

Workspace ONE Factory Provisioning with Google Directory

Technical Guide

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

©2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

1. Summary	4
2. Prerequisites	5
2.1. Requirements	5
2.2. Assumptions	5
3. Configuration Example	6
3.1. User experience and end result.....	6
3.2. Workspace ONE UEM configuration.....	6
3.3. Workspace ONE Access configuration	16
3.4. Windows 10 enrolment (factory)	27

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

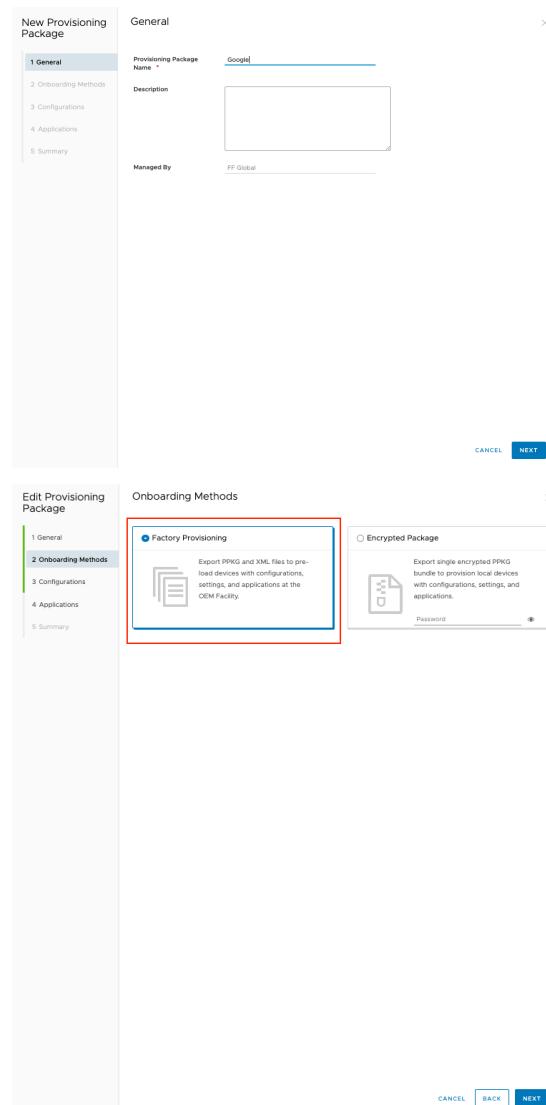
3.1. User experience and end result

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



Edit Provisioning Package

Configurations

Active Directory

Active Directory Type *

OOBE Configuration

EULA Page

Privacy Settings

Online Account Settings

Operating System Language *

Region and Keyboard Settings

Region and Keyboard *

System Configuration

Workgroup *

Registered Owner

Registered Organization

Computer Name

Remove Windows 10 Consumer Apps

Product Key *

Create Local User

Local Username *

Local User Password *

Make Administrator *

Enable Administrator Account

Administrator Password

User Account Control *

Additional Synchronous Commands

First Logon Commands

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</CommandLine>
<Description>Executing First Commands</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

The screenshot shows the 'Edit Provisioning Package' interface. On the left, a sidebar lists steps: 1 General, 2 Onboarding Methods, 3 Configurations, 4 Applications (selected), and 5 Summary. The main area is titled 'Applications' and contains a table of installed applications. Two specific rows are highlighted with a red box: 'Google Chrome' (version 84.0.4147) and 'Google Credential Provider for Windows' (version 68.21.49283). Both have checkboxes checked. At the bottom right of the table, it says 'Items 1 - 10 of 21' and has navigation arrows.

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

The screenshot shows the 'Shared Device' configuration page under 'Devices & Users > General'. On the left, there's a sidebar with various system and device-related settings. The main panel shows 'Shared Device' settings. Under 'Group Assignment Mode', the radio button for 'Fixed Organization Group' is selected and highlighted with a red box. There are other options like 'Prompt User For Organization Group' and 'User Group Organization Group'. Below this, there are sections for 'Always Prompt for Terms of Use' and 'Security'.

Settings > Devices & Users > General > Enrollment > Grouping

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

The screenshot shows the VMware Workspace ONE UEM interface. On the left, there's a navigation tree under 'Devices & Users' for 'General' settings. The main panel is titled 'Enrollment' and has tabs for 'Authentication', 'Management Mode', 'Terms of Use', 'Grouping' (which is selected), 'Restrictions', 'Optional Prompt', and 'Customization'. Under 'Grouping', the 'Current Setting' dropdown is set to 'Override'. The 'Group ID Assignment Mode' dropdown is set to 'Default' (highlighted with a red box). Below that, the 'Default' section shows 'Default Device Ownership' set to 'Corporate - Dedicated' (highlighted with a red box), 'Default Role' set to 'Full Access', and 'Default Action For Inactive Users' set to 'Enterprise Wipe Currently Enrolled Devices'.

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

Turn off undesired Privacy prompts

The screenshot shows the VMware Workspace ONE UEM interface. On the left, there's a navigation tree under 'Devices & Users' for 'Windows' and 'Windows Desktop' settings. The main panel is titled 'Intelligent Hub Settings' and has tabs for 'Current Setting' (set to 'Override') and 'MDM Settings' (set to 'None'). The 'Privacy' section is expanded, showing two buttons: 'Show Privacy Screen*' set to 'ENABLED' and 'Collect Analytics*' set to 'DISABLED' (highlighted with a red box).

3.2.3. UEM Cloud Connector

Make sure the UEM Cloud Connector is installed and working correctly

The screenshot shows the VMware Workspace ONE UEM interface. On the left, there's a navigation tree under 'Systems' for 'Enterprise Integration' and 'Cloud Connector' settings. The main panel is titled 'Cloud Connector' and has tabs for 'General' (selected) and 'Advanced'. Under 'General', the 'Current Setting' dropdown is set to 'Override'. The 'Enable AirWatch Cloud Connector' and 'Enable Auto Update' checkboxes are both checked ('ENABLED') (highlighted with a red box). A note at the bottom states 'The Workspace ONE Access Connector Installer is no longer included with the AirWatch Cloud Connector installer.'

3.2.4. LDAP Directory Settings

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

The screenshot shows the 'Server' tab of the LDAP configuration page. On the left, a sidebar lists various system and enterprise integration settings. The main area shows the following configuration:

- Current Setting:** Inherit (radio button) is selected.
- Directory Type:** LDAP - Other LDAP
- LDAP:**
 - Server:** 127.0.0.1
 - Encryption Type:** START TLS (selected)
 - Port:** 1636
 - Protocol Version:** 3
 - Use Service Account Credentials:** DISABLED (selected)
 - Bind Authentication Type:** BASIC (selected)
 - Bind Username:** PalatableC
 - Bind Password:** (redacted)
- Domain:** (empty input field)
- Server:** (empty input field)
- Add Domain:** ADD DOMAIN button

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 Filter syntax with: uid

The screenshot shows the 'User' tab of the LDAP configuration page. The navigation bar indicates 'System > Enterprise Integration > Directory Services'. The main area shows the following configuration:

- Current Setting:** Inherit (radio button) is selected.
- Domain:** Base DN*
- User Object Class:** person
- User Search Filter:** (&(objectClass=person)(uid=(EnrollmentUser)))

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)

Directory Services

Server User **Group**

Current Setting Inherit Override

Domain Base DN* 

Group Object Class* 

Organizational Unit Object Class* 

Advanced

Group Search Filter 

Membership Attribute User Attribute("Member of") Group Attribute("Member")

Auto Sync Default Automatically add/remove users in User Groups based on membership in LDAP/AD

Auto Merge Default Automatically apply sync changes without administrative approval

Maximum Allowable Changes

Auto-Update Friendly Name  ENABLED DISABLED 

Attribute	Mapping Value
Object Identifier	<input type="text" value="objectGUID"/>  
Name	<input type="text" value="name"/>  
Member	<input type="text" value="member"/>  
Common Name	<input type="text" value="cn"/>  
Member Of	<input type="text" value="memberOf"/>  
Distinguished Name	<input type="text" value="distinguishedName"/>  
Group Object Class	<input type="text" value="objectClass"/>  
Organizational Unit	<input type="text" value="ou"/>  
Organizational Unit Object Class	<input type="text" value="objectClass"/>  

Run a test and confirm fields are correct:

Test Connection

Server

Domain	Status
Binding information: PalatableC Server IP: 127.0.0.1 Connection successful with the given server name, bind username, and password.	

[TEST AGAIN](#)

User Group

Username

[CHECK USER](#)

User Attribute

Attribute	Mapping Value
Username	dhawkins
First Name	Damon
Middle Name	
Last Name	Hawkins
Full Name	Damon Hawkins
Display Name	Damon Hawkins
Email Address	dhawkins@wsone.co.uk
Email Username	
Phone Number	
Mobile Phone	
Distinguished Name	
User Principal Name	dhawkins@wsone.co.uk
Department	
Status	
Lockout Time	
Object Identifier	8d7f7491-745e-4d01-a1a0-f477d725aaf2
Object Class	top, person, organizationalPerson, inetOrgPerson, posixAccount
Last Modified	
Member Of	
Binding Attribute	
Employee ID	
Manager Distinguished Name	

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

The screenshot shows the my.vmware.com website with a search bar and navigation links for Products, Support, and Knowledge. Below the search bar, there's a 'Read More' link. Underneath it, there are two download links: 'Update Connector Configuration Script' (1.81 KB, bat file) and 'Hotfix HW-122490 KB Article Missing X-Frame-Options Header in cfg/shortcuts' (81.92 MB, zip file). Both have 'Read More' links and 'DOWNLOAD NOW' buttons. At the bottom, there's a section for the 'Workspace ONE Access Connector (VMware Identity Manager Connector)' with a red box around it. It lists 'Workspace ONE Access Connector 20.01.0.1' and 'Workspace ONE Access Standalone Connector Installer for Windows'. Both have 'Read More' links and 'DOWNLOAD NOW' buttons.

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)

The screenshot shows the VMware Identity Manager interface with a top navigation bar for Dashboard, Users & Groups, Catalog, Identity & Access Management (selected), Roles, and a search bar. Below the navigation is a secondary navigation bar for Connectors, Custom Branding, User Attributes, Terms of Use, Preferences, Auto Discovery, Okta, and VMware Workspace ONE UEM. The main content area has tabs for NEW, MANAGE, and RESET VIRTUAL APP USAGE. A table lists connectors under the 'Host' column, showing one entry: 'Google.hz4awx5ihmmuveisubfzvOwmrd.zx.internal.cloudapp.net' with 'Enterprise Service' as 'Directory Sync', 'Status' as 'Active', 'Health' as green, and 'Version' as '20.01.0.1'. There are also 'Manage' and 'Edit' buttons for this entry.

3.3.2. Directory

Add an LDAP Directory

The screenshot shows the VMware Identity Manager interface with a top navigation bar for Dashboard, Users & Groups, Catalog, Identity & Access Management (selected), Roles, and a search bar. Below the navigation is a secondary navigation bar for Directories, Identity Providers, Password Recovery Assistant, Authentication Methods, Policies, and Enterprise Authentication Methods. The main content area has tabs for Directories (selected), Identity Providers, Password Recovery Assistant, Authentication Methods, Policies, and Enterprise Authentication Methods. A table lists directories under the 'Directories (2)' heading, showing one entry: 'System Directory' with 'Type' as 'Local Directory', 'Domains' as 1, 'Synced Groups' as 0, 'Synced Users' as 2, and 'Last Sync' as N/A. There is a 'Manage' button for this entry. In the bottom right corner of the table, there is a red box around the 'Add LDAP Directory' button.

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

Add Directory

Directory Name*

Directory Sync and Authentication Select at least one active directory sync host that syncs users from Active Directory to the VMware Workspace ONE Access directory.

Directory Sync Hosts* Google.hz4awx5lhmmuveisubfv0wmrd.zx.internal.cloudapp.net (Active)

Authentication Do you want to set up the Password authentication method for this directory? If you choose Yes, select at least one of the active hosts listed in User Auth Hosts. If you choose No, you can set up authentication methods later.

Yes
 No

User Auth Hosts* Google.hz4awx5lhmmuveisubfv0wmrd.zx.internal.cloudapp.net (Active)

Add Directory

User Name*

Custom Directory Search Attribute for Users

Custom Directory Search Attribute for Groups

Server Location Enter the LDAP Directory server host name and port.

Server Host*

Server Port*

LDAP Configuration Enter the LDAP filter queries and attributes that VMware Workspace ONE Access can use to query your LDAP directory.

Add Directory

LDAP Configuration

Enter the LDAP filter queries and attributes that VMware Workspace ONE Access can use to query your LDAP directory.

Filter Queries

Groups*	(objectClass=groupOfNames)
Filter query to get groups.	
Bind user*	(objectClass=person)
Filter query to get bind user.	
Users*	(objectClass=person)
Filter query to get users.	

Attributes

Membership*	member
-------------	--------

Add Directory

The attribute that defines members of a group.

External ID*

The attribute to use as the unique identifier of users and groups in the Workspace ONE Access directory.

Distinguished Name*

The attribute that defines the distinguished name of a user or group.

Enable advanced LDAP configuration

Certificates

If your LDAP Directory requires access over SSL/TLS, select the check box below and provide the LDAP Directory SSL certificate.

This Directory requires all connections to use SSL

Bind User Details

In the Base DN field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. In the Bind User DN field, enter the account that can search for users. For example, CN=user1,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Base DN*	dc=wsone,dc=co,dc=uk
Bind User DN*	uid=dhawkins,ou=Users,dc=wsone,dc=co,dc=uk
Bind User Password*	<input type="password"/>

Enter your LDAP bind account password.

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

The screenshot shows the VMware Workspace ONE Access interface under the 'Identity & Access Management' tab. The 'Directories' section is selected, displaying two entries:

Directory Name	Type	Domains	Synced Groups	Synced Users	Last Sync
System Directory	Local Directory	1	0	2	
Google-LDAP	LDAP Directory	1	0	1	Oct 27, 2020 11:57:43 PM ✓

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

<ffg-265.vmwareidentity.co.uk/SAAS/admin/userGroups>

The screenshot shows the 'Users & Groups' section of the VMware Workspace ONE Access interface. A user profile for 'Damon Hawkins' is displayed, including fields for First Name (Damon), Last Name (Hawkins), Username (dhawkins), Email (dhawkins@wsone.co.uk), and Role (User). Below the profile, there is a red box highlighting the 'Principal Name' (dhawkins@wsone.co.uk), 'Distinguished Name' (UID=DHAWKINS,OU=USERS,DC=WSONE,DC=O,DC=UK), and 'External ID' (8d7f7491-745e-4d01-a1a0-f477d725aaaf2). At the bottom left, there is a checked checkbox labeled 'Enable'.

Check the Identity providers enabled

Identity Providers (3)

Identity Provider Name	Auth Methods	Directory	Network Ranges	Type	Status
System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES	Built-in	Enabled
IDP for Google-LDAP	Certificate (cloud deployment) Mobile SSO (for Android) Mobile SSO (for iOS) Password (cloud deployment)	Google-LDAP	ALL RANGES	Built-in	Enabled

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

Back to IdP List

The screenshot shows the configuration for the 'System Identity Provider'. It includes sections for 'Users' (with 'System Directory' selected) and 'Network' (with 'ALL RANGES' selected). In the 'Authentication Methods' section, 'Password (Local Directory)' is checked, while 'Mobile SSO (for iOS)', 'Mobile SSO (for Android)', and 'Certificate (cloud deployment)' are unchecked. Buttons for 'Disable IdP' and 'Delete IdP' are visible at the bottom.

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)

The screenshot shows the VMware Identity Management interface under 'Identity & Access Management'. A red box highlights the 'Authentication Methods' section, which includes 'Connector Authentication Methods' (listing 'Password (cloud deployment)' with a checked checkbox) and 'Authentication Methods' (listing 'Mobile SSO (for iOS)', 'Password (Local Directory)', 'Mobile SSO (for Android)', and 'Certificate (cloud deployment)' with checked checkboxes).

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

The screenshot shows the Google Admin Console Step 1: Enable SSO for SAML Application. It lists various services with 'Provisioning supported' status. 'Adaptive Insights' is selected. A red box highlights the 'SETUP MY OWN CUSTOM APP' button at the bottom.

Download the IDP metadata

Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. [Learn more](#)

Option 1

SSO URL <https://accounts.google.com/o/saml2/idp?idpid=C041llk0s>
Entity ID <https://accounts.google.com/o/saml2?idpid=C041llk0s>
Certificate **Google_2025-10-25-151636_SAML2.0**
Expires Oct 25, 2025

[DOWNLOAD](#)

OR

Option 2

IDP metadata

[DOWNLOAD](#)

[PREVIOUS](#)

[CANCEL](#) [NEXT](#)

Set the application name and icon as required

Step 3 of 5

Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name *

Workspace ONE

app-id: workspace_one

Description

Upload logo

CHOOSE FILE

370959.png

2.01 KB

This logo will be displayed for all users who have access to this application.
Please upload a .png or .gif image of size 256 x 256 pixels.

[PREVIOUS](#)

[CANCEL](#) [NEXT](#)

From Workspace ONE Access

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

Where xxxx is your Workspace ONE Access tenant name

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

The screenshot shows the VMware Workspace ONE Access interface. The top navigation bar has tabs for Catalog, Identity, Access Management, and Roles. The Catalog tab is active. Below the tabs, there are buttons for NEW, EDIT, and a search bar. A sidebar on the left lists Application and Google Apps. The main content area is titled "SAML Settings" and contains sections for Approvals, SaaS Apps, and SAML Metadata. The SAML Metadata section is highlighted with a red box. It includes fields for Identity Provider (IdP) metadata and Service Provider (SP) metadata, each with a "Copy URL" button. Below this is a "Signing Certificate" section with details like expiration date (October 25, 2030) and issuer (C=US, O=FFG-265:SAML, CN=VMware Identity Manager). A large text area labeled "-----BEGIN CERTIFICATE-----" contains the certificate content.

Step 4 of 5
Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *	https://ffg-265.vmwareidentity.co.uk/SAAS/auth/sar
Entity ID *	https://ffg-265.vmwareidentity.co.uk/SAAS/auth/sar
Start URL	<input type="text"/>
Signed Response	<input checked="" type="checkbox"/>
Name ID	Basic Information <input type="button" value="▼"/> Primary Email <input type="button" value="▼"/>
Name ID Format	UNSPECIFIED <input type="button" value="▼"/>

PREVIOUS CANCEL NEXT

Set attribute mapping

Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

userNmae	Basic Information <input type="button" value="▼"/>	Primary Email <input type="button" value="▼"/>
email	Basic Information <input type="button" value="▼"/>	Primary Email <input type="button" value="▼"/>
firstName	Basic Information <input type="button" value="▼"/>	First Name <input type="button" value="▼"/>
lastName	Basic Information <input type="button" value="▼"/>	Last Name <input type="button" value="▼"/>

Enable the app for everyone

The screenshot shows the Google Admin interface under the 'SAML Apps' section. It lists a single entry for 'Workspace ONE' with a status of 'On for everyone'. A certificate named 'Google_2025-10-25-151636_SAML2.0' is attached, set to expire on Oct 25, 2025.

In Workspace ONE Access create a 3rd party IDP

The screenshot shows the 'Identity Providers' page in Workspace ONE Access. A context menu is open over the first row, with the option 'Create Third Party IDP' highlighted by a red box.

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

The screenshot shows the 'SAML Metadata' configuration page. The 'Identity Provider Metadata (URL or XML)' field contains the pasted SAML metadata. A large red box highlights this field and the 'Process IdP Metadata' button below it.

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

The screenshot shows the 'Name ID format' configuration. A dropdown menu is open, showing several options for mapping names. The option 'urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified' is selected and highlighted with a blue border. Other options listed include 'urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress', 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent', and 'urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName'.

Name ID format mapping from SAML Response

Name ID Format	Name ID Value	
urn:oasis:names:tc:SAML:1.1:nameid-format:email	emails	x +
urn:oasis:names:tc:SAML:1.1:nameid-format:username	user_name	x +

Name ID Policy in SAML Request

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

Just-in-Time User Provisioning

Configure Just-in-Time provisioning to create users in the Workspace ONE Access service dynamically when they first log in, based on SAML assertions.

Enable

Users

Select which users can authenticate using this IdP. Choose from the available directories from the list below.

Google-LDAP

Network

Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

ALL RANGES

Authentication Methods

Select which authentication methods are available for this Identity Provider.

Authentication Methods

Google-Password

Single Sign-Out

Enable

Build 90e6531545b8ef2c6a7edf48c0d0276920dbb7b. Copyright © 2013-2020 VM

You should now have three Identity Providers as shown:

ffg-265.vmwareidentity.co.uk/SaaS/admin/identity

Damon Hawk

Workspace ONE® Access

Identity & Access Management

Directories Identity Providers Password Recovery Assistant Authentication Methods Policies Enterprise Authentication Methods

Identity Providers (3)

Identity Provider Name	Auth Methods	Directory	Network Ranges	Type	Status
System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES	Built-in	Enabled
IDP for Google-LDAP	Certificate (cloud deployment) Mobile SSO (for Android) Mobile SSO (for iOS) Password (cloud deployment)	Google-LDAP	ALL RANGES	Built-in	Enabled
Google	Google-Password	Google-LDAP	ALL RANGES	SAML	Enabled

Add Identity Provider

3.3.4. Access Policies

Lastly, we need to configure the Policies:

Edit the default Policy

The screenshot shows the VMware Identity Cloud Service (SaaS) Identity & Access Management interface. The top navigation bar includes links for Dashboard, Users & Groups, Catalog, Identity & Access Management (which is selected and highlighted in blue), and Roles. Below the navigation is a secondary menu with tabs for Directories, Identity Providers, Password Recovery Assistant, Authentication Methods, Policies, and Enterprise Authentication Methods. In the center, there are buttons for ADD POLICY, EDIT, DELETE, EDIT DEFAULT POLICY (which is highlighted with a red box), and NETWORK RANGES. A table below lists a policy named 'default_access_policy_set' which applies to 1 Application(s) and contains 5 Rule(s).

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

Edit Policy

The screenshot shows the 'Edit Policy' configuration page. On the left, a sidebar has three tabs: 1 Definition, 2 Configuration (which is selected and highlighted in blue), and 3 Summary. The main area contains a table of rules:

Network Range	Device Type	Authentication	Re-authenticate
ALL RANGES	Windows 10	Certificate (cloud depl...)	8 Hour(s)
ALL RANGES	Android	Mobile SSO (for Andro...)	8 Hour(s)
ALL RANGES	iOS	Mobile SSO (for iOS)+1	8 Hour(s)
ALL RANGES	Web Browser	Password (cloud depl...)	8 Hour(s)
ALL RANGES	Workspace ONE App ...	Password (cloud depl...)	2160 Hour(s)

At the bottom, there is a dashed box containing a '+ ADD POLICY RULE' button.

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.

The screenshot shows the 'Edit Policy Rule' configuration page. The rule is defined as follows:

- and the user accessing content from * Windows 10
- and user belongs to group(s)
- Rule applies to all users if no group(s) selected.
- Then perform this action Authenticate using...
- then the user may authenticate using * Google-Password
- If the preceding method fails or is not applicable, then Password (cloud deployment)
- Re-authenticate after * 8 Hours

At the bottom, there is a '+ ADD FALBACK METHOD' button.

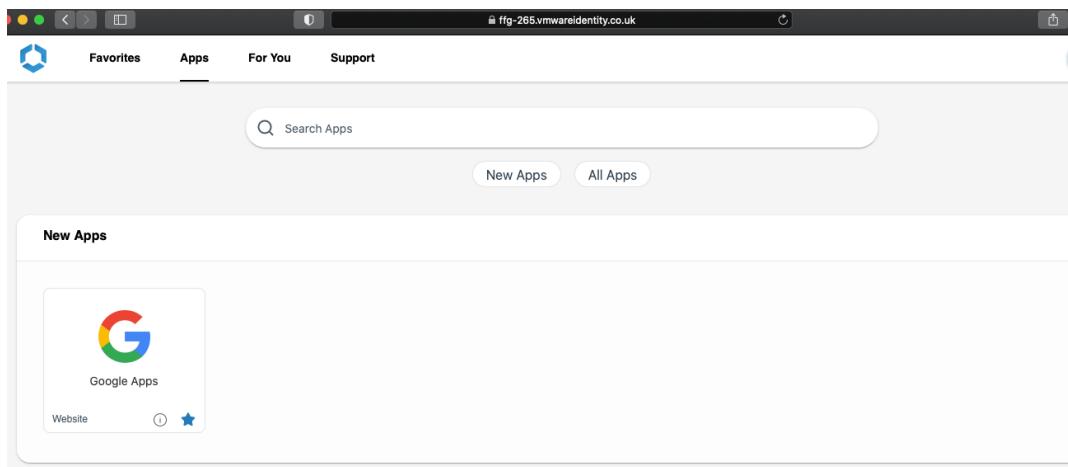
Test the authentication to the Workspace ONE Access URL with a web browser:



The screenshot shows the Google Sign-in page. At the top is the Google logo and the word "Sign in". Below that is the text "Use your Google Account". There is a text input field labeled "Email or phone" with a placeholder "Email or phone". Below the input field is a link "Forgot email?". Further down is a note: "Not your computer? Use Private Browsing windows to sign in. [Learn more](#)". At the bottom left is a link "Create account" and at the bottom right is a blue "Next" button.

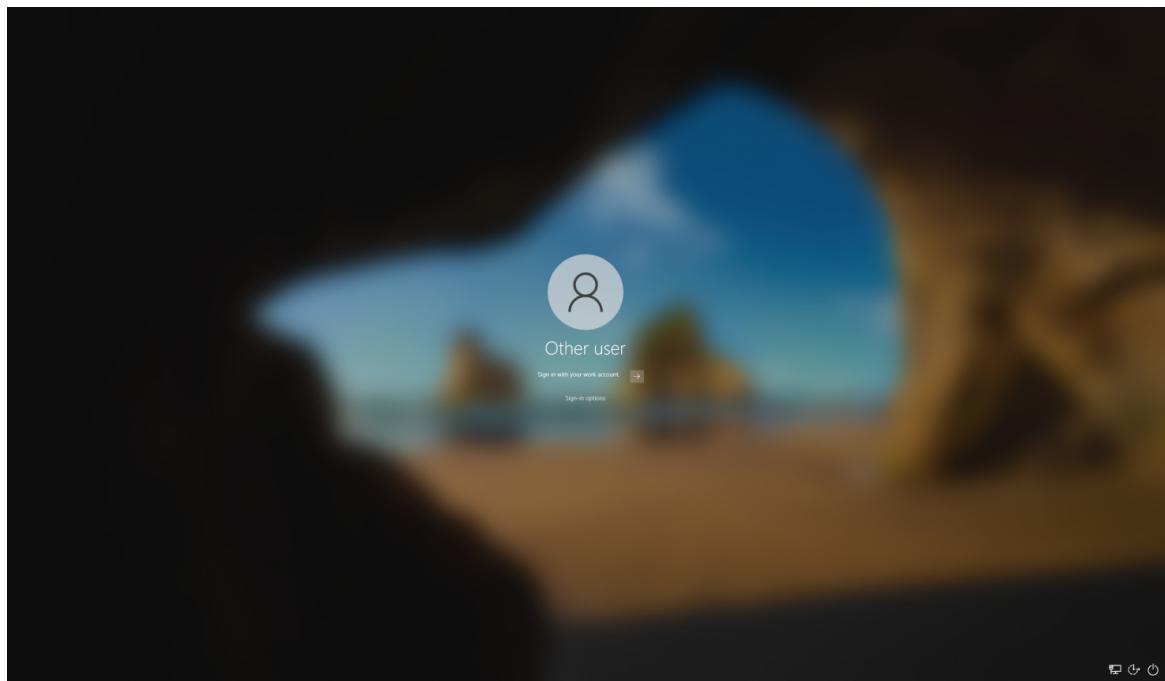


The screenshot shows the Google Password Entry page. At the top is the Google logo and the name "Damon Hawkins". Below that is an email address "d.hawkins@wsone.co.uk" with a dropdown arrow. There is a password input field with the placeholder "Enter your password" containing several dots. To the right of the input field are icons for a lock, a dropdown arrow, and an eye symbol. Below the input field is a link "Forgot password?". At the bottom right is a blue "Next" button. At the very bottom of the page are links for "English (United Kingdom) ▾", "Help", "Privacy", and "Terms".

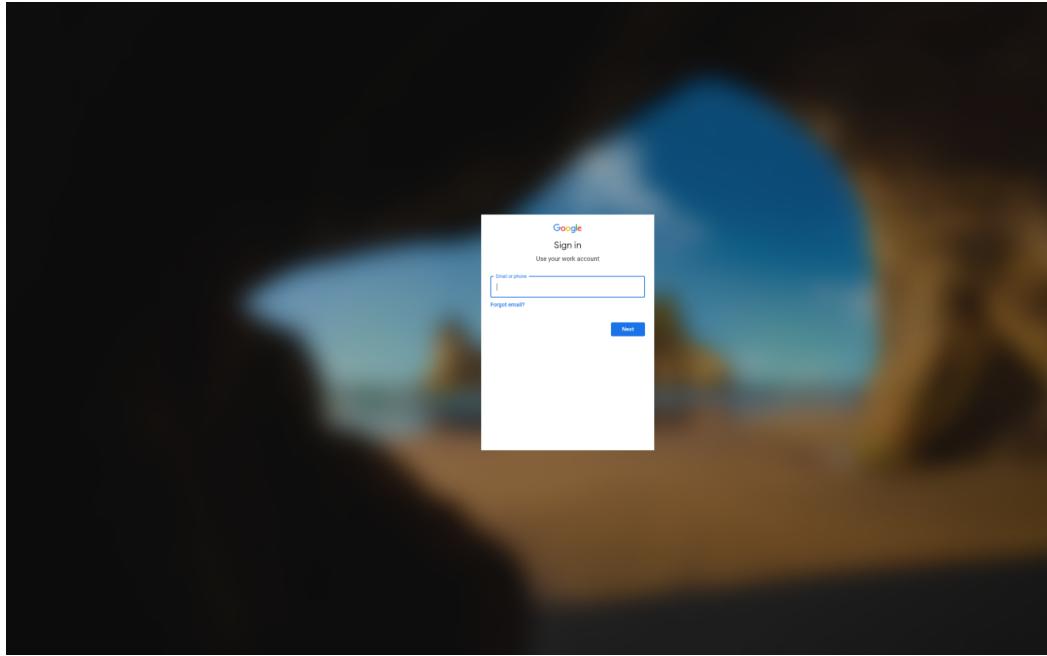


Authentication confirmed working, now ready to test device enrolment.

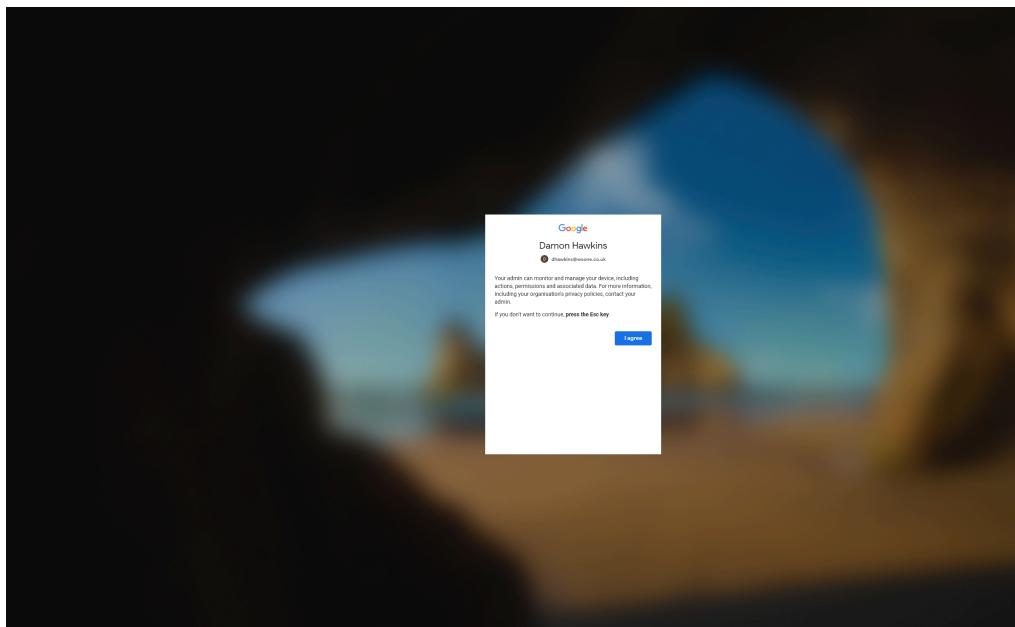
3.4. Windows 10 enrolment (factory)



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



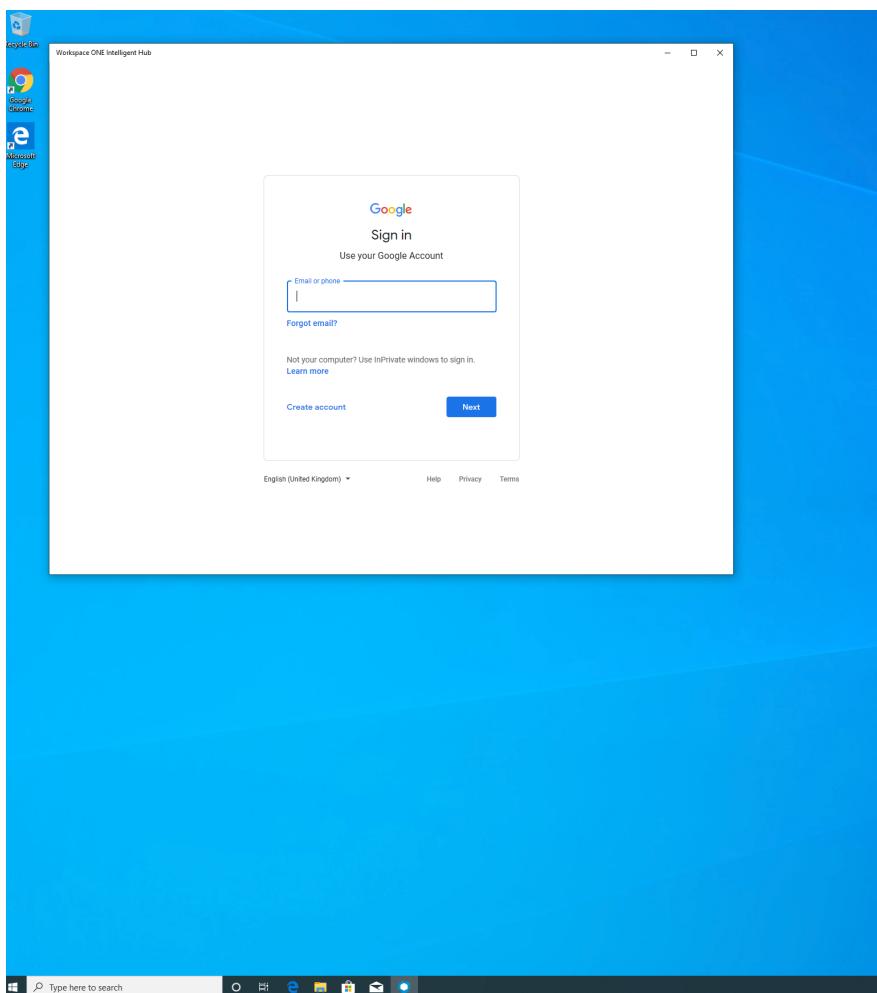
Enter Google account email address and password



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).

Devices

List View

General Info	Platform	User	Tags	Enrollment
stagingNHSXTEST Desktop Windows Desktop 10... / FFG / NHSX Test UEM Managed Corporate - Dedicated	Windows Desktop Desktop 10.0.19041	staging@NHSXTEST.com stagingNHSXTEST staging NHSXTEST		Enrolled

Hub has now reassigned to the end-user

The screenshot shows the VMware ONE Intelligent Hub interface. On the left, there's a sidebar with 'Apps' and categories like 'All Apps', 'Windows Apps', and 'Websites'. The main area displays 'Favorites' with icons for Google and Microsoft Edge. Below that are sections for 'New' and 'Recommended' apps. On the right, there's a user profile for 'Damon Hawkins' (dhawkins@wsone.co.uk) with a 'Sync Device' button. The 'About' section shows the version is 20.10. The 'Device' section provides details like the device ID (FFGFFG-45Q03L4), enrollment status (Enrolled), and network information (Connected). The 'Support' section includes links for Email Support, Collect Logs, and Hub Status.

Device reassigned in the console

Devices

List View

General Info	Platform	User	Tags	Enrollment
dhawkins Desktop Windows Desktop 10.0.1904... / FFG / NHSX Test UEM Managed Corporate - Dedicated	Windows Desktop VMware Virtual Platform 10.0.19041	dhawkins@wsone.co.uk dhawkins Damon Hawkins		Enrolled