

# Customer Windows 10 OOBE and Office 365 SSO - PoC Walk Through

A detailed guide, outlining how to configure AirWatch, vIDM and Azure to facilitate O365 SSO and Window 10 out of the box experience. This has been setout as a walk through, to present any readers a technical step by step guide to configure this themselves.

Written by Charlie Hodge - CHodge@vmware.com

Project Overview	3
2 - Download and Test Enterprise System Connector	4
3 - Configure Directory integration and User/Group Sync	4
4 - Map ObjectGUID and Sync	5
5 - Join AirWatch console to vIDM to Syncronise User's/Groups	6
6 - Confirm Users are within vIDM	6
7 - Install Azure Connect client on On-Premise server to sync users to Azure	7
8 - Install Azure Active Directory Module for Powershell on On-Premise Server	. 10
9 - Configure Office 365 application within vIDM	.11
10 - Run powershell commands from On-Premise server to federate Azure AD to vIDM	.12
11 - Test The Federation	. 15
12 - Configure SAML integration between vIDM and AirWatch	. 19
Testing the AirWatch SAML authentication:	.22
13 - Install AirWatch by VMware enterprise application into Azure (Windows OOBE)	.23

# **Project Overview**

### **Project Description**

- SSO into O365 tenant from iOS, Windows 10 and Mac device
- SSO into Salesforce (development trial),
- Link the AirWatch and WSONE together unified catalogue
- Customer to provide some iOS, Mac and Win32 legacy apps Office, AV, Disk encryption to deploy to Windows 10 devices
- Horizon app integration full desktop and app presentation (for example Notepad, calculator)
- Demo the DEP, Autopilot deployment of iOS, Windows 10 and Mac devices

### Topology:

- To provide SSO from O365 we require, ACC/vIDM Connector and Azure Connect. Both installed on-premise.
- Workspace ONE will be integrated with AirWatch, leveraging device compliance and unified catalog.



### Approach

### Configuration steps for proposed topology

### Pre-req's provided by Customer:

1 x On-Premise server with Directory Services

1 x On-Premise server for Vmware Enterprise System Connector installation (on-domain)

1 x Azure Premium Trial

1 x Customer owned DNS name, added to Azure with Name Servers updated

1 x On-Premise server for Azure connect application (Sync users to Azure Directory)

1 x Office 365 Trial

\*\*All on-premise installations can be on the same server\*\*

### **Technical configuration steps:**

- 1. Confirm pre-req's are in place
- 2. Install and configure Enterprise System Connector on On-Premise domain joined server
- 3. Confirm domain User's/Group connection to AirWatch
- 4. Join AirWatch console to vIDM to Synchronise User's/Groups
- 5. Map objectGUID attribute and Sync
- 6. Confirm Users are within vIDM
- 7. Install Azure Connect client on On-Premise server to sync users to Azure
- 8. Install Azure Active Directory Module for Page 3 PowerShell on On-Premise Server

# 2 - Download and Test Enterprise System Connector

- Login to AirWatch Environment
- Download Enterprise System Connector
- Install ACC only
- Login to AirWatch Environment and test connection:

System > Enterprise Integration >	
VMware Enterprise Systems	Connector 📀
	General Advanced
Current Setting	O Inherit O Override
Enable VMware Enterprise Systems Connector	Enables secure connection to enterprise components
Enable Auto Update	Enabling Auto Update will seamlessly update the VMware Enterprise Systems Connector installed on your server after the corresponding Ai Show More
Download VMware Enterprise Syster For help with configuring, refer to the VMware Enter	ns Connector Installer 🕹 Irprise Systems Connector Guide
Child Permission *	O Inherit only O Override only O Inherit or Override
	Save Test Connection VMware Enterprise Systems Connector is active.

## 3 - Configure Directory integration and User/Group Sync

- From AW Navigate to System->Enterprise Integration->Directory Services Insert relevant information
- Test Connection, test user's/groups base DN is populated

Directory Services ⑦							
		Server	User	Group			
Current Setting	OInherit Override						
LDAP							
Directory Type*	Active Directory				• ()		
DNS SRV	Enabled Disabled (i)						
Server*	ch-productions.co.uk				(i)		
Encryption Type*	None SSL Start TLS	()					
Port*	389				()		
Protocol Version*	3				()		
Use Service Account Credentials	Enabled Disabled ()						
Bind Authentication Type*	Anonymous Basic Digest	Kerberos	NTLM	GSS-NEGOTIA	те ()		
Bind User Name	ch-productions\ServiceAW	ch-productions\ServiceAW					
Clear Bind Password	□ ()						
Bind Password				<b>≯</b> s	now		
	Domain			Server			
	ch-productions.co.uk			ch-productions.co.	ık		

Directory Services @		
	Server User Group	
Current Setting	OInherit Override	
Domain	Base DN◆	
ch-productions.co.uk	DC=ch-productions,DC	
User Object Class*	Person	0
User Search Filter*	(&(objectCategory=Person)(sAMAccountName=(EnrollmentUser)))	]0
✓ Advanced		
Auto Merge	Enabled Disabled	
Automatically Sync Enabled Or Disabled User Status	Enabled Disabled	
Value For Disabled Status	2 Flag Bit Match v	
Enable Custom Attributes	Enabled Disabled	
Attribute	Mapping Value	
Object Identifier	objectGUID 🧪 😋	
User name	sAMAccountName 🧪 😋	
Member Of	memberOf 🧪 🖒	

### Make sure the 'objectGUID' is mapped

Directory Services ②					
Oreate your many percenter room		Server	User	Group	
Current Setting	🔿 Inherit 🕲 Override				
Domain		Base DN*			
ch-productions.co.uk		DC=ch-pro	oductions,DC +		
Group Object Class*	group				0
Organizational Unit Object Class*	organizationalUnit				Ū
> Advanced					
Child Permission	O Inherit O Override O Inherit or Override				
	Save	Test Co	onnection	Start Setup Wi	zard

# 4 - Map ObjectGUID and Sync

Login to your vIDM console and make sure that the objectGUID user attribute is being synced:

Identity & Access Management->Setup->User Attribute

Make sure this is done before the AirWatch integration. User attributes cannot be changed after a directory has been added.

🛟 Workspace ONE				Tenant Admin - CHODGE-EU2
Dashboard - Users & Groups Cat	alog 👻 Identity & Access Management Roles			Q Search users, groups or applications
Connectors Custom Branding User	Attributes Auto Discovery Terms of Use AirWatch Pref	erences		Manage Setup
			Required	
		disabled		
		distinguishedName	<b>v</b>	
		domain		
		email	<b>v</b>	
		employeeID		
		firstName	<b>v</b>	
		lastName	<b>v</b>	
		phone		
		userName	<b>v</b>	
		userPrincipalName	✓	
	Add other attributes to use	Add other attributes to sync to the directory. Go to the directory's attributes page to attributes.	o map these	
		objectSUID	<b>x</b> +	

# **5** - Join AirWatch console to vIDM to Syncronise User's/Groups

V/M		
viviware identity Manager 🕖		
Server		
Here you may synchronize the directory at this Organization Group with VMware Iden	tity Manager. This allows VMware Identity Mana	ger to take advantage of your existing directory connection. To configure these settings, directory integration must be configured at this Organization Group. If the Configure button is not available, try changing your Organization
Group. Only one directory per parent/child tree may be synchronized.		
URL http:	s://dysondev.vmwareidentity.eu	
Admin User Name Dyso	nadmin_dev	
Admin Password*		
Directory* dyso	indev	
Mapping Attributes		
Attribute	Mapping Value	
Externalld	Unknown	
Password	Unknown	Manning the Object CLUD attribute is key here
UserStore	Unknown	Mapping the objection attribute is key here,
disabled	Status	this will be used to authenticate against Office 365
distinguishedName	DistinguishedName	_
domain	Domain	
email *	EmailAddress	
employeeID	Employeeldentifier	
firstName *	FirstName	
lastName *	LastName	
objectGUID	UserObjectIdentifier	7
phone	PrimaryTelephone	
roles	Unknown	
usarName *	Literflame	
user Drin de alManne +	UserName	
usermncipalivame *	UserPrincipleName	

## 6 - Confirm Users are within vIDM

	L Wick, John	JWick	ch-productions.co.uk	ch-productions.co.uk	N/A	ALL USERS	Enabled
I							

### Enable AirWatch and VMware Identity Manager Integration

• Login to the AirWatch console - Navigate to Groups and Settings->All Settings->System->Advanced->API->Rest API



#### Now we need to create an Admin account and export the account's certificate:

>Administrators and hit add. >Administrators and hit add. Create your Admin account and assign it a role that has access ie Console Administrator In the API tab change the authentication to certificates Choose a password for the certificate, click save. Now head back into the Admin account that you've just created Addentificate that you just created Addentificate that you just created	Basic Details Roles	n Notes	Within the AirWatch console, navigate to Accounts-
A server	User Type	Rasic Directory	>Administrators and hit add.
Image: Image	User name*	CHAPI	
Bit I and a set of the and the and a set of th	Password*	Chunge	Croate your Admin account and accign it a role that has
mtmm*   Mtmm* Antone Anton	Require password change at n login	ex. Enabled Disabled	
Number   Lattrat*   Lattrat	First Name*	API	access ie Console Administrator
Lut log*   main   main </td <td>Middle Name</td> <td></td> <td></td>	Middle Name		
tind dent*   Oppositions   witted: Wend   Oppositions   witted: Wend   Oppositions Oppositions   witted: Wend   Oppositions Opposit	Last Name*	Admin	In the API tab change the authentication to certificates.
Comparison forms     The bank      The data the set of the case of the ca	Email Address*	chodge@umware.com	
Two Doors   Londer   Londer   Inder Stragborg   Inder Stragborg   Inder Stragborg   Now head back into the Admin account that you've just created and export the certificate that you just created and export the	Organization Group	AirWatch Internal / CHodge (CHProductions)	Choose a password for the certificate, click save.
tuning*	Time Zone*	(GMT-05:00) Eastern Time (US & Canada) v	
<pre>nutLooker Page<sup>1</sup></pre>	Locale*	English (United Kingdom) [English (United Kingdom)] v	Now head back into the Admin account that you've just
	Initial Landing Page*	Devices > Dashboard Q	created and expert the certificate that you just created
See See	Two-Factor Authentication N	Aethod	
Autorication*   Basic   Description   Iscal Description   Iscal Description   Valid Frame   1/2/2017 200 AM   Thrappint   Scale Scalesof Statication Control   Control   Description   Immediate   Scale Control   Immediate   Scale Control   Scale   Immediate	Basic Details Roles	API Notes	
isuadiy on OuiS17/CMM Vali Promote STATICASTCOTO Vali Promote STATICASTCOTO Vali Promote STATICASTCOTO Vali Promote STATICASTCOTO Tumaparia Chest Centificate Centificate Passend III Controt Centificate Information StaticastCoto StaticastCo	Authentication*	Basic Directory Certificates	
Valid From     1/17/2017 200 AM       Valid To     1/17/2017 200 AM       Tumbaprint     6AA5316220005880078800CBU-X7311C0ETCCTCD       Centificate Password     Immedia       Epent Clent Centificate     1mmedia	Issued by	CN=15477:CHAPI	
Valia To 1/0/2037 200 AAA   Thumbarrint 6x6358(259000858105/9300.CD/C7.CT/CD)   Clear Clent Centificate 5xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Valid From	11/7/2017 7:00 AM	
Thumbapire     66A336239008388969488028804733102FCCC/CD     Image: Comparing the comparing th	Valid To	11/2/2037 7:00 AM	
Cetificate Password Sow	Thumbprint	60A53E629300B58890F9880CBD47331C0E7CC7CD	
Certificate Password Store		Clear Client Certificate	
Eport Clett Cetticue	Certificate Password		
		3how	
		Export Cherd Certificate	
		Export Client Certificate	
		Eport Client Certificate	
		Eport Client Certificate	
		Eport Cliere Certificate	
		Export Chere Certificate	
		Export Cleret Ceretificate	

Page 7

Head back over to the vIDM console and import the AirWatch certificate and copy the Admin/Enrolled user API keys:

🛟 Workspace ONE™			Tenant Admin ~ CHODGE-EU2
Dashboard - Users & Groups Catalog - Iden	tity & Access Management Roles		Q Search users, groups or applications
Directories Identity Providers Password Recovery As	sizent Authentication Methods Policies		Manage Setup
Directories (2)			Add Directory
Directory Name	Туре	Domains Synced Groups Synced Users	Last Sync Alerts
System Directory	Local Directory	1 0 4	
ch-productions.co.uk	Other Directory	1 1 3	

Click on 'Identity & Access Management' and 'Setup'

😂 Wo	rkspace Of	NE™							Tenant Admin - CHOE	DGE-EU2
Dashboard	- Users & Groups	Catalog -	Identity & Access N	Management	Roles			Q Search u	sers, groups or applications	
Connectors	Custom Branding	User Attributes	Auto Discovery	Terms of L	lse AirWatch	Preferences			Manage	Setup
					AirWatch					
					AirWatch Config	uration Configure AirWatch setting configure the settings click	s to integrate AirWatch with VMware Identity Manager. After you Save. You can then enable other feature options with AirWatch.			
						AirWatch API URL*	https://cn763.awmdm.com			
							Enter the AirWatch API URL.			
						AirWatch API Certificate*	Upload Certificate Show Certificate Details			
						Certificate Password*				
							Enter the certificate password.			
						AirWatch Admin API Key*	KxW8Ud2J3MFm4ZEdan7Ktk66D/KTYhiPlf/CMtcxNY4=			
							Enter the AirWatch admin API key copied from the AirWatch console.			
						AirWatch Enrolled User API Key*	vuoxGFII7cfHInvnz7FyofvgksomRLLRNHgRVXWw5AM=			
							Enter the AirWatch enrolled user API key copied from the AirWatch console.			
						AirWatch Group ID*	CHodge			
							Enter the AirWatch Organization Group ID for this integration.			
						Map Domains to Multiple Organization Groups	Man Methodale Control and an analysis (CC) to the united descelo in			
							Identity manager to register the user's device to the OG.			
						Save				
					Unified Catalog	Enable Unified Catalog to r	nerge applications setup in the AirWatch catalog to the Unified Catalog			
				VMware Ider int	tity Manager™ Build ellectual property law	3294dc6b307cf8d94e6772b0684d562315365d3 s in the United States and other countries as well	<ol> <li>Copyright © 2013-2018 VMware, Inc. All rights reserved. This product is protected by copy as by international treatiles. VMware products are covered by one or more patients listed at</li> </ol>	right and		
https://chodge-eu2.vr	nwareidentity.eu/ws-admi	n/apps#!/airwatch				http://ww	w vmware.com/go/patents.			

Under the 'AirWatch' option you have the ability to upload the information exported from AirWatch.

AirWatch			Add the URL of your AirWatch environment.
AirWatch Configuration	Configure AirWatch settings to inte configure the settings click Save.	tegrate AirWatch with VMware Identity Manager. After you You can then enable other feature options with AirWatch.	
	AirWatch API URL*	ttps://cn763.awmdm.com	Upload the certificate you
	AirWatch API Certificate*	ter the AirWatch API URL Upload Certificate How Certificate Details pload the AirWatch .p12 certificate used for API calls.	exported from AirWatch on page 7.
	Certificate Password*	nter the certificate password.	
	AirWatch Admin API Key* Ki	xW8Ud2j3MFm4ZEdan7Ktk66D/KTYhiPif/CMfcxNY4=	Copy the Admin API key created
	AirWatch Enrolled User API Key*	uoxGFII7cfHInvnz7FyofvgksomRLLRNHgRVXWw5AM=	on page 7.
	AirWatch Group ID*	Insole. CHodge	Copy the Enrolled user API key
	Map Domains to Multiple Organization Groups ide	ap Ai/Watch Organization Groups (OG) to the user's domain in entity manager to register the user's device to the OG.	created on page 7.
	Save		Add the GroupID of your AirWatch envionrment.
Unified Catalog	Enable Unified Catalog to merge a	applications setup in the AirWatch catalog to the Unified Catalog	

After the integration is complete, scroll down and enable 'User Passwaord Authentication through AirWatch':

Unified Catalog	Enable Unified Catalog to merge applications setup in the AirWatch catalog to the Unified Catalog <ul> <li>Enable</li> <li>Disable</li> </ul>
	Save
Compliance Check	Enable Compliance Check to verify that managed devices adhere to AirWatch compliance policies.
	Save
User Password Authentication through AirWatch	Enable user password authentication through AirWatch.
	Save
User External Access Token Authentication	Enable user external access token authentication through AirWatch.
	Save

You will then need to update the Authentication Methods into vIDM to enable 'Password (AirWatch Connector)' and assign that authentication method to your domain.

### 7 - Install Azure Connect client on On-Premise server to sync users to Azure

Pre-reqs:

- Azure Premium with custom domain names added.
- DNS Name servers updated.
- Domain must be verified.

![](_page_9_Picture_5.jpeg)

Download the Azure Connect Client to the On-Premise Server and install as AD global administrator: <u>https://download.microsoft.com/download/B/0/0/B00291D0-5A83-4DE7-86F5-</u> <u>980BC00DE05A/AzureADConnect.msi</u>

This will then sync all users in the specified AD OU into Azure:

•	W	John Wick	JWick@ch-productions.co.uk	Member	Windows Server AD
---	---	-----------	----------------------------	--------	-------------------

### 8 - Install Azure Active Directory Module for Powershell on On-Premise Server

- Install Microsoft Azure Active Directory Module: <u>https://docs.microsoft.com/en-us/powershell/azure/install-azurerm-ps?view=azurermps-5.6.0</u>
  - Open Microsoft Azure Active Directory Module.
  - Connect to your Azure by running the following: Connect-AzureRmAccount

Administrator: Microsoft Azure Active Direct     PS C:\Windows\system32> Connect-MSo1	ory Module for Windows PowerStell	X
zc c	Microsoft Sign in someone@example.com Next	
	Can't access your account? You're seeing our <b>new sign-in experience</b> Go back to the old one	×

# 9 - Configure Office 365 application within vIDM

Edit Assign Delete Copy Export			
Name		Description	
Office365		Office 365 federated login that allows organizations to federate to Office 365 Portal using VMware	Identity Manager as Identity P
Icon		Categories	
0		-	
Cigning Cartificate		Launch IID	
		https://chodge.eu2.vmwareidentity.eu/443/SAAS/API/1.0/GET/apps/launch/app/b30ec050-10a5-43	Conville
		https://clouge-euz.viiwaredentity.eu.++s/sAAs/Ari/1.0/dc1/apps/adiici/app/bs0ec030-10as-+s	copy one
Configuration - Single Sign-On			
Authentication Type		Target URL	
WSFed 1.2		-	
Single Circ On 101		Application ID	
single sign-on the	ComulIDI	Application Misrosoft Opline	ComulIPI
https://ogin.microsoftoniine.com/ogin.sn	Сору ОКС	umiederation.microsoftOmine	Сору ОКС
Username Format		Username Value	
Unspecified		\${user.userName}	
Advanced Properties V			
Configuration - Access Policies			
Access Policy		VMware Browser	
default_access_policy_set		No	

This is to get the application within Workspace One ready for the federation process. After the app is setup, we will then head back to the on-premise server and run the federation commands.

Edit SaaS Application					Single Sign- On URL: Office Login URL (This is	
	<ul> <li>Single Sign-On UI</li> </ul>	RL 💿			filled in by default)	
Definition	https://login.micro	softonline.com/login.srf				
	* Application ID					
	urn:federation:Mic	rosoftOnline				
Access Policies	* Username Forma	it 🛞				
	Unspecified			~		
Provisioning	Username Value 🏐					
User Provisioning	\${user.userName}			*	Towney to Very we sistered Office 205	
	Application Pa	rameters			ienant: Your registered Office365	
Group Provisioning	News	Description	Default Value	Maha	Domain	
	Name	Description	Default value	value		
Summary	tenant	Office 365 Domain		ch-productions.co.uk	<b>Issuer</b> = unique identifier. Can be	
	issuer	Office 365 issuer URI		workspace.ch-productior	anything if not used by someone	
	Advanced Dropertie				else in O365.	
				Cancel Prev Next		

# **10** - Run powershell commands from On-Premise server to federate Azure AD to vIDM

The following will not work if you only have the default DNS name within Azure: chproductions.onmicrosoft.com. You need to make sure that the custom domain name has been added (Step 7).

|--|

First we need to download the Metadata from WorkspaceOne/vIDM:

New Edit Assign Dal	Inte Categories y More y Cattions	2 Itom = Saarch
Application		Gaterrales
Application	Ale and a second se	Categories
AirWatch	SAME 2.0 Tee Application	Recommended Saas Apps
Office365	WS-Fed Web Application	Recommended SaaS Apps
Salesforce	SAML 2.0 Web Application	Recommended SaaS Apps
4 4 1 <b>F</b> H		
Settings	×	
Approvals	Download SAML Metadata Generate CSR	<ol> <li>Under CataLog click on settings</li> <li>Click on SAML Metadata</li> </ol>
SAML Metadata	This is your organization's SAML signing certificate. It is used to authenticate logins from identity	2 Click on Identity Provider metadata
Application Sources	below and send it to the relying applications, such as webck or Google Apps. Copy and paste the certificate	3. Click on identity Provider metadata
	integrating with other relying applications utilizing SAML 2.0, you can use the metadata URLS	, 4. This will open a new tab, double
		click the first certificate so that it's
	Identity Provider (IdP) metadata Copy URL	all highlighted and copy, ready to
	Service Provider (SP) metadata 🖄 Copy URL	create your powershell commands.
	Signing Certificate	
	Expires	
	December 10, 2027	
	Issuer	
	C=US, O=DYSONDEV, CN=VMware Identity Manager	
	BEGIN CERTIFICATE MIIFFDCCAvygAwiBAgiGGGeld0w6MA0GCSqGSIb3DQEBCwUAMEIxiDAeBgNVBAMM F1ZNd2PyZSBJZCVudGi0e5BNYW5hZ2VyMREwDwYDVQQKDAhEWVNPTKRVJELMAkG A1UEBMKCVMwHhcNMTcxMJEyMTAwMDMyWhcNMJcxMJgcMjEwMTAwMDMyWJBCMS_wHgYD V0DDBrdWTXrdhcmuJsSWBhondHstTWEI.WWdicIEBMARGA1LIECewJREITUSER/Wx	
	Copy Download Regenerate	
s XML file does not appear to have a md:EntityDescriptor xmlns:md="	any style information associated with it. The document tree is shown below. urnicoasis:sames:tc:SAUL:2.0:metudata" cacheDuration="POYON3OD70NOM0.0000" stityID="https://chodge-eu2.vmware	voidentity.cu/SAAS/AFI/1.0/GET/metadata/idp.xml* validUntil="2027-09-24T18:41:26.0002">
<pre>w <md:keydescriptor http<="" pre="" use="signi&lt;br&gt;w &lt;ds:KeyInfo xmlns:ds="></md:keydescriptor></pre>	ng"> t//www.w3.org/2000/09/xmldsig#">	
<pre>v<ds:x509data> v<ds:x509certificate> MIIFGDCCAwCgAwIBAgIGR:</ds:x509certificate></ds:x509data></pre>	m7N+b2CMA0GCSgGS1b3D0EBCwUAME0x1DAeBgNVBAMME12Nd2Fv2SBJZGVudG10eSBNYW5b22VvMRMwE0YDV00KDAbDSE9ER0UtRVUvM0mvC0	OYDVOGEwJVUzAeFw0xNzA5MiYxODOxMiZaFw0vNzA5MiOxODOxMiZaME0xIDAeBcNVBAMMF1ZNd2FvZSBJZCVudC
<pre>v<md:reydescriptor use="encry" v<ds:keyinfo="" xmlns:ds="http x&lt;ds:Y500Data&gt;&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;ption &gt;&lt;br&gt;//www.w3.org/2000/09/xmldsig#"></md:reydescriptor></pre>		
<pre>v <ds:x509data> v <ds:x509certificate> MIIFGDCCAwCgAwIBAgIGR</ds:x509certificate></ds:x509data></pre>	m7N+b2CMA0GCSgGSIb3D0EBCwUAME0xIDAeBgNVBAMME12Nd2Fv2SBJZGVudG10eSBNYW5h22VvMRMwE0YDV00KDAbDSE9ER0UtRVUvM0ewC0	: CYDVOOGEwJVUzAeFw0xNzA5MiYxODOxNiZaFw0vNzA5MiOxODOxNiZaMEOxIDAeBaNVBAMMF1ZNd2FvZSBJZGVudG:
<md:artifactresolutionservic <md:singlelogoutservice bind<="" td=""><td>e Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/aut ling="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/</td><td><pre>ith/saml/artifact/resolve" index="0" isDefault="true"/&gt; S/auth/logout" ResponseLocation="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/logout"/&gt;</pre></td></md:singlelogoutservice></md:artifactresolutionservic 	e Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/aut ling="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/	<pre>ith/saml/artifact/resolve" index="0" isDefault="true"/&gt; S/auth/logout" ResponseLocation="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/logout"/&gt;</pre>
<pre>v <md:nameidformat>     urn:oasis:names:tc:SAML:1.     </md:nameidformat></pre>	1:nameid-format:unspecified	
<pre>v <md:nameidformat>     urn:oasis:names:tc:SAMI:1.</md:nameidformat></pre>	l:nameid-format:emailAddress	
 <pre>v<md:nameidformat></md:nameidformat></pre>		
urn:oasis:names:tc:SAML:2. 	J:nameid-format:persistent	
<pre>v <md:nameidformat>     urn:oasis:names:tc:SAML:1.</md:nameidformat></pre>	1:nameid-format:x509SubjectName	
<pre> <md:singlesignonservice <md:singlesignonservice="" bind="" bind<="" pre=""></md:singlesignonservice></pre>	<pre>img="urn:oasis:names:tc:SAML:2.0;bindings:HTTP-Redirect" Location="https://chodge-eu2.vmwareidentity.eu/SAMS/ img="urn:oasis:names:tc:SAML:2.0;bindings:HTTP-POST" Location="https://chodge-eu2.vmwareidentity.eu/SAMS/aut</pre>	<pre>J/auth/federation/sso"/&gt; th/federation/sso"/&gt;</pre>
<md:additionalmetadatalocation< td=""><td><pre>namespace="urn:oasis:names:tc:SAML:2.0:metadata"&gt;</pre></td><td></td></md:additionalmetadatalocation<>	<pre>namespace="urn:oasis:names:tc:SAML:2.0:metadata"&gt;</pre>	
https://chodge-eu2.vmwareide	ntity.eu/SAAS/API/1.0/GET/metadata/sp.xml	

### Navigate back to the On-Premise Machine with Azure Powershell Installed (Step 8)

### Use the following as a template:

Below are the variables of the powershell script.

Attribute	Variable Syntax	Example
-DomainName	Email.Domain.com	This domain needs to be registered inside of Azure, it has to be a secondary domain name such as email.com NOT email.onmicrosoft.com To register the domain name, if not already in place -
-IssuerUri	Identity.domain.com	This is the FQDN of the Identity Manager service domain. identity.domain.com
-	Arbitrary_Name	This is an Alias – Myldentity, or Company_Name will suffice.
FederationBrandName		
-PassiveLogOnUri	Hostname:port/excess	https://identity.domain.com/SAAS/API/1.0/POST/sso
-ActiveLogOnUri	Hostname:port/excess	https://identity.domain.com/SAAS/auth/wsfed/activelogon
-LogOffUri	Hostname:port/excess	https://login.microsoftonline.com/logout.srf
۔ MetadataExchangeUri	Hostname:port/excess	https://identity.domain.com/SAAS/auth/wsfed/services/mex
-SigningCertificate	SAML Singing Cert from IDM	Exclude the text " BEGIN CERTIFICATE" and "END CERTIFICATE" Also remove any line breaks. Should just read - aXpvbiBTQU1MIFNlbGYtU2lnbmVkIE

### **Template Scripts:**

### Script 1:

Set-MsolDomainAuthentication -DomainName < 0365 registered Domain > -Authentication Federated -IssuerUri "<serviceportal.customer>" -FederationBrandName "<Customer.com>" -PassiveLogOnUri "https://< mycompany.vmwareidentity.com >/SAAS/API/1.0/POST/sso" -ActiveLogOnUri "https://< mycompany.vmwareidentity.com >/SAAS/auth/wsfed/activelogon" -LogOffUri "<u>https://login.microsoftonline.com/logout.srf</u>"

### Script 2:

Set-MsolDomainFederationSettings -DomainName < O365 registered Domain > -MetadataExchangeUri "https:// mycompany.vmwareidentity.com SAAS/auth/wsfed/services/mex" -SigningCertificate < X509Certificate >

### 1 - Connect to your Azure using the Azure Powershell by running the following: Connect-MSolService

This will bring up a login box. Use your Azure admin account eg. admin@chproductions.onmicrosoft.com

el	Administrator: Microsoft Azure Active Dire PS C:\Windows\system32> Connect-HSo1	ectory Module for Windows Powerstell	X
sc		Microsoft	
lc.		Sign in	
di		Next	
		Can't access your account?	
		You're seeing our <b>new sign-in experience</b> Go back to the old one	×

### 2 - Customize the above template to match your environment. Here's mine:

#### CH-productions Script 1 - This is setting the variables for federated access into O365:

Set-MsolDomainAuthentication -DomainName ch-productions.co.uk -Authentication Federated -IssuerUri workspace.chproductions -PassiveLogOnUri "<u>https://chodge-eu2.vmwareidentity.eu/SAAS/API/1.0/POST/sso</u>" -ActiveLogOnUri "<u>https://chodge-eu2.vmwareidentity.eu/SAAS/auth/wsfed/activelogon</u>" -LogOffUri "https://login.microsoftonline.com/logout.srf"

# <u>CH-productions Script 2 -</u> This command is to check the federation settings and should return nothing. This means the domain is not yet federated which is good:

Get-MsolDomainFederationSettings -DomainName ch-productions.co.uk

# <u>CH-productions Script 3 -</u> This is to change the federation settings and apply the signing certificate exported from Workspace One (above):

Set-MsolDomainFederationSettings -DomainName ch-productions.co.uk -MetadataExchangeUri <u>https://chodge-eu2.vmwareidentity.eu/SAAS/auth/wsfed/services/mex</u> -SigningCertificate

MIIFFDCCAvygAwIBAgIGGGeld0w6MA0GCSqGSIb3DQEBCwUAMEIxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMREwDwYDV QQKDAhEWVNPTkRFVjELMAkGA1UEBhMCVVMwHhcNMTcxMjEyMTAwMDMyWhcNMjcxMjEwMTAwMDMyWjBCMSAwHgYDVQQDDBdW TXdhcmUgSWRlbnRpdHkgTWFuYWdlcjERMA8GA1UECgwIRFITT05ERVYxCzAJBgNVBAYTAIVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCg KCAgEApQFJT7I0cGi+Hxb9tfVIyXPIHwnGqpoQrfWyi07k9+vIJK86kdHDVrfl3Nv1T5Vbjgs73p/sqEvmJ9171GayZbaikSBrjAJC2/gsSn9ScIPAikqBm SGRWUYUEZ3NVQ2kV54i1P3EoS45ypt54nKoS2jz82Gz5xPwun2FdnqAAh8M2+qJ+PhOWqF0rtAMxWB6JoDqGJyRz39gAeoRbUXC/4E6gBRjcL uiUftLPJxz6VX+bAQTDtAXYQ7WdN/BQV4jjF6iGfggnw9Ul8UsTDpx4/DhU8zdfpNQ9aCsjzjSKBXElKuleNsCX0fLpgiL2WJ2h6CGV/WxhQ5Pq7nh TyJoxgID46E3+tRRsRAJImRMhOkUzck/XdfVDOFZWy+7eL5r85YeVAsR1BCLzHFaZ+RKB0MIv/20MSMbWOgMySInhS/WTbBioJ7gwNgabAT8uS aLIMVKdfyjQtsjHqlx+6qrH/D98ekRWwMMgdX4ycf5jgCpf3HRFjuAhKDWnfJl31PVDHeHj41bWmXCwXRa4cyrPzfGoFxo0CkVbUIs5za9pyovtaSI rBfludNtDDiPwQZNiUQF3B5tGCA2tFmVgelem9ltnX06CuDKra7rIDMwThDuINB0hKDQCn6yV3+bePQCxI+S3t9QhAhGPInM48rV7xxJaJuXk7oa nzjY27JwdpMCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAUu4yf/4/3e7JGK/cAh2xFiojx1jeQyTBZhlDt67Ai culpwpdjDmJNF4Ga6nK1kGmXHEzKqYT/Ej5sphCzAU0NfRVRqEhY/ZrvbJirK8EcrAzE3yL/VQ/gl0KDf9q/0MojSkZuyABBiDe0kCzuTh3uz1W1qxJ Seh187Ts1liF8en89uQvvJpxJ+9nfBTS3aokLirZnsJpvT2Ps1CaryOa5RLMa/3SCTpdkdmTQ2Qrr8lwjRnXZoBeMvwdlmNE8QuOoKFa2Xp2hsnCLU G6gLc1qciaE44XjRNiT4VIH/dUVX0OOO/XWHtcDFmiNYJzWbFngZf1enxmaiwOjx3D1jBas2iS/MLAynqniyJnxll7JeLNeCe/BHfHm/9N77co7JwvN 1MF3jDku5d7cFWr9DRZ7cL6s+C5Y/TZHWeTz6099AXmtzER3TixxtePA5yxjxJiL6BHZb7qxBjZJw78mPcIfMZ/+vU6ggwXw/Onk4InVH75XhAwto KnEEixc/1eSyBmBjI/p/qVW44wE8GPXgdc/m9tt5ld5uc4Nlb7MlXnSTcMt4nQsJDY6gVWa4q2i13VqEQZPeidpZO4/U8IXVelebMCbJd34L/eFQ/2 zS3Fwav7s3Opvp9eEdadlcR2J+i3JVo+KHSTPRzj9c8U6cGSDH2W/Oxhhm4b7oGJTYf/86c=

<u>CH-productions Script 4 -</u> This is to double check that the domain is now federated: Get-MsolDomainFederationSettings –DomainName ch-productions.co.uk

### **11 - Test The Federation**

### Test 1 - vIDM workflow:

 $\mathbf{N}$ 

- Navigate to Workspace One URL <u>https://chodge-eu2.vmwareidentity.eu</u>
- Login with domain credentials (Test user JWick)

O O O Workspace ONE ×	<b>\</b>	
$\leftarrow \  \   \rightarrow \  \  \mathbf{C} \  \   \boxed{\  \   ^{a} \   Secure \  \     \  https://chodge-eu2.vmwareidentity.eu/SAAS/auth/login}$		on ☆ :
	Workspace ONE" Username	
	Password	
	Sign in	
	Forgot Password?	
	<b>vm</b> ware:	

Click on the Office365 app that we setup in step 9 - If this does not appear, make sure that the entitlements are set correctly:

O     O     Workspace ONE	×					<del>.</del>
← → C a Secure   https://	//chodge-eu2.vmwareidentity.eu/ca	atalog-portal/ui?isOnPremise=false	&isMobile=false&userId=813599#,	/bookmarks		\$
	💭 Workspace ONE"		Q, Search		John Wick ~	
	$\langle \rangle$		BO	OKMARKS CATALOG		
		$\backslash$			Sort by A-Z 🐱	
	AirWatch	Office365	Salesforce			

This should then open a new tab, point you to the correct office URL and log you in - The below screen shows that we've been pointed to the office website, our information has been passed and we've been logged in! Result!:

	Office 365				¢	ı @ ?	John Wick 🔗			
	Good after	noon			Search online document	its				
	Apps					Install Office app	ps 🗸	ር ቆ <u></u> ?	John Wick	8
	Outlook	CneDrive	Word	Excel	P PowerPoint	Business center			<b>b</b> -	
	N OneNote	SharePoint	Teams	<b>Y</b> ≑ Yammer	Dynamics 365	Invoicing, email marketing, online presence and more in one.	e. All		ounts	×
	Flow									
	Explore all your apps -	<i>&gt;</i>							l <b>ohn Wick</b> Wick@ch-productions.co.uk	
	Documents				→ Upload	and Open Nev	N ~			
	Recent Pinned	Shared with me Disc	cover					My profile		
				<b>~</b>				My account		
https://po	rtal.office.com/BusinessCenter/Home	2					Feedback	Sign out		

Test 2 - Check federation from the office website:

- Navigate to the office website.
- Click the 'Sign In' button —
- Input the user's credentials (Modern.User2)
- Office should then be logged in

		_	_
Office 365 Login   Microsoft O x			
← → C ≜ Secure https://www.office.com	-	☆	:
Signal Si	jn in		
Office Products ~ Resources ~ Templates Support My account Buy Office 365	>		
Welcome to Office         Our place to create, communicate, collaborate and get great work done.         Get Office       Sign in			
What is Office 2652			

![](_page_16_Picture_0.jpeg)

	Sign in	
	JWick@ch-productions.co.uk	
	Next	
	Can't access your account?	
1		
	Microsoft	
	Taking you to your organisation's sign-in page	
1		

Workspace ONE ×				
Secure https://chodge-eu2.vmwareidentity.eu	I/SAAS/API/1.0/POST/sso	?client-request-id=075e60	15-5a70-45c4-b4bc-2896316eb	a7f&wa=wsignin1.0&wtrealm=ur 🗣
		Workspace ONE <sup>**</sup>		
	Username			
	Password			
		Sign in		
		Forgot Password?		
		Ū		
		<b>vm</b> ware <sup>.</sup>		
Microsoft Office Home ×	_	_		
Microsoft Office Home × a Secure   https://www.office.com/?auth=2				0
Microsoft Office Home × Secure https://www.office.com/?auth=2 xe 365				Ф 🛱 ? John Wic
Microsoft Office Home × Secure https://www.office.com/?auth=2 ce 365				Д ©? John Wic
Microsoft Office Home × Secure https://www.office.com/?auth=2 ce 365 Good afternoon			✓ ķearch online docur	우 🕲 ? John Wic nents
Microsoft Office Home × Secure https://www.office.com/?auth=2 ce 365 Good afternoon Apps				♀ I gohn Wic nents
Microsoft Office Home × Secure https://www.office.com/?auth=2 ce 365 Good afternoon Apps				
Microsoft Office Home × Secure https://www.office.com/?auth=2 to 365 Good afternoon Apps Outlook OneDrive	Word	Excel	Search online docur PowerPoint	Q       Image: Second state of the second sta
Microsoft Office Home × Secure https://www.office.com/?auth=2 te 365 Good afternoon Apps Outlook ConeDrive OneDrive SharePoint	Word Teams	Excel Excel	PowerPoint Dynamics 365	<ul> <li>Q Ø ? John Wic</li> <li>nents</li> <li>Install Office apps ∨</li> <li>C Business center</li> <li>Invoicing, email marketing, online presence and more. All</li> </ul>
Microsoft Office Home × Secure https://www.office.com/?auth=2 ce 365 Good afternoon Apps Outlook OneDrive OneNote So SharePoint	Werd Teams	Excel Ve Yammer	<ul> <li>Þearch online docur</li> <li>ÞowerPoint</li> <li>Þynamics 365</li> </ul>	Q       Image: Second system         nents       Install Office apps         Install Office apps       ✓         Image: Descend system       Business center         Invoicing.email marketing.online presence and more. All in one.       Inone.
Microsoft Office Home   Secure   https://www.office.com/?auth=2   Ce 365   Good afternoon     Apps   Image:	Word Teams	Excel Ve Yammer	<ul> <li>Þearch online docur</li> <li>PowerPoint</li> <li>Dynamics 365</li> </ul>	
Microsoft Office Home ×   Secure https://www.office.com/?auth=2   ce 365   Good afternoon     Apps     Outlook   Outlook   OneDrive   OneNote   OneNote   SharePoint   Flow   Explore all your apps →	Word Teams	Excel Excel Cartery Y Cartery	<ul> <li>Þearch online docur</li> <li>PowerPoint</li> <li>Dynamics 365</li> </ul>	Q       Image: Second system         nents       Install Office apps         Install Office apps       ✓         Business center       Invoicing, email marketing, online presence and more. All in one.
Microsoft Office Home   ▲ Secure   https://www.office.com/?auth=2   cc 365	Word Teams	Excel Sec Ye Yammer	<ul> <li>Þearch online docur</li> <li>PowerPoint</li> <li>Dynamics 365</li> </ul>	Q       Install Office apps         Install Office apps       ✓         Business center       Invoicing, email marketing, online presence and more. All in one.
Microsoft Office Home   Secure   https://www.office.com/?auth=2   cc 365	Werd Teams	Excel Ve Yammer	<ul> <li>✓ bearch online docur</li> <li>PowerPoint</li> <li>✓ Dynamics 365</li> </ul>	Q       Install Office apps         Install Office apps       ✓         Business center       Invoicing, email marketing, online presence and more. All in one.         Install office apps       ✓
Microsoft Office Home ×   ▲ Secure https://www.office.com/?auth=2   cc 365   Good afternoon   Apps   Image: Im	Werd         Teams	Excel Sec Yes Yammer	<ul> <li>✓ bearch online docur</li> <li>PowerPoint</li> <li>✓ Dynamics 365</li> </ul>	Q Install Office apps     Install Office apps     Install Office apps     Business   center     Invoicing, email   marketing, online   presence and more, All   in one.     bad and Open     New ∨
Microsoft Office Home   ▲ Secure   https://www.office.com/?auth=2   ce 365   Good afternoon   Apps   Image: Im	Image: Second	Excel See Yammer	<ul> <li>✓ bearch online docur</li> <li>PowerPoint</li> <li>✓ Dynamics 365</li> </ul>	Q       ②       ?       John Wick         nents       Install Office apps ✓         Install Office apps ✓       ③       Business center         Invoicing, email marketing, online presence and more. All in one.       New ✓         Dad and Open       New ✓
Microsoft Office Home   Secure   https://www.office.com/?auth=2   ce 365   Good afternoon   Apps <ul> <li>Outlook</li> <li>OneDrive</li> <li>OneNote</li> <li>SharePoint</li> <li>OneNote</li> <li>SharePoint</li> </ul> Flow Explore all your apps → Documents Recent Pinned Shared with me Disce	Word         Teams	Keel Keel Keel Keel	<ul> <li>✓ bearch online docur</li> <li>PowerPoint</li> <li>✓ Dynamics 365</li> </ul>	Q       Install Office apps       ✓         Install Office apps       ✓         Install Office apps       ✓         Image: Construction of the second
Microsoft Office Home   ▲ Secure   https://www.office.com/?auth=2   cce 365   Good afternoon   Apps <ul> <li>Outlook</li> <li>OneDrive</li> <li>OneNote</li> <li>SharePoint</li> <li>Compose all your apps →</li> </ul> Documents   Recent Pinned   Shared with me Disce	W       Word         T       Teams	Excel See Yammer	<ul> <li>✓ bearch online docur</li> <li>✓ PowerPoint</li> <li>✓ Dynamics 365</li> </ul>	Q       Image: Second system         Install Office apps       ✓         Install Office apps       ✓         Image: Center Second system       Business center Second system         Invoicing, email marketing, online presence and more. All in one.       All Yes         Dead and Open       New ✓

# **12** - Configure SAML integration between vIDM and AirWatch

						_
1.	Login to the WS	1 portal as Admin	New SaaS Application			
2.	Add AirWatch as	s an application	1 Definition	Definition		
3.	Configure the ap	oplication:	Configuration	Search ()		
	o AWServ	verName –	Configuration	Q, AirWatch		
	ds763.a	wmdm.com	Access Policies	AirWatch AirWatch Mobile Device Managemen	ent	
	○ Ac – CH	lodge	4 Summary	AirWatch Admin		
	<ul> <li>Audiend</li> </ul>	ce - AirWatch	_	Description 🛞		
		$\sim$		Iran @	A	
Γ	Edit SaaS Applicati	ion		icon g		
	O Definition	S{user.userName}			۰	
		Relay State LIRI		$\backslash$	Cancel Next	
	Configuration				*	
	Access Policies	Application De				
		Application Pai	ameters			
	Summary	AWServerName	AirWatch Server Name w	Default Value Value	com	
		ac	Group ID	CHodge		
		audience	Service Provider (AirWatc	AirWatch		
		Advanced Properties	~			
		Open in VMware Bro	wser 🕕			
		No				
				Cancel Prev	Next	
Edit Sa	aaS Application					
🗸 Defini	ition	Access Policies				
		Access policies specify the criteria th	at must be met in order to access appli	cations. Select access policies to manage user	Hit next – This will bring you	
Config	guration	access to specific applications below			Leave this as default, this can	
Access	s Policies	default_access_policy_set	~		be customised later if	
					required.	
Summ	nary				Hit next again – This will	
					bring you to the summary	
					page.	
					Save & Assign – Assign the	
					application as you see fit.	
				Cancel Breet		
				Cancel Prev Next		

4 - Now we need to export the WorkspaceOne/vIDM ipd metafile so we can upload it into the AirWatch console.

• Within vIDM, navigate to Catalog->Web Apps and click Settings

			-								
🚺 V	Vork	sp	ace ONE	ты							
Dashboar	d 🔻	Us	ers & Groups C	♥ Catalog ▼ Identity & Acc	ess Management	Roles	$\backslash$				
	New		Edit Assigr	n Delete Catego	ories 🗸 Mor	e 🗸	Settings				
		Арр	lication					Туре			
		٥	AirWatch					SAML 2.	0 Web Ap	oplication	
		box	Box.Net					SAML 2.	0 Web Ap	oplication	
		۲	DropBox - WS1	Extension				HTML Fo	orm		
Settings							×	SAML 2.	0 Web Ap	oplication	
Global Approvals			Download SAM	/L Metadata Generate CSR				WS-Fed	Web App	lication	
SAAS Apps SAML Metadata Application Source	ces		This is your orga Manager to relyi below and send integrating with below. SAML Metada	anization's SAML-signing certificate ing applications, such as WebEx or I it to the relying applications so the other relying applications utilizing ata	. It is used to authentic Google Apps. Copy and ey can accept logins fro SAML 2.0, you can use	ate logins from d paste the certi m Identity Mana the metadata U	ldentity ificate ager. For JRLs	Right-clic 'Save Link	k on th : As'	e IdP and click	
			Service Provide Signing Certi Expires	Open Link in New Tab Open Link in New Window Open Link in Incognito Window Save Link As Copy Link Address							
			September 2 Issuer C=US, O=CH(	Copy Search Google for "Identity Prov Print	vider (IdP) metadata"						
			BEGIN C MIIFGDCCA F1ZNd2FyZ CQYDVQQG. BgNVBAMM	Inspect Speech Add to iTunes as a Spoken Track IF1ZNd2FyZSBJZGVudGl0eSBNYW5	k hzzvyMRMwEQYDVQQ	(IDAeBgNVBAM R0UtRVUyMQsv MjZaMEQxIDAe KDApDSE9ER0L	IM N P Jt	Save the text' nai	e file as med id	s 'XML  p.	
					Copy Downl	oad Rege	enerate	/			1
						Save A Tag	ks: idp gs:				
						Name	IDP	Data Modified		Q Search	
					Avointes Dropbox Macintos Ar Applicatio Desktop						
					<ul> <li>Downloads</li> <li>Personal</li> <li>OneDrive</li> <li>Documents</li> </ul>						
					Movies  Novies  Control  Contro  Control  Control  Control  Control  Control  Contr						
					Shared						
							Format: XML te	ext	¢		Page
					Hide extension	New Fol	der			Cancel Save	

5 - Head back to the AirWatch console and navigate to the Directory services settings and scroll down to the SAML 2.0 settings:

- Enable 'Use SAML for Authentication' -
- Choose who you want to 'use SAML authentication for'
- 'Use New SAML Authentication Endpoint'—

Settings	AirWatch Internal / CHodge (C 🔻							
System Getting Started	Use SAML For Authentication		Enabled	Disabled				
Branding <ul> <li>Enterprise Integration</li> </ul>	Enable SAML Authentication For*		Admins	Users	Both	i		
Enterprise Integration Services Certificate Authorities	Use New SAML Authentication Endpoint	 •	Enabled	Disabled	i			
VMware Enterprise Systems Connector	SAML 2.0							
Directory Services Email (SMTP)	Import Identity Provider Settings		nd other	acvanced cont	guration o dio	95		

### 6 - Now we need to configure the SAML authentication.

Settings	AirWatch Internal / CHodge (C 🔻		Now we need to upload
System	SAML 2.0		the idp.xml file that we
Getting Started Branding	Import Identity Provider Settings		just exported from our
<ul> <li>Enterprise Integration</li> <li>Enterprise Integration</li> <li>Services</li> </ul>	To load the imported settings, click save. Any	changes made to the form will be lost.	VIDIVI CONSOLE.
Certificate Authorities VMware Enterprise Systems Connector	Service Provider (AirWatch) ID	AirWatch	
Directory Services Email (SMTP) VMware Tunnel	Identity Provider ID	https://chodge-eu2.vmwareidentity.eu/SAAS/API/	Scroll down and hit save. This will update the SSO URL
Peer Distribution Third-Party Proxies SMS	Enabling SAML authentication for directory t	sers will bypass other authentication modes.	and the Identity Provider ID
Pull Service Installers Syslog	Request	/	
Remote Management	Request Binding Type	🔿 Redirect 🝳 POST 🔿 Artifact	
<ul> <li>VMware Identity Manager</li> </ul>	Identity Provider Single Sign-On URL	https://chodge-eu2.vowareidentity.eu/SAAS/auth	
<ul> <li>Security Help</li> <li>Localization</li> </ul>	NameID Format*	Unspecified	
Report Subscriptions Terms of Use	Authentication Request Security*	None 🔻	Now we need to change the
<ul> <li>Advanced</li> </ul>	Response		'Request Binding Type' for the
Devices & Users	Response Binding Type	○ Redirect	request and the Response to
Apps	Sp Assertion URL	~/SAML/AssertionService.ashx?binding=HttpPost	'Authentication Response
Content	Authentication Response Security*	Validate Response Signatures	Security'. Make sure the settings
Email	Certificate		are set in the example screen
Telecom	Identity Provider Certificate	Type Cert	51101.
Admin		Valid From 9/26/2017	

### **Testing the AirWatch SAML authentication:**

- Login to Workspace One as your test user —
- Click on the AirWatch Web App
- This should now login to AirWatch SSP This will only work if the user is in vIDM and AirWatch

● ● ② Workspace ONE × ← → ℃ ● Secure   https://chodge-eu2.vi	nwareidentity.eu/catalog-	-portal/ui?isOnPremise=false&isMobile=fal	lse&userId=813599#/bookmarks	
🛟 Workspace ONE"	Q Search	BOOKMARKS CATALOG		Workspace ONE"
	n	salesforce		Username JWick Password
AirWatch	Office365	Salesforce		Sign in Forgot Password?
				vmware

This should open a new tab and login to AirWatch SSP.

AirWatch SSP	Account Dog Out
My Devices JWick Desktop My Devices JWick Desktop My Devices Devices Device	Add Device
JWick Desktop Windows Desktop 10.0.15063 0 c9	Windows Desktop   Desktop 10.0.15063 Ownership: Corporate - Dedicated
ENROLLMENT DATE LAST SEEN STATUS A 5 Issues need to be addressed	Go to Details
BASIC ACTIONS ADVANCED ACTIONS	
Device Query     Lock Device       Request updated information from the device.     Remotely lock this device to pro-	otect data.
Locate Device     Find the most recent location of this device.     Remove corporate settings and	I data from this device.
Send Message     Send Push Notification to Device     Delete the Device from Self-Sec	rvice Portal.
	Copyright © 2018   Powered by AirWatch

# 13 - Install AirWatch by VMware enterprise application into Azure (Windows OOBE)

1 - Login to the Azure Portal: <u>https://portal.azure.com</u>

- 2 Navigate to Azure Active Directory
- 3 Select, 'Mobility (MDM and MAM)'

![](_page_22_Picture_4.jpeg)

Home > chproductions - Mobility (MDM and	MAM) > Configure
Configure AirWatch by VMware	□ ×
🕞 Save 🗙 Discard 🛅 Delete	
MDM user scope   None	Some All
MDM terms of use URL 1 https://ds76.	3.awmdm.com/devicemanagement/enrollment
MDM discovery URL 1 https://ds76.	3.awmdm.com/deviceservices/discovery.aws

If a customer is hosted on a DSaaS or on premise, we will need to add another MDM application as well, so that we can point to the custom URL. Due to the custom URL we can leave the original 'AirWatch' Azure application MDM user scope to 'None'. Hit save and add another MDM application:

e 23

Settings	AirWatch Internal / CHodge (C 🔻		
System	Azure Active Directory		
System Getting Started Branding • Enterprise Integration Enterprise Integration Services Certificate Authorities VMware Enterprise Systems Connector Directory Services Email (SMTP) • VMware Tunnel Peer Distribution Third-Party Proxies SMS Pull Service Installers Syslog Video CDN Remote Management • VMware Identity Manager • Security Help • Localization Report Subscriptions Terms of Use S/MIME • Advanced	Azure Active Directory add the AirWatch by VMware appli 1) Navigate to the AirWatch by VMware appli Start Setup Wizard 2) Follow the instructions in the Azure Marke 3) Configure the AirWatch by VMware applica MDM Enrollment URL MDM Terms of Use URL 4) Enter your Azure Active Directory Tenant I Directory ID* Tenant Name* Immutable ID Mapping Attribute*	cation to your AAD tenant from the Azure Malvetp cation in the Azure Marketplace tplace to add the AirWatch by VMware application ation with the URLs below. https://ds763.awmdm.com/DeviceSe https://ds763.awmdm.com/DeviceMa D. Tenant ID can be found in the URL of your AAD i 02a5c195-1080-4c1d-bd16-868ef34e chodge@chproductions.onmicrosoft. objectGUID	lace. to your directory rvices/discovery.aw inagement/Enrollment Where in AAD 50 I paste this info? instance. i407 com How To Critain Tenant Info
Apps	Mapping Attribute Data Type*	Binary String (i	
AirWatch by VM Miradore Online	Azure Activ Azure Activ Sea OV Qu MANAGE Usu DSM DSM DSM Lightspeed I Lightspeed I On-premises	e Directory rch (Ctrl+/) erview ick start ers Nobi Microsoft Intune K	Add application     NAME     Image: AirWatch by VMware  <
Aid an application	as360 Lightspeed Mobil. Lightspeed Mobil. Microsoft Inture Microsoft Inture Microsoft Inture	Completingenergies with application  Microsoft Corporation  Use Microsoft Azure AD to enable user access to On-premises MDM application.  Requires an existing On-premises MDM application subscription.  Name © On-premises MDM application  Publisher © Microsoft Corporation  URL ©  Logo ©	Add application      NAME      On-premises MDM application      AirWatch by VMware      Microsoft Intune

Page 24

![](_page_24_Picture_0.jpeg)

We now need to configure the application.

On-premises MDM application	×	Settings	×	Required permissions	□ >
🛱 Save 🗙 Discard 🛅 Delete				🗕 Add 🛛 🍽 Grant Permissions	
MDM user scope  None Some All		GENERAL		ΑΡΙ	APPLICATION PERMI DELEGATED PERMIS
MDM terms of use URL I https://ds763.awmdm.com/DeviceN	Aanagement/Enrollment 🗸	Properties	>	Windows Azure Active Directory	1 0
MDM discovery URL  https://ds763.awmdm.com/DeviceS	ervices/discovery.aws 🗸	📒 Reply URLs	>		
On-premises MDM application settings		Owners	>		T I
•		API ACCESS			
		Required permissions	>		
		💡 Keys	>		
		TROUBLESHOOTING + SUPPORT			
		X Troubleshoot	>		
		New support request	>		
Click on 'Required Permis     Click on 'Windows Azure	sions' Active Directory'				
<ul> <li>Click on 'Required Permis.</li> <li>Click on 'Windows Azure /</li> </ul>	sions' Active Directory' Required permissions		×	Enable Access Windows Azure Active Directory	
<ul> <li>Click on 'Required Permis:</li> <li>Click on 'Windows Azure /</li> <li>Make sure the permissions</li> </ul>	sions' Active Directory' Required permissions + Add & Grant Permissions		×	Enable Access Windows Azure Active Directory	
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> </ul> Make sure the permissions	Sions' Active Directory' Required permissions API API Windows Asure Active Directory	APPLICATION PERMI DE	X	Enable Access Windows Azure Active Directory Save  Delete  APPLICATION PERMISSIONS  Read directory data	
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> </ul>	Sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	X	Enable Access Windows Azure Active Directory Save  Delete APPLICATION PERMISSIONS Read directory data Read and write domains	Ta REQUIRES ADMIN Ta Ves Ves
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the same as the Windows Desktop</li> </ul>	Sions' Active Directory Required permissions APL Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access Windows Azure Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains V Read and write directory data	*     REQUIRES ADMIN     *       @ Yes     @ Yes       @ Yes       @ Yes
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states</li> </ul>	Sions' Active Directory' Required permissions ARI API Windows Azure Active Directory	APPLICATION PERMI DE	X	Enable Access Windows Azure Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write directory data Read and write devices	
<ul> <li>Click on 'Required Permission's</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states.</li> </ul>	Sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LIGATED PERMIS	Enable Access Windows Azura Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write devices Read all hidden memberships	*     REQUIRES ADMIN     *       © Yes
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states.</li> </ul>	Sions' Active Directory' Required permissions Add Grant Permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access Windows Axue Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write devices Read all hidden memberships Manage apps that this app creates or owns	**     REQUIRES ADMIN     **       •     Yes
<ul> <li>Click on 'Required Permission's</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions of the application are set the same as the Windows Desktop</li> <li>Platform guide states.</li> <li>9. Change the Permissions as follows:</li> </ul>	Sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access Windows Asure Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write directory data Read and write directory data Read and write devices Read and write app creates or owns Read and write all applications	*     REQUIRES ADMIN     *       •     Yes
<ul> <li>Click on 'Required Permission's</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions of the application are set the same as the Windows Desktop</li> <li>Platform guide states.</li> <li>9. Change the Permissions as follows:         <ul> <li>Application Permissions</li> <li>Scient Pard and write directory data</li> </ul> </li> </ul>	Sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access Windows Azure Active Dilectory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write directory data Read and write directory data Read and write devices Read and write devices Read and write devices Read and write directory data Read and write directory data	<ul> <li>REQUIRES ADMIN</li> <li>Yes</li> </ul>
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states.</li> <li>9. Change the Permissions as follows:         <ul> <li>Application Permissions</li> <li>Select Read and write directory dat</li> <li>Select Read and write directory dat</li> </ul> </li> </ul>	sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERM DE 2 3	LEGATED PERMIS	Enable Access Windows Axure Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write directory data Read and write directory data Read and write devices Read and write devices Read and write devices Read and write domains Read and write all applications Read and write domains Read and write domains Read and write domains Read and write domains	*     REQUIRES ADMIN     **       •     Yes
<ul> <li>Click on 'Required Permission's</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions of the application are set the same as the Windows Desktop</li> <li>Platform guide states.</li> <li>9. Change the Permissions as follows:         <ul> <li>Application Permissions</li> <li>Select Read and write directory dat</li> <li>Select Read and write devices.</li> </ul> </li> </ul>	Active Directory'          Required permissions         + Add         • Add         • Mindows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access Windows Azura Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write directory data Read and write devices Read and write all applications Read and write all applications Read and write all applications Read and write domains PELEGATED PERMISSIONS Access the directory as the signed-in user	*     REQUIRES ADMIN     *       •     Yes       •     No
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states.</li> <li>9. Change the Permissions as follows:         <ul> <li>Application Permissions</li> <li>Select Read and write directory dat</li> <li>Select Read and write devices.</li> <li>Delegated Permissions</li> </ul> </li> </ul>	sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access   Windows Asure Active Dilectory   Save   Save   Pelte     APPLICATION PERMISSIONS   Read directory data   Read and write domains   Read and write directory data   Read and write directory data   Read and write devices   Read and write devices   Read and write domains   Read and write directory data   Read and write directory data   Read and write directory as the signed-in user   Access the directory as the signed-in user   Read directory data	*     REQUIRES ADMIN     *+       @ Yes     Yes       @ No     *+       @ Yes     Yes
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states.</li> <li>Platform guide states.</li> <li>Application Permissions</li> <li>Select Read and write directory dat</li> <li>Select Read and write devices.</li> <li>Delegated Permissions</li> <li>Select Access the directory as the si</li> </ul>	Sions' Active Directory' Required permissions API Windows Azure Active Directory a.	APPLICATION PERM DE 2 3	LEGATED PERMIS	Enable Access Windows Axue Active Directory      Save Delete      APPLICATION PERMISSIONS      Read directory data      Read and write directory data      Read and write devices      Read and write devices      Read and write domains      PELEGATED PERMISSIONS      Access the directory as the signed-in user      Read and write directory data      Read and write directory data      Read and write directory as the signed-in user      Read and write directory data	*     REQUIRES ADMIN     **       •     Yes       •     Yes
<ul> <li>Click on 'Required Permiss</li> <li>Click on 'Windows Azure A</li> <li>Make sure the permissions</li> <li>of the application are set the</li> <li>same as the Windows Desktop</li> <li>Platform guide states.</li> <li>Platform guide states.</li> <li>Change the Permissions as follows:         <ul> <li>Application Permissions</li> <li>Select Read and write directory dat</li> <li>Select Read and write devices.</li> <li>Delegated Permissions</li> <li>Select Read directory data.</li> </ul> </li> </ul>	Sions' Active Directory' Required permissions API Windows Azure Active Directory	APPLICATION PERMI DE 2 3	LEGATED PERMIS	Enable Access Windows Azura Active Directory Save Delete APPLICATION PERMISSIONS Read directory data Read and write domains Read and write directory data Read and write directory data Read and write devices Read and write directory data DELEGATED PERMISSIONS Access the directory as the signed-in user Read and write directory data Read and write directory data	*     REQUIRES ADMIN     *       •     Yes       •     No       •     Yes       •     Yes

Read all users' basic profiles

Read hidden memberships

✓ Sign in and read user profile

🗢 No

🗢 No

🥝 Yes

Save the permission changes and head back to the properties of the application. This is where you add the App ID mentioned above.

Configure	(WDW and WDW) 3 Configure 3 Settings 3 Properus	×	Settings	×	Properties 🗖 🗙
n-premises MDM application			J.		
Save 🗙 Discard 🛅	Delete				R Save X Discard
DM user scope 🛛	None Some All	$\mathbf{n}$	GENERAL		* Name <b>0</b>
DM terms of use URL 🛛 ht	tps://ds763.awmdm.com/DeviceManagement/Enrollment 🗸		Properties	>	
M discovery URL 0	tps://ds763.awmdm.com/DeviceServices/discovery.aws		🚝 Reply URLs	>	65bf6a26-e18b-4d0a-8220-91a9d1c9ff05
Dn-premises MDM applicatio	n settings		Owners	>	Application ID 0
					37a153eb-4b68-4f0e-90ed-c16c555(3b60
			API ACCESS		* App ID URI
			Required permissions	>	https://cn/b3.awmdm.com
			📍 Keys	>	Logo
			TROUBLESHOOTING + SUPPORT		
			X Troubleshoot	>	
			New support request	>	Upload new logo
					Select a file
					Home page URL
					https://cn763.awmdm.com
					Logout URL
					Terms of service URL <b>0</b>
					Privacy statement URL 🛛
					Application type
					Web app / API
					Multi-tenanted 0
					Yes No

Now we just need to update our settings within the AirWatch console to match what we have in Azure and we should be able to enroll a Windows 10 device out of the box.

Settings	AirWatch Internal / CHodge (C 🝷					
System	Azure Active Directory					
Getting Started Branding	add the AirWatch by VMware application to your AAD tenant from the Azure Marketplace.					
Enterprise Integration Enterprise Integration Services	- 1) Navigate to the AirWatch by VMwa	are application in the Azure Marketplace				
Certificate Authorities VMware Enterprise Systems Connector	Start Setup Wizard		Now we need to fill in the Azure Directory ID and the			
Directory Services Email (SMTP)	2) Follow the instructions in the Azur	e Marketplace to add the AirWatch by VMware a				
<ul> <li>VMware Tunnel</li> <li>Peer Distribution</li> </ul>	3) Configure the AirWatch by VMware	e application with the URLs below.	tenant name	C		
SMS Rull Septice Installers	MDM Enrollment URL	https://ds763.awmdm.com/	/DeviceServices/discovery.aws	Where in Add do I paste the info? Where in Add do I paste the info? Where in Add do I paste the info?		
Syslog Video CDN	MDM Terms of Use URL	https://ds763.awmdm.com/	/DeviceManagement/Enrollment			
Remote Management VMware Identity Manager Convirts	4) Enter your Azure Active Directory 1	Tenant ID. Tenant ID can be found in the URL of y	Where in Add do I paste this info?			
Help Localization Report Subscriptions Terms of Use	Directory ID*	02a5c195-1080-4c1d-bd16-	868ef34e1407	AD Properties (see below	·)	
	Tenant Name*	chodge@chproductions.on	microsoft.com			
Advanced	Immutable ID Mapping Attribute*	Home > chproductions - Properties chproductions - Properties Azure Active Directory				
Apps	Mapping Attribute Data Type*	Search (Ctrl+/) «	R Save X Discard			
		() Overview	* Name CHProductions			
		💅 Quick start	Country or region			
		MANAGE	Location			
		🔓 Users	EU Model Clause compliant datacenters			
		Groups	English	~		
		Enterprise applications	Global admin can manage Azure Subscriptions and Management Groups		Page 26	
		App registrations	Directory ID			
		Application proxy	02a5c195-1080-4c1d-bd16-868ef34e1407			
		🔓 Licenses	Technical contact chodge@vmware.com			