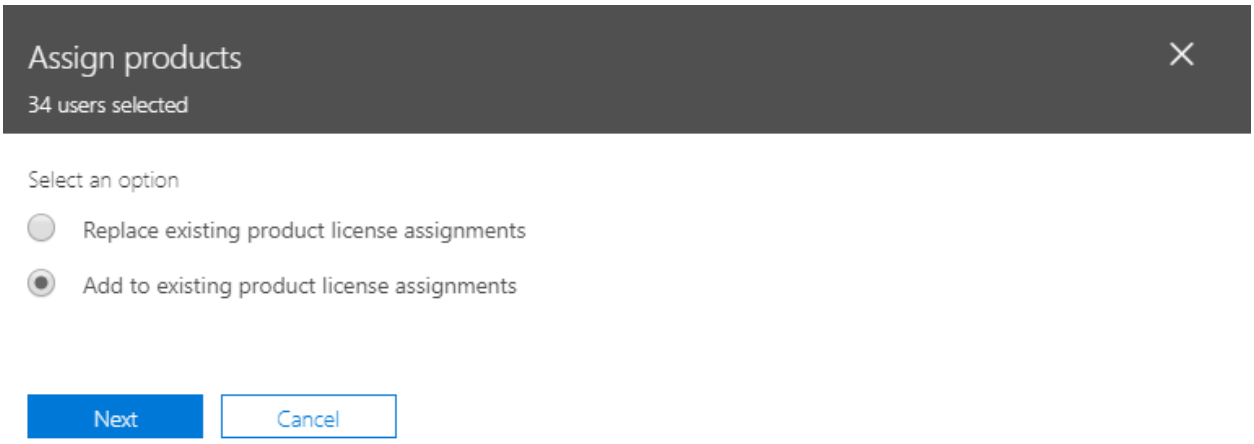
```
#Bulk Import Users with Passwords#

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

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

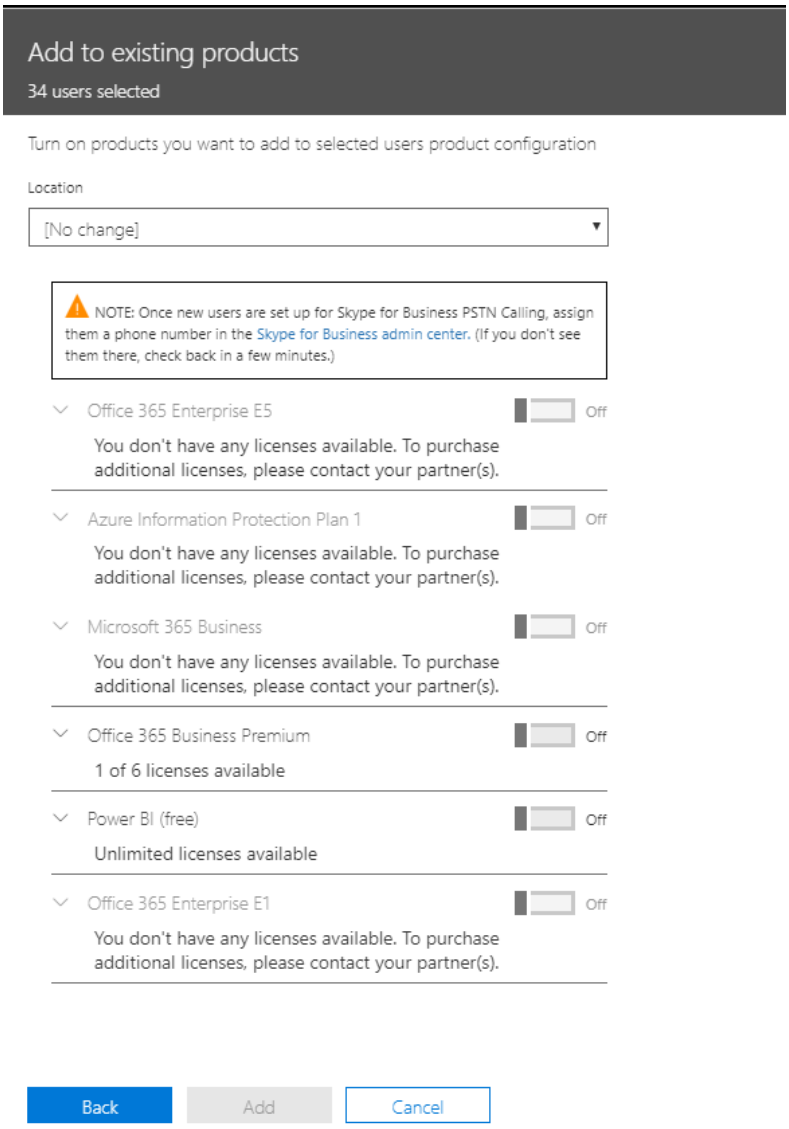
7. Apply Licenses to Users by going to Active Users>Bulk Select Users>Click Edit Product Licenses



8. Click Add to existing product licenses Assignments



9.Toggle on the Appropriate License and Click Add



10. Bulk Upload Distribution List (If applicable)

```
#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}
```

1. Contact BAE support (supportdb@silversky.com) to set admin user with full impersonation rights for all accounts

“Hey Team,

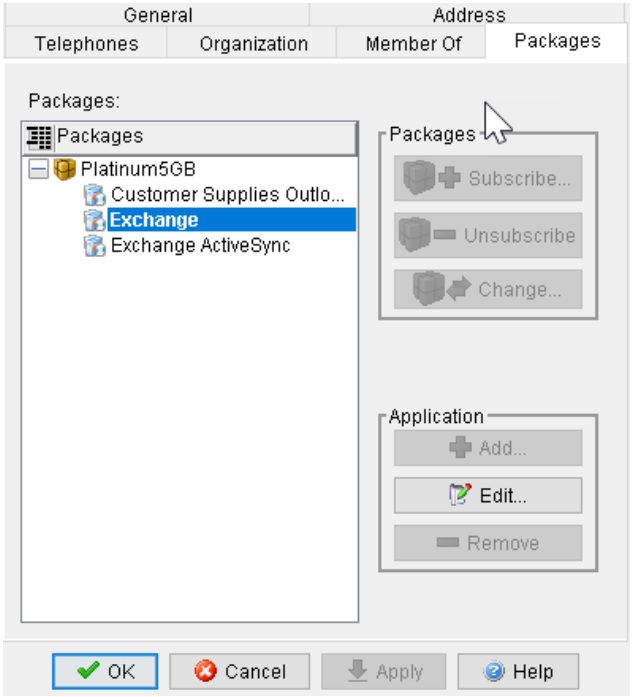
Partner:
Customer:
BAE Product: (ex.BAE Systems 2010 Exchange 25GB)

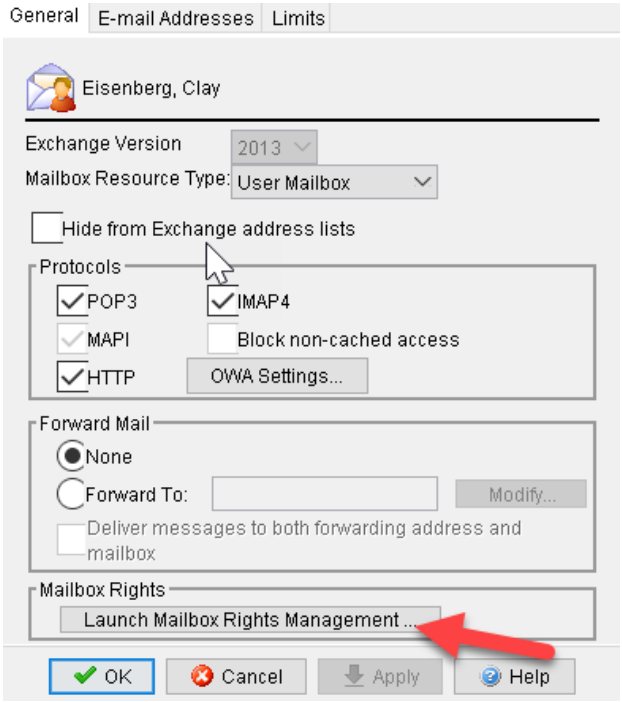
I am performing a migration for this customer. In checking the admin user for BAE, I see that they do not have sufficient permission to impersonate the users mailboxes (This avoids us having to get creds for each user). We just need to run this powershell script for the admin user for this account:

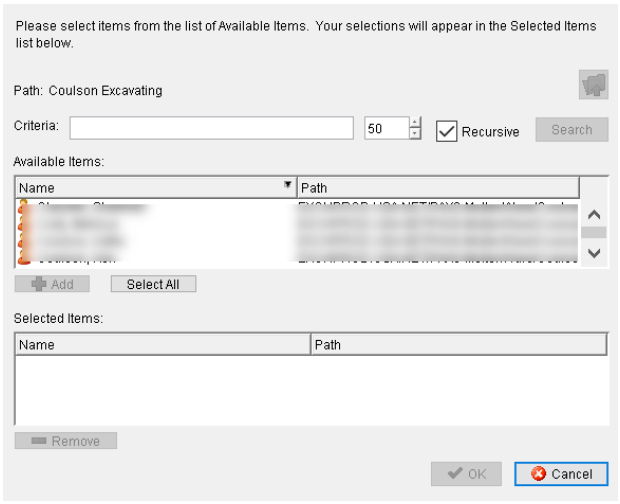
Can you please run this command for the account:
Get-Mailbox -ResultSize Unlimited | Add-MailboxPermission -AccessRights FullAccess -User <admin user>

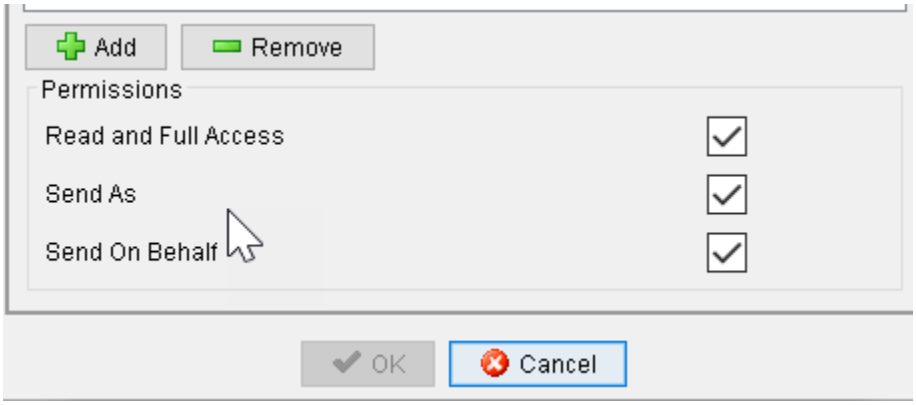
Please let me know if you have any additional questions.

2. If this is a smaller migration, you can also do this manually in the provisor for each user: To give the admin user full mailbox rights to each Users, double click on the User > Packages > Highlight Exchange > Edit > Click
"Launch Mailbox Rights Management" > add the cusrpt and give it Read and Full access









3. 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
```

4. Set Impersonation on Office365. 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
```

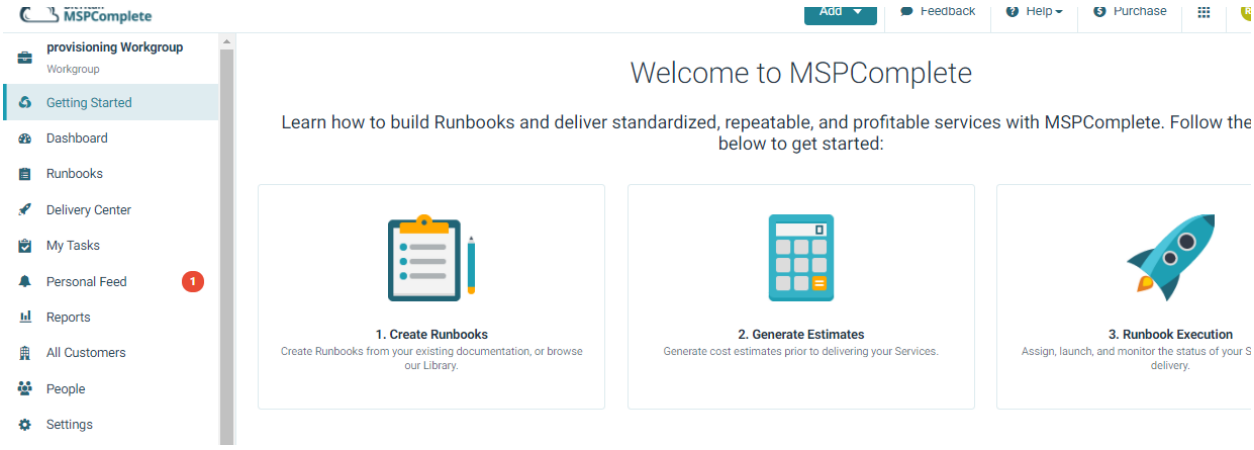
Prep Work Phase 3: Push out DMA agent

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

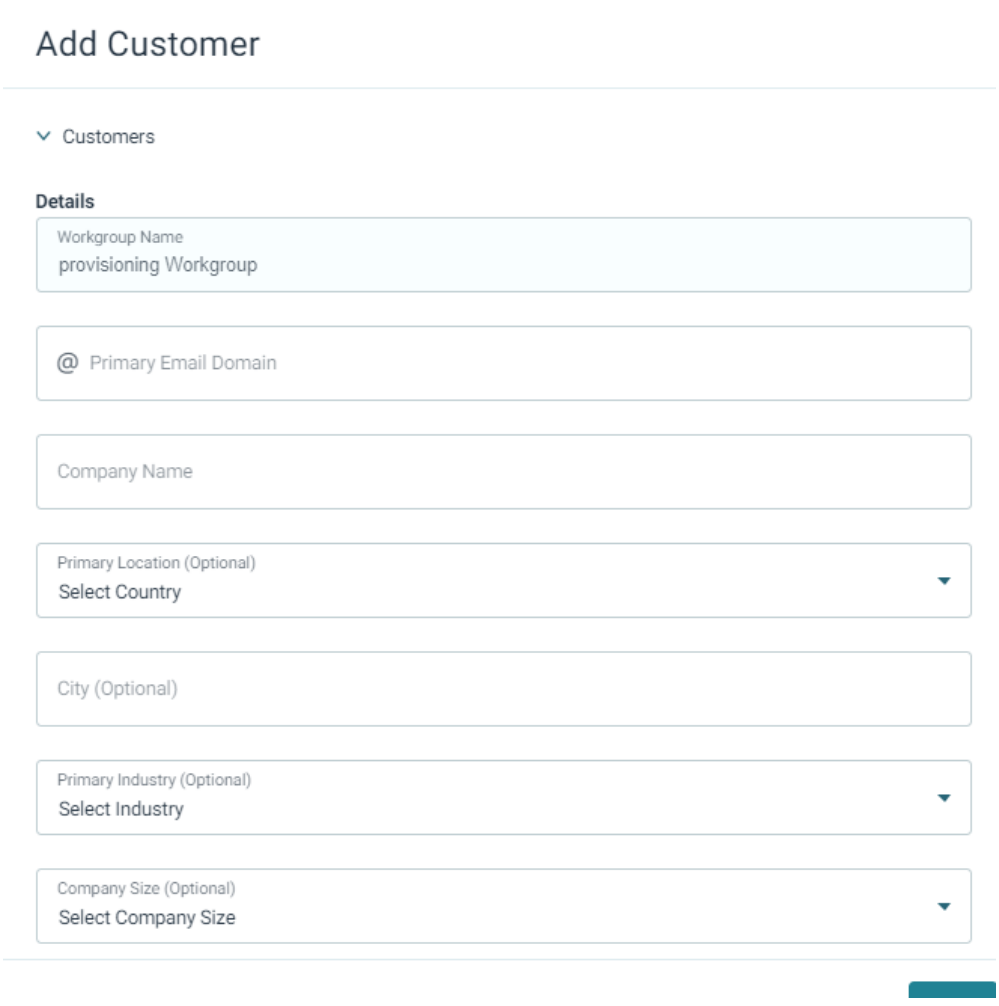
a. GPO
b. Email

Note If we are deploying the agent via gpo, users will just receive a popup asking them to authenticate to 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



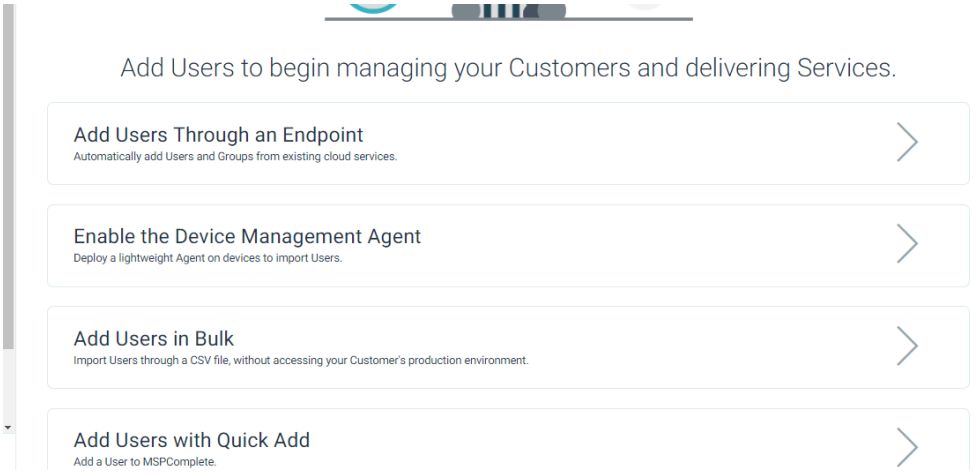
Follow Steps **3-15** if you are choosing to deploy the agent via **GPO**

3. Remote into Primary DC

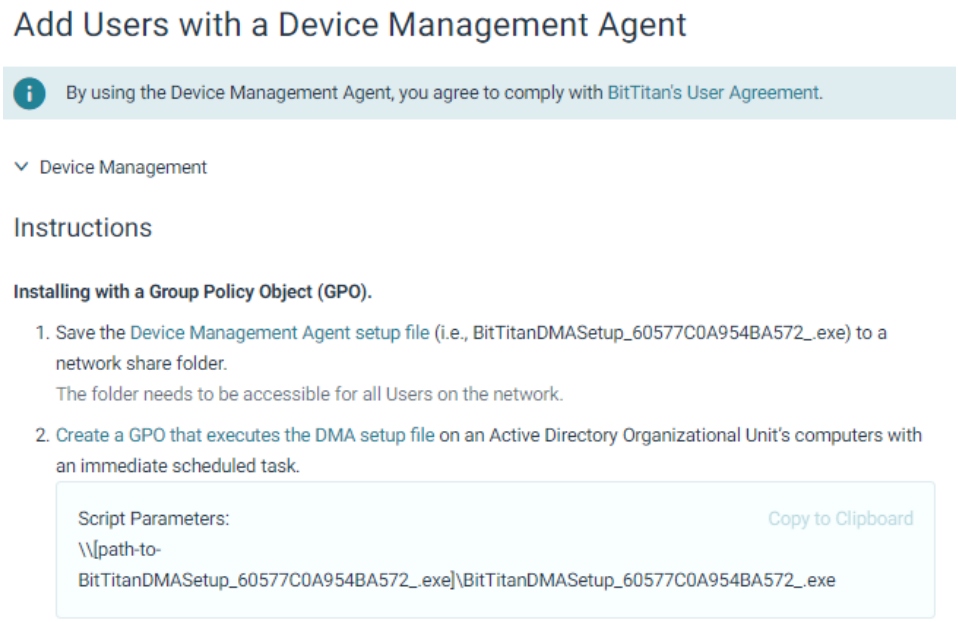
4. Open Browser and Login to BiTitan.com

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

6. Click “Enable the Device Management Agent”

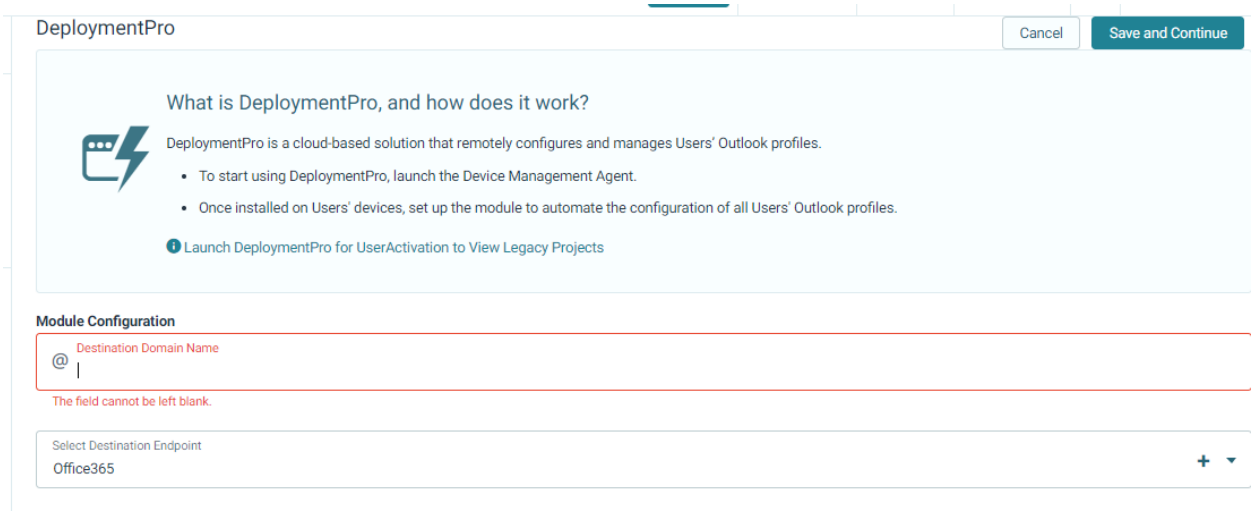


7. Follow the steps from the following KB Article which walks you through setting up a new share, placing the exe in the share, creating the gpo, and scheduling it to run:https://help.bittitan.com/hc/en-us/articles/115008110847

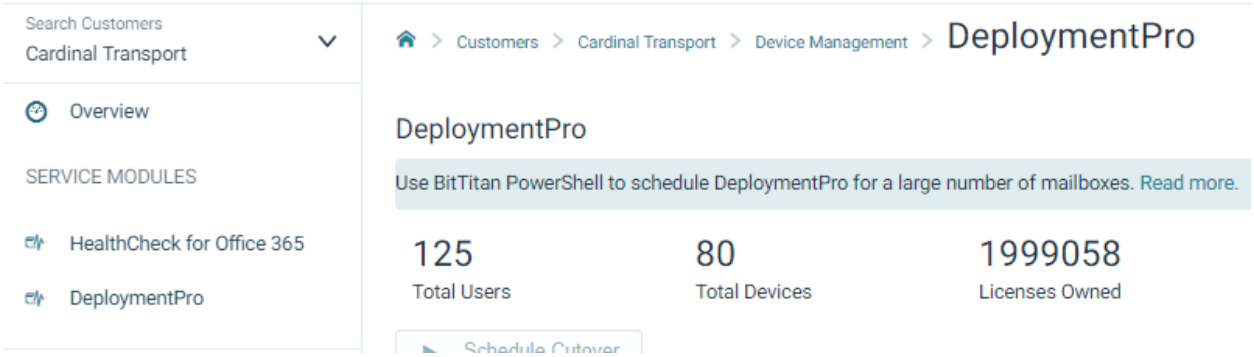


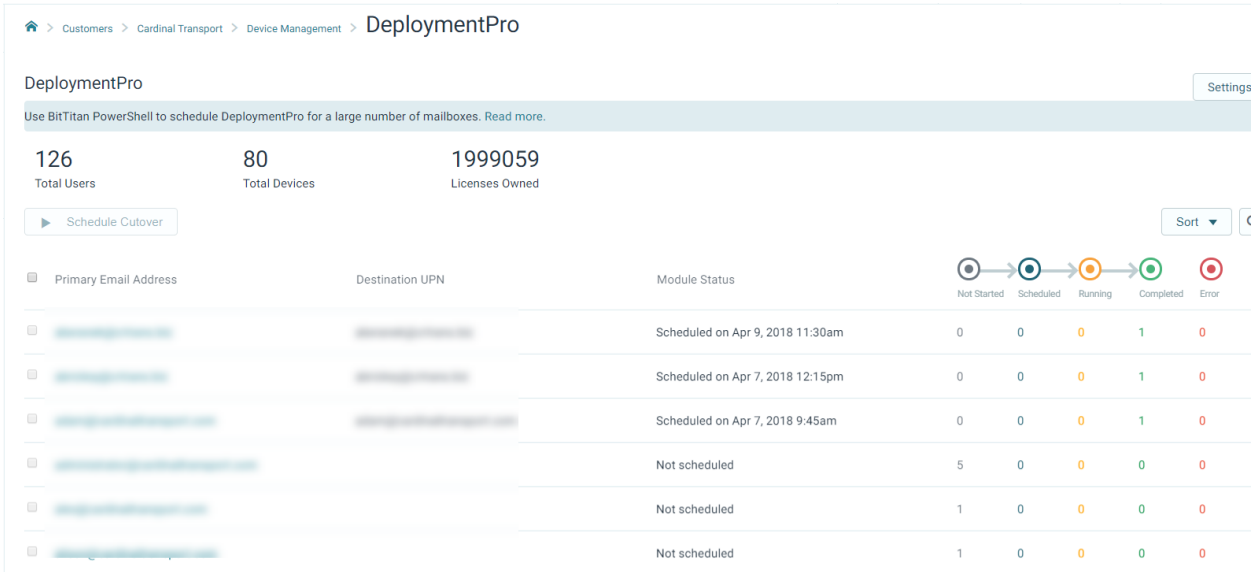
8. Monitor users that successfully have the agent installed by going to Customers>Select customers>Manage>Device Management>Deployment pro

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

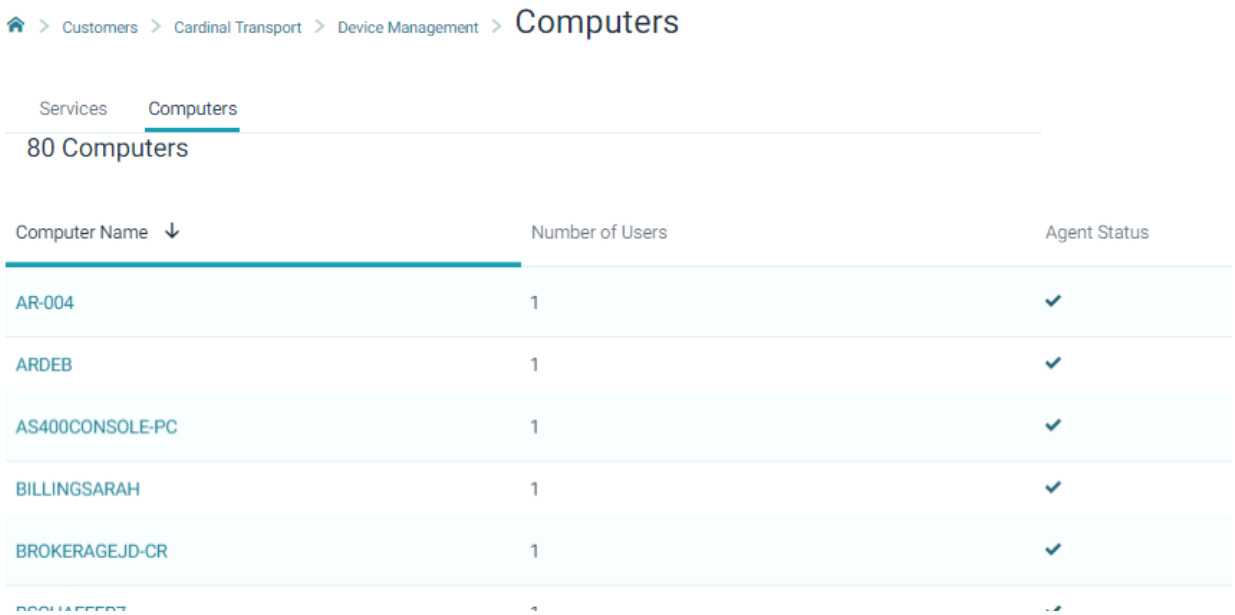


Once users start to login to their computers, their device will be registered and their primary UPN will be listed “Primary Email Address” column

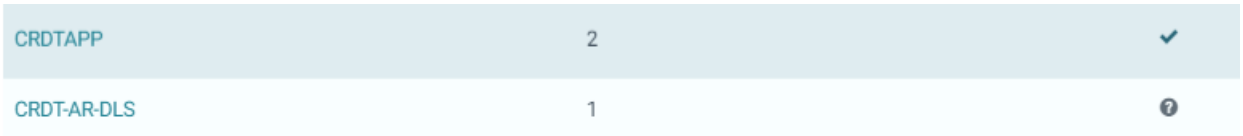




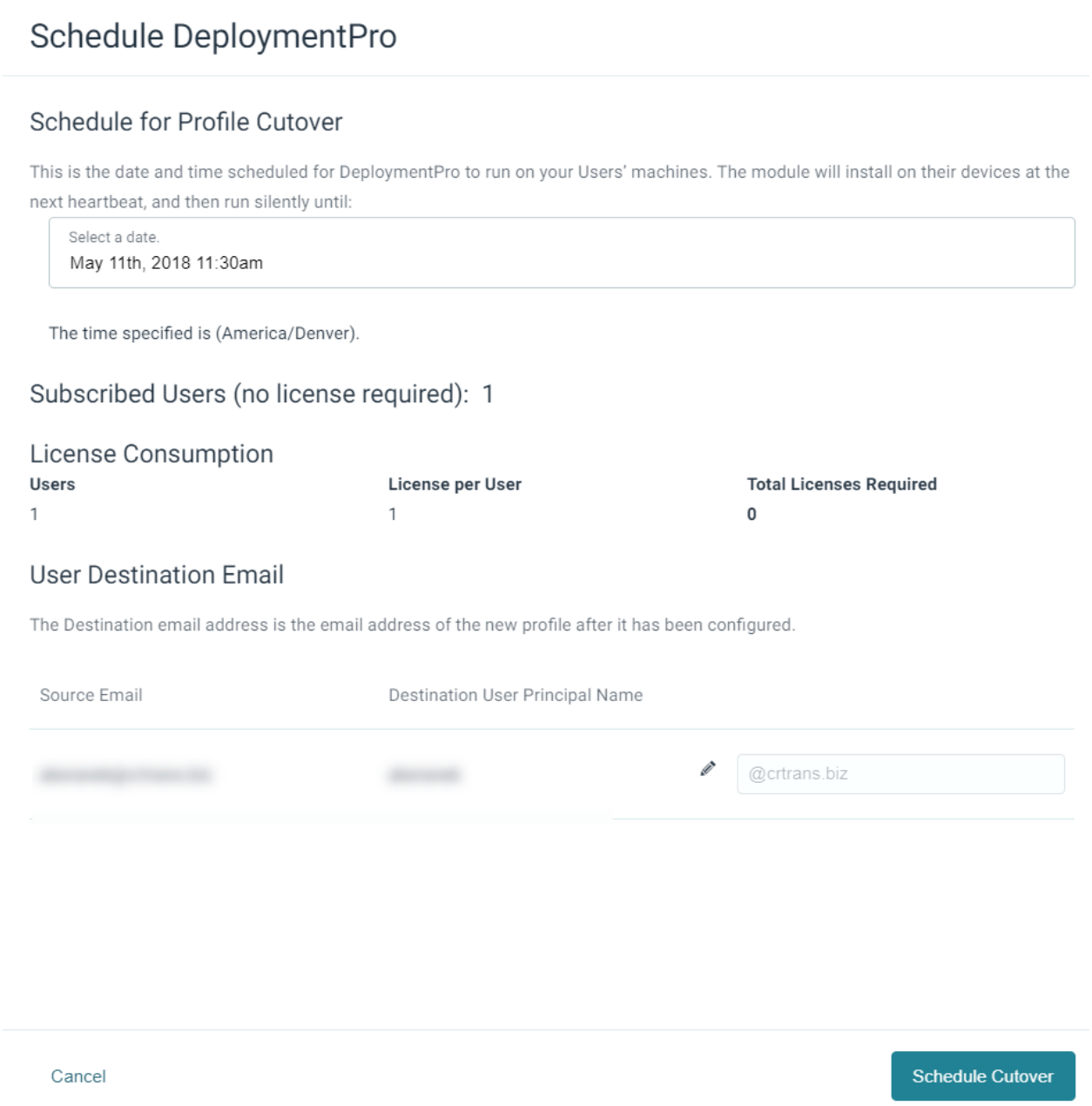
9. Users computers will be listed and will have a "heartbeat". Once a user signs into the device their email will be tied to the device in a one to one relationship.



10.* If a status shows a ? symbol it most likely means the computer is shut down and the tool has been able to find a heartbeat in over 4 hours*

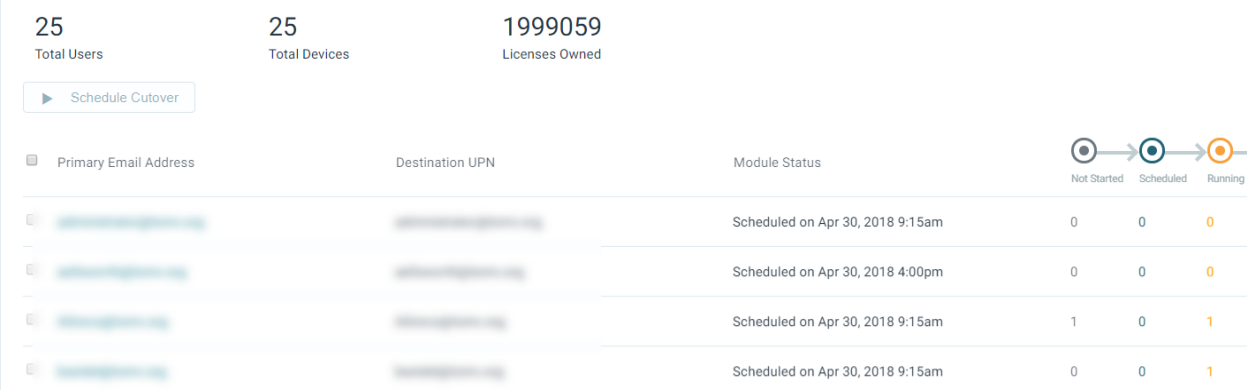


11. Once all users have populated with a and have the DMA agent installed, Schedule the cutover date for the agent to run on their computer. (This is after you cutover MX records)



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 the one remote emote user:

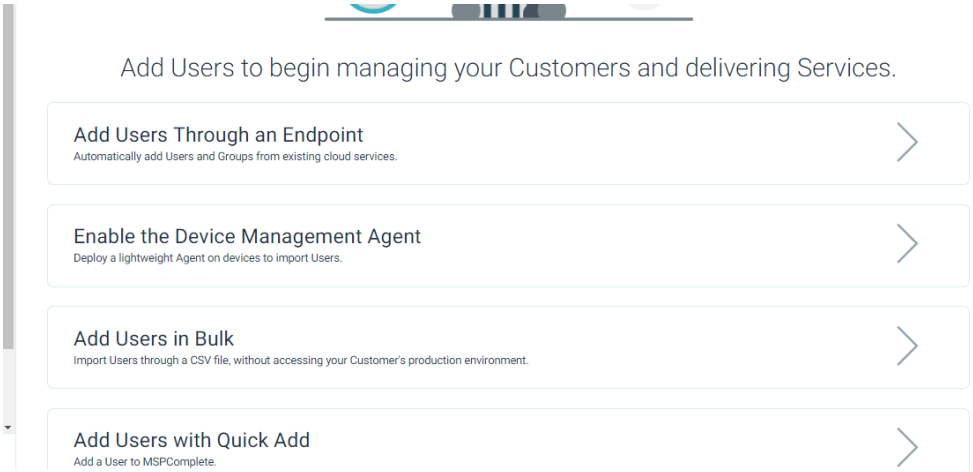
- Run Gpresult on their computer to see if the GPO is running
- If the GPO is running, try running the exe manually to see if it is blocked but a firewall setting
- If it is blocked then create an exception to the firewall to allow the exe to run.
- If it is not being blocked check to see if there are 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.

Deploying DMA via EMAIL

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

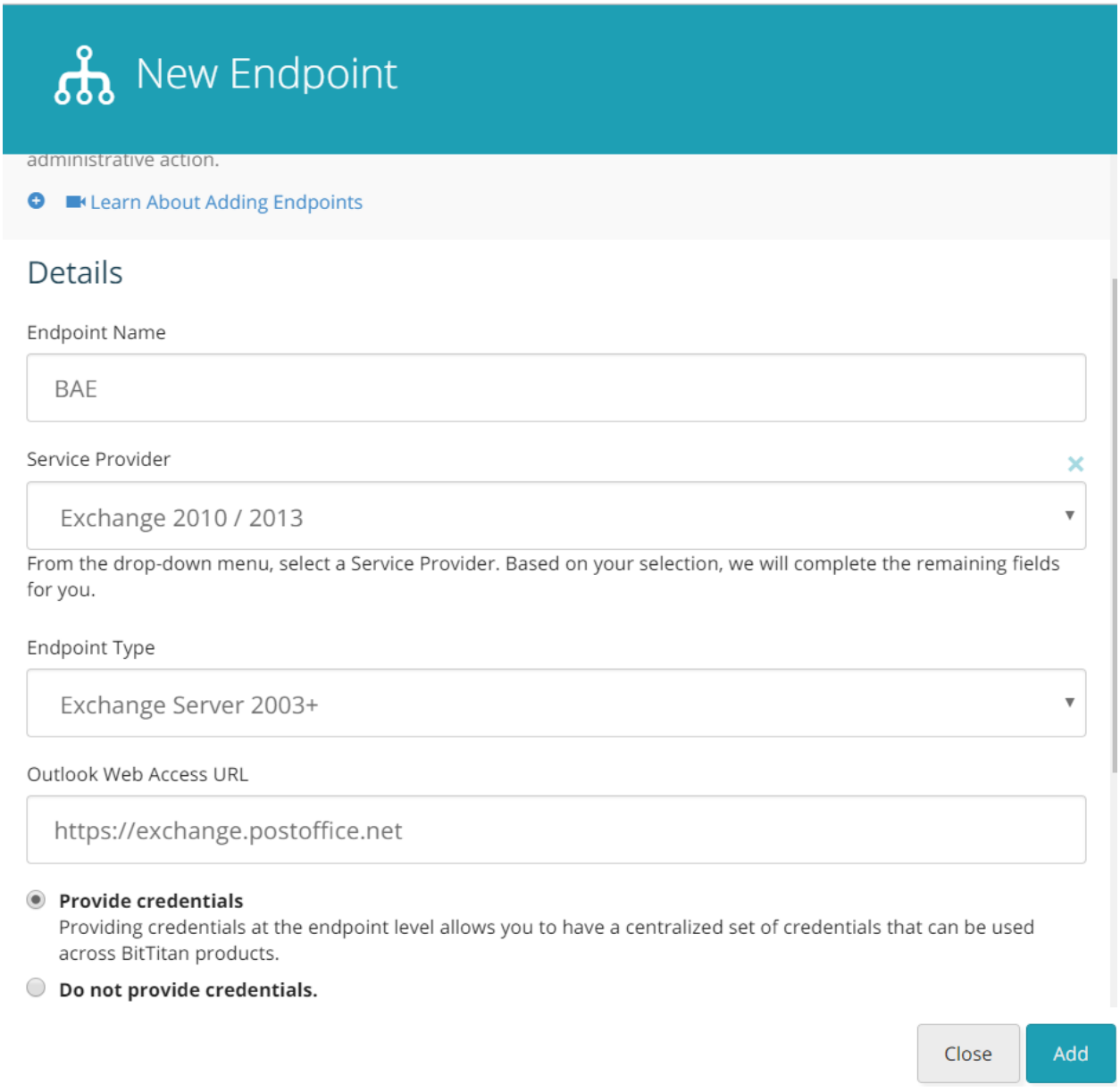
17. Click Add Users Through An Endpoint



18. Click Manage Endpoint>Add Endpoint

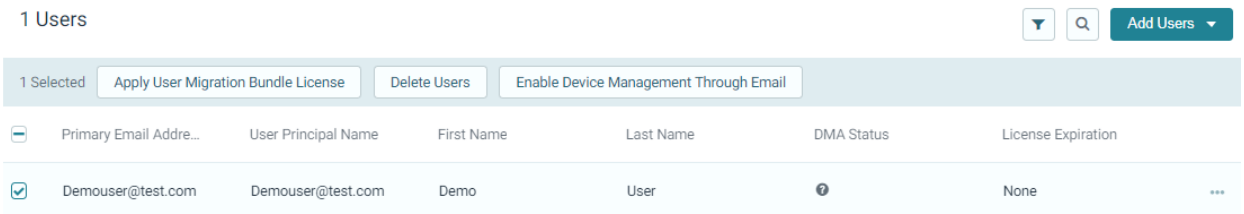
19. Add the BAE Endpoint from the “Find my Service Provider” dropdown and Provide the Administrative Credentials

Note This is found alphabetically under “Silversky”

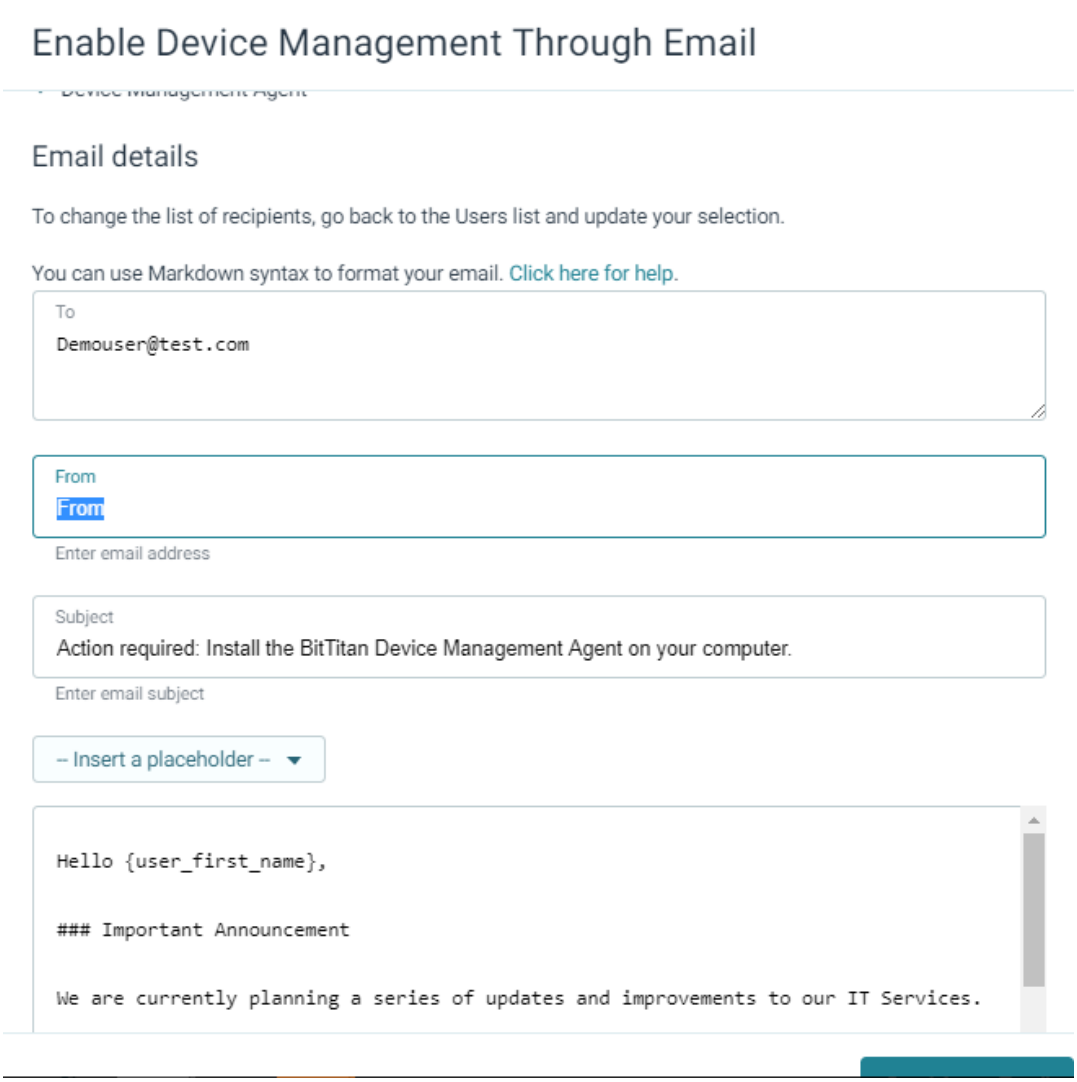


Note This will autodiscover users from BAE and populate them in the BitTitan portal

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



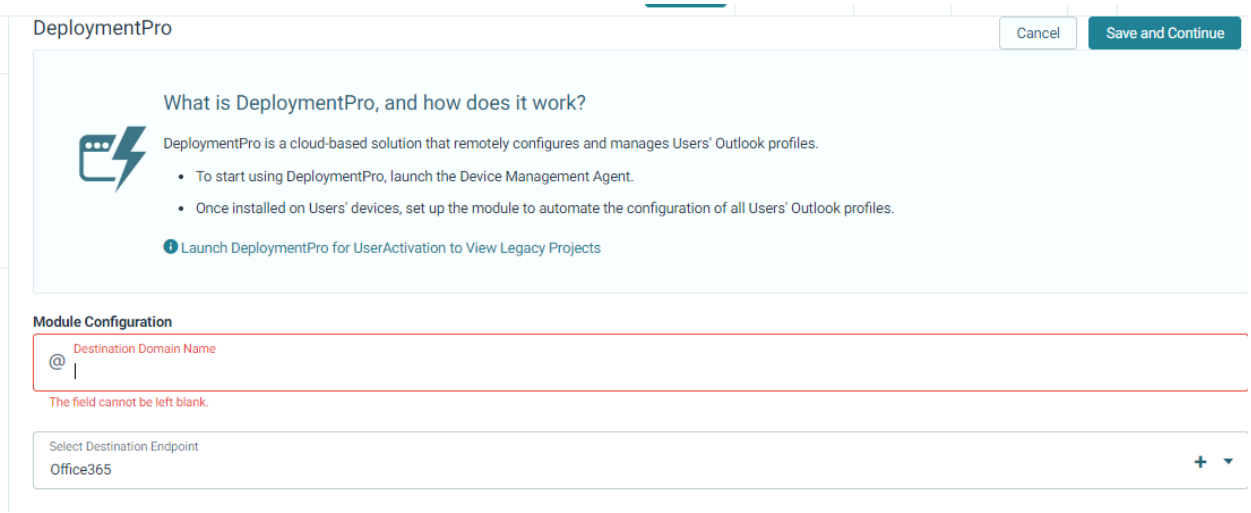
21.Enter a valid email in the “From” section of the template and click Send Email



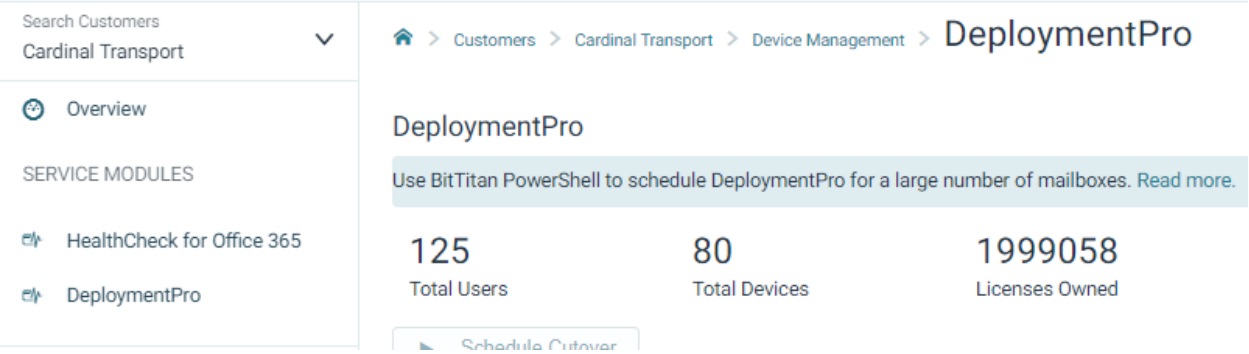
Note You can white label this email specific to the content you want users to receive. This email is specific to the user and cannot be forwarded to another user for them to click on the link for the exe file. The User Simply clicks on a link to open up a new page and click on one more link to download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

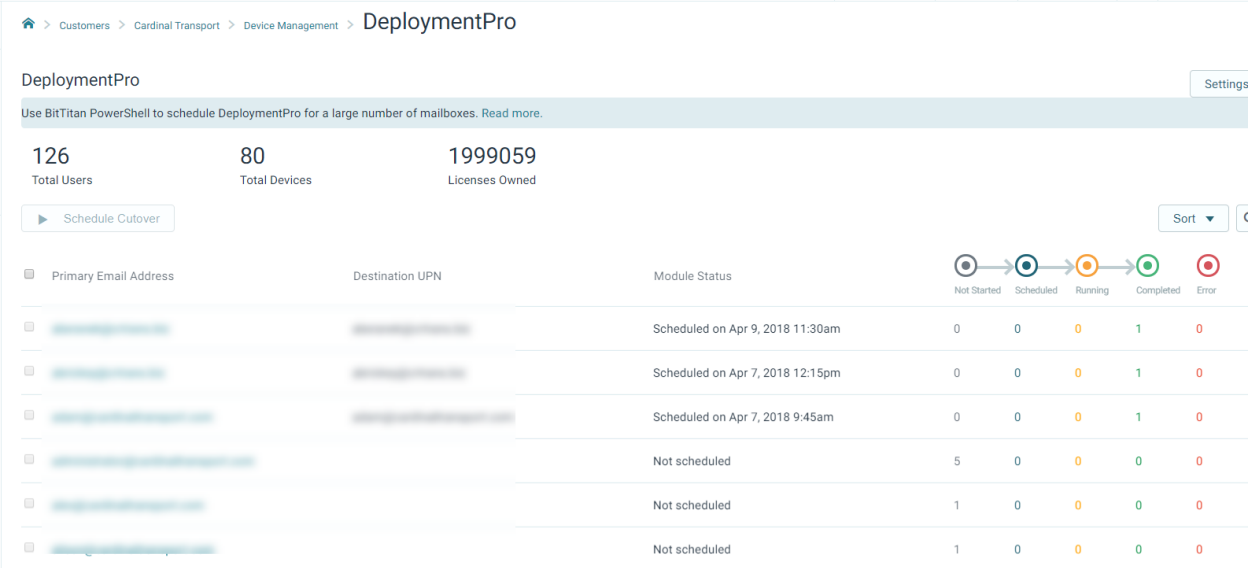
22. Monitor users that successfully have the agent installed by going to Customers>Select customers>Manage>Device Management>Deployment pro

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

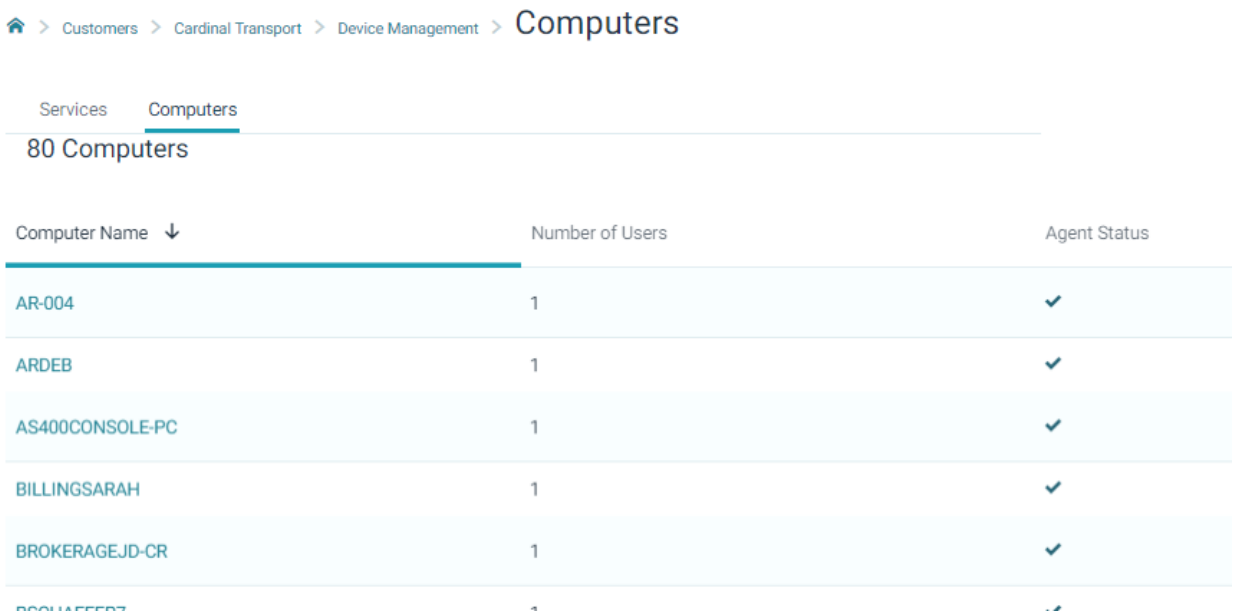


Once users start to login to their computers, thier device will be registered and their primary upn will be listed “Primary Email Address” column

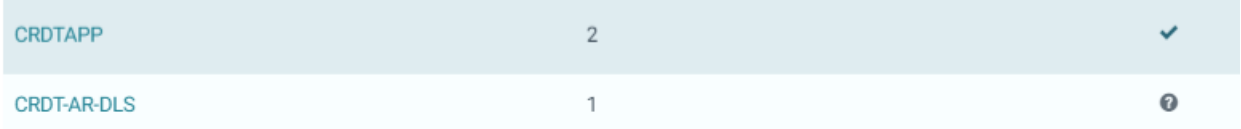




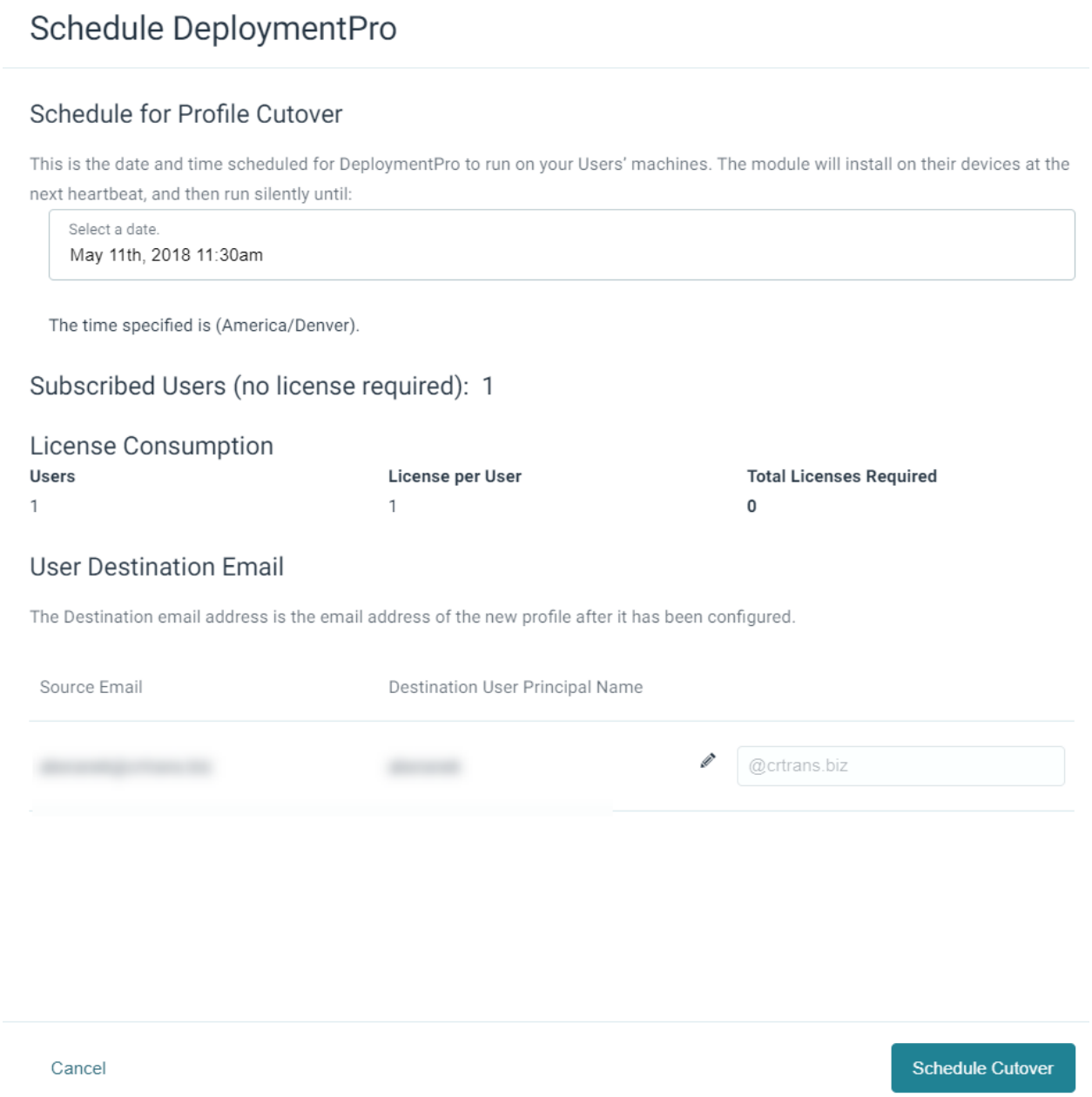
23. Users computers will be listed and will have a "heartbeat". Once a user signs into the device their email will be tied to the device in a one to one relationship.



* If a status shows a ? symbol it most likely means the computer is shut down and the tool has been able to find a heartbeat in over 4 hours*

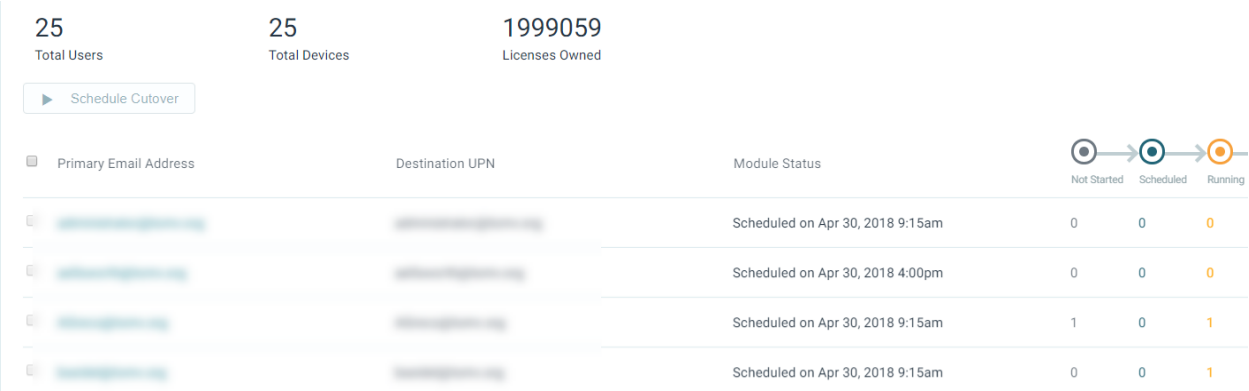


24. Once all users have populated with a and have the DMA agent installed, Schedule the cutover date for the agent to run on their computer. (This is after you cutover MX records)



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

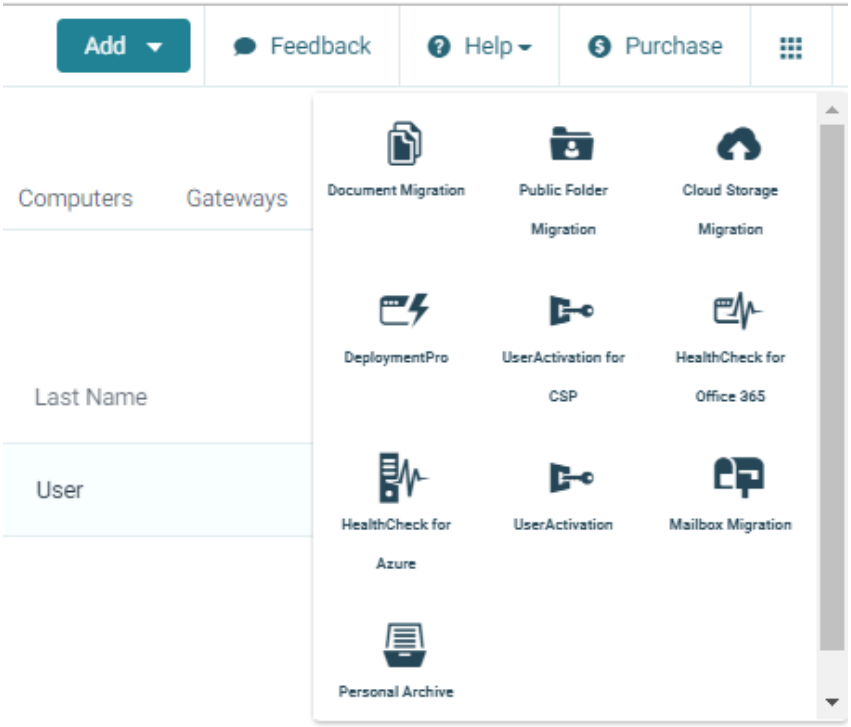
25. Once the agent is scheduled successfully, all users should change to a status of "running"



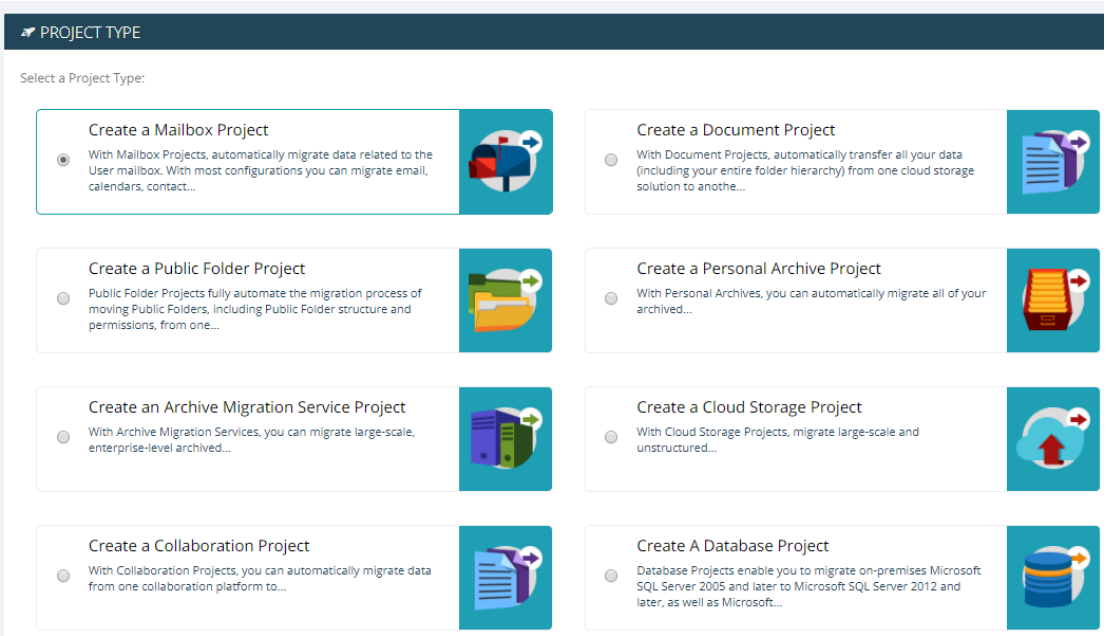
26.If the status does not say "running" but remains in "scheduled" reschedule again until it moves into a **running status**

Prep Work Phase 4: Setup BitTitan Project

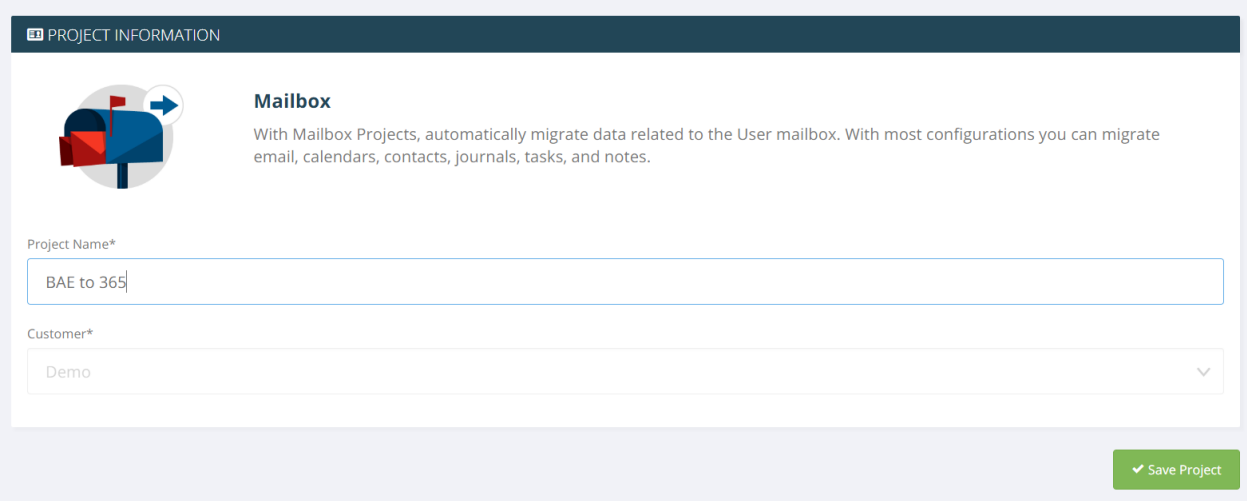
1. In BitTitan Portal, Open MigrationWiz by clicking on waffle icon at top of the page>Click Mailbox Migration



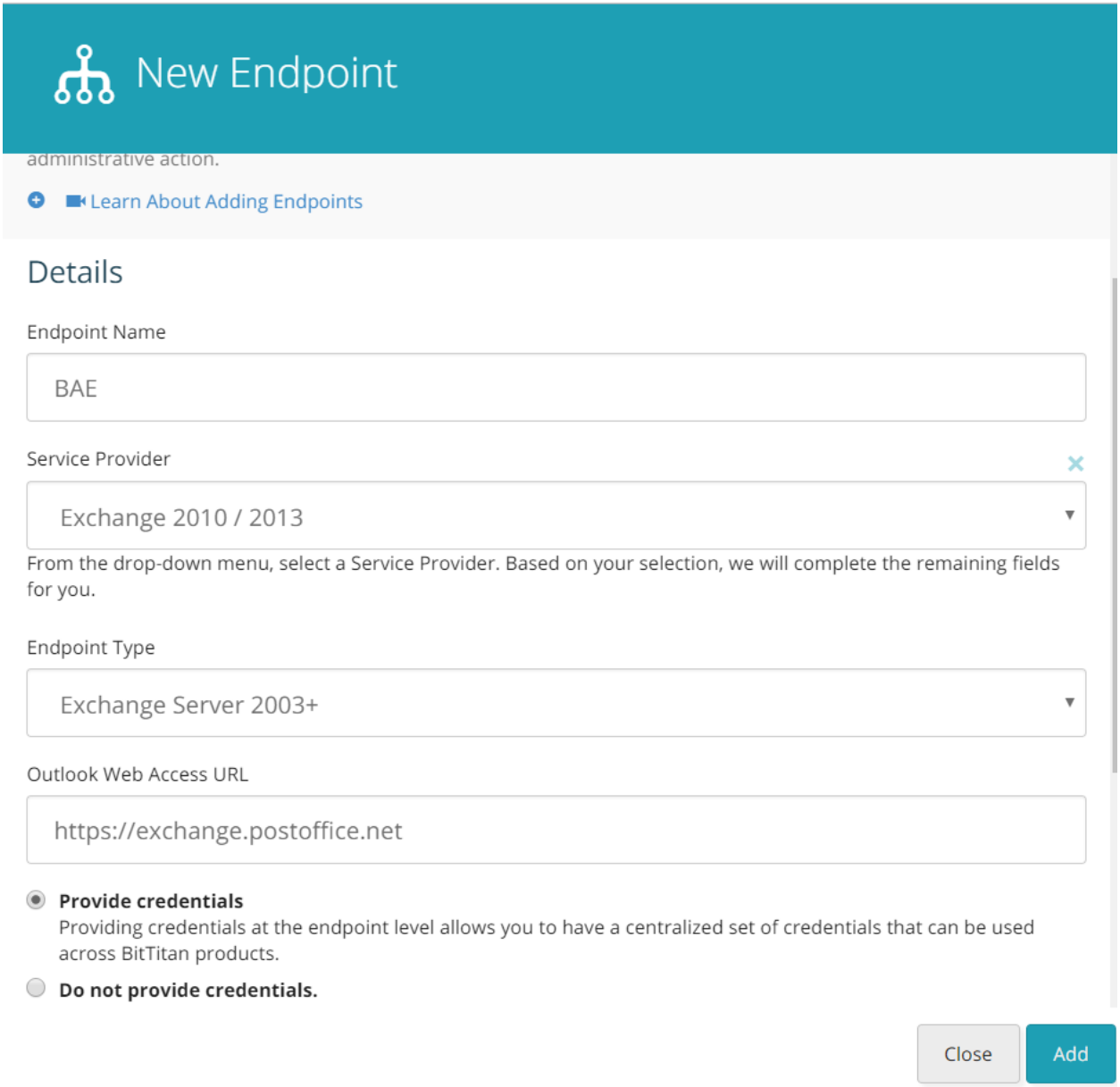
2. Click Create Project>Select Mailbox Project



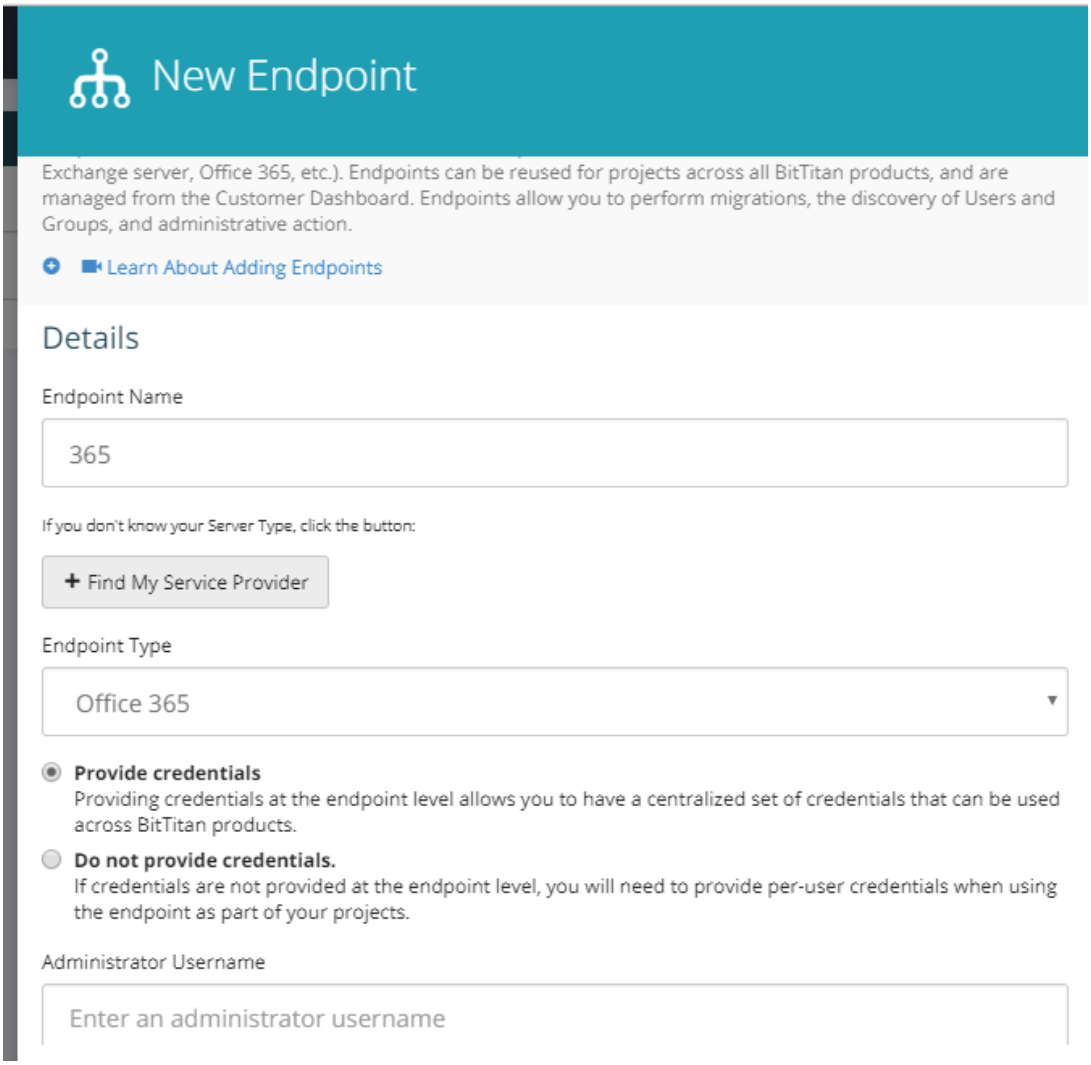
2. Name the Project and select your customer from the dropdown>Click Next Step



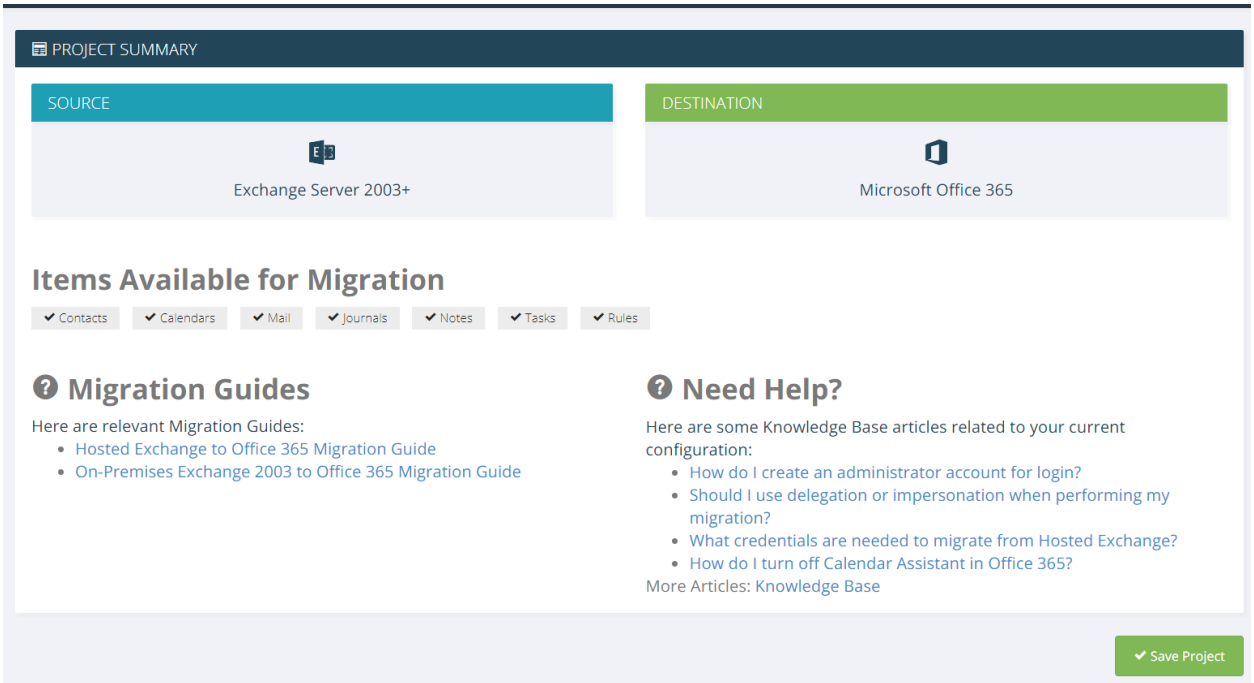
4. If you followed the steps for email deployment for the DMA agent you should be able to select your endpoint from the dropdown. If you did not, Select New and fill out the fields as shown below:



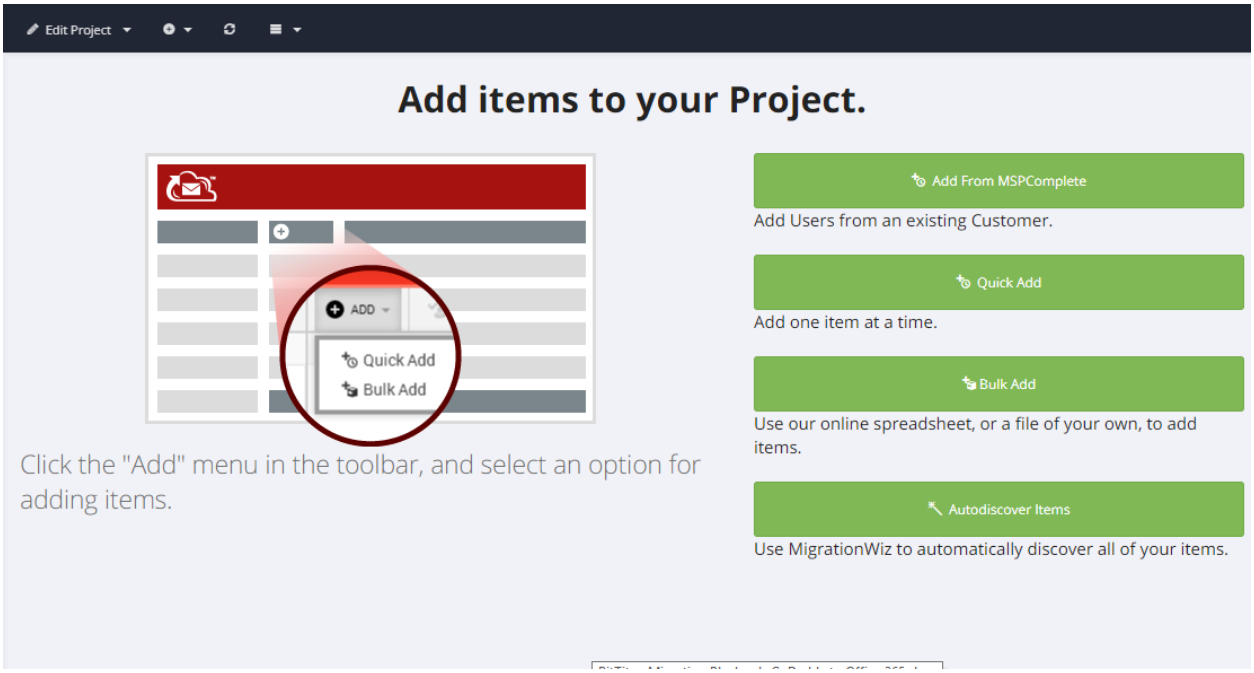
5. In the Destination Settings, Click New, and add the 365 endpoint. Providing the admin credentials



6. Click “Save and Go to Summary” This tells you whats eligible to move and give you additional KB articles you can reference:

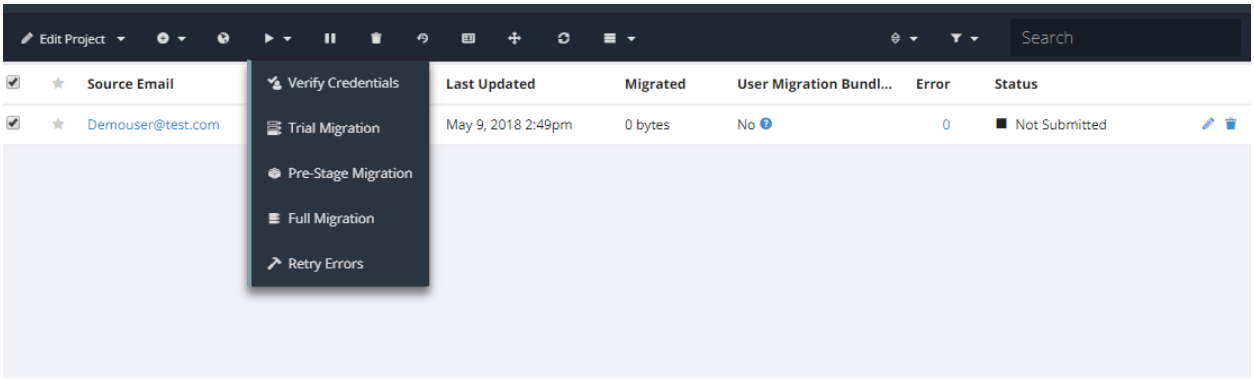


7. Add items to your project. If you already added users to the MSP complete portal either through GPO or an endpoint. You can select “Add from MSP Complete”. If you have not yet, then you can select Autodiscover items to import users to the portal



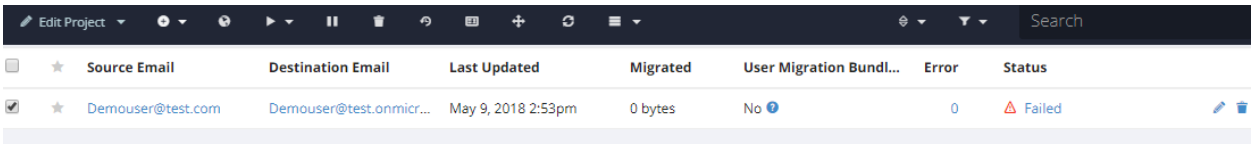
8. Audit User names and Domains on both the Source and Destination (Make sure they match BAE and 365), Cleanup user list.

9. Select All Users>Verify Credentials

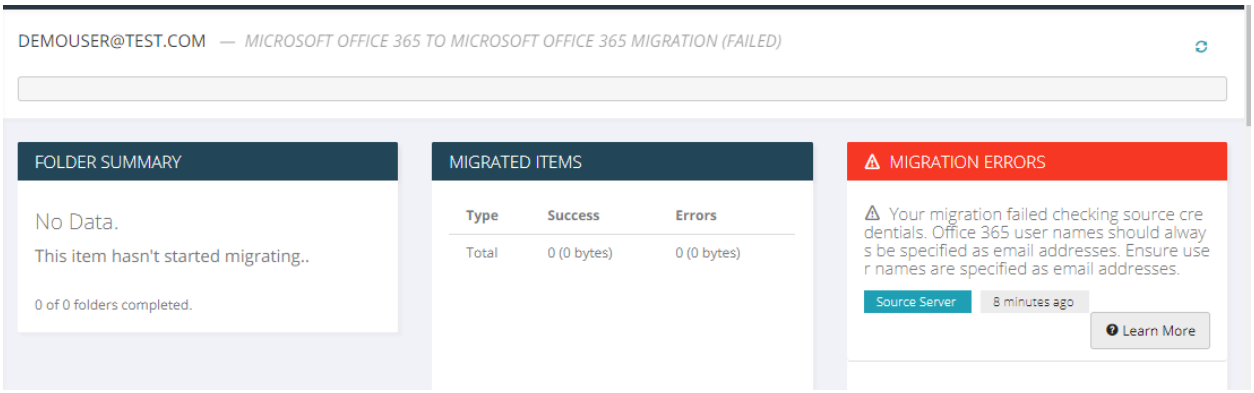


10. There are numerous errors that could appear here. Most of the steps I made for prep work will make it so that you avoid most of these errors. Refer to BitTitans KB articles for most common errors and how to troubleshoot. https://help.bittitan.com/hc/en-us/sections/115003465187-Mailbox-Error-Lookup?page=2

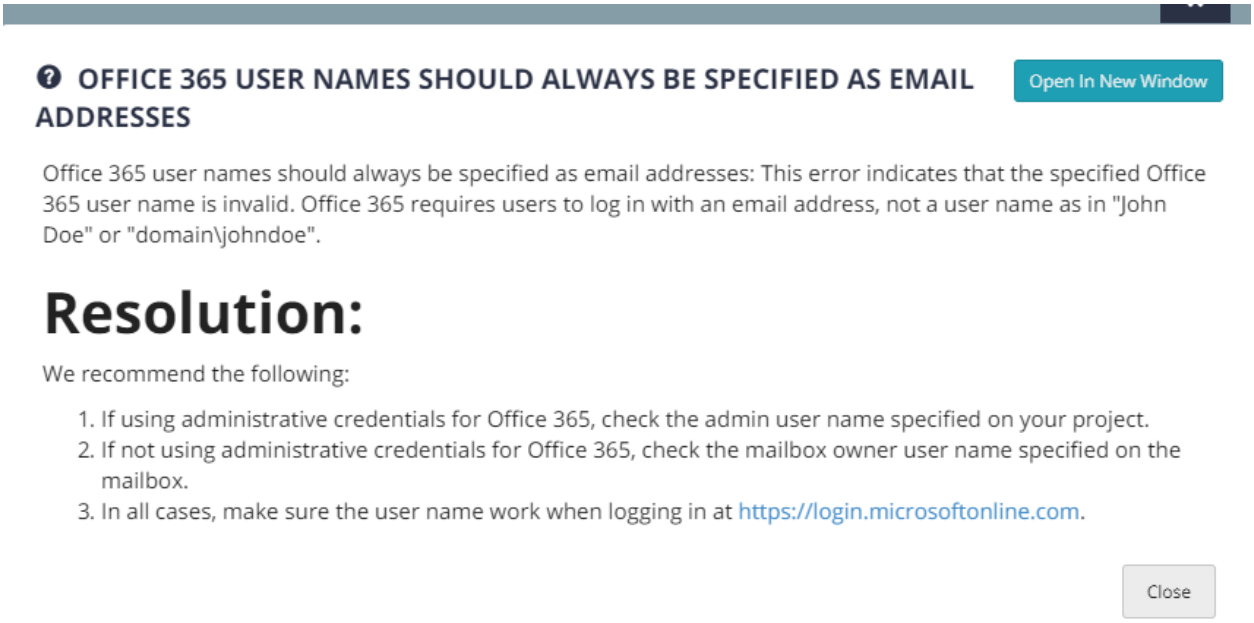
Unsuccessful verification will show a “Failed” Message



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

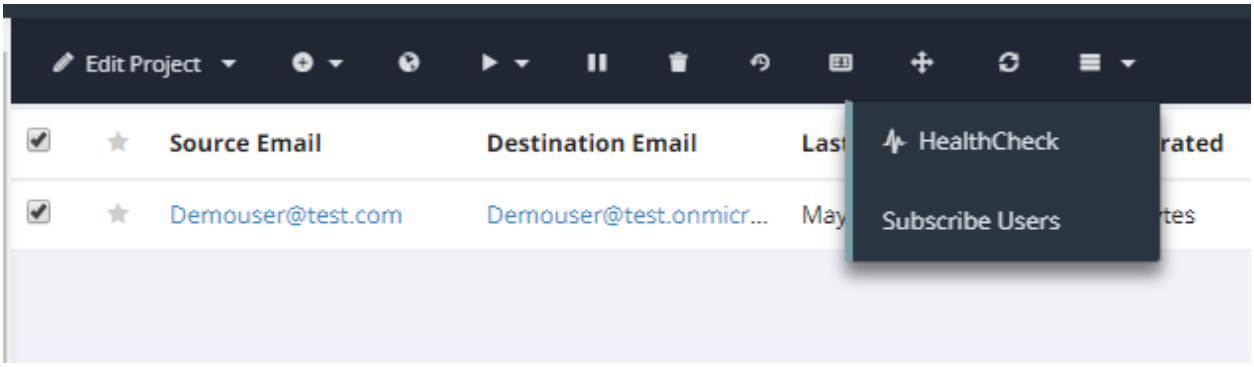


Click on “Learn More” to access BitTitan’s Relevant kb articles specific to the error:

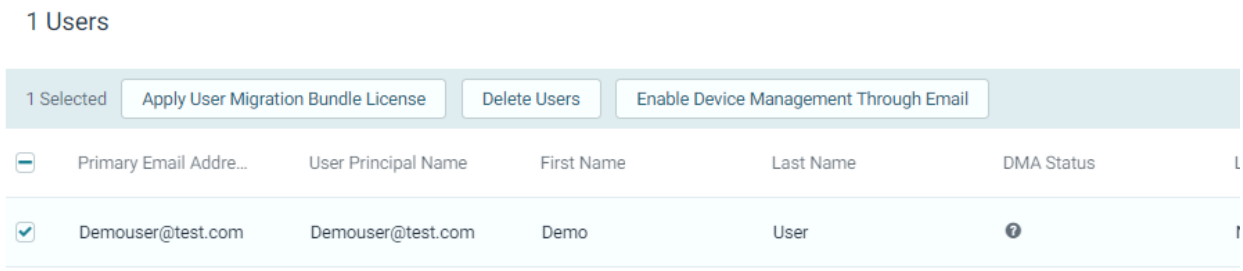


Successful Verification will show a “Completed(Verification)” message

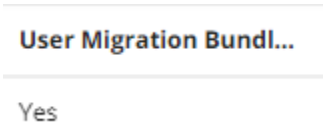
11. After all users have successfully completed verification, Select All users>Click on the Hamburger icon at the top of the toolbar> Click Subscribe Users



12. This will bring you back to the MSP complete portal. Select all users>Click Apply User Migration Bundle

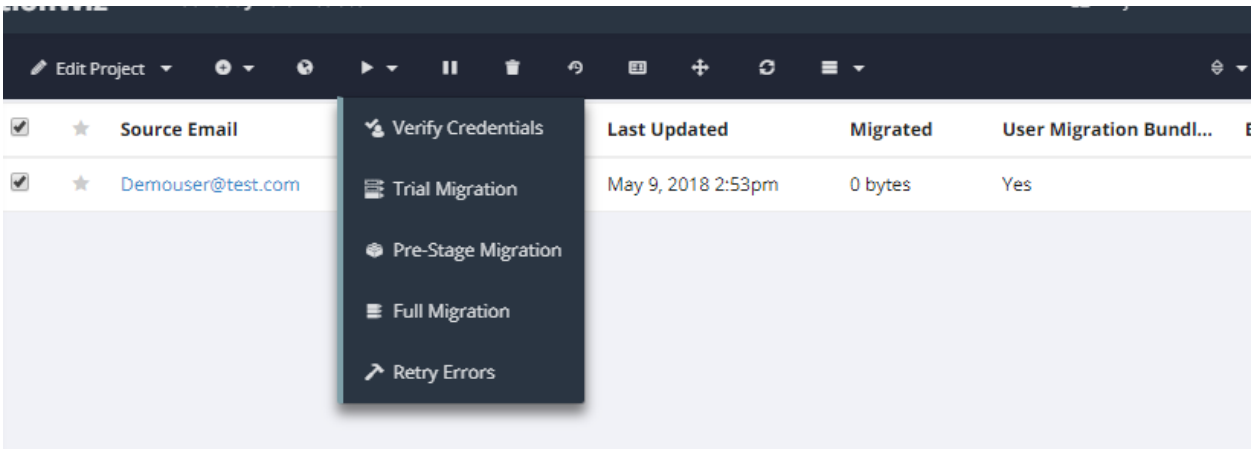


13. This takes a couple of minutes to propagate but after, in the migrationwiz portal the “User Migration Bundle” column will change from “No” to “Yes”

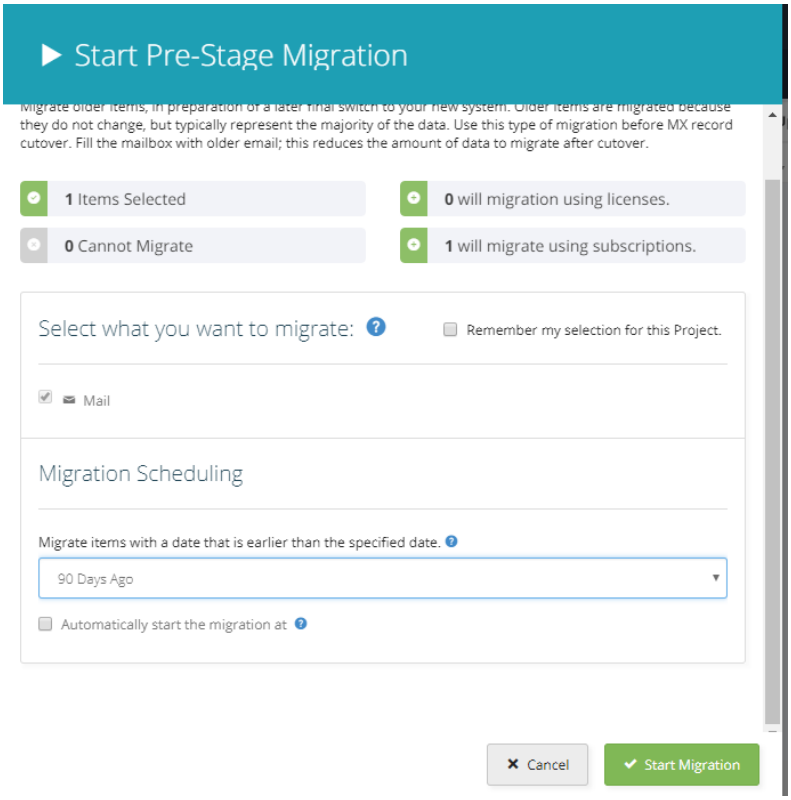


Migration Phase 1

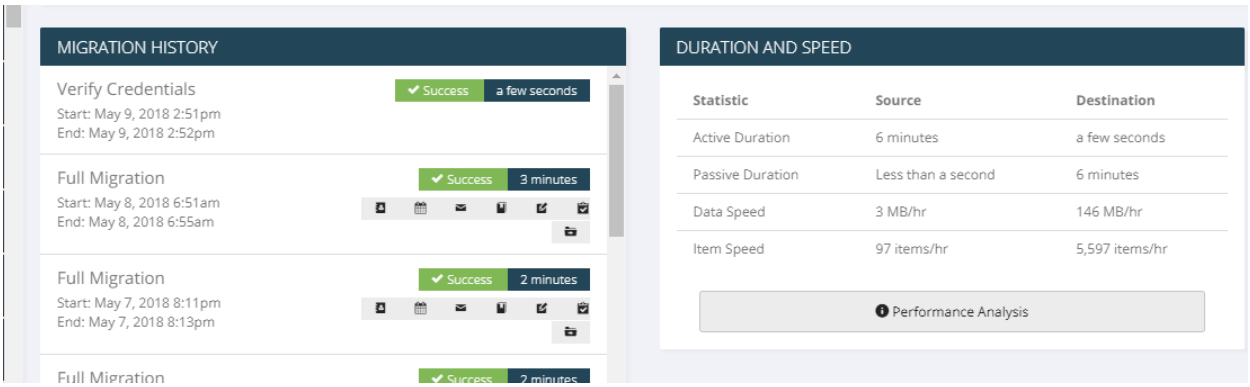
1. Preferably start at beginning of the week, plan for MX Cutover on Friday evening
2. Select All Users>Click on the start button>Pre-stage Pass



3. Select a time range from the dropdown of prior to 90 days>Start Migration

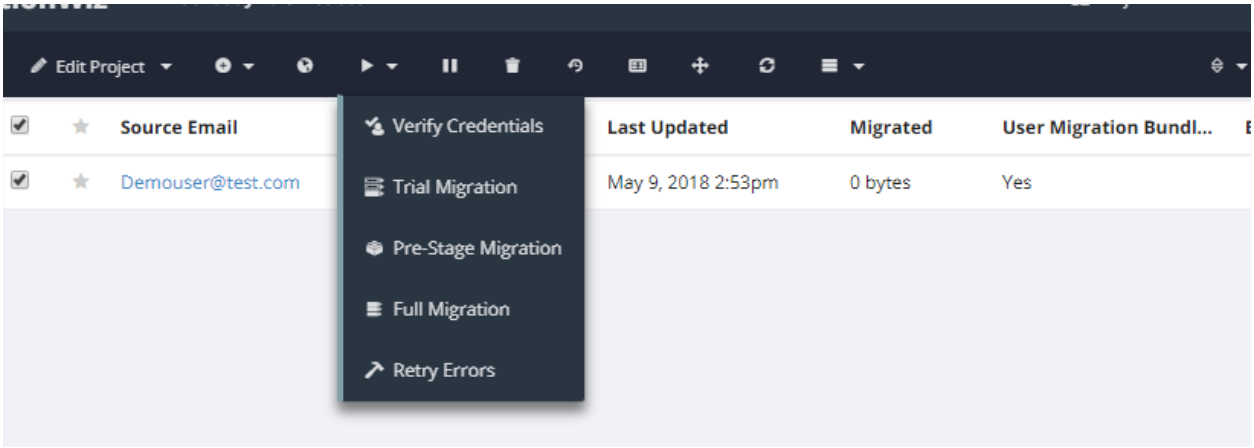


4. This will give you a status bar and show the amount of data moved over in the “bytes” column. If any users fail, it’s usually do to server timeout. Simply rerun the pre-stage pass on these users to restart where it left off. If you click on any user’s name, you can see metrics like upload speeds:

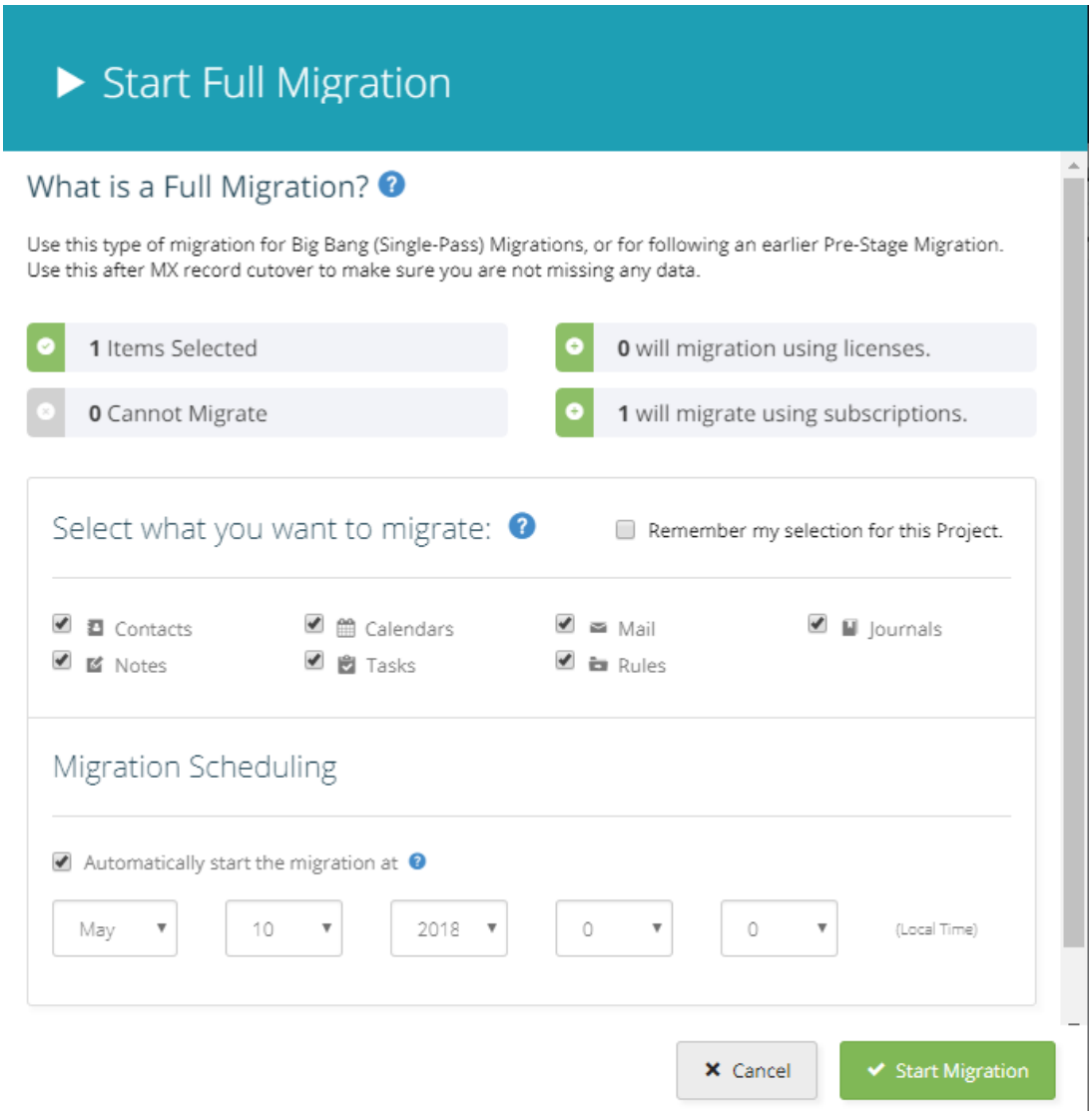


5. Once the pre-stage migration has run for all users and is in a "Completed" Status

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/Delta Pass

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**

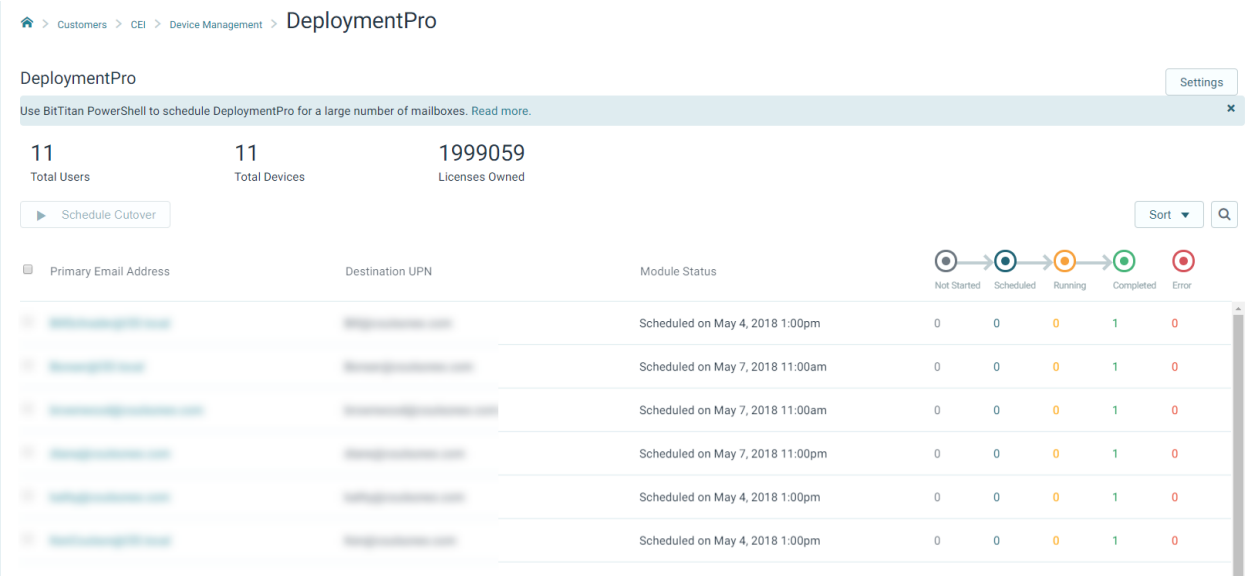
2. Run another Full Pass. This will perform a **delta sync** to pull over any residual data that may have been missed.

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