Workspace ONE Factory Provisioning with Google Directory

Technical Guide

vmware

Revision History

The following table contains the history of revisions made to this document, and by whom they were made.

Date	Authors	Change Description	Reviewers
28 Oct 2020	Damon Hawkins	Initial Draft	

Legal Notice

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

Contents

1. Summary

This guide documents an example integration between VMware Workspace ONE and Google Cloud Directory in regard to Factory provisioning Microsoft Windows 10 devices.

This is not an official VMware document and only is provided as an example.

2. Prerequisites

2.1. Requirements

- **Windows 10 –** Endpoints should be built with Windows 10 1909+ for best results
- **GCPW –** GCPW is required to be installed in standalone mode as part of the factory provisioning
- **Chrome –** Google Chrome is required to be installed on the endpoints as part of the factory provisioning
- **Workgroup** - Devices will be workgroup only

2.2. Assumptions

- Workspace ONE UEM is already integrated with Workspace ONE Access
- Google Secure LDAP has been used to provision users into Workspace ONE UEM
- Stunnel has been installed onto the server hosting the cloud Connector.
- There is no Active Directory or Azure AD used in the environment

3. Configuration Example

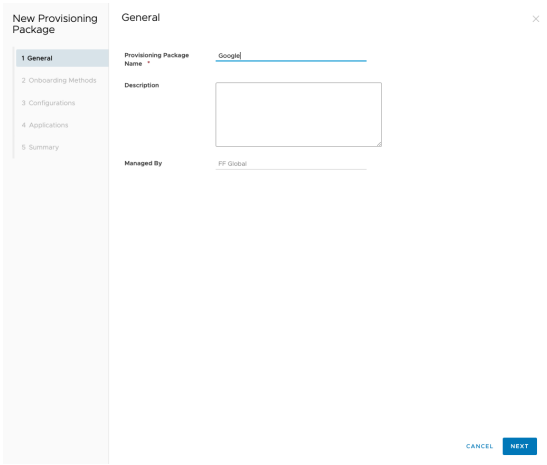
3.1. User experience and end result

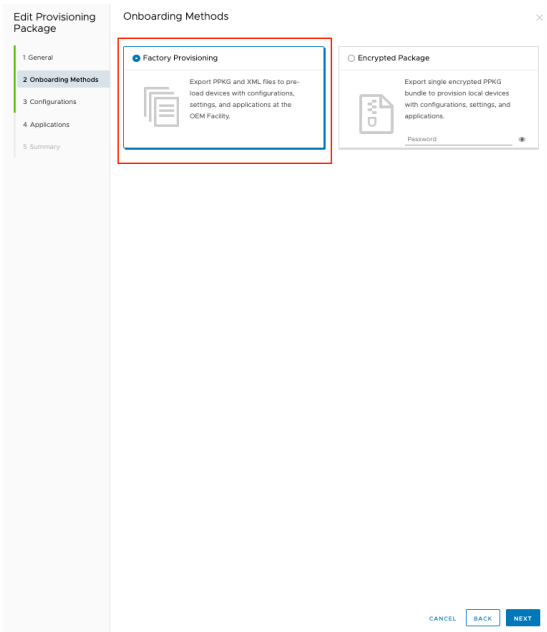
The following video demonstrates the achieved end user experience: https://youtu.be/6LDDq7R0XZ4

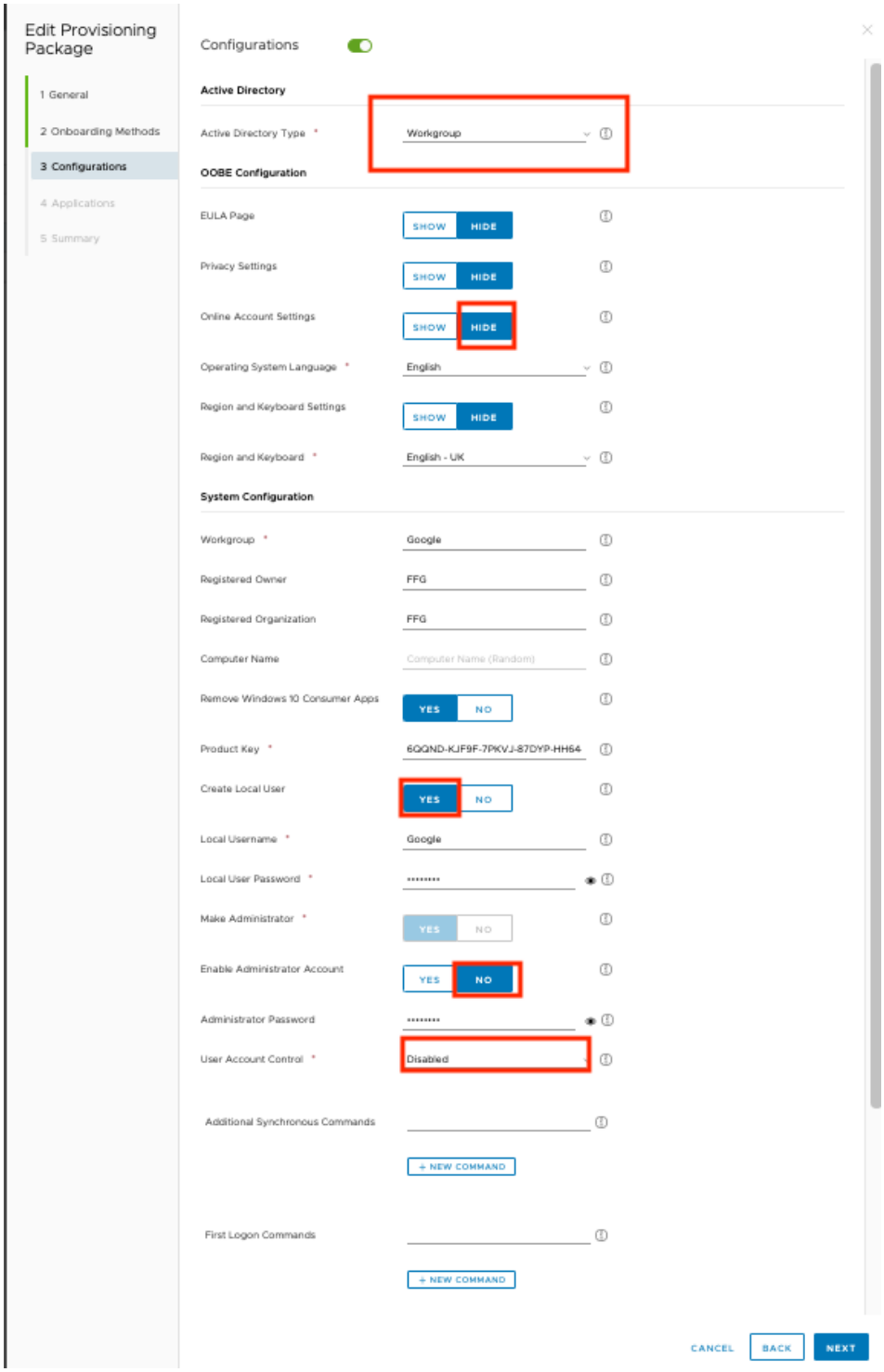
3.2. Workspace ONE UEM configuration

3.2.1. Factory provisioning

Create a PPKG and unattend.xml from Devices > Staging > Windows







Set the highlighted options

Populate with correct staging user details

Additional Synchronous and First logon commands will be required (please reference the unattend.xml sample located here: https://github.com/damonhaw/wsone/blob/main/factory%20provisioning/Google/unattend.xml to:

- Configure GCPW settings
- Hide all other account options except for GCPW login
- Elevate permission on the local account that is created by GCPW to allow the enrolment process to complete.
- Remove and set correct permissions after the enrolment kicks off, as we will know the username.

Additional synchronous commands:

```
cmd /c net localgroup "Administrators" "Authenticated Users" /add
cmd /c reg ADD HKLM\Software\Google\GCPW /v domains_allowed_to_login /t REG_SZ /d “wsone.co.uk” /f
cmd /c reg ADD HKLM\Software\Google\GCPW /v enable_dm_enrollment /t REG_DWORD /d 0 /f
cmd /c reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon\SpecialAccounts\UserList" /v googletemp /t REG_DWORD /d 0
cmd /c reg ADD HKLM\Software\Google\GCPW /v use_shorter_account_name /t REG_DWORD /d 1 /f
```

*replace **wsone.co.uk** with your Google domain and **googletemp** with the username of the local account created in the unattend.xml*

Additional first logon commands:

```
cmd /c net localgroup "Administrators" %username% /add
cmd /c net localgroup "Administrators" "Authenticated Users" /delete
```

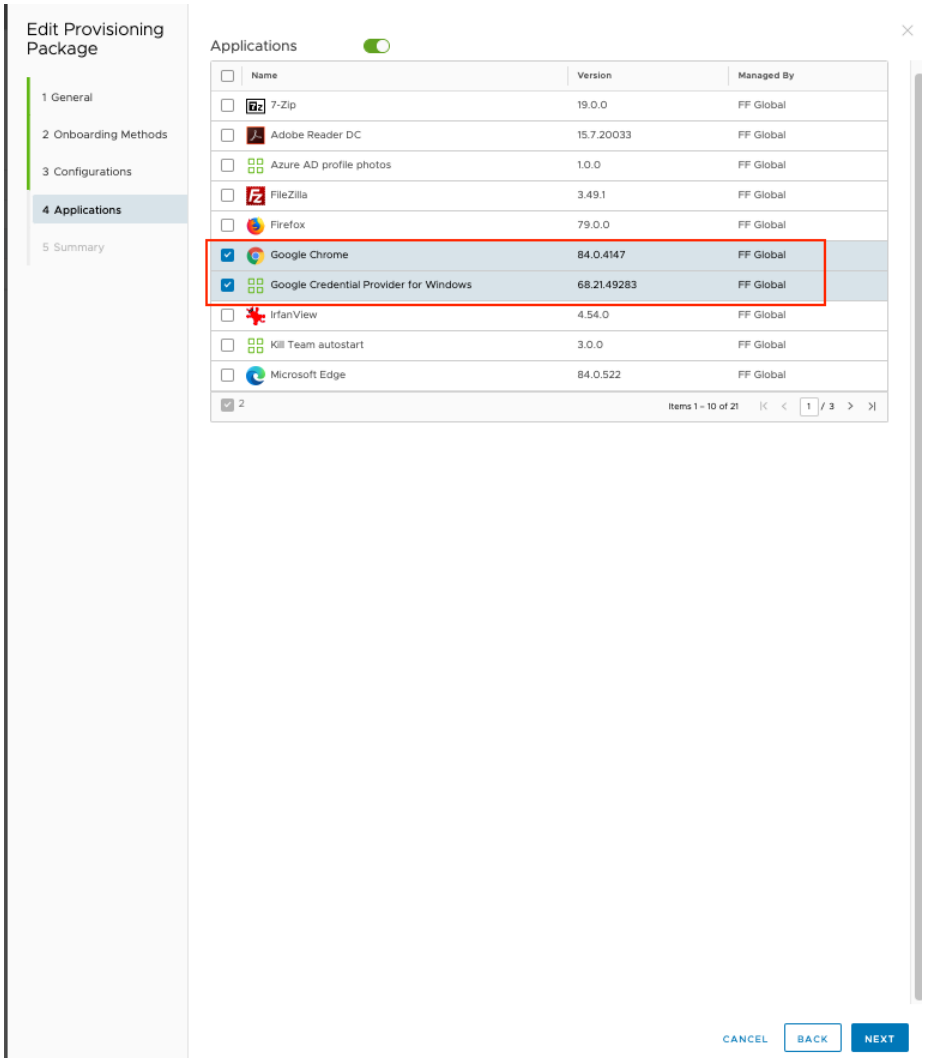
Check agent install command line in unattend.xml and make sure path msi path and password are contained in “ “. Also remove DOWNLOAD BUNDLE=TRUE as this is no longer required.

```
<SynchronousCommand wcm:action="add">
<CommandLine>msiexec /i "c:\Recovery\OEM\AirwatchAgent.msi" /qn ENROLL=Y SERVER=https://ds531.awmdm.com LGNAME=NHSXTEST USERNAME=staging@NHSXTEST.com PASSWORD="C*lE7W" ASSIGNTOLOGGEDINUSER=y</Com
<Description>Executing First Commands 2</Description>
```

I also recommend setting in the VMwareWS1ProvisioningTool.exe.config file

<add key="WorkspaceOneInstallerStagingEnabled" value="false" />

So that the legacy Workspace ONE app does not become part of the build



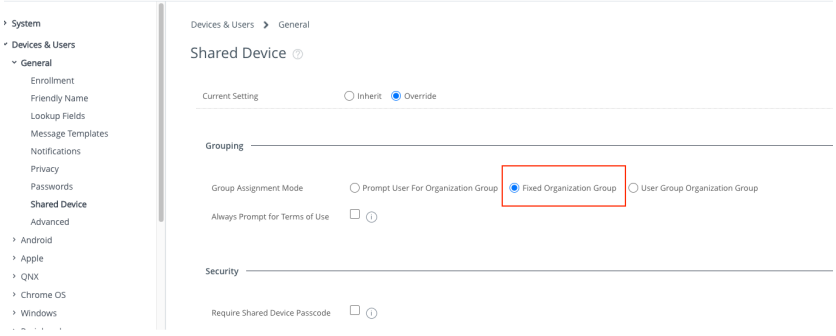
Install as a minimum Google Chrome and GCPW into the PPKG

Build Windows 10 machine following normal guidelines

3.2.2. Console settings

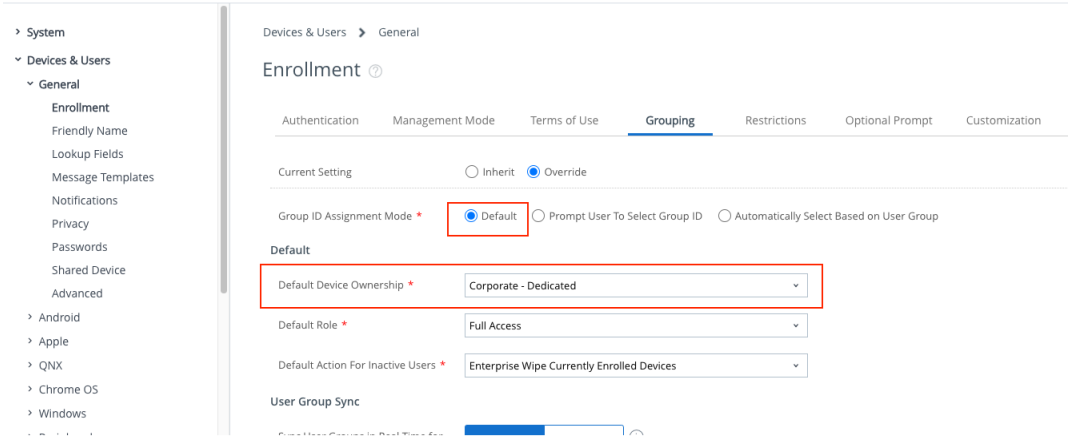
Settings > Devices & Users > General > Share Device

Make sure this is set to Fixed Organization Group



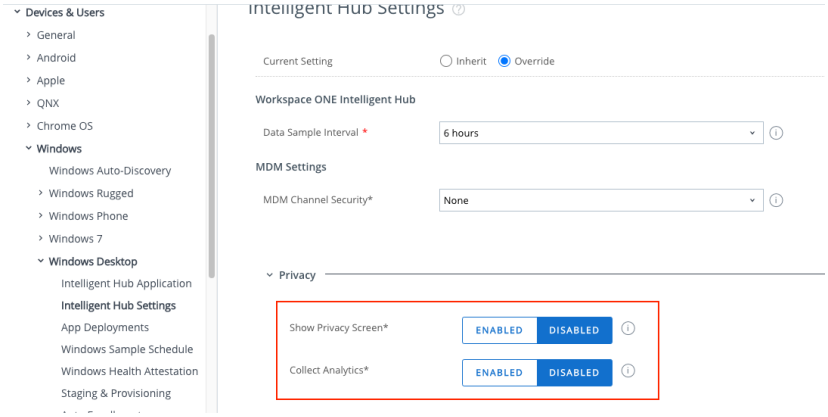
Settings > Devices & Users > General > Enrollment > Grouping

Make sure this is set to Default Group ID Assignment Mode and Corporate – Dedicated



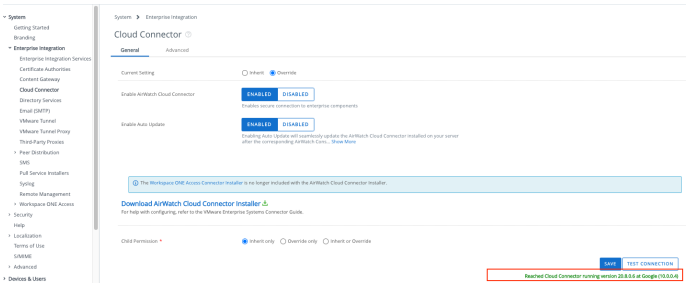
Settings > Devices & Users > Windows > Windows Desktop > Entelligent Hub Settings

Turn off undesired Privacy prompts



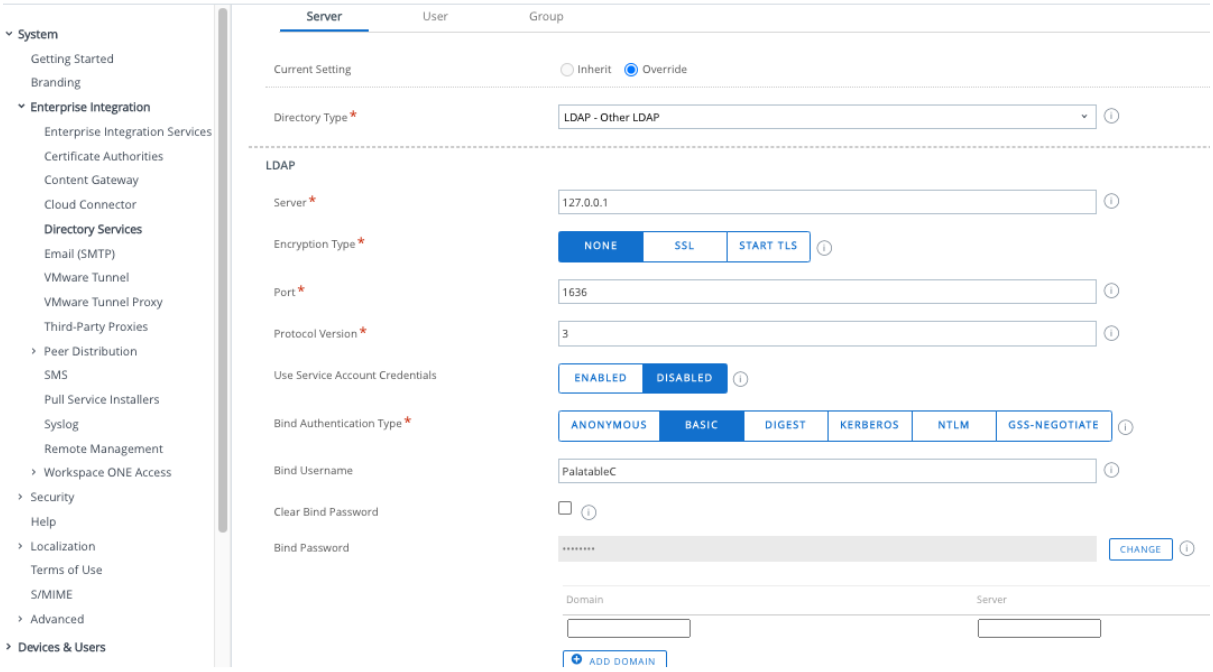
3.2.3. UEM Cloud Connector

Make sure the UEM Cloud Connector is installed and working correctly



3.2.4. LDAP Directory Settings

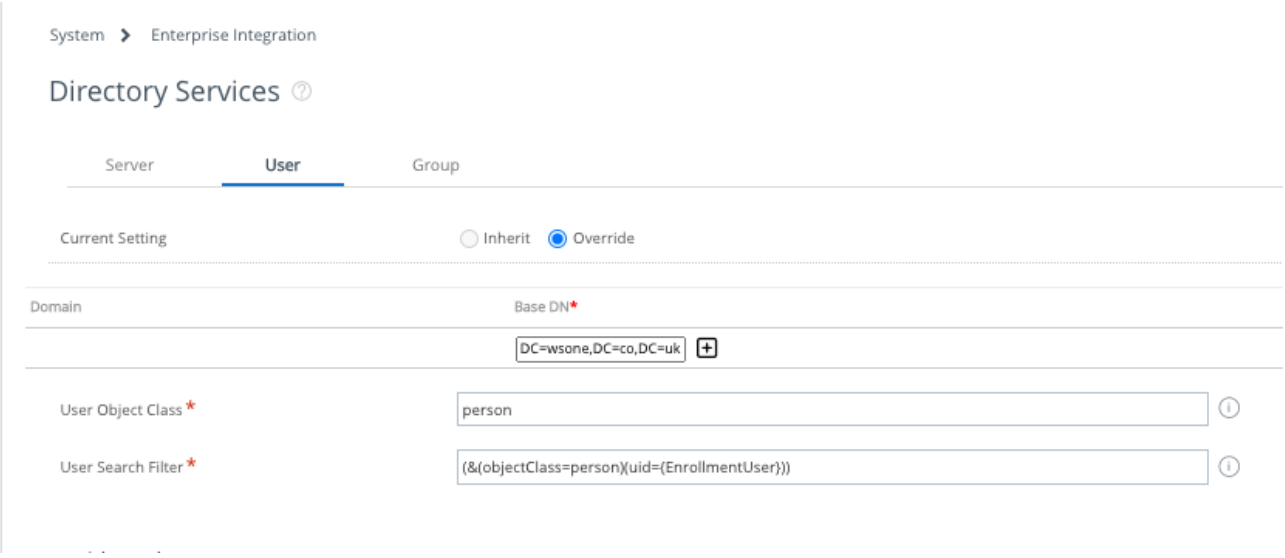
It is assumed stunnel has been installed/configured onto the cloud connector server and confirmed working



Note the domain entry is not populated as this will prepend to the bind username which is undesired for Google LDAP.

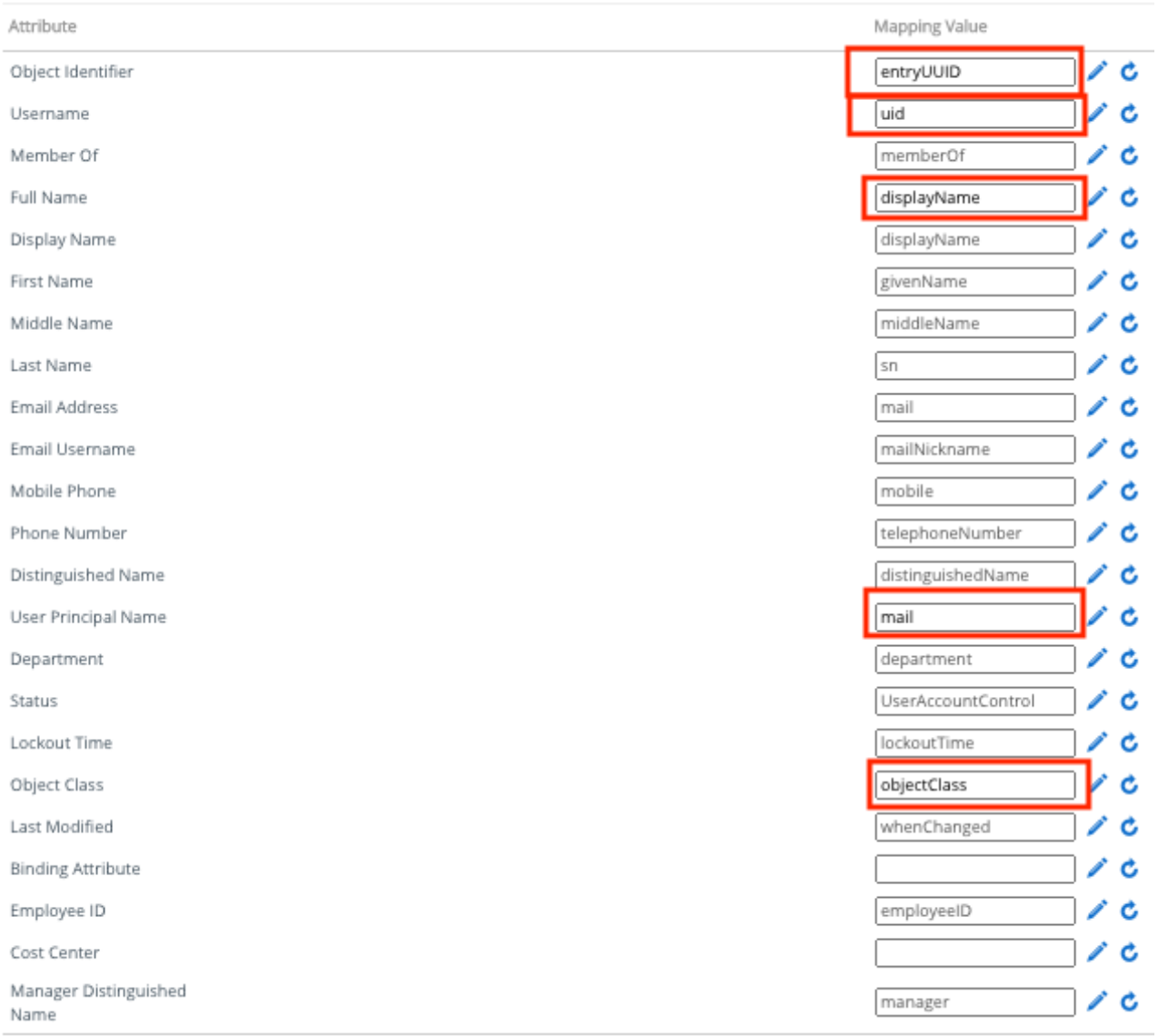
Base DN needs to be set for Users and Group

Also, note the User Search Filer syntax with: uid



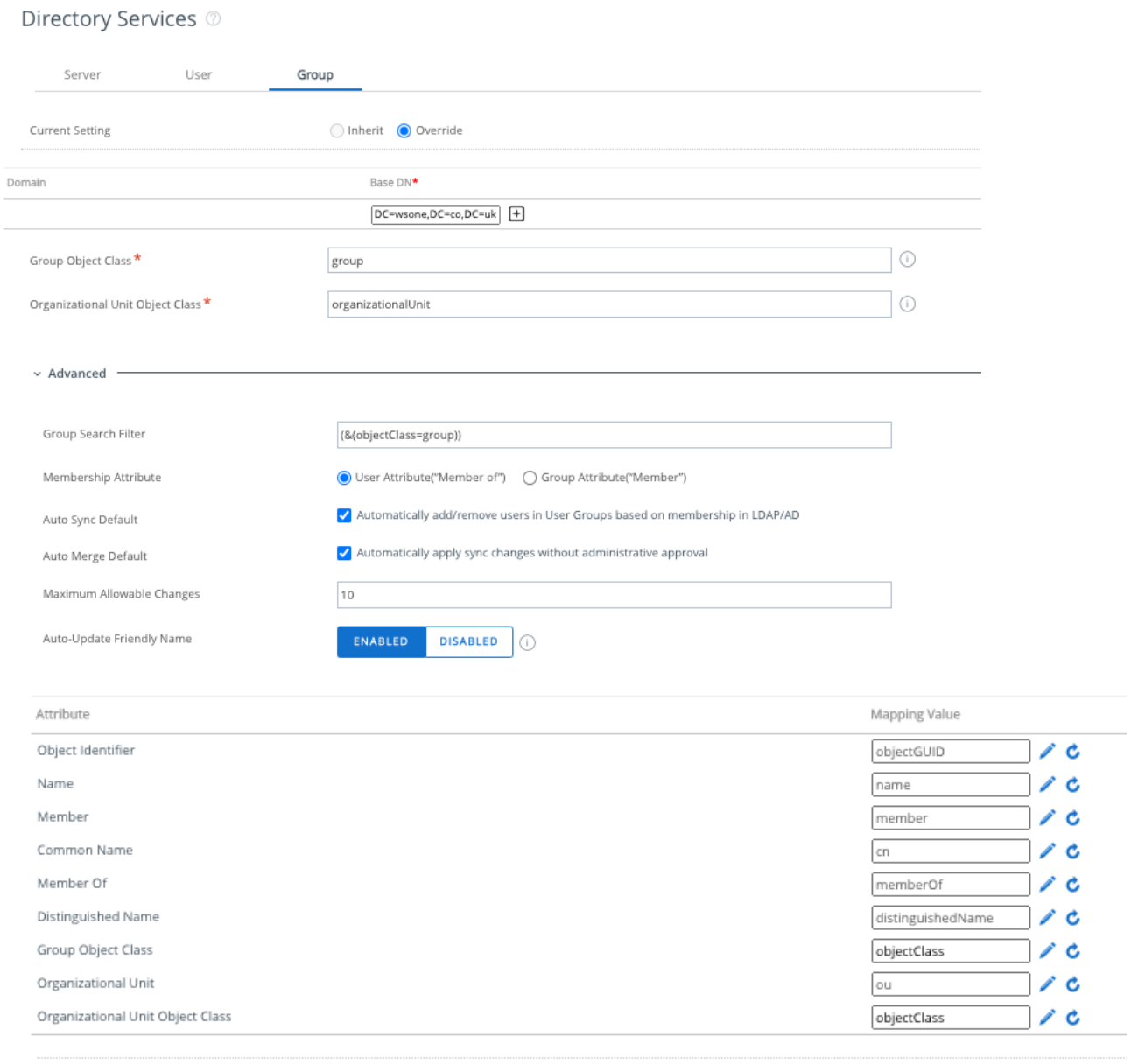
Attribute mappings will need to be modified.

Special notice to Object Identifier which I have set to entryUUID. This will provide a GUID which is required for the Intelligent Hub when enrolling from Access/SAML.

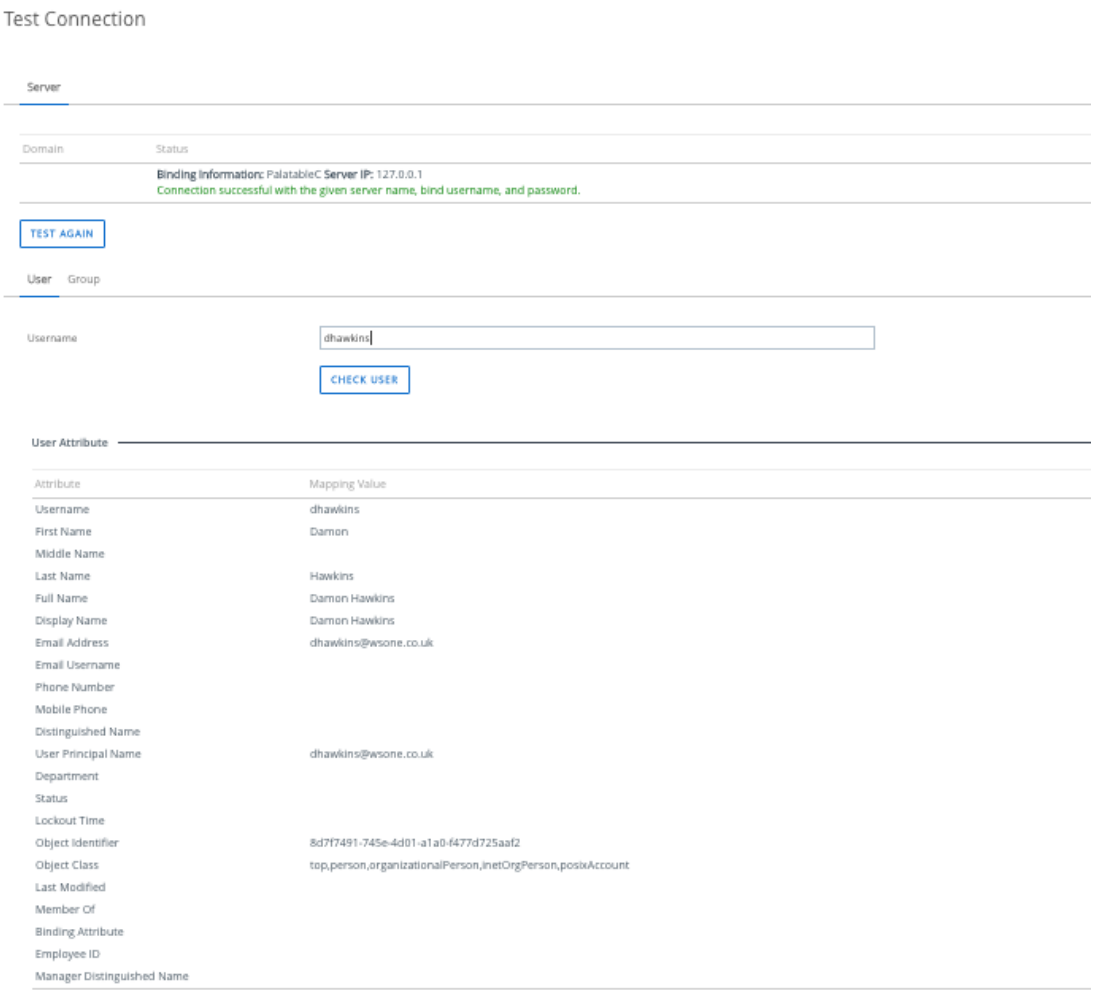


Attribute	Mapping Value
Object Identifier	entryUUID
Username	uid
Member Of	memberOf
Full Name	displayName
Display Name	displayName
First Name	givenName
Middle Name	middleName
Last Name	sn
Email Address	mail
Email Username	mailNickname
Mobile Phone	mobile
Phone Number	telephoneNumber
Distinguished Name	distinguishedName
User Principal Name	mail
Department	department
Status	UserAccountControl
Lockout Time	lockoutTime
Object Class	objectClass
Last Modified	whenChanged
Binding Attribute	
Employee ID	employeeID
Cost Center	
Manager Distinguished Name	manager

Group settings below (currently untested due to time constraints)

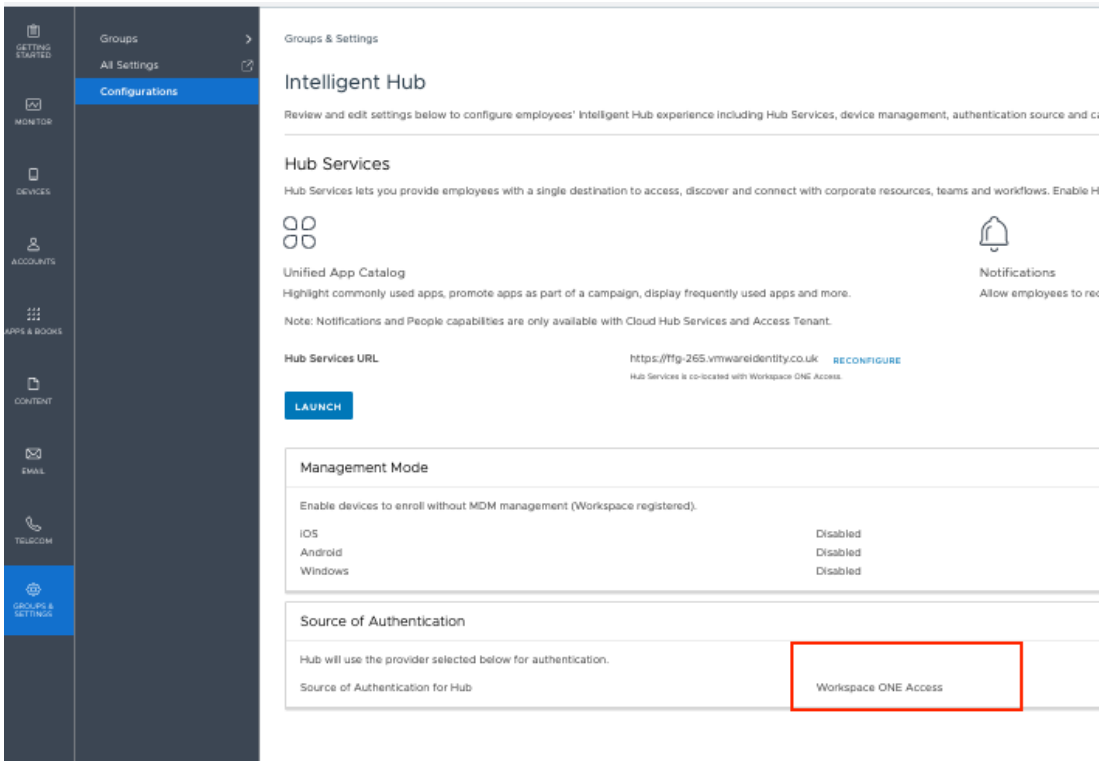


Run a test and confirm fields are correct:

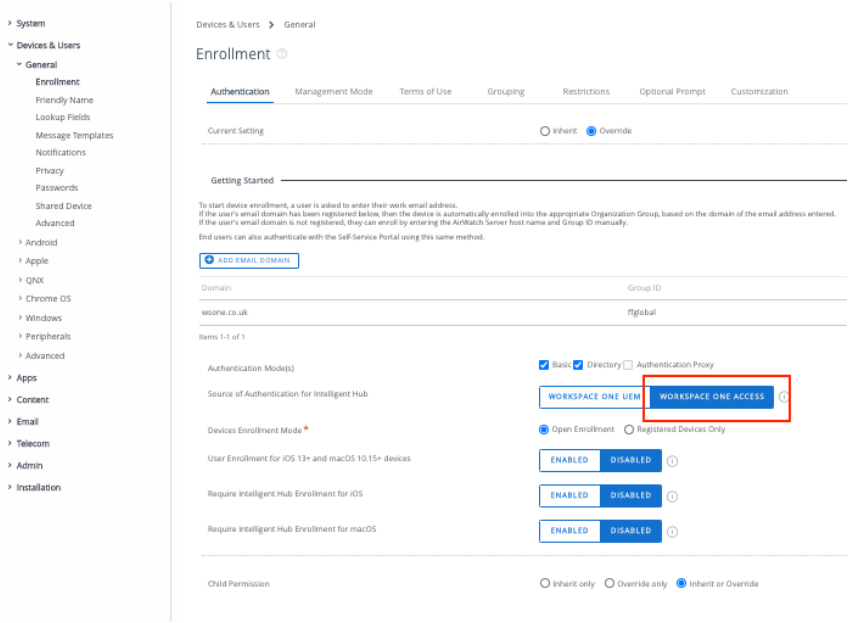


3.2.5. Hub Services

Configure Hub services as required. Make sure Source of Authentication for Hub is set to Workspace ONE Access



This setting can be changed under Settings > Devices & Users > Enrollment > Authentication



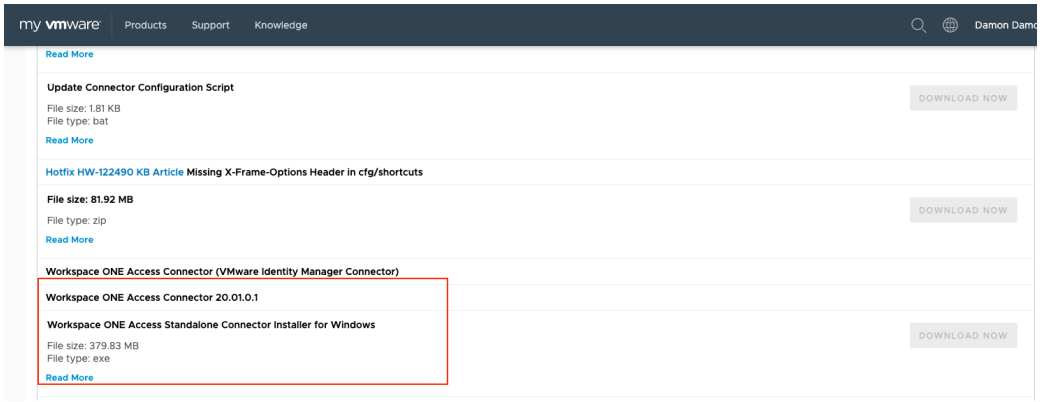
3.3. Workspace ONE Access configuration

3.3.1. Connector

Due to the fact Google Cloud Directory SAML does not appear to support the UUID as an attribute, using JIT user provisioning may fail when used for device enrolment.

Therefore, I provisioned the Workspace ONE Access connector to integrate with LDAP.

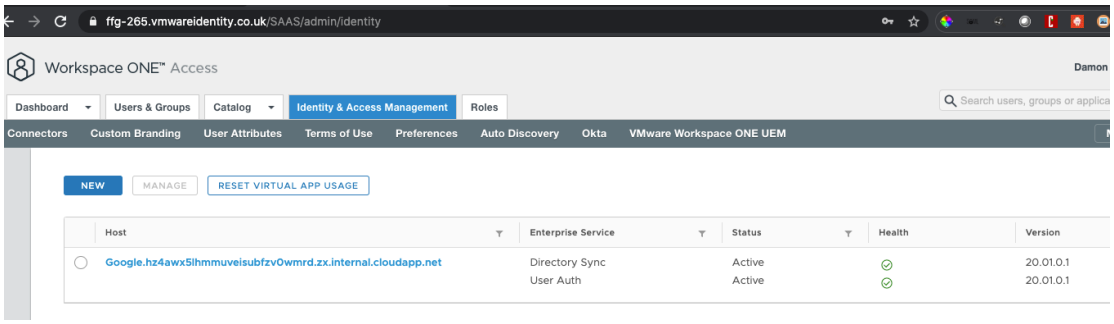
Download the Workspace ONE Access Connector from my.vmware.com



Reference the following guide:

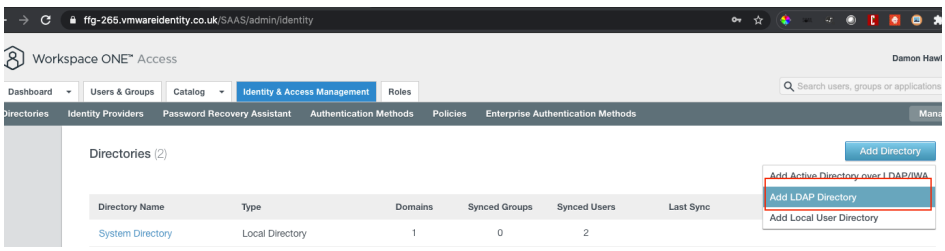
https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/ws1_access_connector_install/GUID-271C47F6-856C-40F0-97AB-A8AD95025F9C.html

Confirm the connector is active (green)

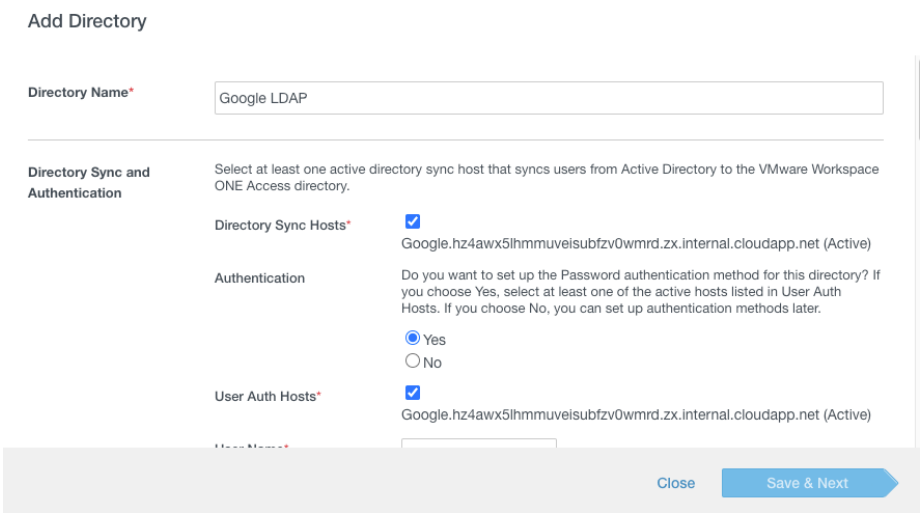


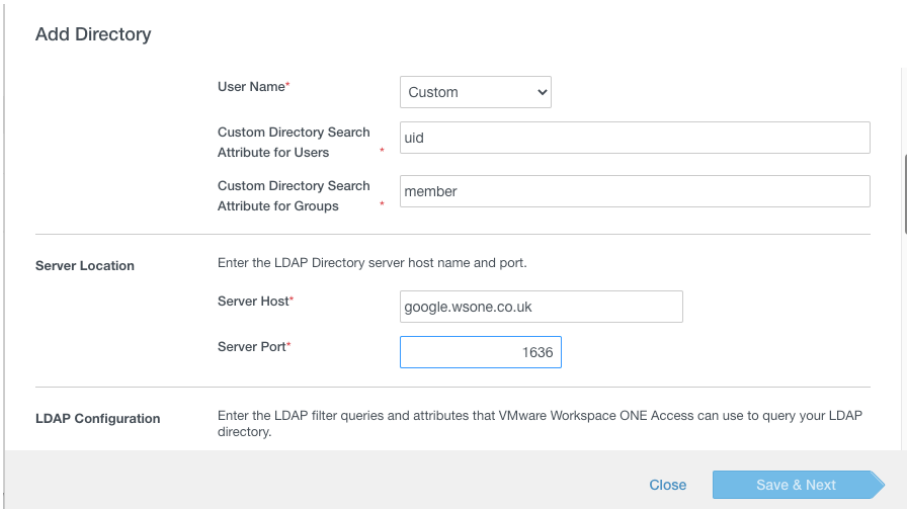
3.3.2. Directory

Add an LDAP Directory

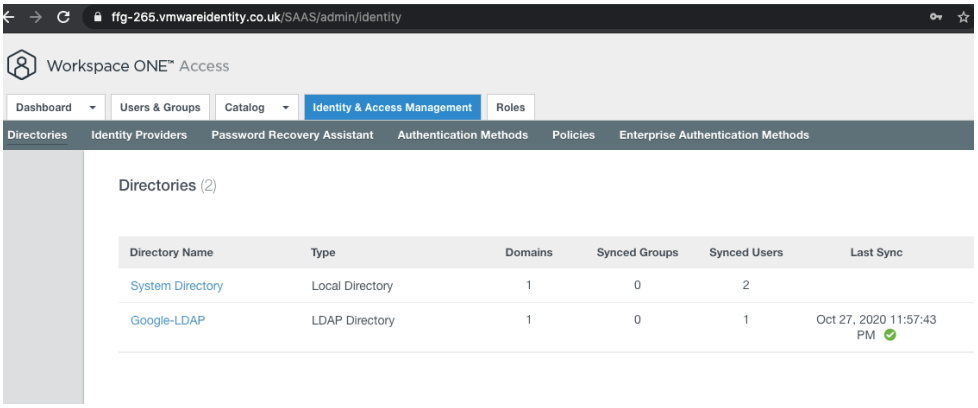


Set a Directory Name as desired, make sure show options are selected

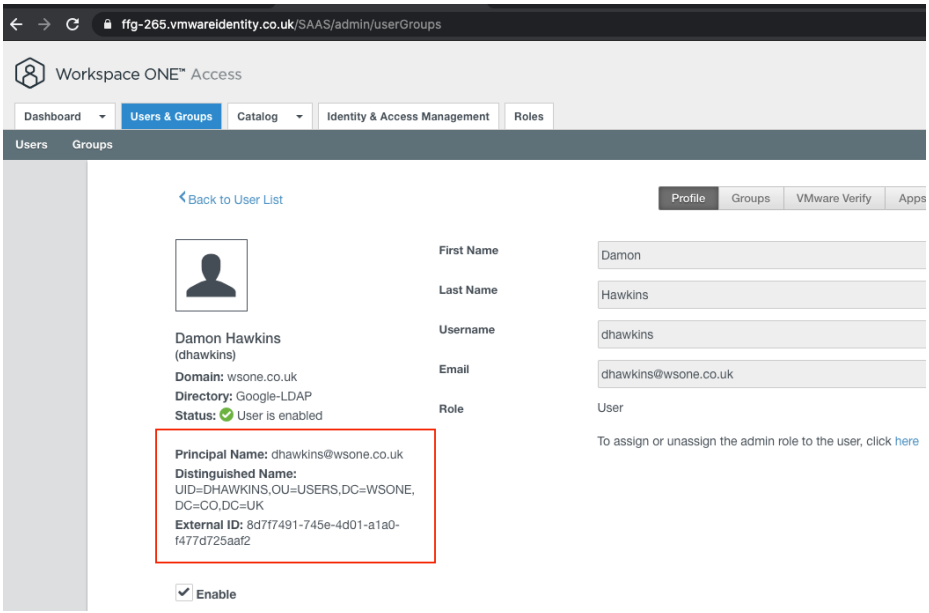




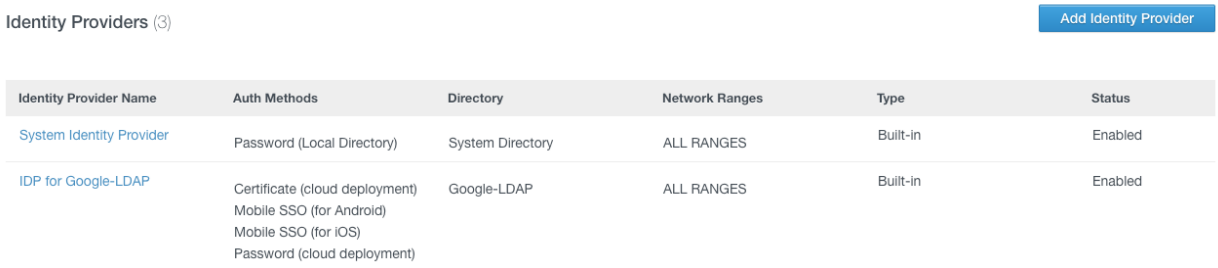
Note the bind account just needs to be a Google directory user with non-admin permissions only.



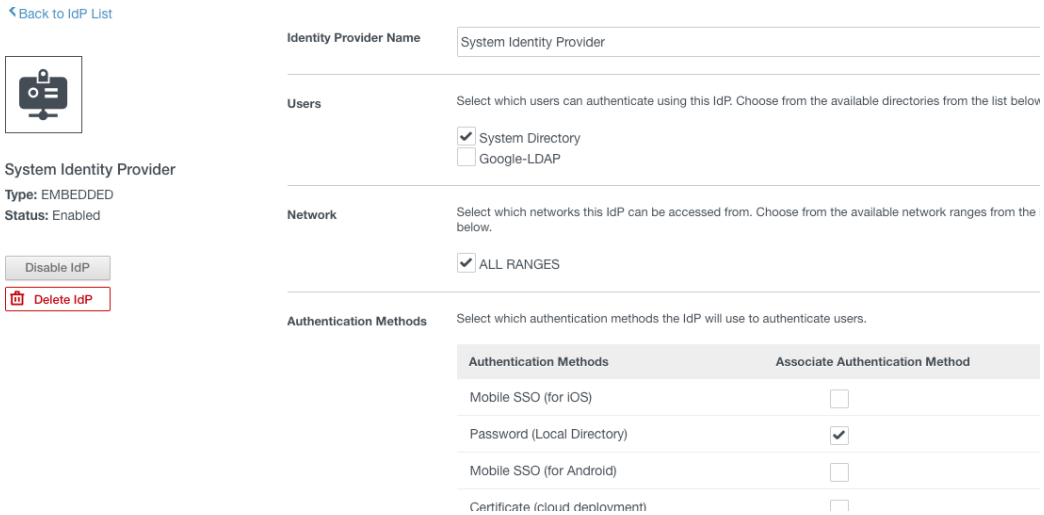
Directory can now be synced with desired users, check an account attributes



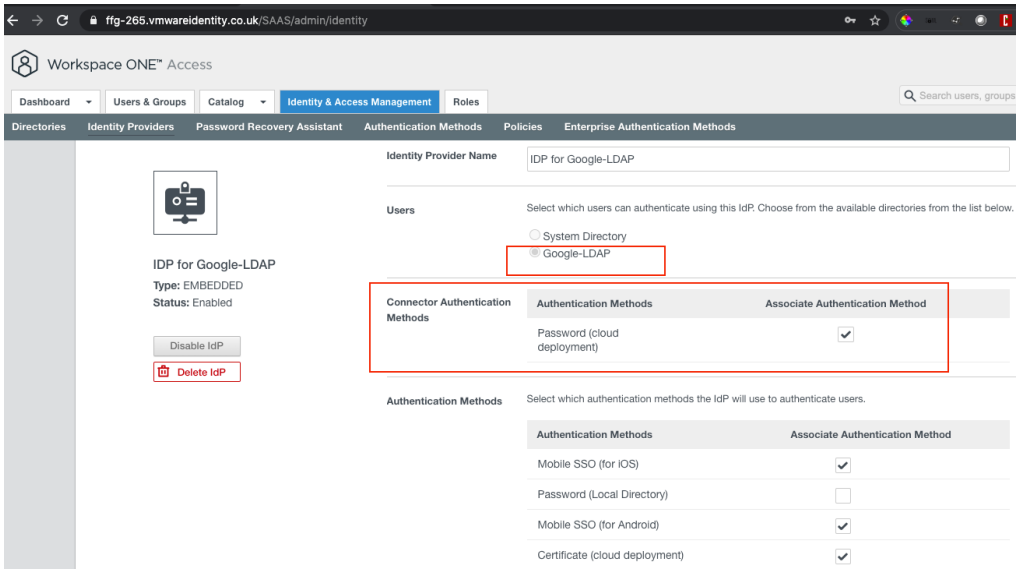
Check the Identity providers enabled



System Identity provider should only be associated with Password (Local Directory)



The build-in IDP for the Google-LDAP should be associated with the directory created and Password (cloud deployment) and other authentication methods such as SSO desired but not Password (Local Directory)

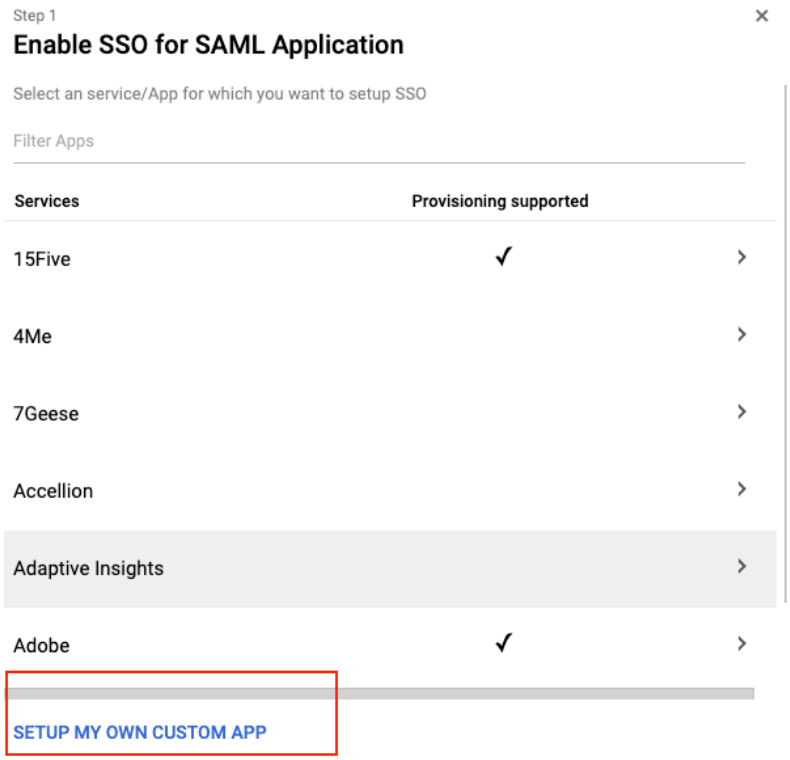


3.3.3. Google IDP

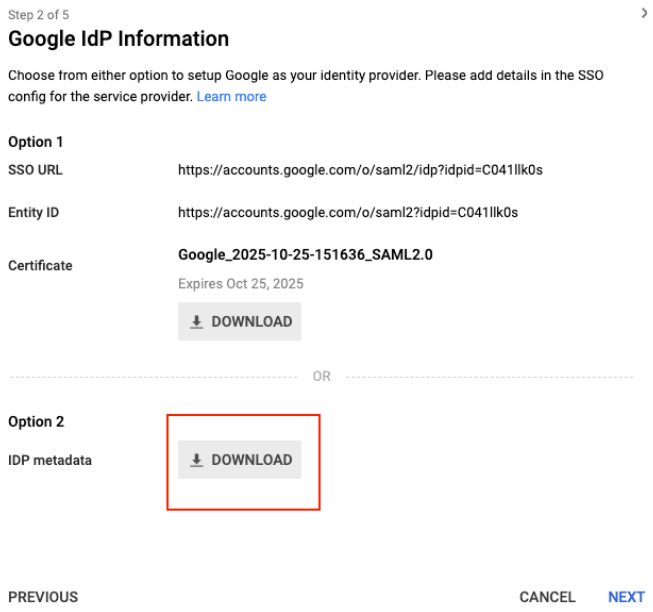
Google SAML can also be added as an a 3rd party IDP:

In the google admin console https://admin.google.com Add a SAML App

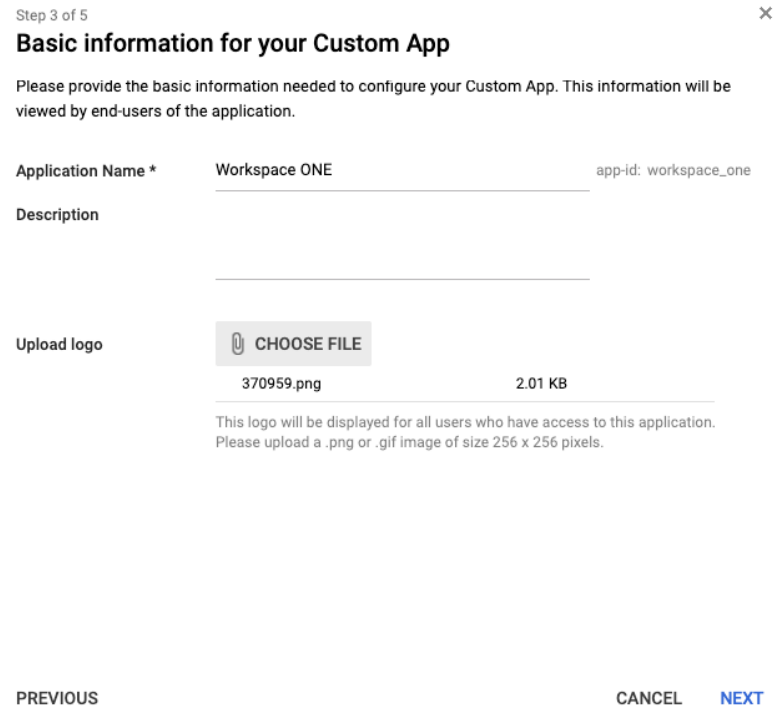
Choose Setup my own custom app



Download the IDP metadata



Set the application name and icon as required

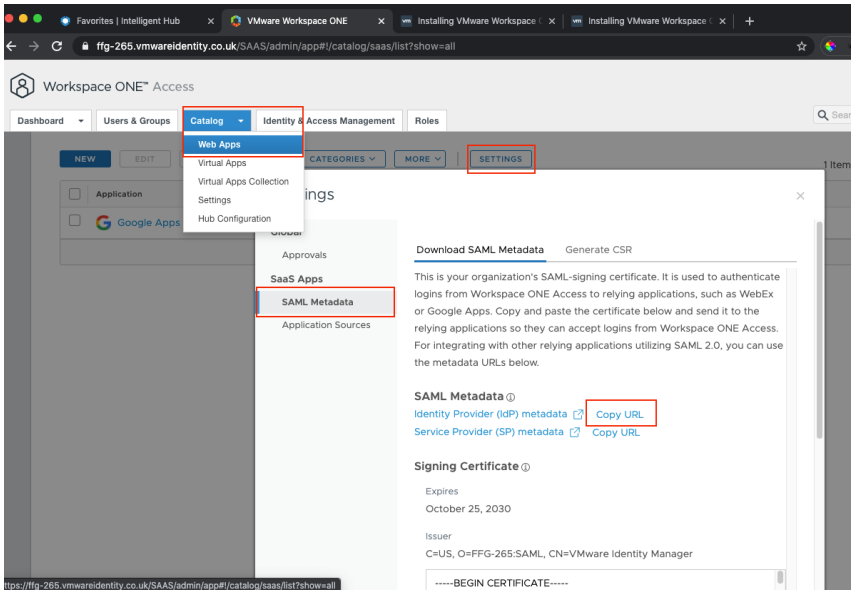


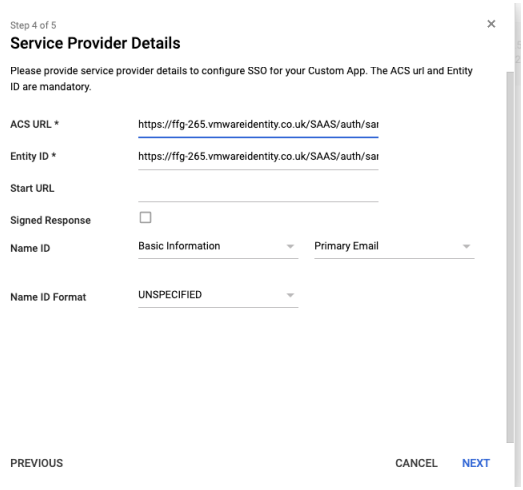
From Workspace ONE Access

Set the ACL URL to: https://xxxxx.vmwareidentity.co.uk/SAAS/auth/saml/response

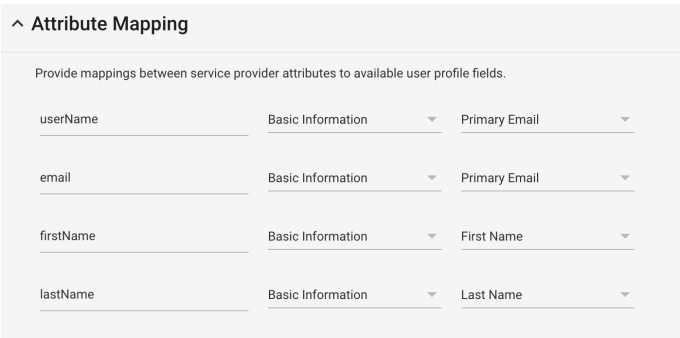
Where xxxxx is your Workspace ONE Access tenant hame

Then copy the SP URL from Workspace ONE Access and paste this into the Entity ID field:

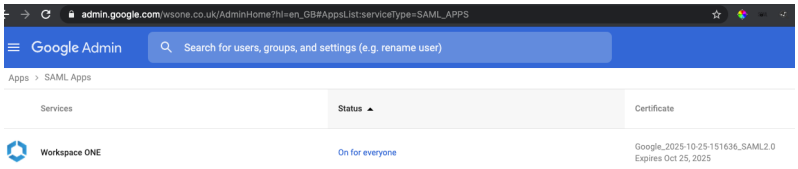




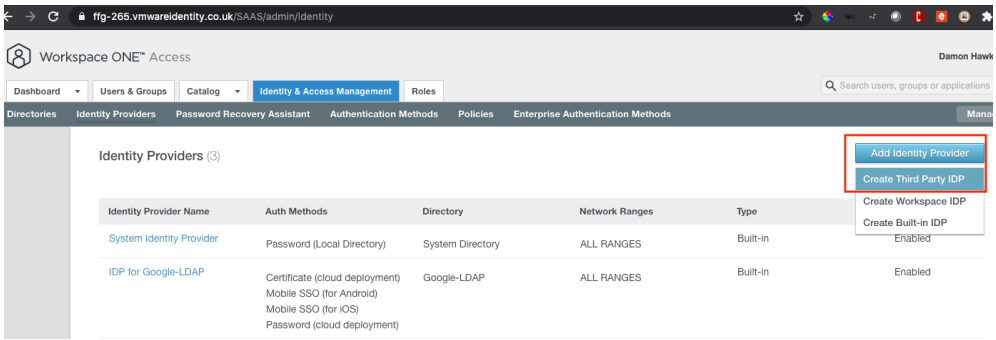
Set attribute mapping



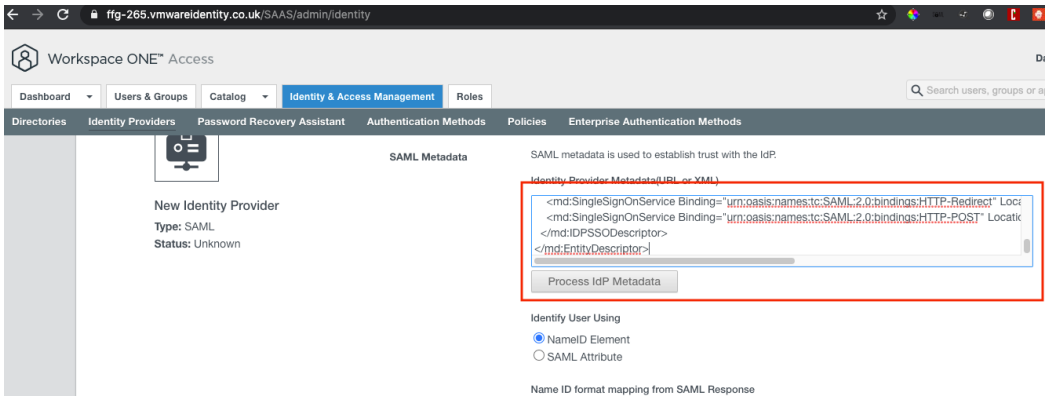
Enable the app for everyone



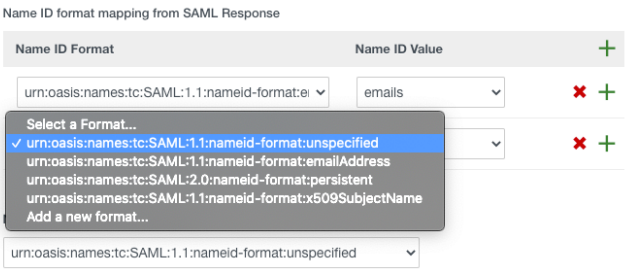
In Workspace ONE Access create a 3rd party IDP

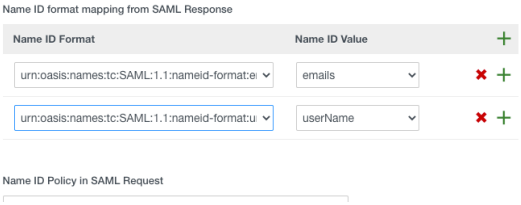


Paste in the downloaded GoogleIDPMetadata from the previous step and click process

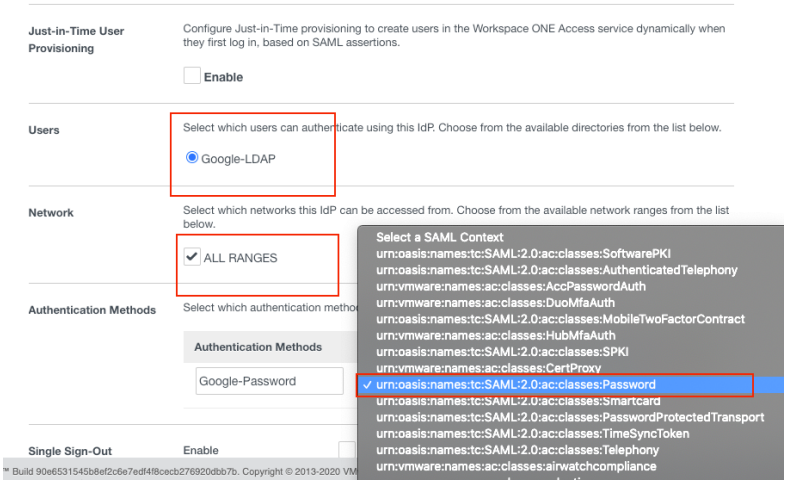


Add a second Name ID format mapping from SAML Response for username as shown

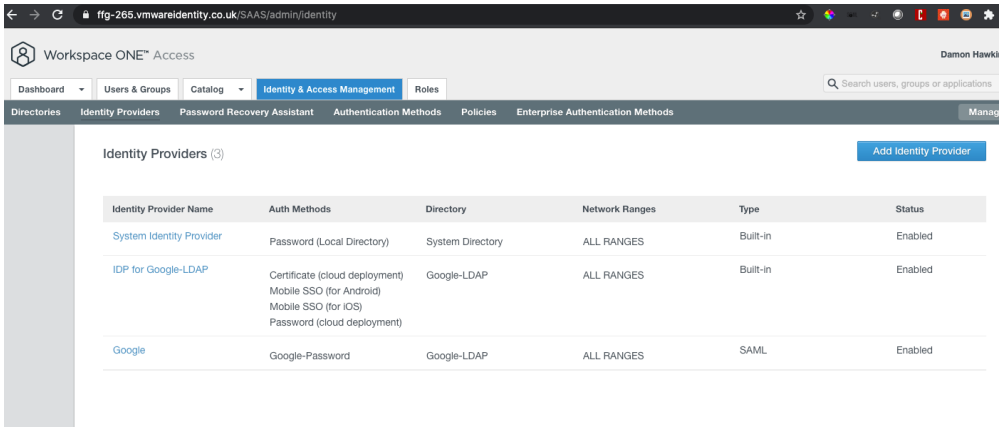




Select the Google-LDAP Users, All Range for Network. Then add Authentication Method as: Google-Password, selecting the Context as shown.



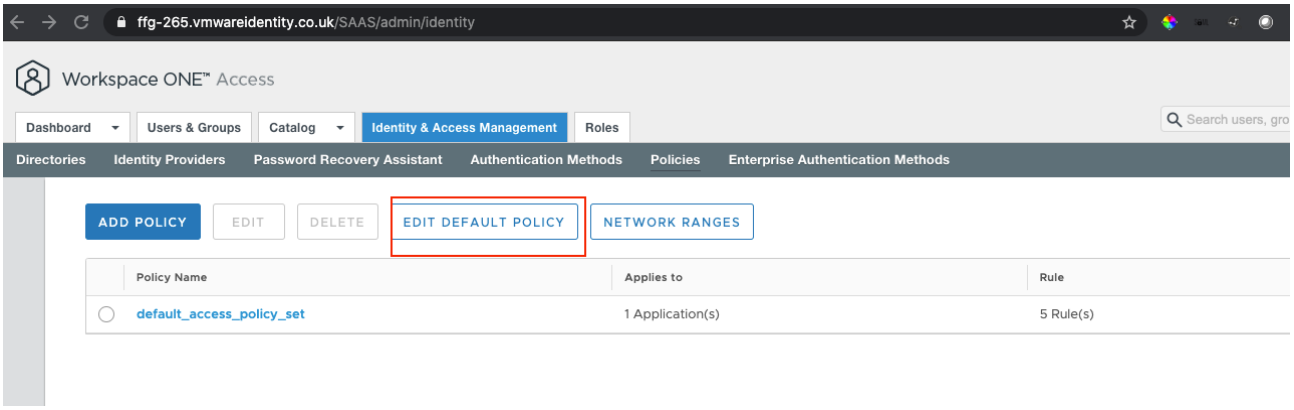
You should now have three Identity Providers as shown:



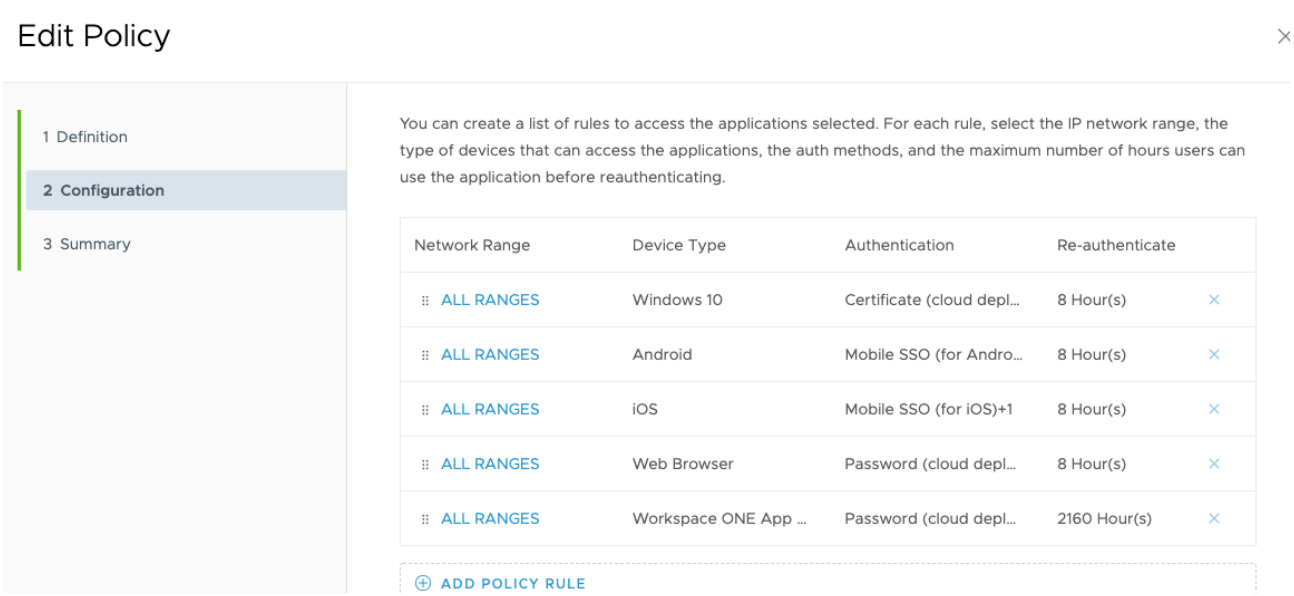
3.3.4. Access Polices

Lastly, we need to configure the Polices:

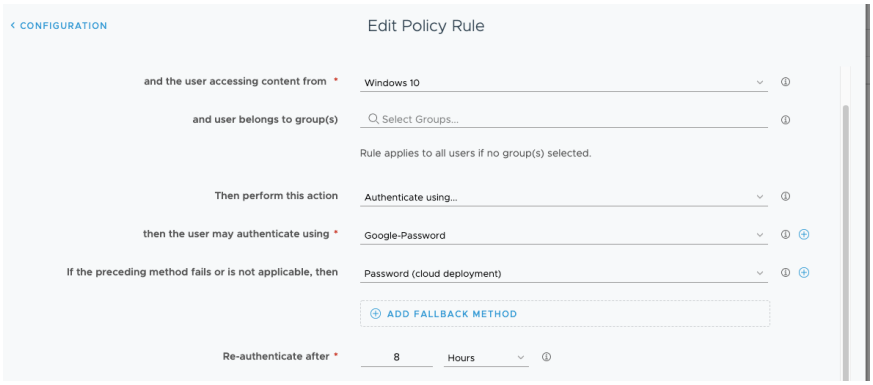
Edit the default Policy



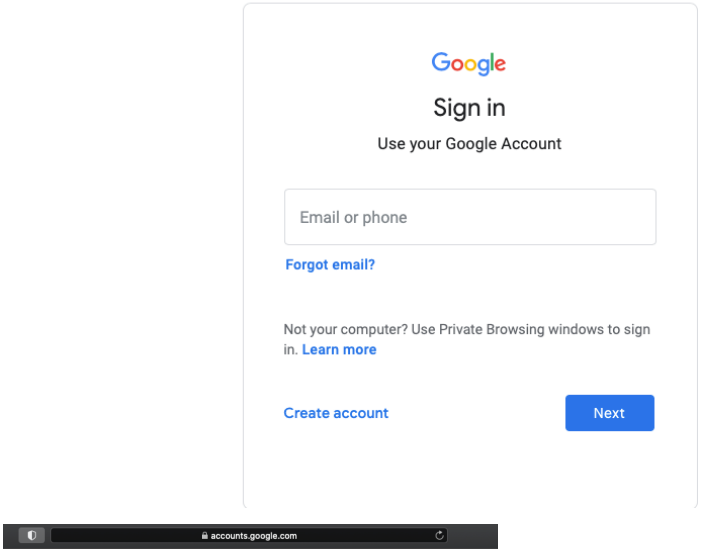
Configure rules for supported Operating system. Note that Specific OS rules should sit above, Web browser and the Workspace ONE App

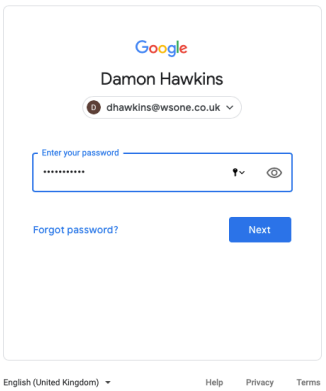


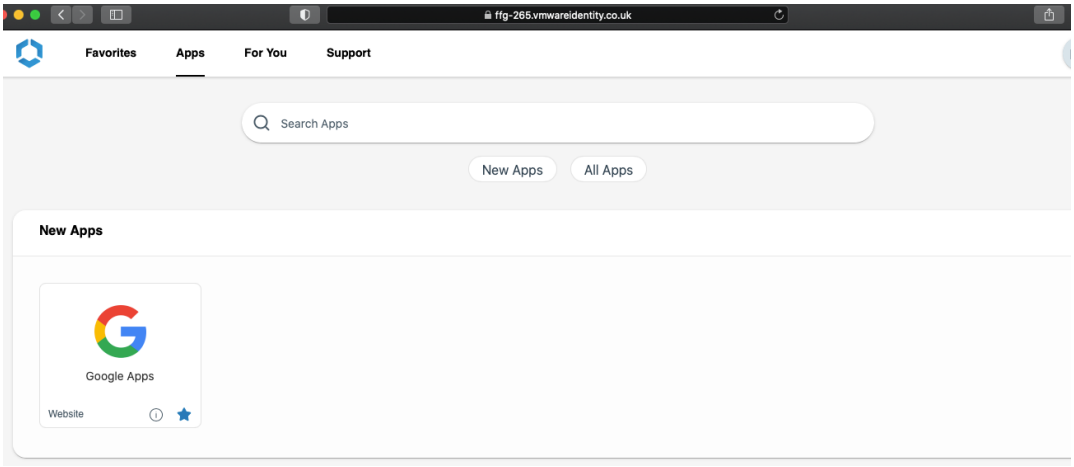
In this Windows 10 example. We are first attempting to authenticate Google, with a fall back to Password (Cloud deployment) which will use Access to authenticate via LDAP.



Test the authentication to the Workspace ONE Access URL with a web browser:

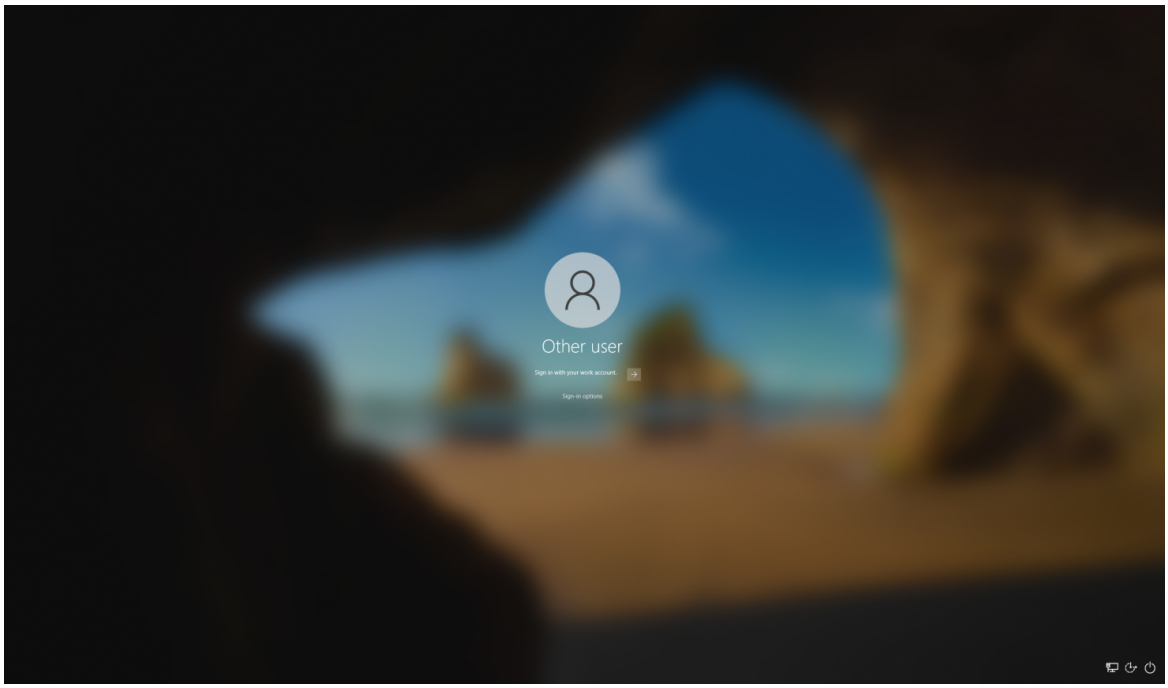




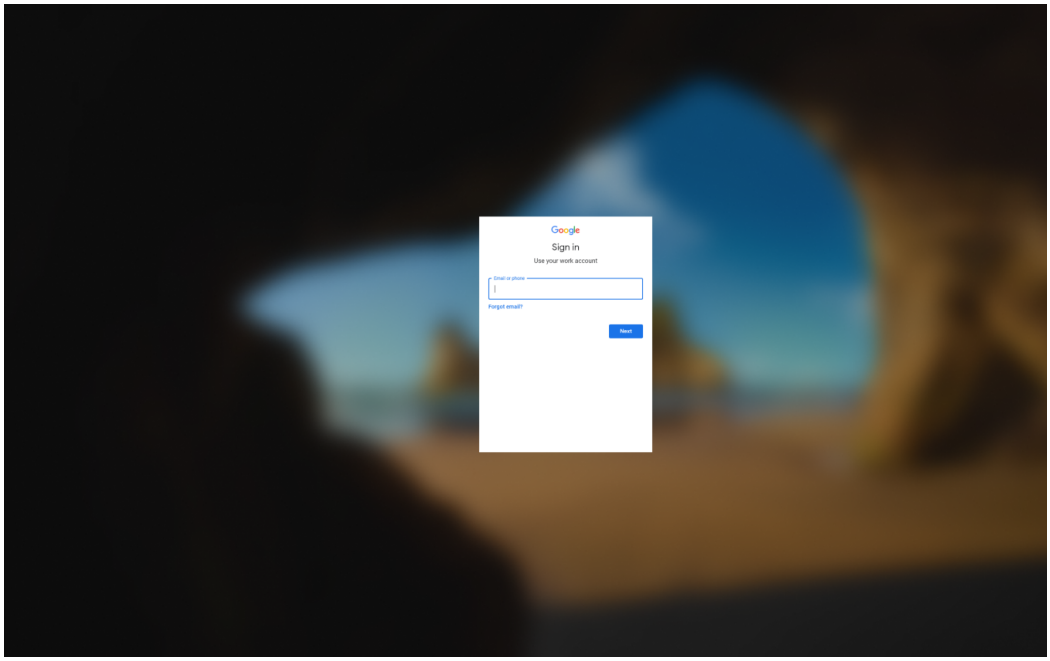


Authentication confirmed working, now ready to test device enrolment.

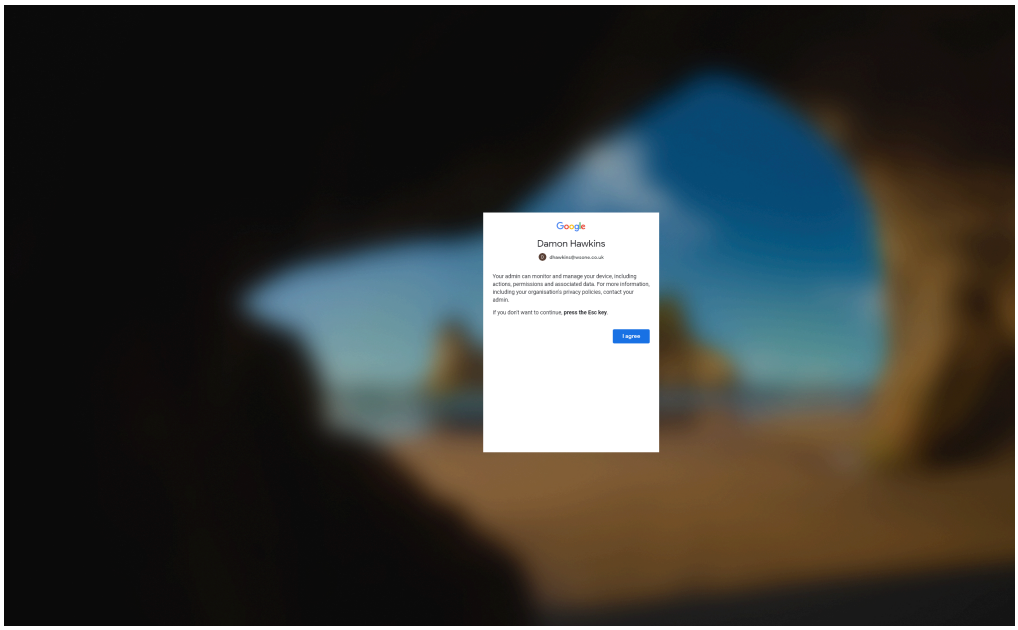
3.4. Windows 10 enrolment (factory)



User is presenting with only one option to click “sign in with your work account”

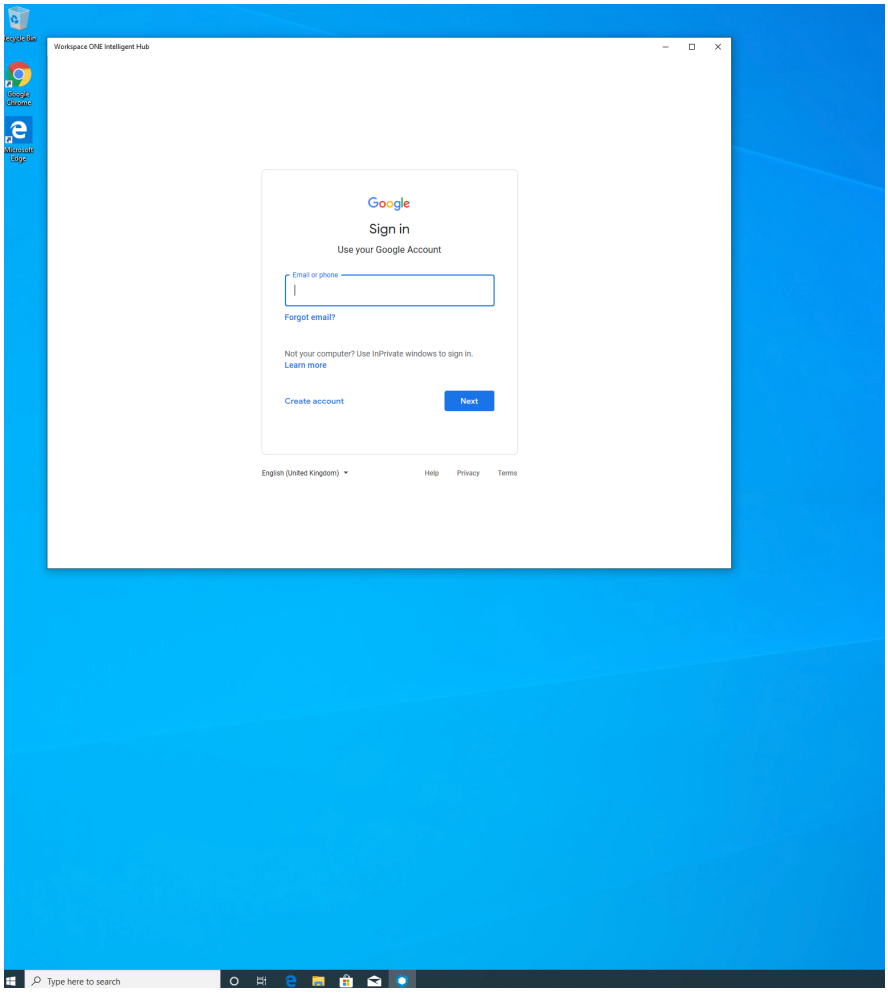


Enter Google account email address and password

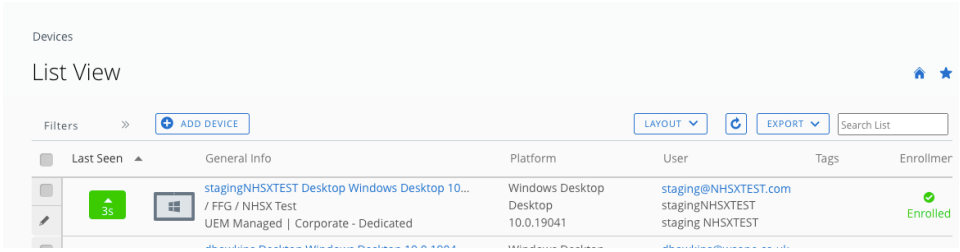


Accept T&Cs and device finishing provisioning

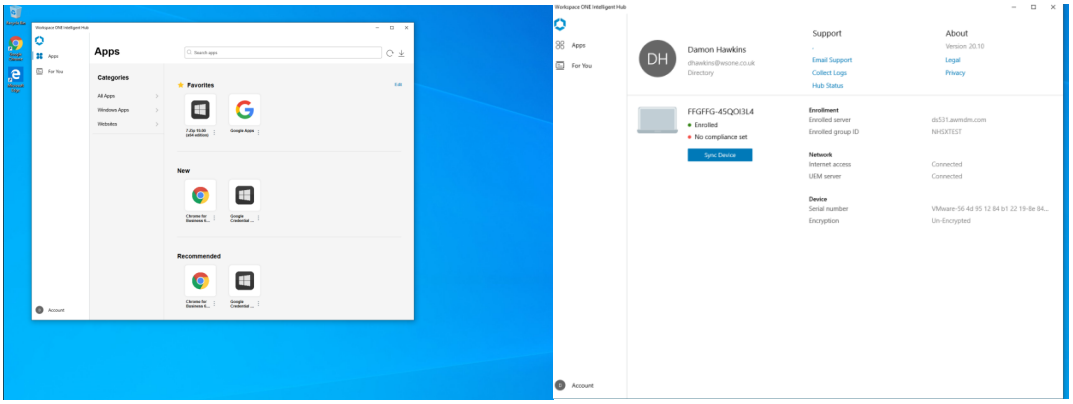
Desktop is exposed and the Hub launches for user to log in with their Google account



User enters their email address and password (at this stage the device is enrolled under the staging user).



Hub has now reassigned to the end-user



Device reassigned in the console