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

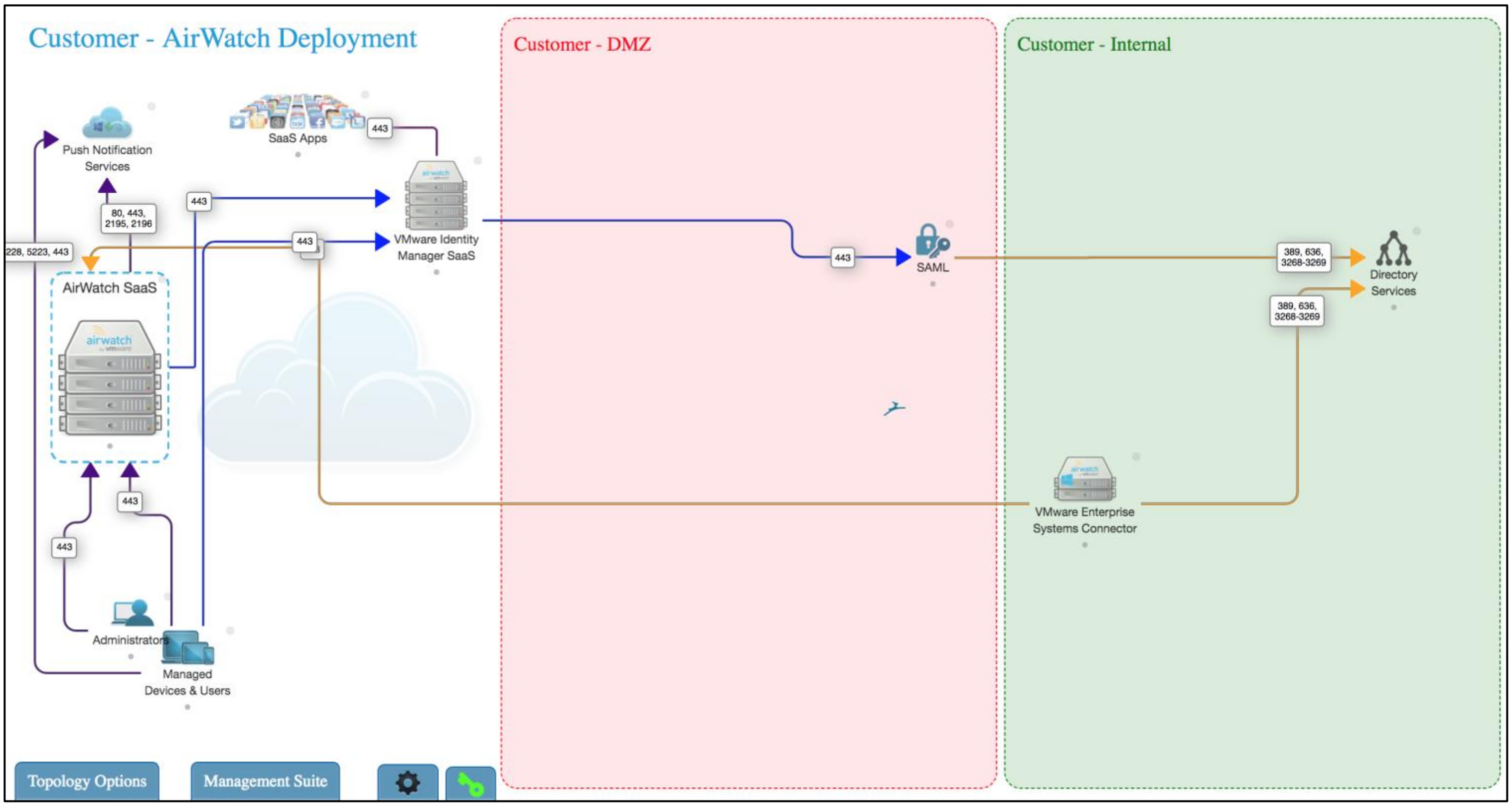
Project Overview

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

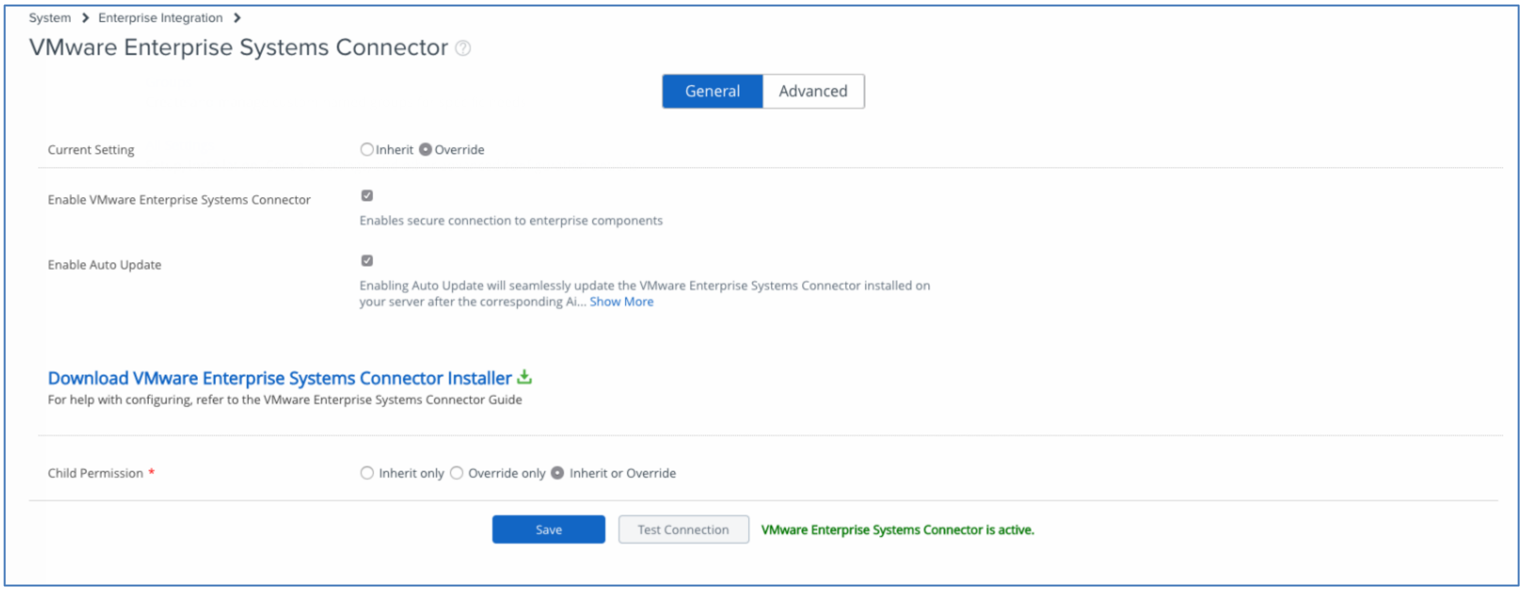
****All on-premise installations can be on the same server****

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 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

Current Setting ○ Inherit ● 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

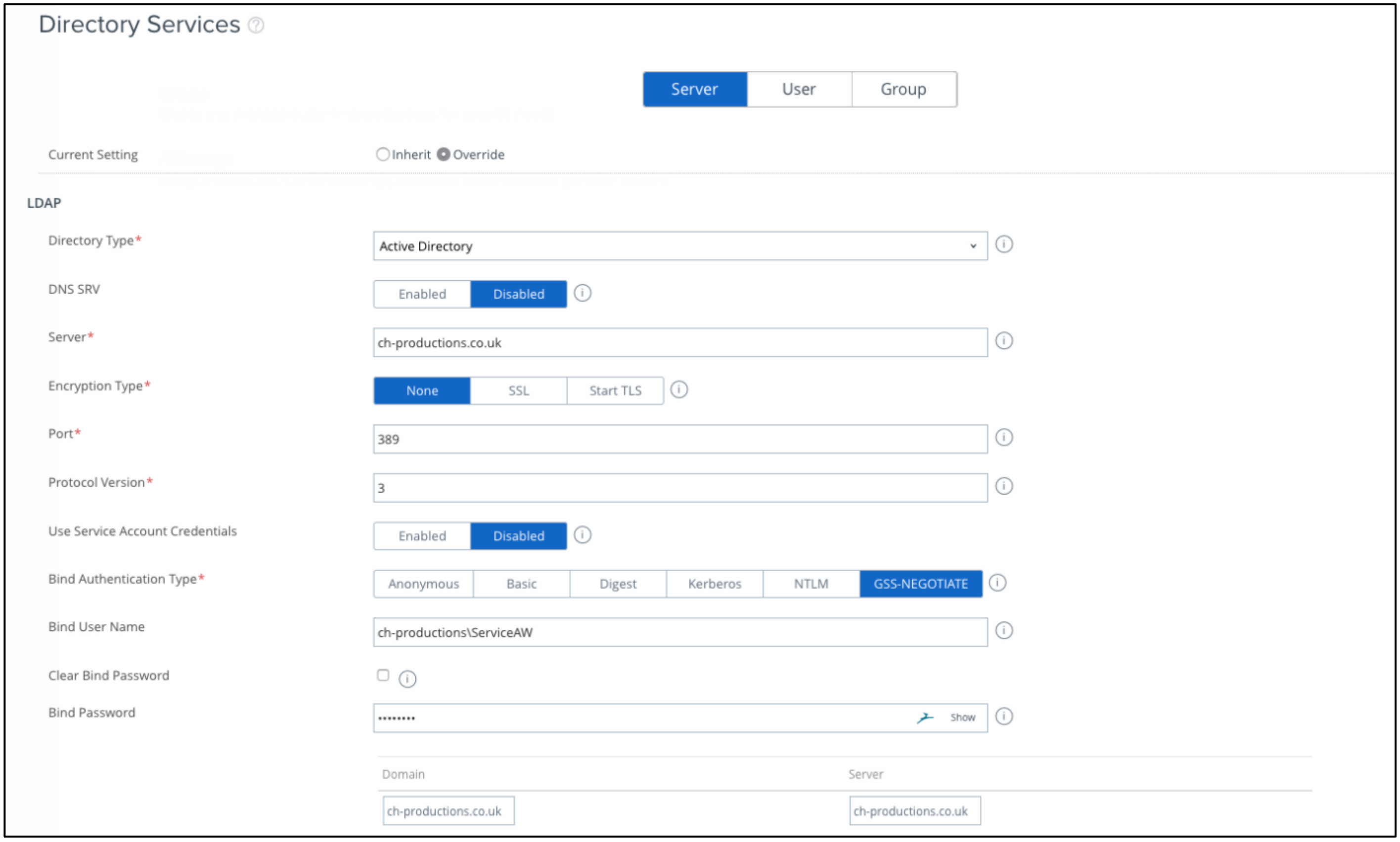
Download VMware Enterprise Systems Connector Installer
For help with configuring, refer to the VMware Enterprise Systems Connector Guide

Child Permission * ○ Inherit only ○ Override only ● Inherit or Override

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

Current Setting ○ Inherit ● Override

LDAP

Directory Type* Active Directory

DNS SRV: Enabled [✓ Disabled]

Server* ch-productions.co.uk

Encryption Type* [✓ None] SSL Start TLS

Port* 389

Protocol Version* 3

Use Service Account Credentials: Enabled [✓ Disabled]

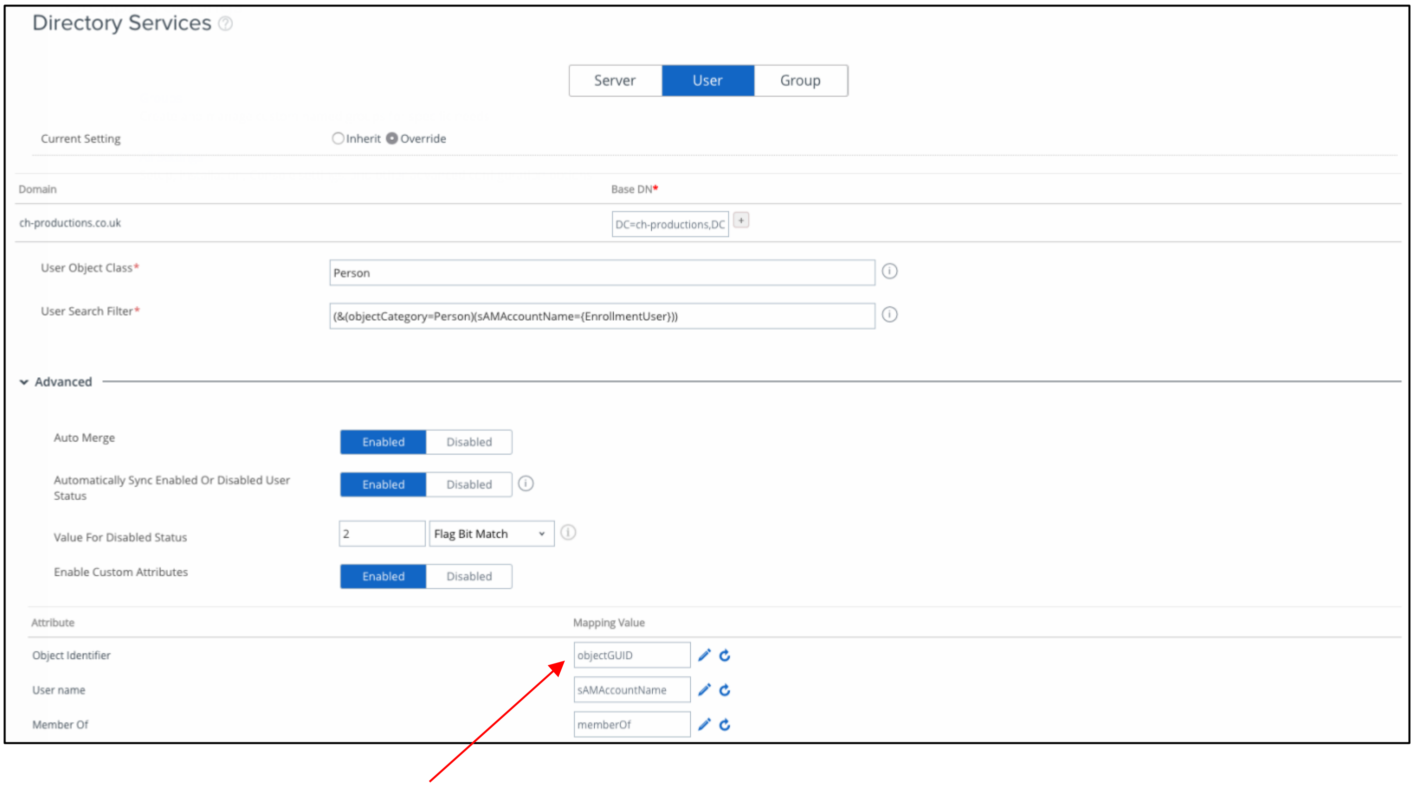
Bind Authentication Type* Anonymous Basic Digest Kerberos NTLM [✓ GSS-NEGOTIATE]

Bind User Name ch-productions\ServiceAW

Clear Bind Password □

Bind Password •••••••• Show

Domain	Server
ch-productions.co.uk	ch-productions.co.uk



Directory Services

Current Setting: ○ Inherit ● Override

Domain	Base DN*
ch-productions.co.uk	DC=ch-productions,DC

User Object Class*: Person

User Search Filter*: (&(objectCategory=Person)(sAMAccountName={EnrollmentUser}))

Advanced

Auto Merge: Enabled

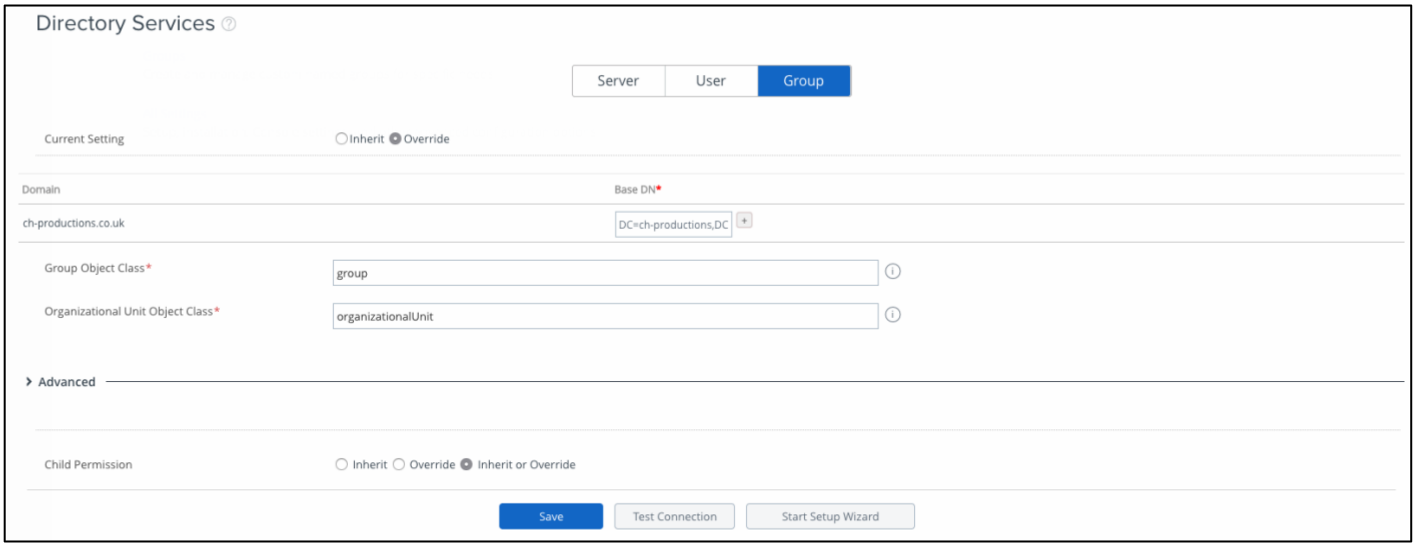
Automatically Sync Enabled Or Disabled User Status: Enabled

Value For Disabled Status: 2 Flag Bit Match

Enable Custom Attributes: Enabled

Attribute	Mapping Value
Object Identifier	objectGUID
User name	sAMAccountName
Member Of	memberOf

Make sure the 'objectGUID' is mapped



Directory Services

Current Setting: ○ Inherit ● Override

Domain	Base DN*
ch-productions.co.uk	DC=ch-productions,DC

Group Object Class*: group

Organizational Unit Object Class*: organizationalUnit

Advanced

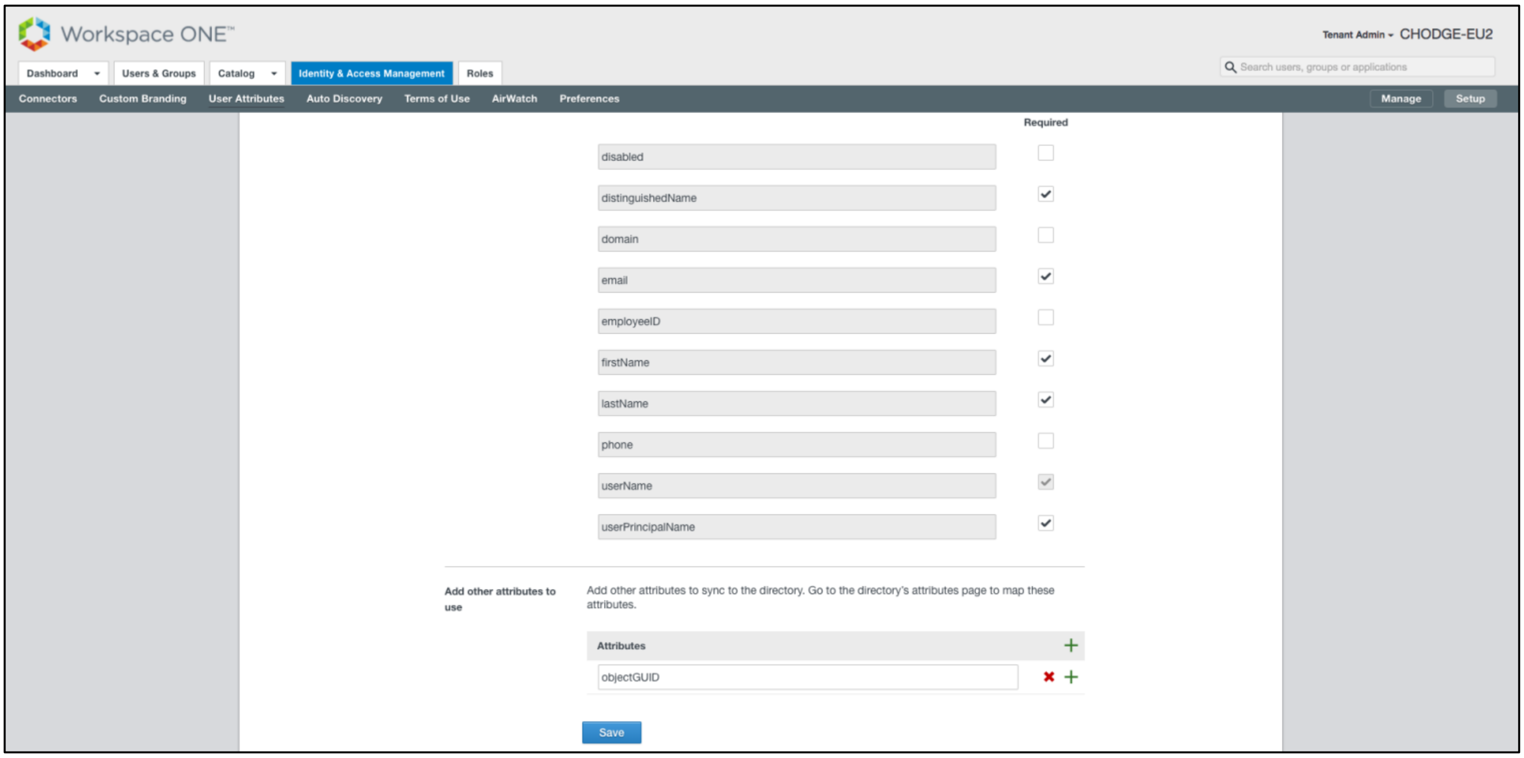
Child Permission: ○ Inherit ○ Override ● Inherit or Override

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.



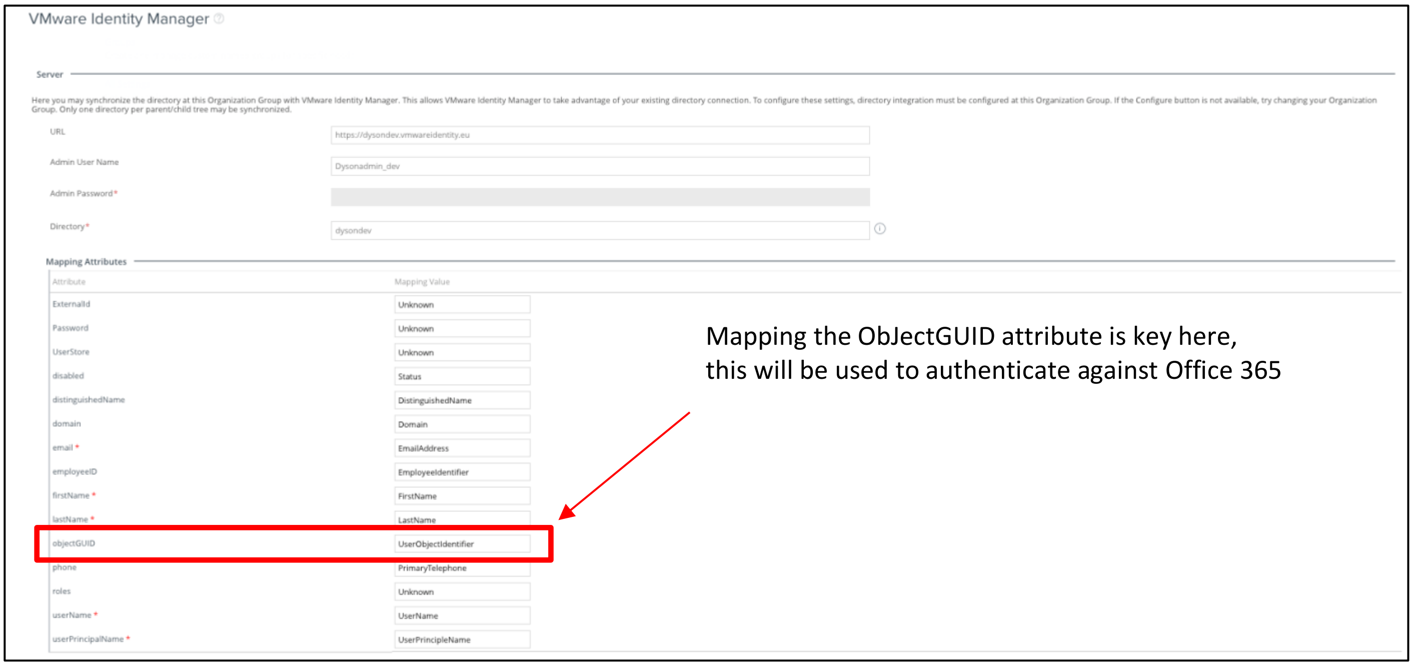
	Required
disabled	□
distinguishedName	☑
domain	□
email	☑
employeeID	□
firstName	☑
lastName	☑
phone	□
userName	☑
userPrincipalName	☑

Add other attributes to use

Add other attributes to sync to the directory. Go to the directory's attributes page to map these attributes.

Attributes
objectGUID

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



VMware Identity Manager

Server

Here you may synchronize the directory at this Organization Group with VMware Identity Manager. This allows VMware Identity Manager 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.

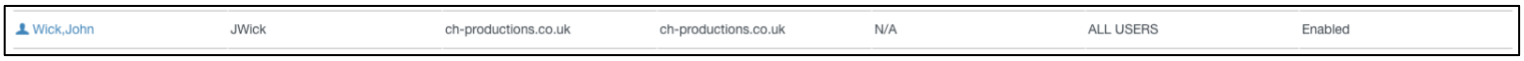
URL	https://dysondev.vmwareidentity.eu
Admin User Name	Dysonadmin_dev
Admin Password*	
Directory*	dysondev

Mapping Attributes

Attribute	Mapping Value
ExternalId	Unknown
Password	Unknown
UserStore	Unknown
disabled	Status
distinguishedName	DistinguishedName
domain	Domain
email *	EmailAddress
employeeID	EmployeeIdentifier
firstName *	FirstName
lastName *	LastName
objectGUID	UserObjectIdentifier
phone	PrimaryTelephone
roles	Unknown
userName *	UserName
userPrincipalName *	UserPrincipleName

Mapping the ObJectGUID attribute is key here,
this will be used to authenticate against Office 365

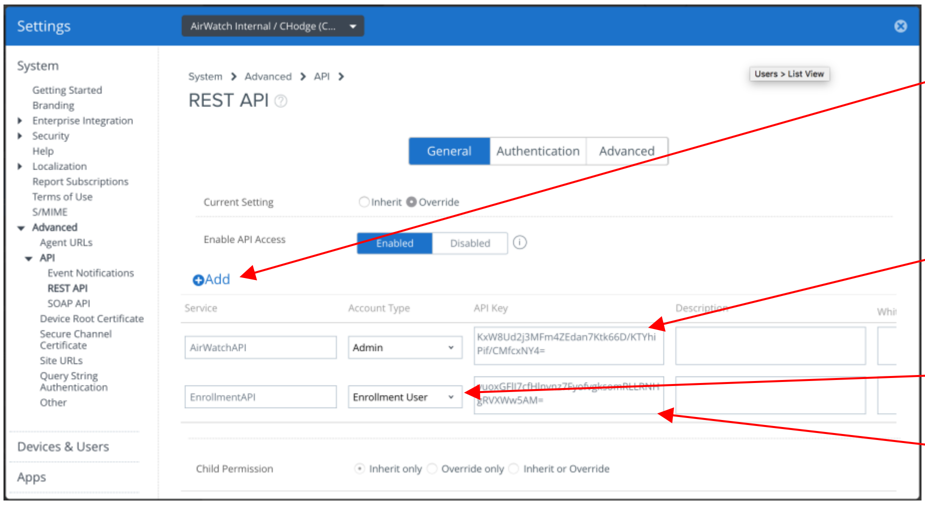
6 - Confirm Users are within vIDM



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

Enable AirWatch and VMware Identity Manager Integration

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



REST API

Current Setting: ○ Inherit ● Override

Enable API Access: Enabled

Service	Account Type	API Key	Description
AirWatchAPI	Admin	KxW8Ud2j3MFm4ZEdan7Ktk66D/KTYhiPif/CMfcxNY4=	
EnrollmentAPI	Enrollment User	uoxGFlI7cfHlnvnz7FyofvgksomRLLRNHgRVXWw5AM=	

Child Permission: ● Inherit only ○ Override only ○ Inherit or Override

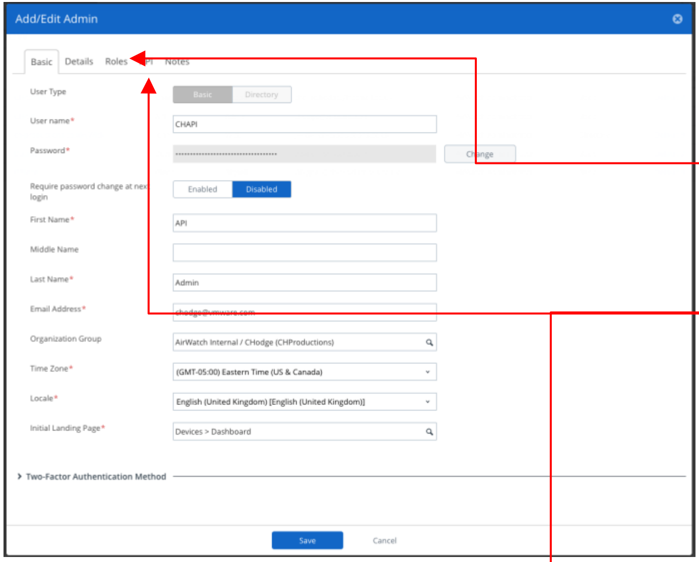
Click Add and create an API key. Set the Account type to Admin.

Copy the API key generated.

Click Add and create an API key names Identity Manager User. Set the account Type to Enrollment User.

Copy the API key.

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



User Type: Basic

User name*: CHAPI

Password*: ••••••••••••••••••••••••••••••••••

Require password change at next login: Disabled

First Name*: API

Middle Name:

Last Name*: Admin

Email Address*: chodge@vmware.com

Organization Group: AirWatch Internal / CHodge (CHProductions)

Time Zone*: (GMT-05:00) Eastern Time (US & Canada)

Locale*: English (United Kingdom) [English (United Kingdom)]

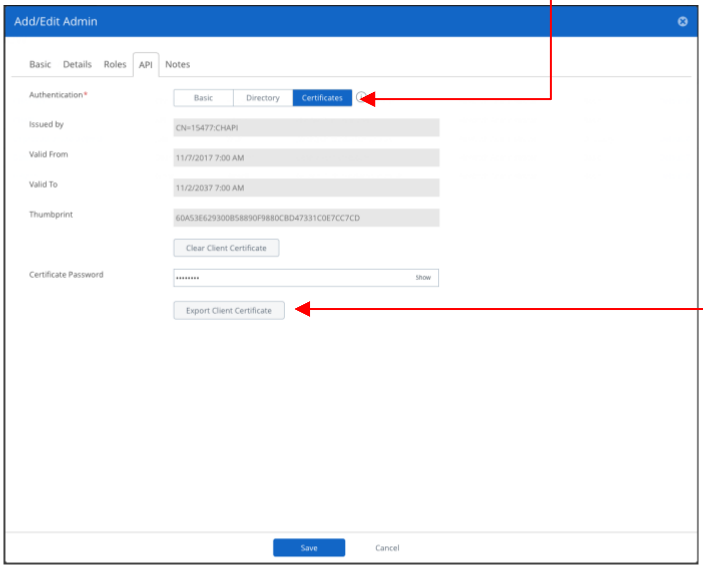
Initial Landing Page*: Devices > Dashboard

Within the AirWatch console, navigate to Accounts->Administrators and hit add.

Create your Admin account and assign it a role that has API 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 and export the certificate that you just created.



Authentication*: Certificates

Issued by: CN=15477:CHAPI

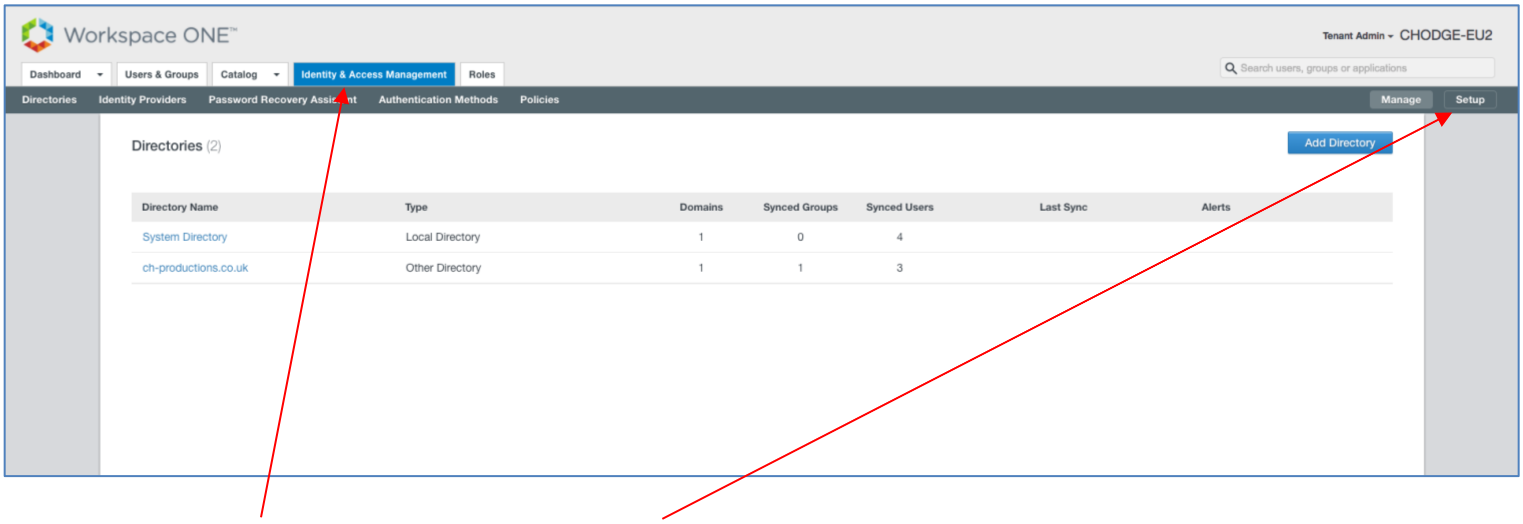
Valid From: 11/7/2017 7:00 AM

Valid To: 11/2/2037 7:00 AM

Thumbprint: 60A53E629300B58890F9880CBD47331C0E7CC7CD

Certificate Password: •••••••••

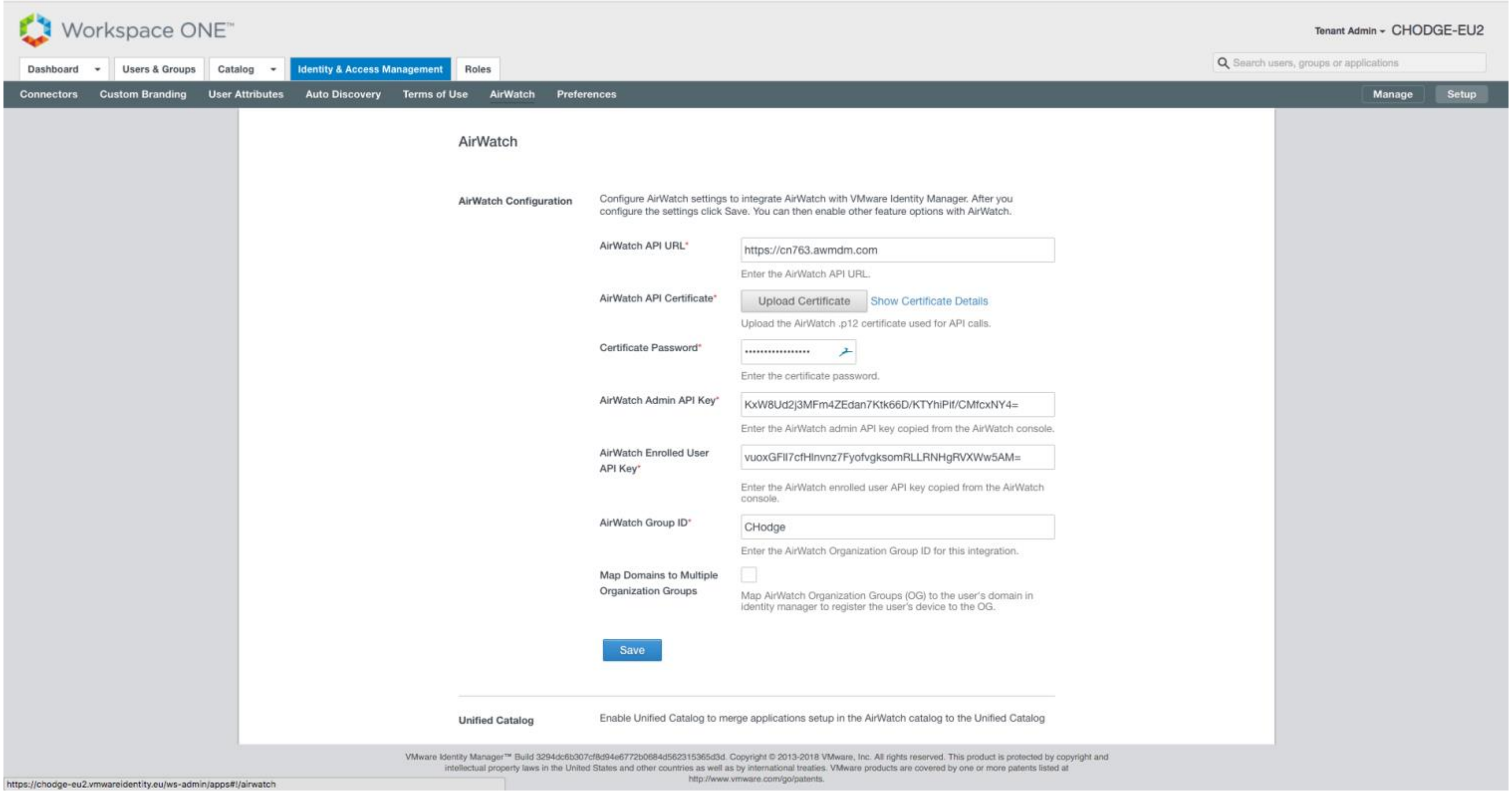
Head back over to the vIDM console and import the AirWatch certificate and copy the Admin/Enrolled user API keys:



Directories (2)

Directory Name	Type	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’



AirWatch

AirWatch Configuration Configure AirWatch settings to integrate AirWatch with VMware Identity Manager. After you configure the settings click 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
Upload the AirWatch .p12 certificate used for API calls.

Certificate Password*: ••••••••••••••••••
Enter the certificate password.

AirWatch Admin API Key*: KxW8Ud2j3MFm4ZEdan7Ktk66D/KTYhiPif/CMfcxNY4=
Enter the AirWatch admin API key copied from the AirWatch console.

AirWatch Enrolled User API Key*: vuoxGFlI7cfHlnvnz7FyofvgksomRLLRNHgRVXWw5AM=
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 □
Map AirWatch Organization Groups (OG) to the user's domain in identity manager to register the user's device to the OG.

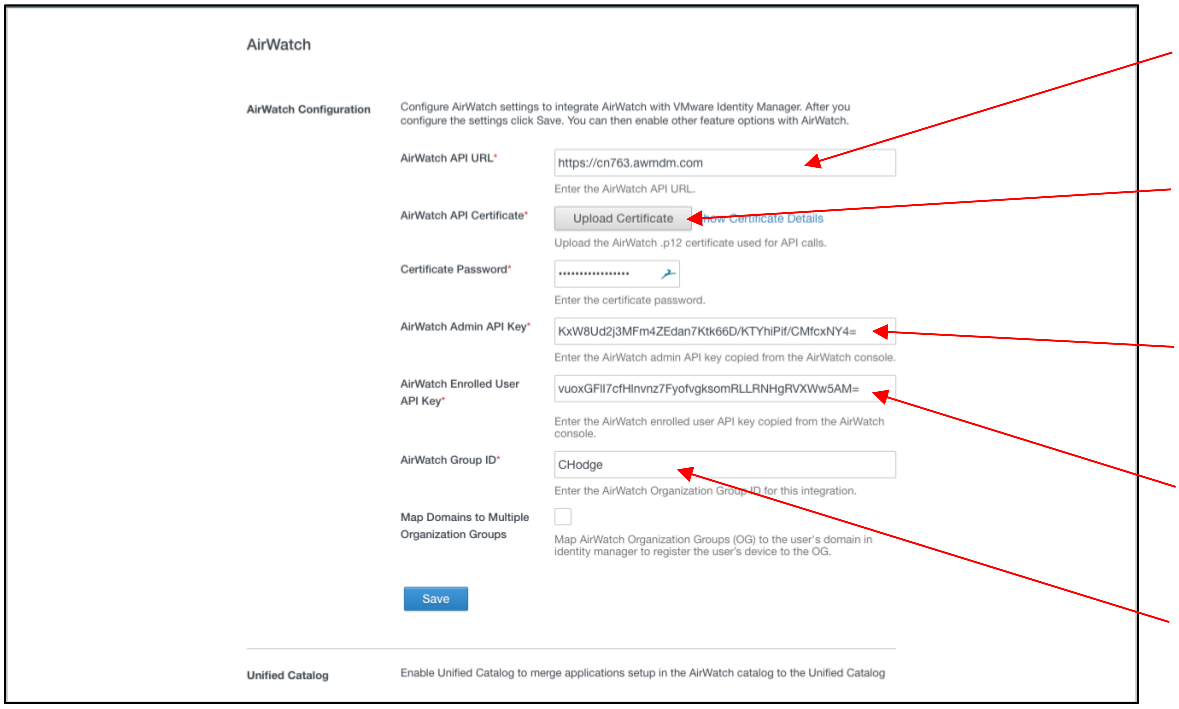
Save

Unified Catalog Enable Unified Catalog to merge applications setup in the AirWatch catalog to the Unified Catalog

VMware Identity Manager™ Build 3294dc6b307cf8d94e6772b0684d562315365d3d. Copyright © 2013-2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

https://chodge-eu2.vmwareidentity.eu/ws-admin/apps#!/airwatch

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



AirWatch

AirWatch Configuration

Configure AirWatch settings to integrate AirWatch with VMware Identity Manager. After you configure the settings click 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
Upload the AirWatch .p12 certificate used for API calls.

Certificate Password*: ••••••••••••••••••
Enter the certificate password.

AirWatch Admin API Key*: KxW8Ud2j3MFm4ZEdan7Ktk66D/KTYhiPif/CMfcxNY4=
Enter the AirWatch admin API key copied from the AirWatch console.

AirWatch Enrolled User API Key*: vuoxGFIl7cfHlnvnz7FyofvgksomRLLRNHgRVXWw5AM=
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 □
Map AirWatch Organization Groups (OG) to the user's domain in identity manager to register the user's device to the OG.

Unified Catalog

Enable Unified Catalog to merge applications setup in the AirWatch catalog to the Unified Catalog

Add the URL of your AirWatch environment.

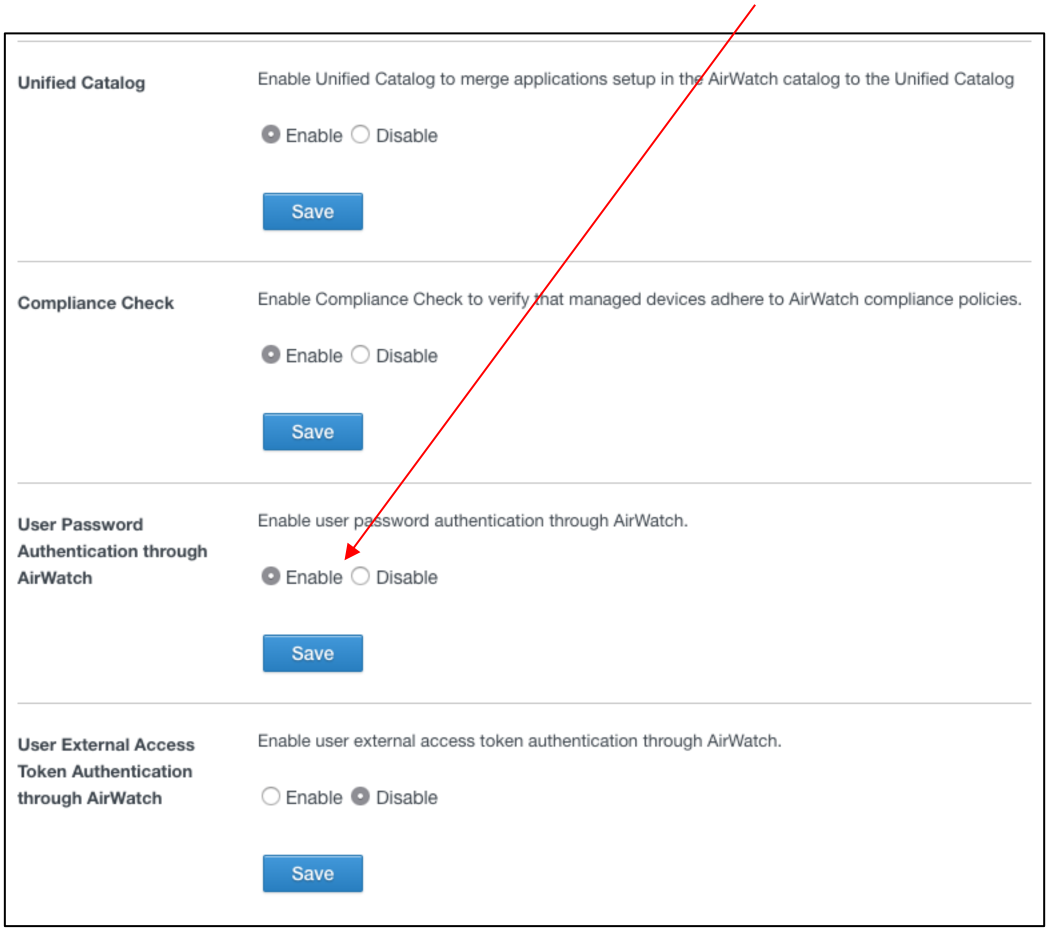
Upload the certificate you exported from AirWatch on page 7.

Copy the Admin API key created on page 7.

Copy the Enrolled user API key created on page 7.

Add the GroupID of your AirWatch envionrment.

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

● Enable ○ Disable

Compliance Check

Enable Compliance Check to verify that managed devices adhere to AirWatch compliance policies.

● Enable ○ Disable

User Password Authentication through AirWatch

Enable user password authentication through AirWatch.

● Enable ○ Disable

User External Access Token Authentication through AirWatch

Enable user external access token authentication through AirWatch.

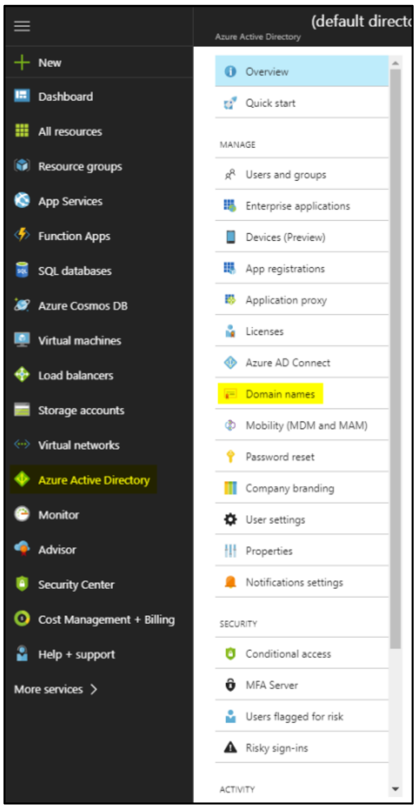
○ Enable ● Disable

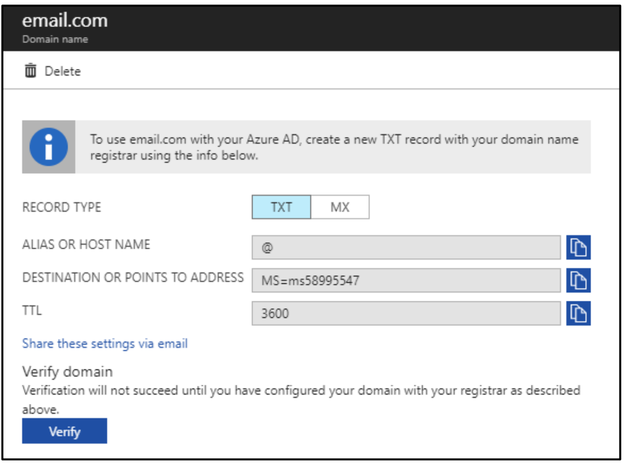
You will then need to update the Authentication Methods into vIDM to enable ‘Password (AirWatch Connector)’ and assign that authentication method to your domain.

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.





To use email.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE: TXT / MX

ALIAS OR HOST NAME: @

DESTINATION OR POINTS TO ADDRESS: MS=ms58995547

TTL: 3600

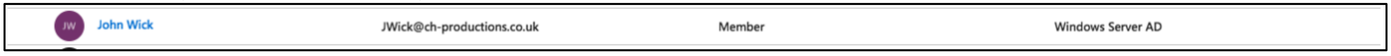
Share these settings via email

Verify domain

Verification will not succeed until you have configured your domain with your registrar as described above.

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

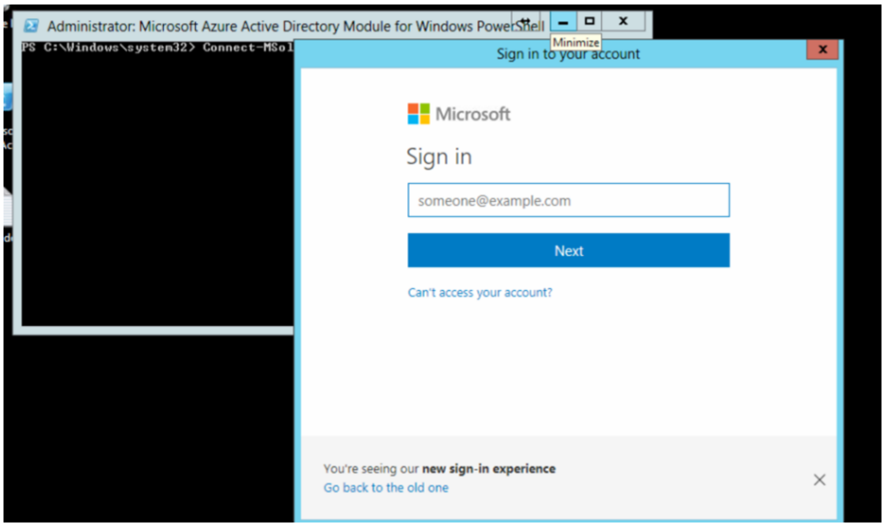
This will then sync all users in the specified AD OU into Azure:



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

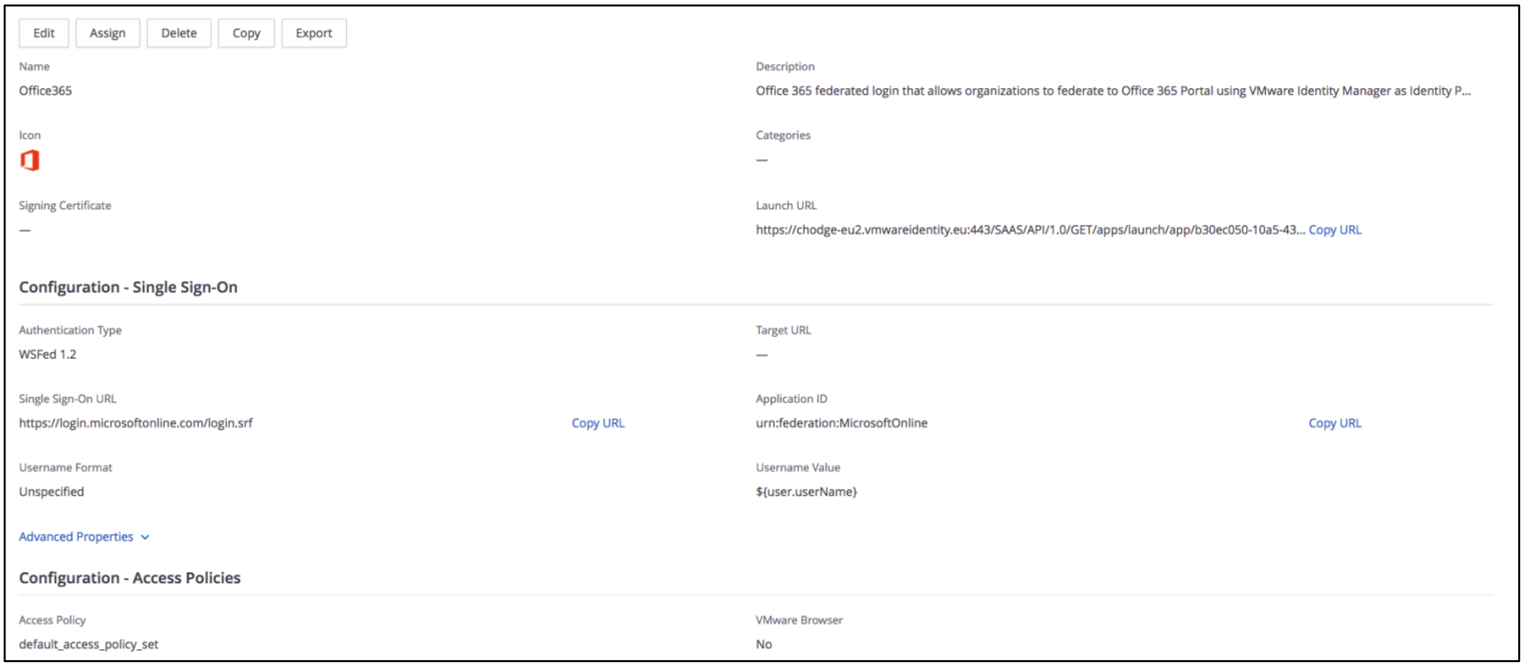
8 - Install Azure Active Directory Module for Powershell on On-Premise Server

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


Administrator: Microsoft Azure Active Directory Module for Windows PowerShell
Minimize
Sign in to your account
Microsoft
Sign in
someone@example.com
Next
Can't access your account?
You're seeing our **new sign-in experience**
Go back to the old one

```
PS C:\Windows\system32> Connect-MSol
```

9 - Configure Office 365 application within vIDM



Name
Office365

Description
Office 365 federated login that allows organizations to federate to Office 365 Portal using VMware Identity Manager as Identity P...

Icon

Categories
—

Signing Certificate
—

Launch URL
https://chodge-eu2.vmwareidentity.eu:443/SAAS/API/1.0/GET/apps/launch/app/b30ec050-10a5-43... Copy URL

Configuration - Single Sign-On

Authentication Type
WSFed 1.2

Target URL
—

Single Sign-On URL
https://login.microsoftonline.com/login.srf Copy URL

Application ID
urn:federation:MicrosoftOnline Copy URL

Username Format
Unspecified

Username Value
${user.userName}

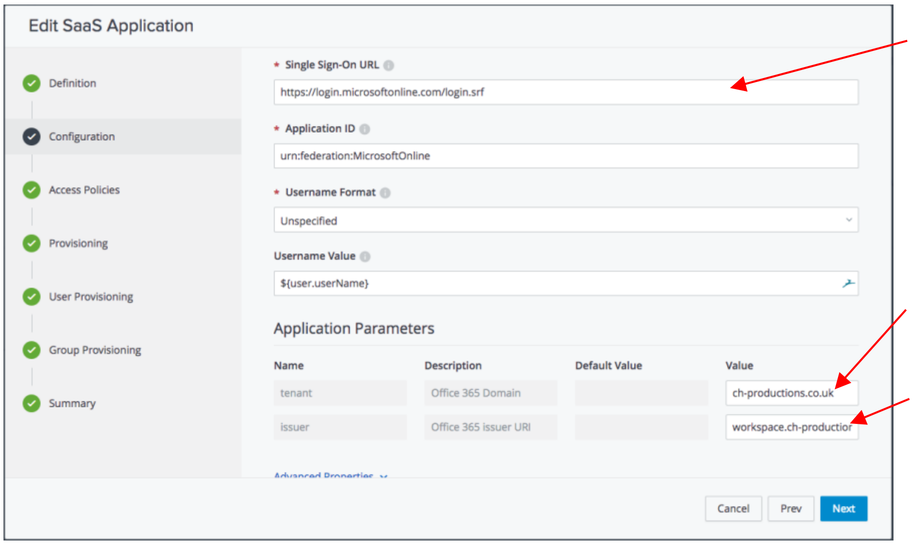
Advanced Properties

Configuration - Access Policies

Access Policy
default_access_policy_set

VMware Browser
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.



* Single Sign-On URL
https://login.microsoftonline.com/login.srf

* Application ID
urn:federation:MicrosoftOnline

* Username Format
Unspecified

Username Value
${user.userName}

Application Parameters

Name	Description	Default Value	Value
tenant	Office 365 Domain		ch-productions.co.uk
issuer	Office 365 issuer URI		workspace.ch-productior

Advanced Properties

Single Sign- On URL: Office Login URL (This is filled in by default)

Tenant: Your registered Office365 Domain

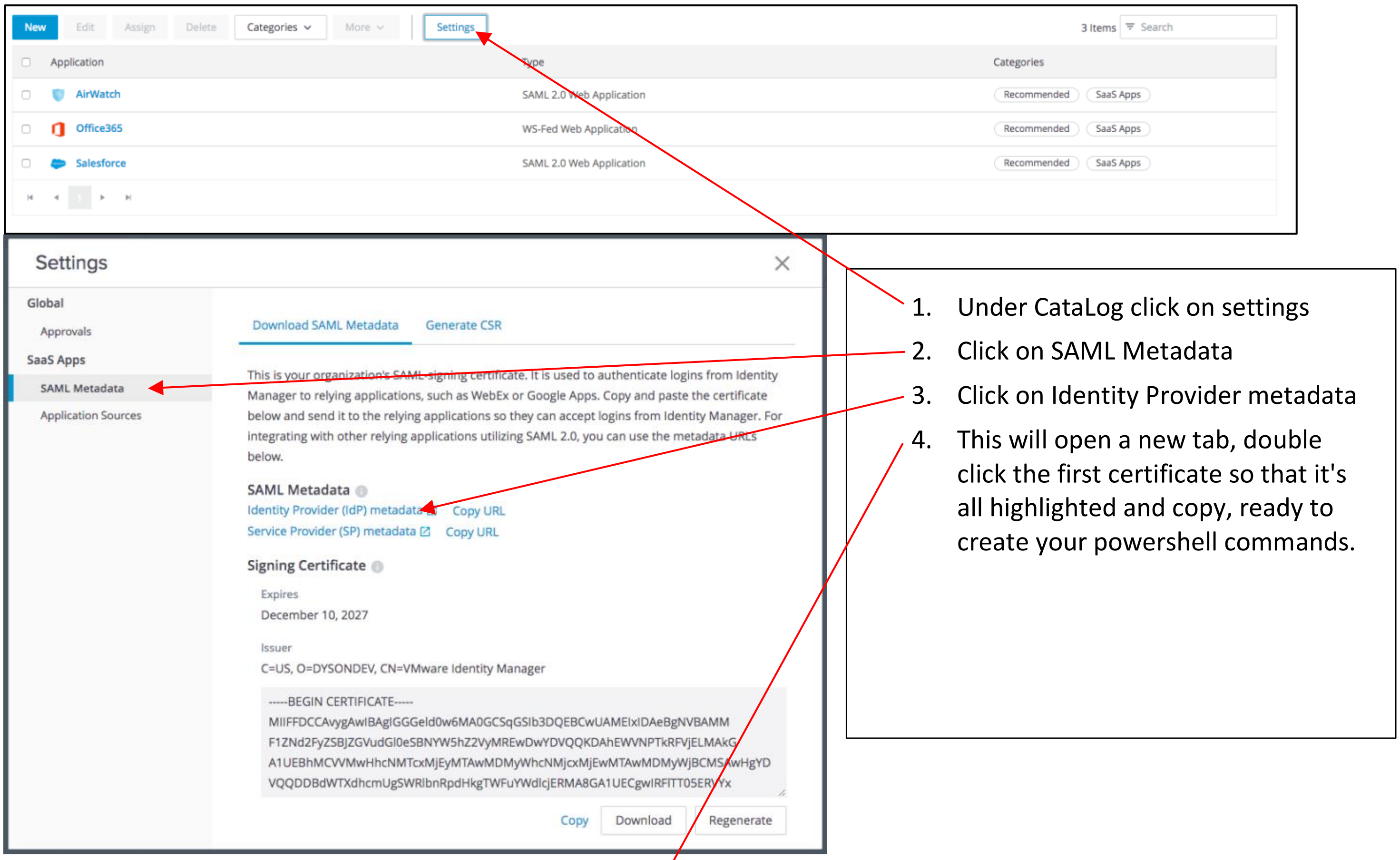
Issuer = unique identifier. Can be anything if not used by someone else in O365.

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).

chproductions.onmicrosoft.com ✓ Available

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



☐	Application	Type	Categories
☐	AirWatch	SAML 2.0 Web Application	Recommended SaaS Apps
☐	Office365	WS-Fed Web Application	Recommended SaaS Apps
☐	Salesforce	SAML 2.0 Web Application	Recommended SaaS Apps

Settings

This is your organization's SAML-signing certificate. It is used to authenticate logins from Identity Manager to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Identity Manager. For integrating with other relying applications utilizing SAML 2.0, you can use the metadata URLs below.

SAML Metadata

Identity Provider (IdP) metadata Copy URL

Service Provider (SP) metadata Copy URL

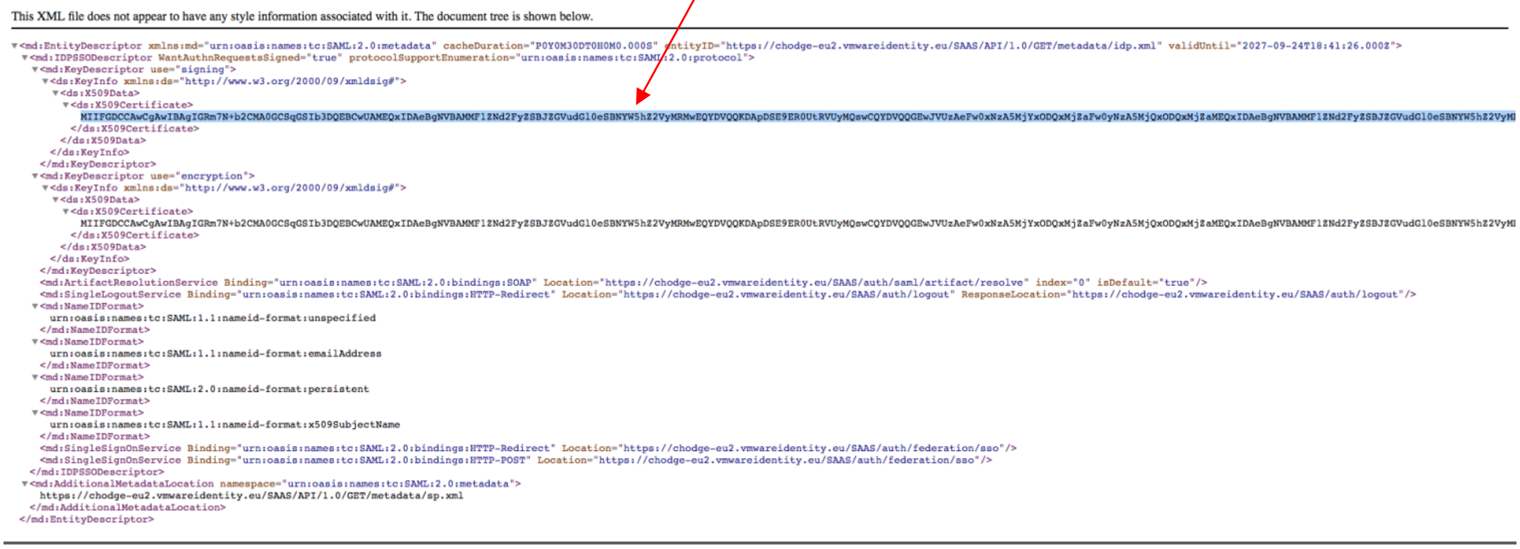
Signing Certificate

Expires
December 10, 2027

Issuer
C=US, O=DYSONDEV, CN=VMware Identity Manager

```
-----BEGIN CERTIFICATE-----
MIIFFDCCAvygAwIBAgIGGeld0w6MA0GCSqGSIb3DQEBCwUAMEIxIDAeBgNVBAMM
F1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMREwDwYDVQQKDAhEWVNPTkRFVjELMAkG
A1UEBhMCVVMwHhcNMTcxMjEyMTAwMDMyWhcNMjcxMjEwMTAwMDMyWjBCMSAwHgYD
VQQDDBdWTXdhcmUgSWRlbnRpdHkgTWFuYWdlcjERMA8GA1UECgwIRFlTT05ERVYx
```

1. Under CataLog click on settings
2. Click on SAML Metadata
3. Click on Identity Provider metadata
4. This will open a new tab, double click the first certificate so that it's all highlighted and copy, ready to create your powershell commands.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" cacheDuration="P0Y0M30DT0H0M0.000S" entityID="https://chodge-eu2.vmwareidentity.eu/SAAS/API/1.0/GET/metadata/idp.xml" validUntil="2027-09-24T18:41:26.000Z">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
          ▼<ds:X509Certificate>
              MIIFGDCCAwCgAwIBAgIGRm7N+b2CMA0GCSqGSIb3DQEBCwUAMEQxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMRMwEQYDVQQKDApDSE9ER0UtRVUyMQswCQYDVQQGEwJVUzAeFw0xNzA5MjYxODQxMjZaFw0yNzA5MjQxODQxMjZaMEQxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyM
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
    ▼<md:KeyDescriptor use="encryption">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
          ▼<ds:X509Certificate>
              MIIFGDCCAwCgAwIBAgIGRm7N+b2CMA0GCSqGSIb3DQEBCwUAMEQxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMRMwEQYDVQQKDApDSE9ER0UtRVUyMQswCQYDVQQGEwJVUzAeFw0xNzA5MjYxODQxMjZaFw0yNzA5MjQxODQxMjZaMEQxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyM
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/saml/artifact/resolve" index="0" isDefault="true"/>
      <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/logout" ResponseLocation="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/logout"/>
    ▼<md:NameIDFormat>
        urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
      </md:NameIDFormat>
    ▼<md:NameIDFormat>
        urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
      </md:NameIDFormat>
    ▼<md:NameIDFormat>
        urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
      </md:NameIDFormat>
    ▼<md:NameIDFormat>
        urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName
      </md:NameIDFormat>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/federation/sso"/>
      <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://chodge-eu2.vmwareidentity.eu/SAAS/auth/federation/sso"/>
    </md:IDPSSODescriptor>
  ▼<md:AdditionalMetadataLocation namespace="urn:oasis:names:tc:SAML:2.0:metadata">
      https://chodge-eu2.vmwareidentity.eu/SAAS/API/1.0/GET/metadata/sp.xml
    </md:AdditionalMetadataLocation>
</md:EntityDescriptor>
```

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
-FederationBrandName	Arbitrary_Name	This is an Alias – MyIdentity, or Company_Name will suffice.
-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:

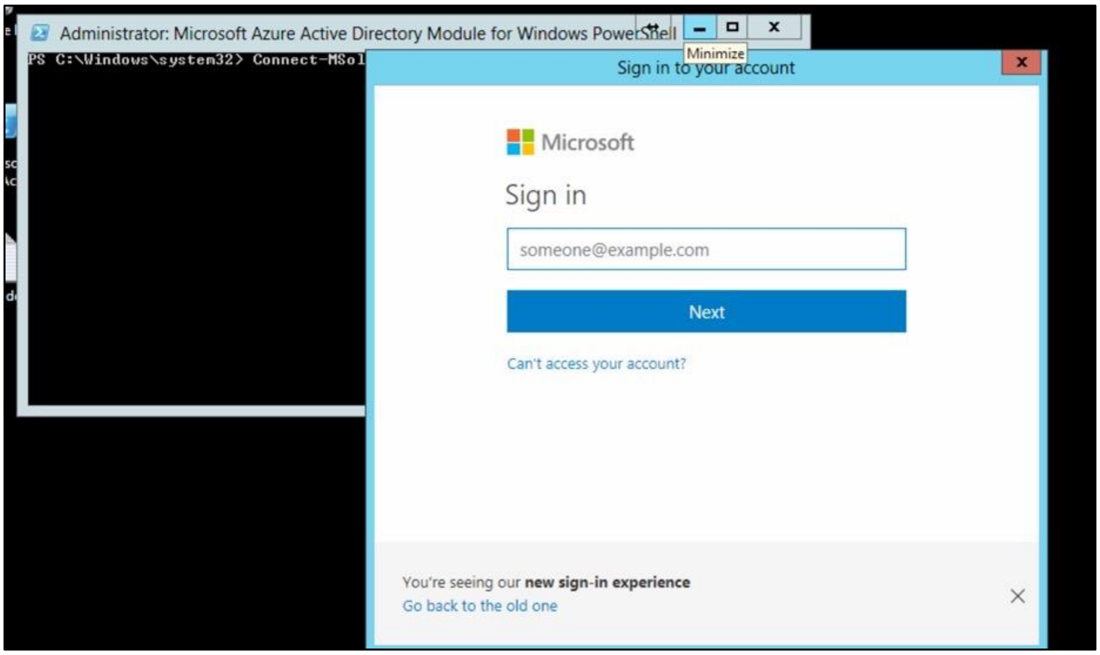
Script 1:

```
Set-MsolDomainAuthentication -DomainName < O365 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 "https://login.microsoftonline.com/logout.srf"
```

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



Administrator: Microsoft Azure Active Directory Module for Windows PowerShell

```
PS C:\Windows\system32> Connect-MSol
```

Sign in to your account

Microsoft

Sign in

someone@example.com

You're seeing our **new sign-in experience**

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.ch-productions -PassiveLogOnUri "https://chodge-eu2.vmwareidentity.eu/SAAS/API/1.0/POST/sso" -ActiveLogOnUri "https://chodge-eu2.vmwareidentity.eu/SAAS/auth/wsfed/activelogon" -LogOffUri "https://login.microsoftonline.com/logout.srf"

CH-productions Script 2 - 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

CH-productions Script 3 - 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 https://chodge-eu2.vmwareidentity.eu/SAAS/auth/wsfed/services/mex -SigningCertificate

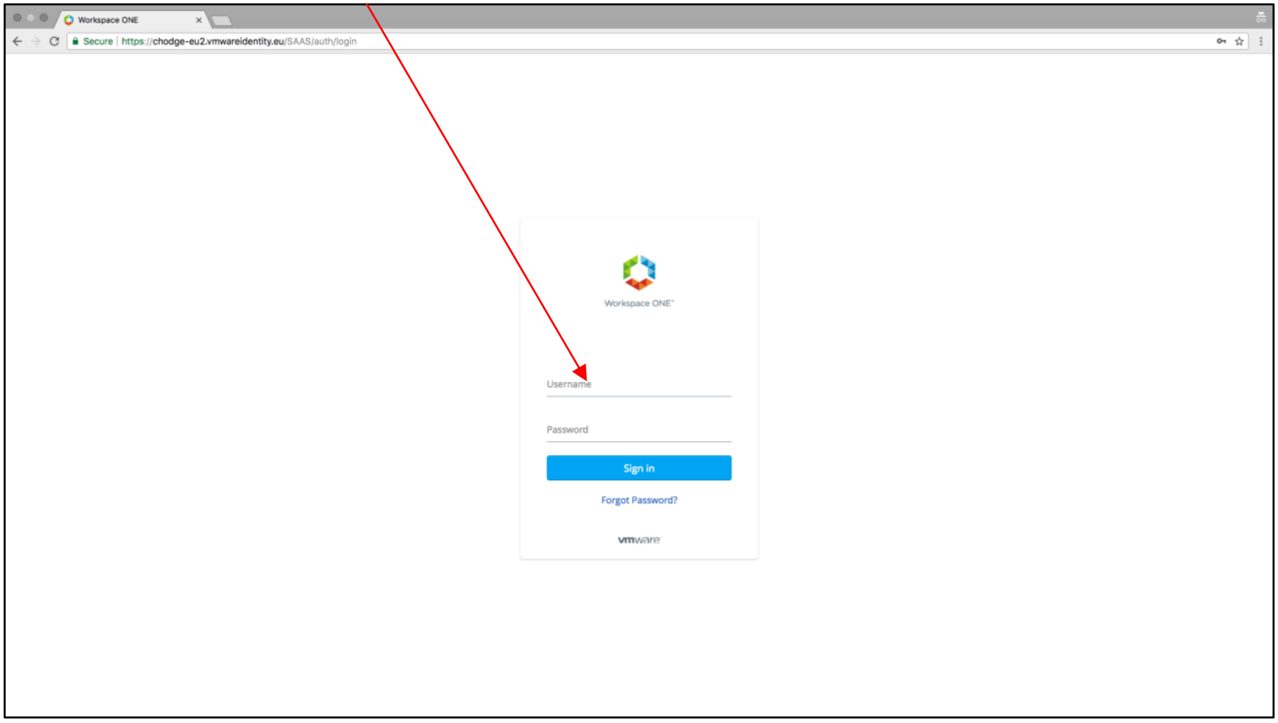
MIIFFDCCAvygAwIBAgIGGGeld0w6MA0GCSqGSIb3DQEBCwUAMEIxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMREwDwYDV
QQKDAhEWVNPTkRFVjELMAkGA1UEBhMCVVMwHhcNMTcxMjEyMTAwMDMyWhcNMjcxMjEwMTAwMDMyWjBCMSAwHgYDVQQDDBdW
TXdhcmUgSWRlbnRpdHkgTWFuYWdlcjERMA8GA1UECgwIRFlTT05ERVYxCzAJBgNVBAYTAlVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCg
KCAgEApQFJT7I0cGi+Hxb9tfVIyXPlHwnGqpoQrfWyi07k9+vlJK86kdHDVrfl3Nv1T5Vbjgs73p/sqEvmJ9171GayZbaikSBrjAJC2/gsSn9ScIPAikqBm
SGRWUYUEZ3NVQ2kV54i1P3EoS45ypt54nKoS2jz82Gz5xPwun2FdnqAAh8M2+qJ+PhOWqF0rtAMxWB6JoDqGJyRz39gAeoRbUXC/4E6gBRjcL
uiUftLPJxz6VX+bAQTDtAXYQ7WdN/BQV4jjF6iGfggnw9UI8UsTDpx4/DhU8zdfpNQ9aCsjzjSKBXElKuIeNsCX0fLpgiL2WJ2h6CGV/WxhQ5Pq7nh
TyIoxglD46E3+tRRsRAJlmRMhOkUzck/XdfVDOFZWy+7eL5r85YeVAsR1BCLzHFaZ+RKB0MIv/20MSMbWOgMySInhS/WTbBioJ7gwNgabAT8uS
aLIMVKdfyjQtsjHqIx+6qrH/D98ekRWwMMgdX4ycf5jgCpf3HRFjuAhKDWnfJl31PVDHeHj41bWmXCwXRa4cyrPzfGoFxo0CkVbUIs5za9pyovtaSI
rBfludNtDDiPwQZNiUQF3B5tGCA2tFmVqeIem9ItnX06CuDKra7rIDMwThDuINB0hKDQCn6yV3+bePQCxI+S3t9QhAhGPlnM48rV7xxJaJuXk7oa
nzjY27JwdpMCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAUu4yf/4/3e7JGK/cAh2xFiojx1jeQyTBZhlDt67Ai
culpwpdjDmJNF4Ga6nK1kGmXHEzKqYT/Ej5sphCzAU0NfRVRqEhY/ZrvbJirK8EcrAzE3yL/VQ/gl0KDf9q/0MojSkZuyABBiDe0kCzuTh3uz1W1qxJ
Seh187Ts1IiF8en89uQvvJpxJ+9nfBTS3aokLirZnsJpvT2Ps1CaryOa5RLMa/3SCTpdkdmTQ2Qrr8lwjRnXZoBeMvwdlmNE8QuOoKFa2Xp2hsnCLU
G6gLc1qciaE44XjRNiT4VIH/dUVX0OOO/XWHtcDFmiNYJzWbFngZf1enxmaiwOjx3D1jBas2iS/MLAynqniyJnxlI7JeLNeCe/BHfHm/9N77co7JwvN
1MF3jDku5d7cFWr9DRZ7cL6s+C5Y/TZHWeTz6099AXmtzER3TixxtePA5yxjxJiL6BHZb7qxBjZJw78mPcIfMZ/+vU6ggwXw/Onk4lnVH75XhAwto
KnEEixc/1eSyBmBjI/p/qVW44wE8GPXgdc/m9tt5ld5uc4Nlb7MlXnSTcMt4nQsJDY6gVWa4q2i13VqEQZPeidpZO4/U8IXVeIebMCbJd34L/eFQ/2
zS3Fwav7s3Opvp9eEdadlcR2J+i3JVo+KHSTPRzj9c8U6cGSDH2W/Oxhhm4b7oGJTYf/86c=

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

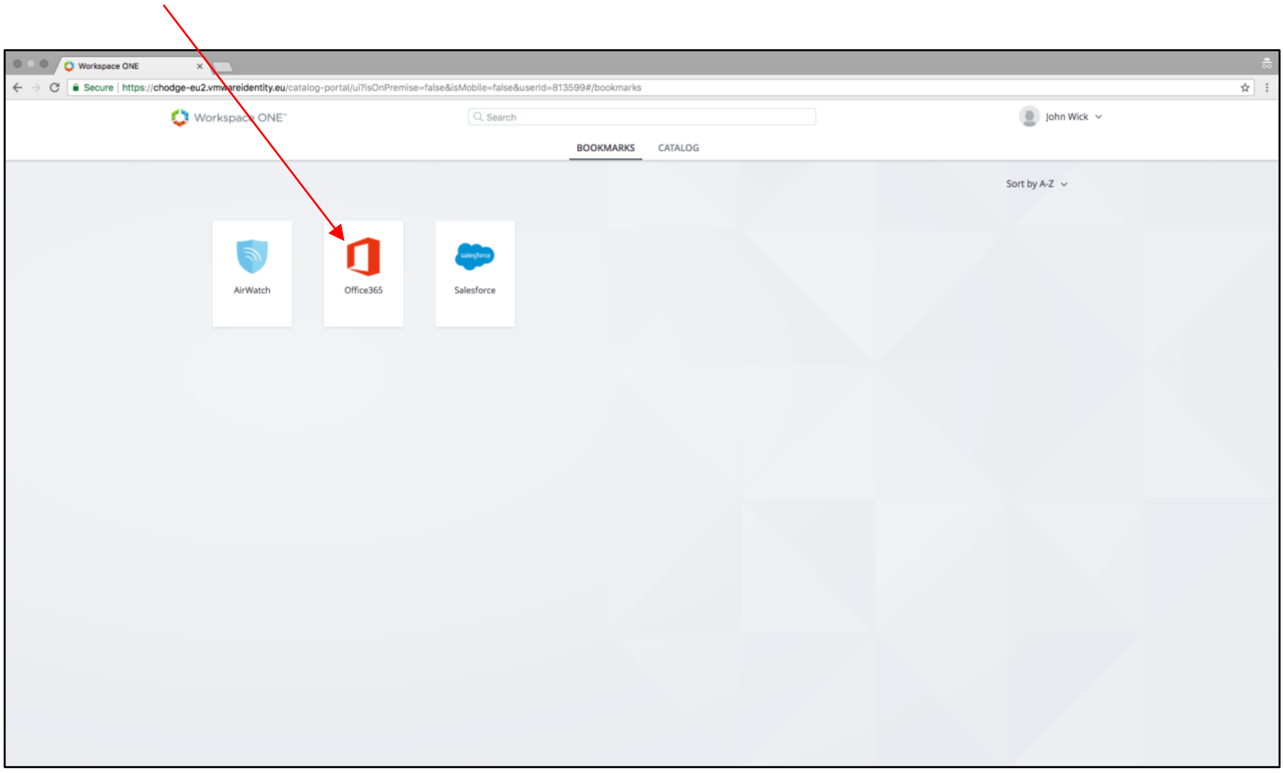
11 - Test The Federation

Test 1 - vIDM workflow:

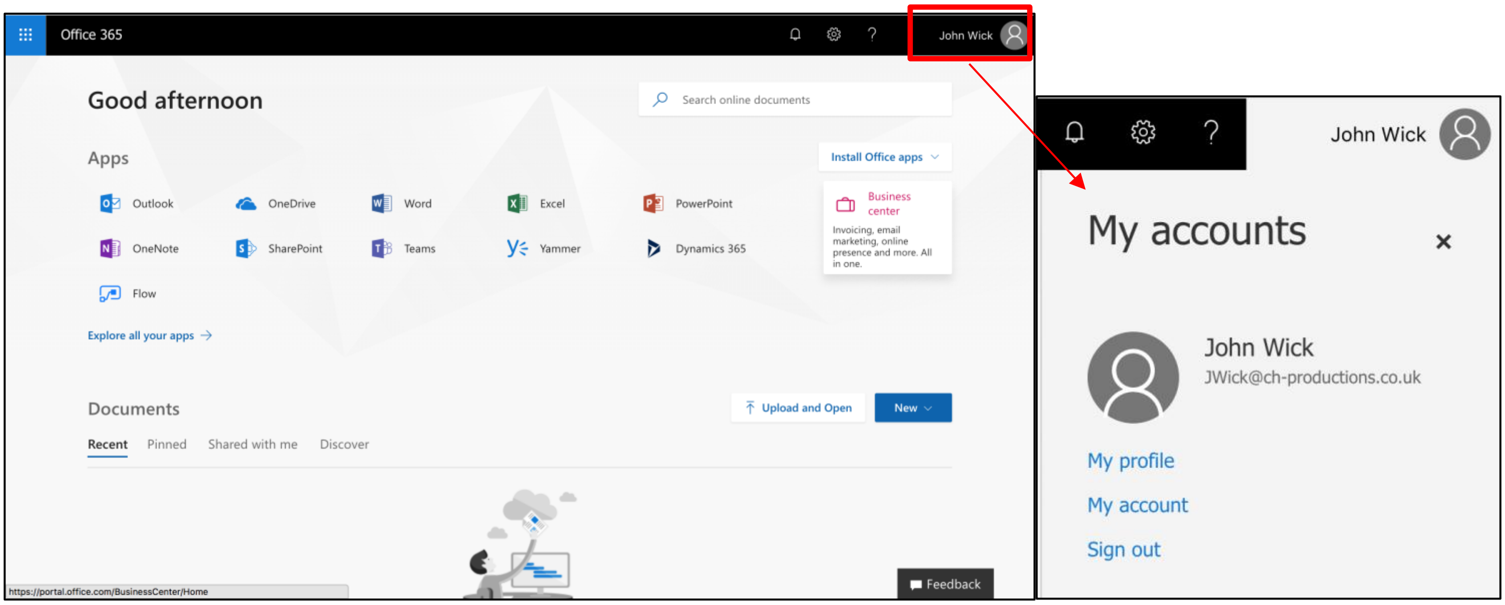
- Navigate to Workspace One URL - https://chodge-eu2.vmwareidentity.eu
- Login with domain credentials (Test user - JWick)



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

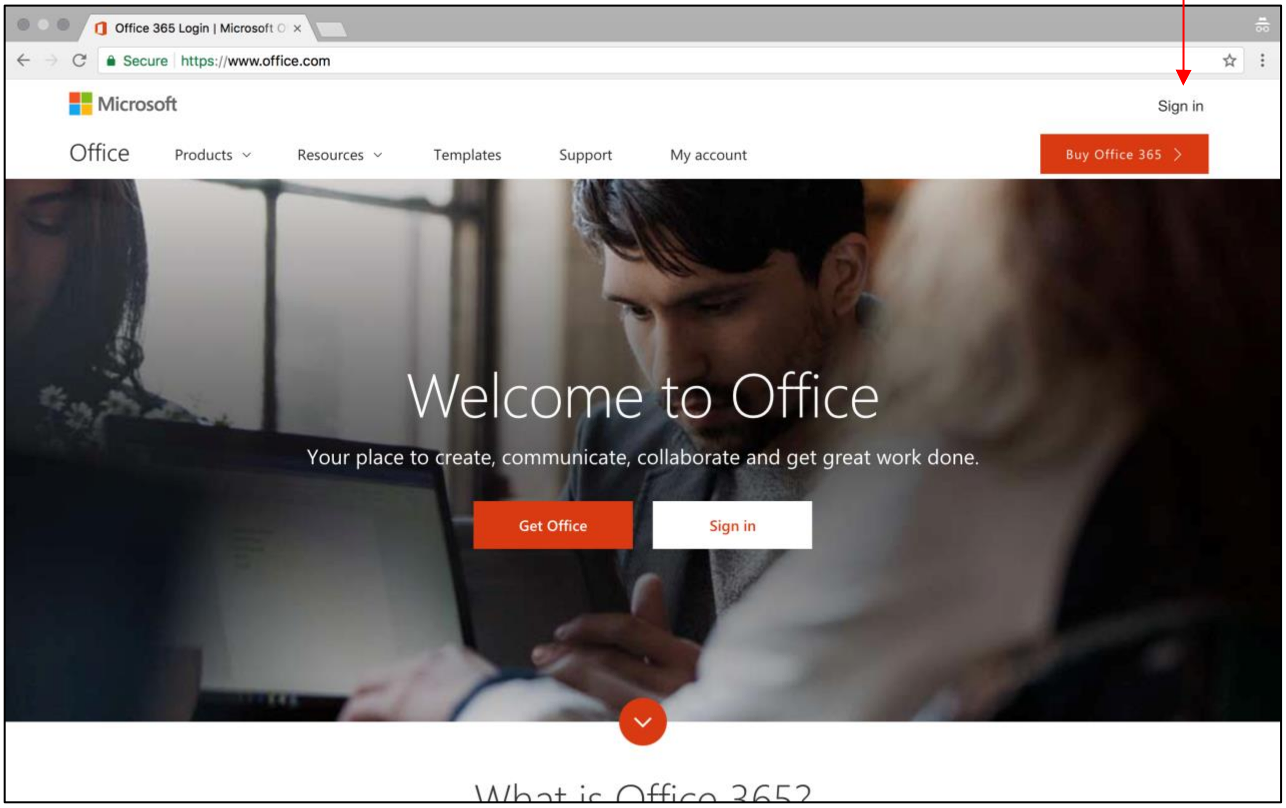

Workspace ONE
Secure | https://chodge-eu2.vmwareidentity.eu/catalog-portal/ui?isOnPremise=false&isMobile=false&userId=813599#/bookmarks
Workspace ONE
Search
John Wick
BOOKMARKS
CATALOG
Sort by A-Z
AirWatch
Office365
Salesforce

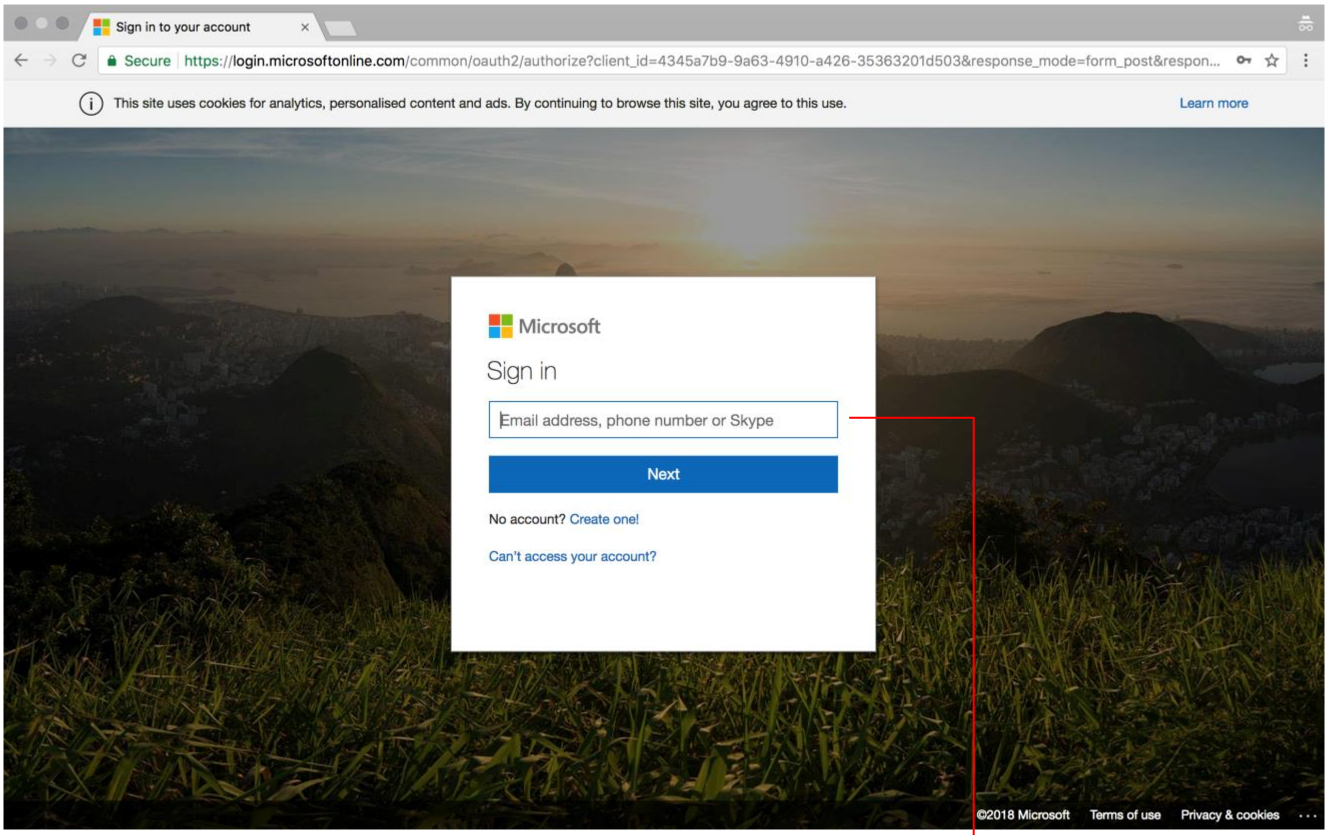
This should then open a new tab, point you to the correct office URL and log you in - The below screen shows that we've been pointed to the office website, our information has been passed and we've been logged in! Result!:



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





Sign in to your account
Secure
https://login.microsoftonline.com/common/oauth2/authorize?client_id=4345a7b9-9a63-4910-a426-35363201d503&response_mode=form_post&respon...
Learn more
Next
Create one!
Can't access your account?
©2018 Microsoft
Terms of use
Privacy & cookies

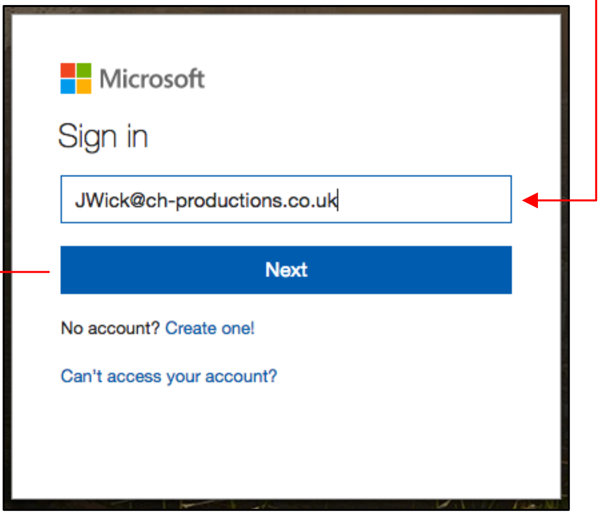
This site uses cookies for analytics, personalised content and ads. By continuing to browse this site, you agree to this use.

Microsoft

Sign in

Email address, phone number or Skype

No account? Create one!

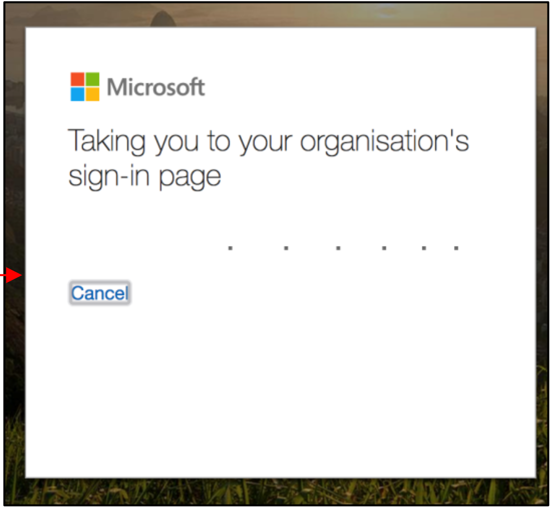


Microsoft

Sign in

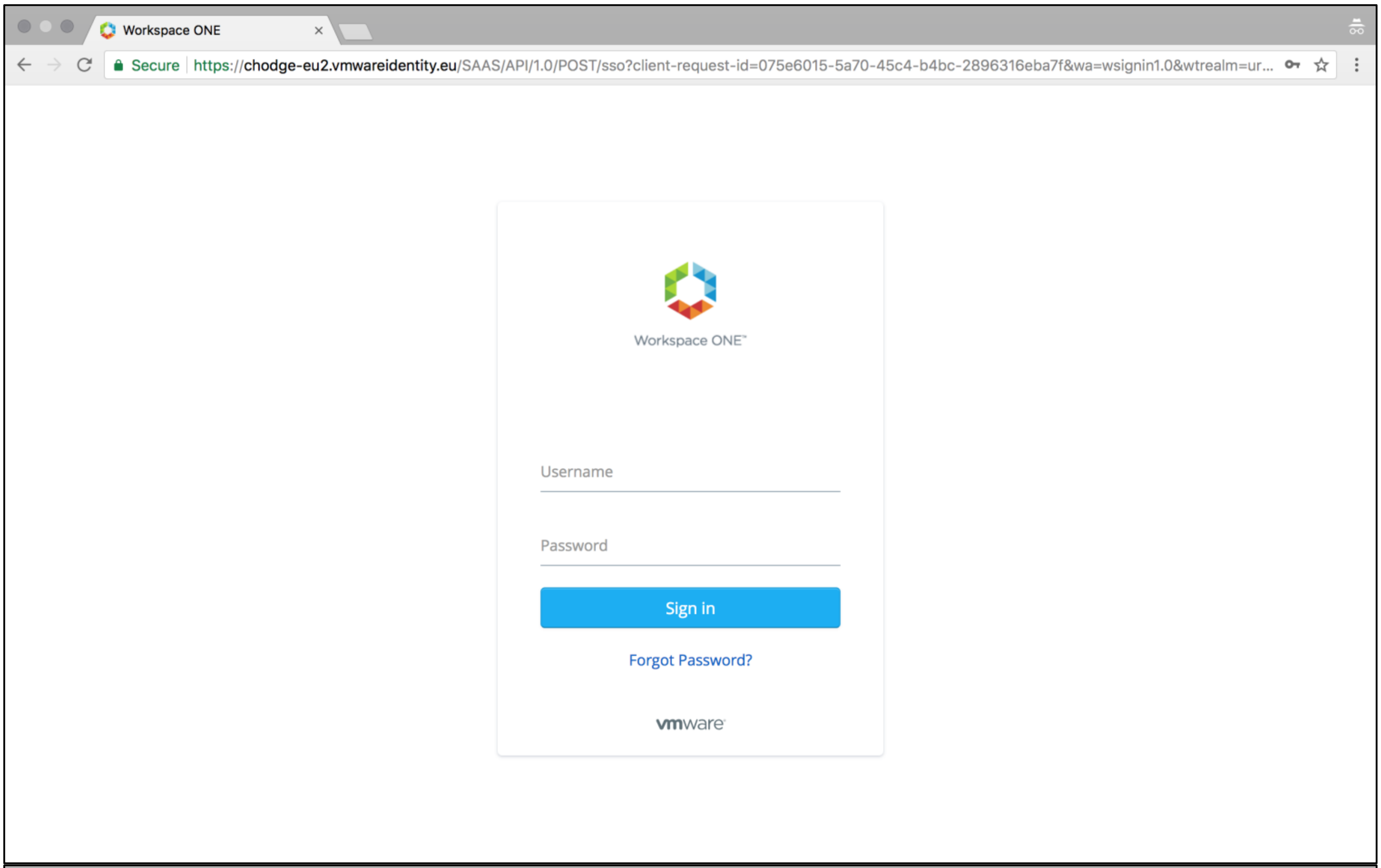
JWick@ch-productions.co.uk

No account? Create one!

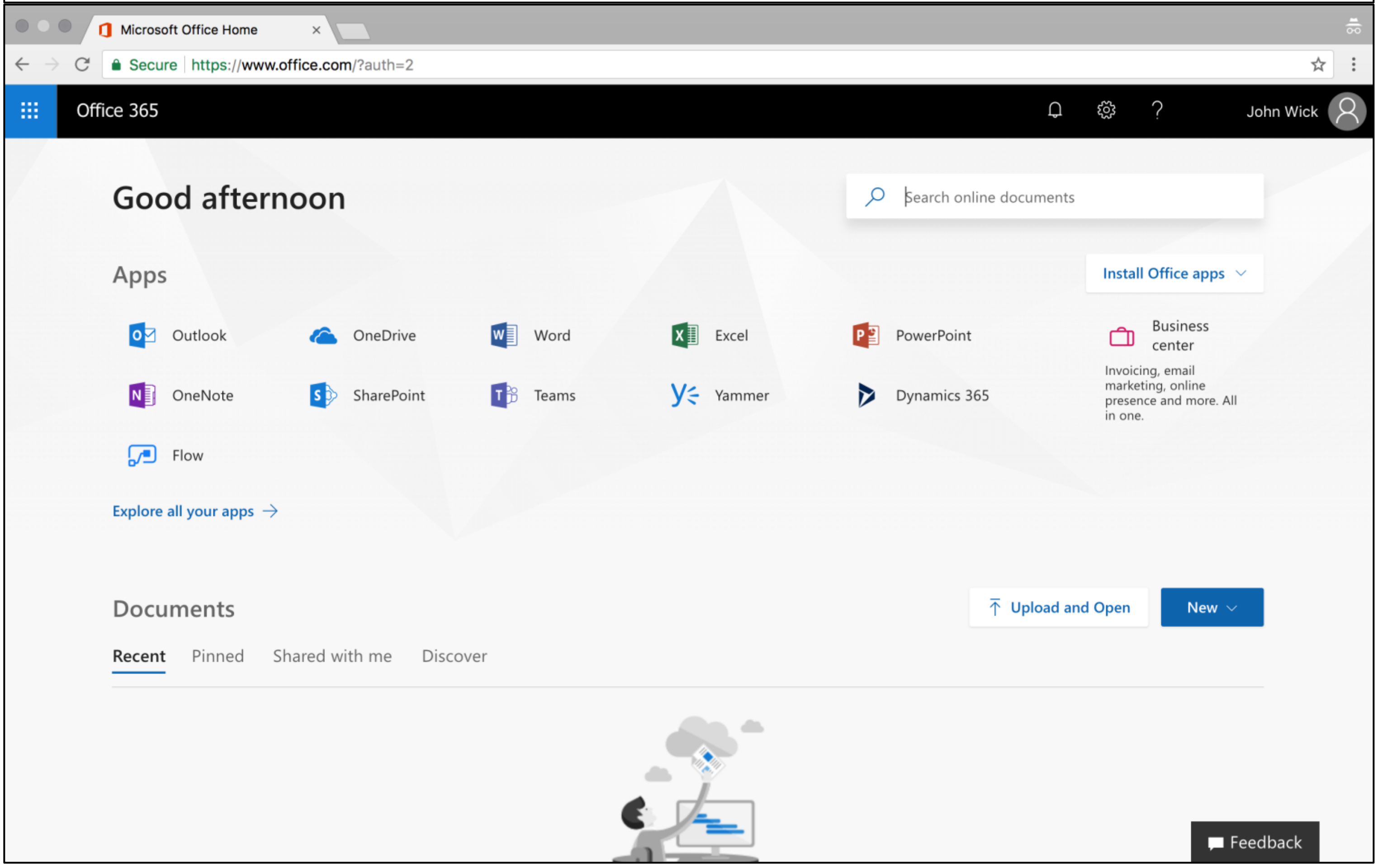


Microsoft

Taking you to your organisation's sign-in page



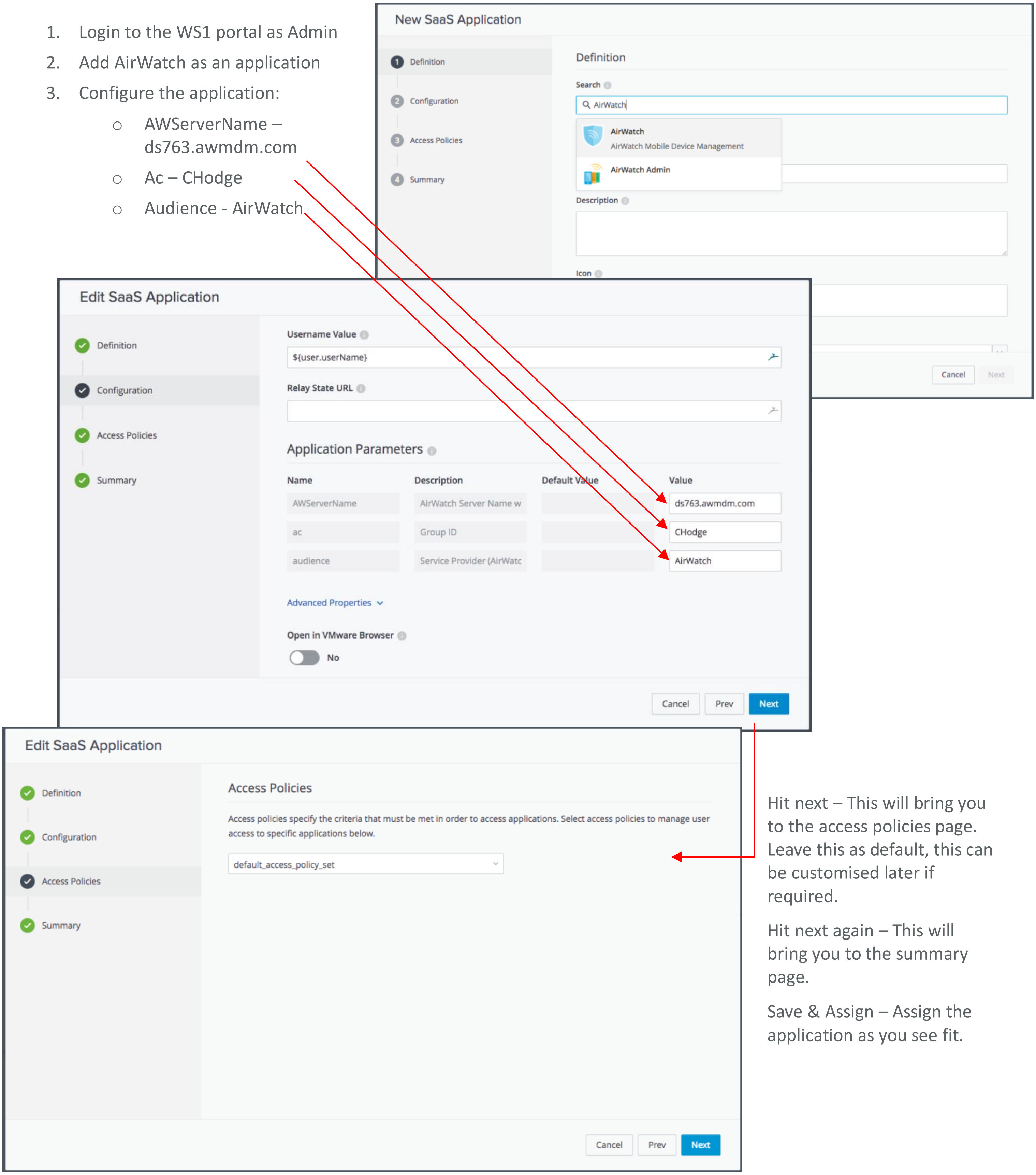
Secure | https://chodge-eu2.vmwareidentity.eu/SAAS/API/1.0/POST/sso?client-request-id=075e6015-5a70-45c4-b4bc-2896316eba7f&wa=wsignin1.0&wtrealm=ur...



Secure | https://www.office.com/?auth=2

12 - Configure SAML integration between vIDM and AirWatch

1. Login to the WS1 portal as Admin
2. Add AirWatch as an application
3. Configure the application:
    - AWServerName – ds763.awmdm.com
    - Ac – CHodge
    - Audience - AirWatch



New SaaS Application

Definition

Search: AirWatch

Edit SaaS Application

Username Value: ${user.userName}

Relay State URL:

Application Parameters

Name	Description	Default Value	Value
AWServerName	AirWatch Server Name w		ds763.awmdm.com
ac	Group ID		CHodge
audience	Service Provider (AirWatc		AirWatch

Open in VMware Browser: No

Edit SaaS Application

Access Policies

Access policies specify the criteria that must be met in order to access applications. Select access policies to manage user access to specific applications below.

default_access_policy_set

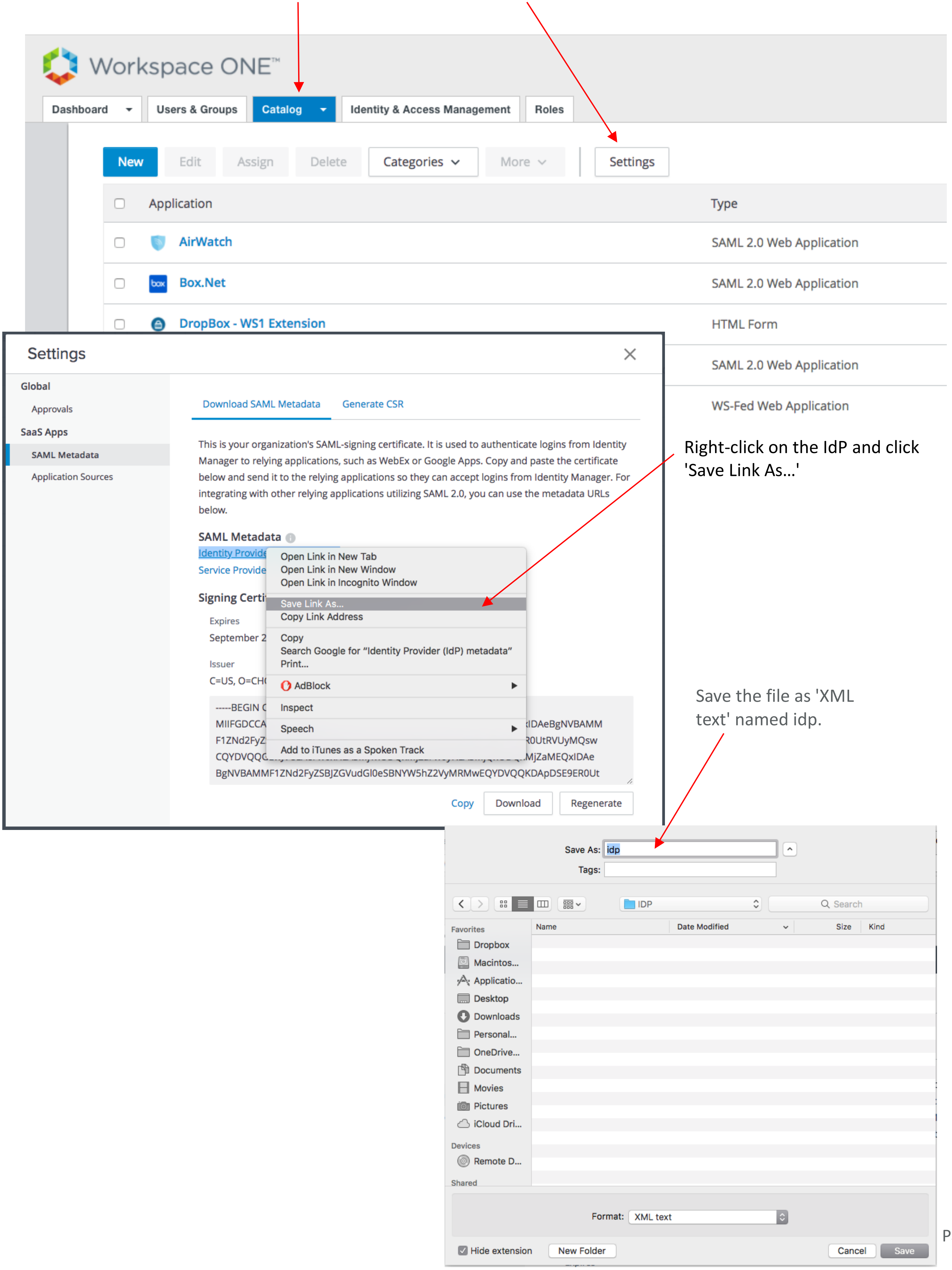
Hit next – This will bring you to the access policies page. Leave this as default, this can be customised later if required.

Hit next again – This will bring you to the summary page.

Save & Assign – Assign the application as you see fit.

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



Application	Type
AirWatch	SAML 2.0 Web Application
Box.Net	SAML 2.0 Web Application
DropBox - WS1 Extension	HTML Form
	SAML 2.0 Web Application
	WS-Fed Web Application

This is your organization's SAML-signing certificate. It is used to authenticate logins from Identity Manager to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Identity Manager. For integrating with other relying applications utilizing SAML 2.0, you can use the metadata URLs below.

Right-click on the IdP and click 'Save Link As...'

Save the file as 'XML text' named idp.

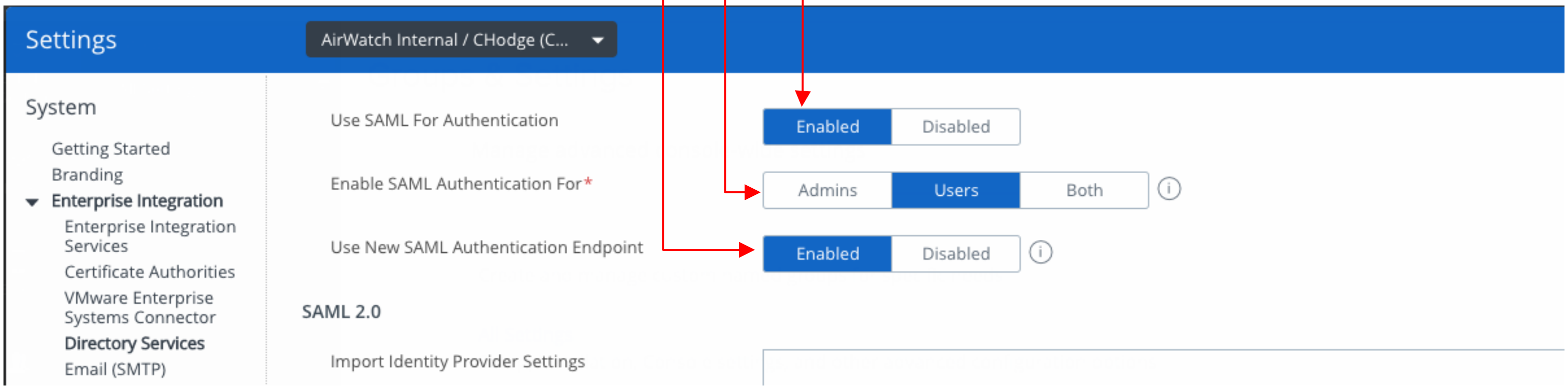
Save As: idp

Tags:

Format: XML text

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'



Use SAML For Authentication: [✓ Enabled] Disabled

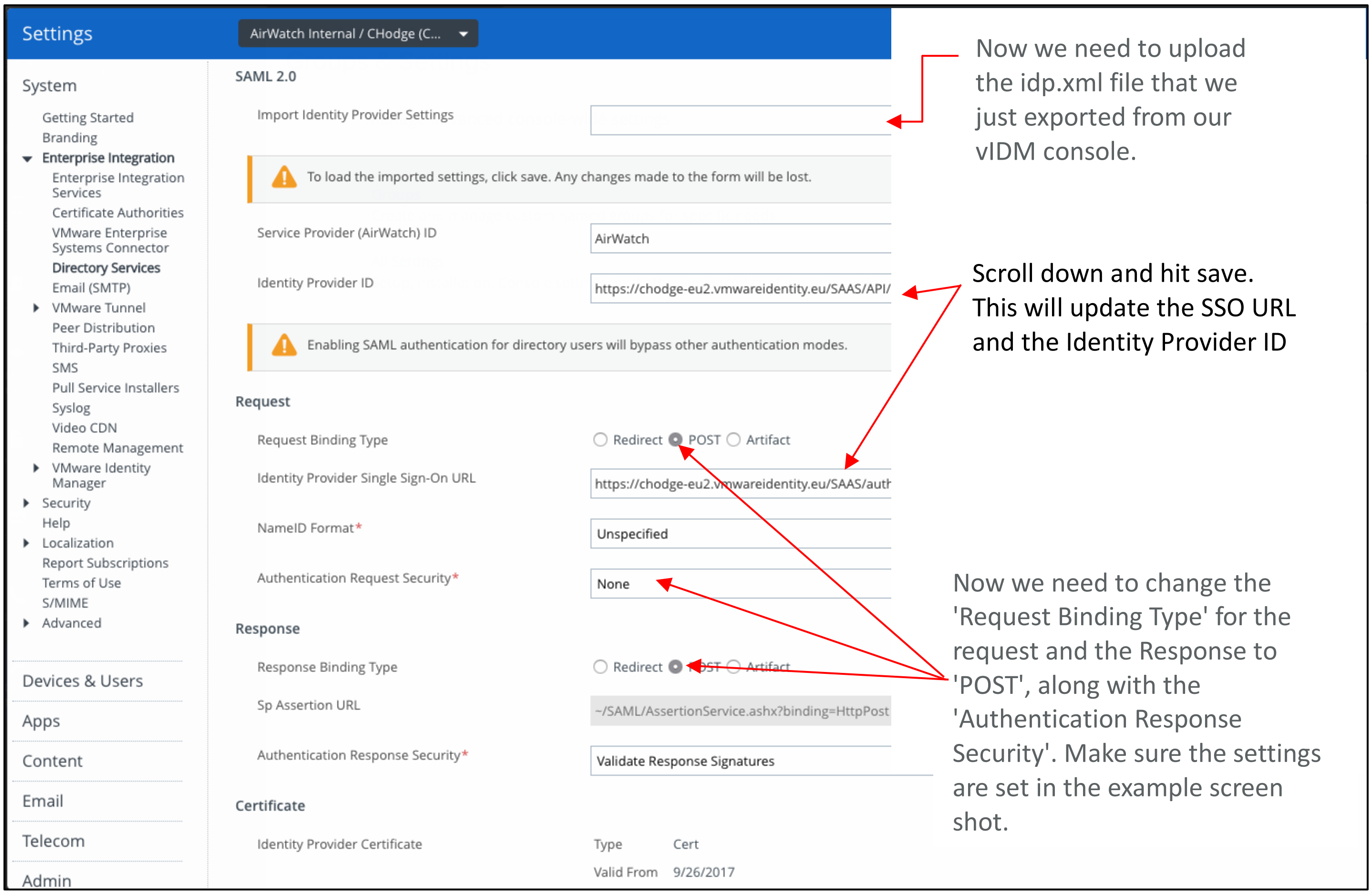
Enable SAML Authentication For*: Admins [✓ Users] Both

Use New SAML Authentication Endpoint: [✓ Enabled] Disabled

SAML 2.0

Import Identity Provider Settings

6 - Now we need to configure the SAML authentication.



SAML 2.0

Import Identity Provider Settings

To load the imported settings, click save. Any changes made to the form will be lost.

Service Provider (AirWatch) ID: AirWatch

Identity Provider ID: https://chodge-eu2.vmwareidentity.eu/SAAS/API/

Enabling SAML authentication for directory users will bypass other authentication modes.

Request

Request Binding Type: ○ Redirect ● POST ○ Artifact

Identity Provider Single Sign-On URL: https://chodge-eu2.vmwareidentity.eu/SAAS/auth

NameID Format*: Unspecified

Authentication Request Security*: None

Response

Response Binding Type: ○ Redirect ● POST ○ Artifact

Sp Assertion URL: ~/SAML/AssertionService.ashx?binding=HttpPost

Authentication Response Security*: Validate Response Signatures

Certificate

Identity Provider Certificate: Type Cert

Valid From 9/26/2017

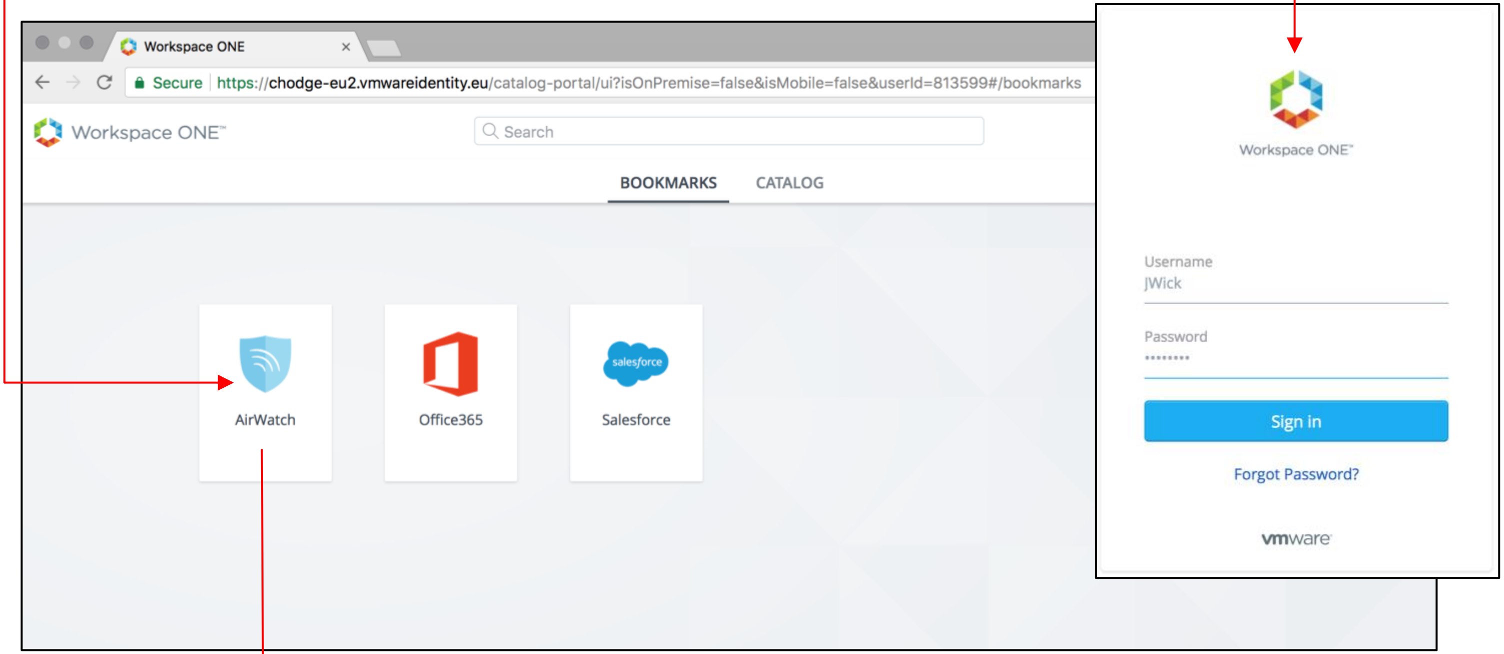
Now we need to upload the idp.xml file that we just exported from our vIDM console.

Scroll down and hit save. This will update the SSO URL and the Identity Provider ID

Now we need to change the 'Request Binding Type' for the request and the Response to 'POST', along with the 'Authentication Response Security'. Make sure the settings are set in the example screen shot.

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*



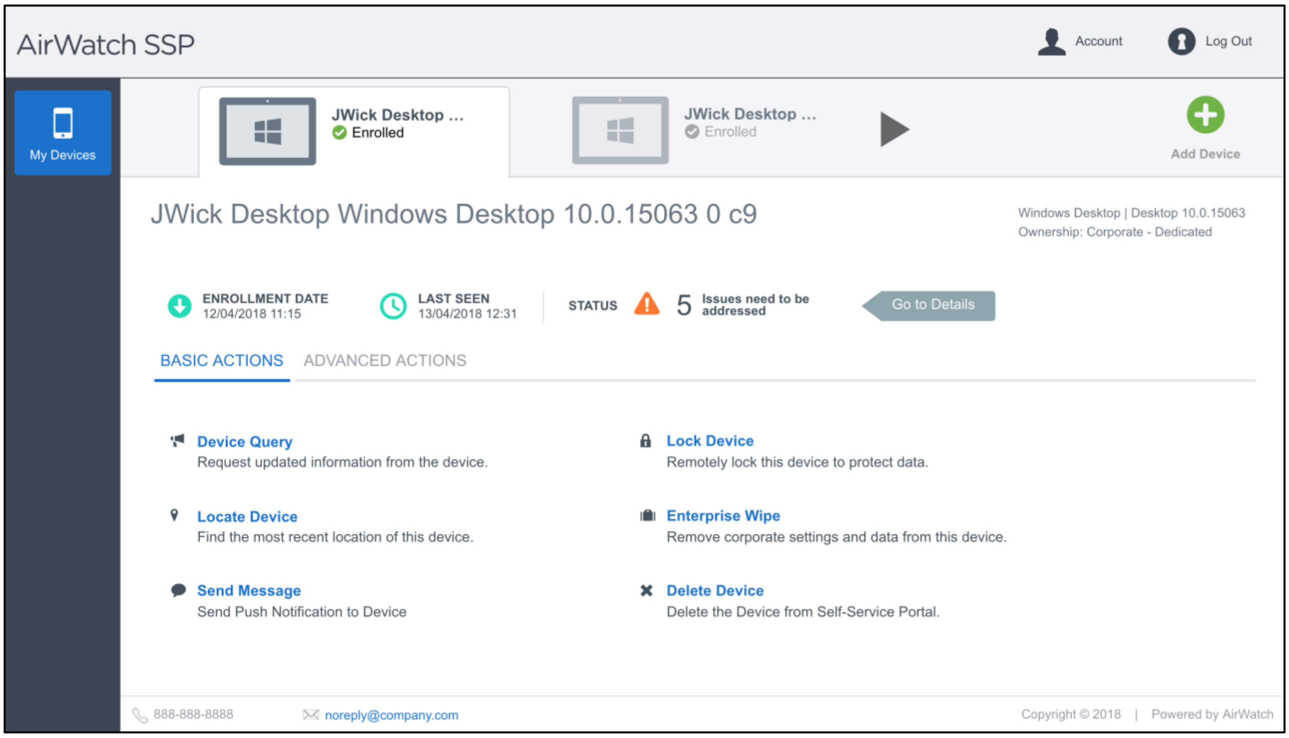
Workspace ONE

https://chodge-eu2.vmwareidentity.eu/catalog-portal/ui?isOnPremise=false&isMobile=false&userId=813599#/bookmarks

Username: JWick

Password: ********

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



AirWatch SSP

JWick Desktop Windows Desktop 10.0.15063 0 c9

Windows Desktop | Desktop 10.0.15063
Ownership: Corporate - Dedicated

ENROLLMENT DATE 12/04/2018 11:15

LAST SEEN 13/04/2018 12:31

STATUS 5 Issues need to be addressed

Device Query – Request updated information from the device.

Lock Device – Remotely lock this device to protect data.

Locate Device – Find the most recent location of this device.

Enterprise Wipe – Remove corporate settings and data from this device.

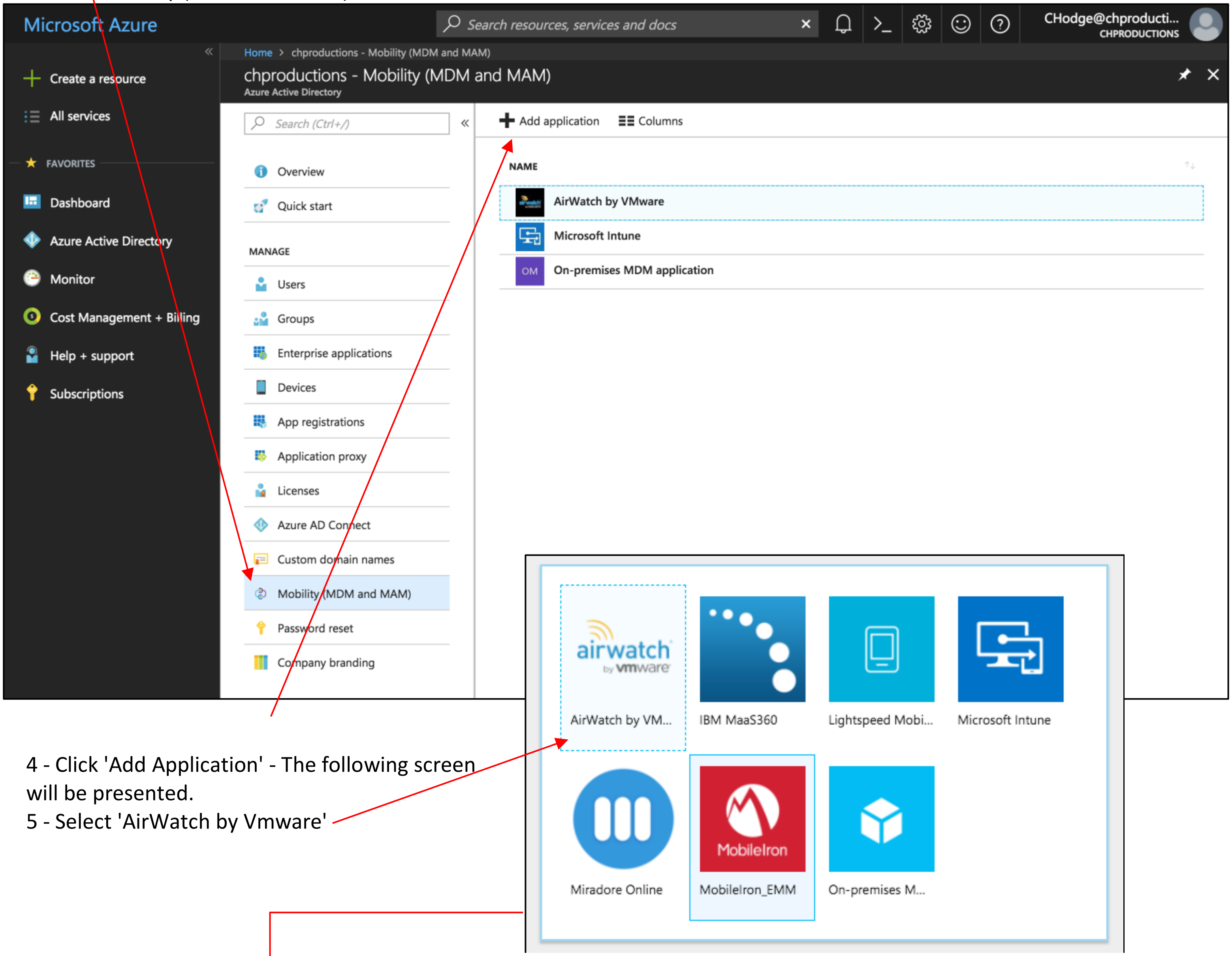
Send Message – Send Push Notification to Device

Delete Device – Delete the Device from Self-Service Portal.

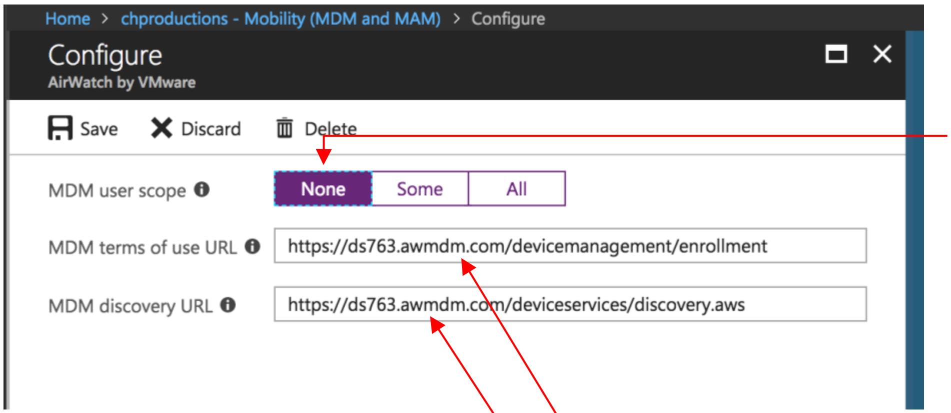
888-888-8888 noreply@company.com Copyright © 2018 | Powered by AirWatch

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

1 - Login to the Azure Portal: https://portal.azure.com
2 - Navigate to Azure Active Directory
3 - Select 'Mobility (MDM and MAM)'



4 - Click 'Add Application' - The following screen will be presented.
5 - Select 'AirWatch by Vmware'

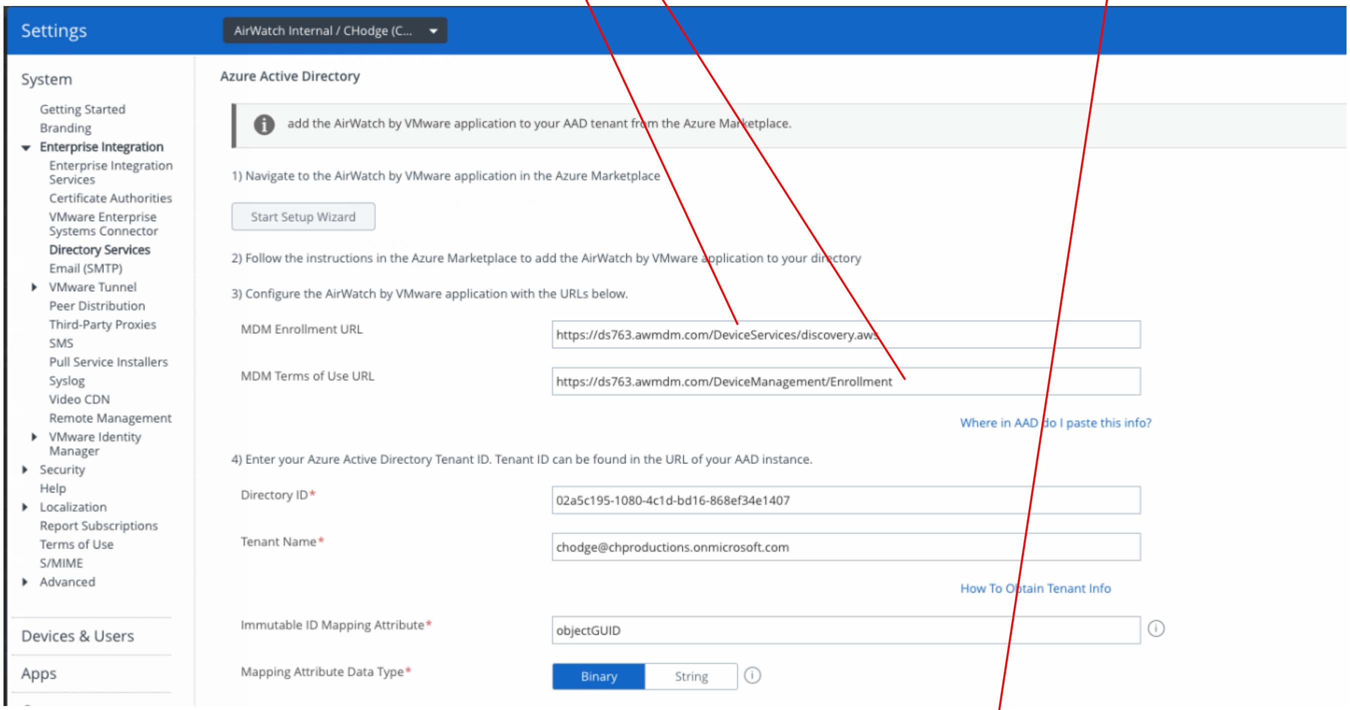


MDM user scope: [✓ None] Some All

MDM terms of use URL: https://ds763.awmdm.com/devicemanagement/enrollment

MDM discovery URL: https://ds763.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:



Azure Active Directory

add the AirWatch by VMware application to your AAD tenant from the Azure Marketplace.

1) Navigate to the AirWatch by VMware application in the Azure Marketplace

Start Setup Wizard

2) Follow the instructions in the Azure Marketplace to add the AirWatch by VMware application to your directory

3) Configure the AirWatch by VMware application with the URLs below.

MDM Enrollment URL: https://ds763.awmdm.com/DeviceServices/discovery.aws

MDM Terms of Use URL: https://ds763.awmdm.com/DeviceManagement/Enrollment

Where in AAD do I paste this info?

4) Enter your Azure Active Directory Tenant ID. Tenant ID can be found in the URL of your AAD instance.

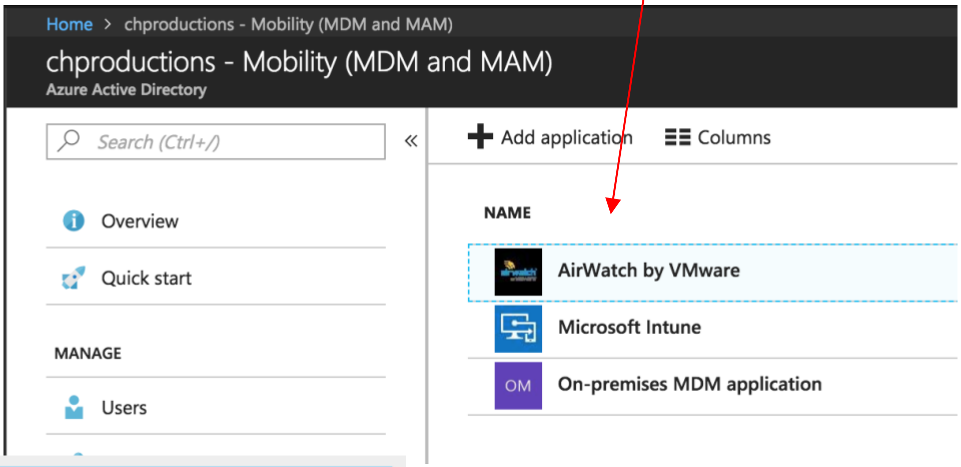
Directory ID*: 02a5c195-1080-4c1d-bd16-868ef34e1407

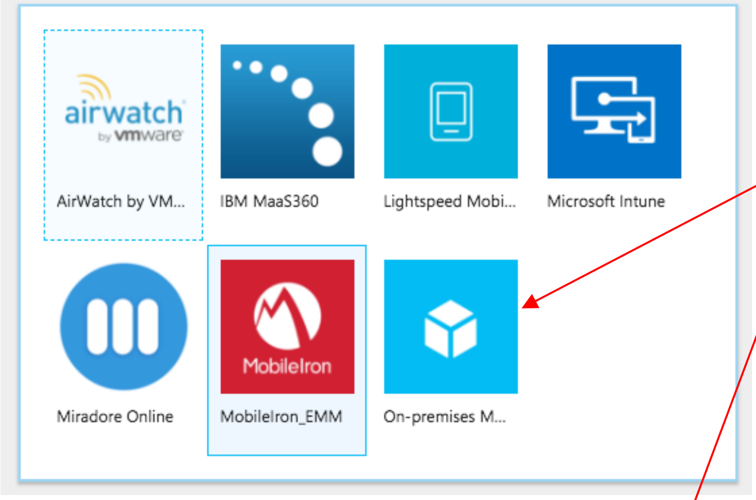
Tenant Name*: chodge@chproductions.onmicrosoft.com

How To Obtain Tenant Info

Immutable ID Mapping Attribute*: objectGUID

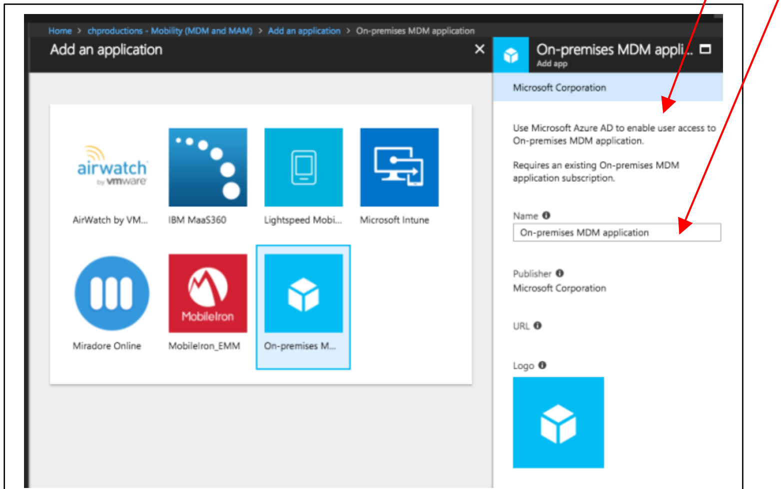
Mapping Attribute Data Type*: Binary String





This time, choose 'On-Premise MDM Application'. Now we will need to configure the Application:

You can name the application whatever you want and upload a new Logo is required. Click 'Add' to setup the application. Now you will have another application in your list of MDM application within Azure:



Use Microsoft Azure AD to enable user access to On-premises MDM application.

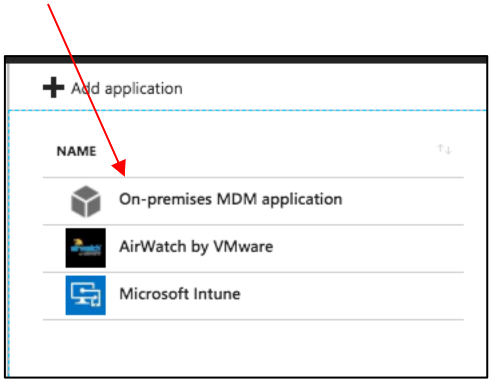
Requires an existing On-premises MDM application subscription.

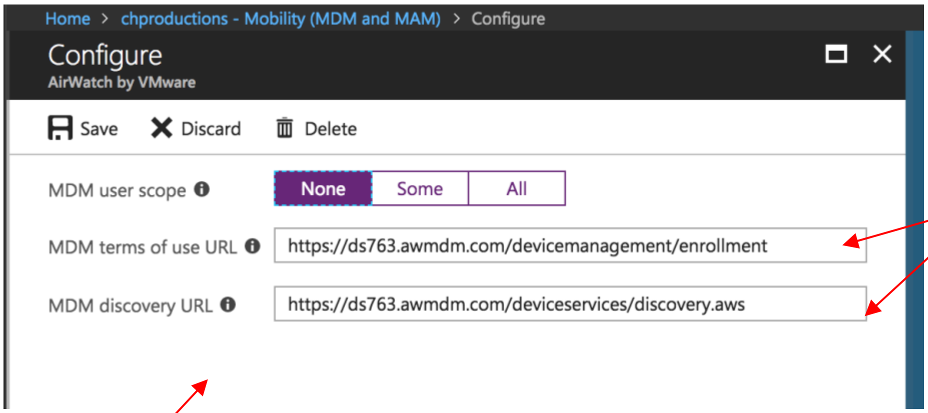
Name: On-premises MDM application

Publisher: Microsoft Corporation

URL

Logo





Home > chproductions - Mobility (MDM and MAM) > Configure

Configure

AirWatch by VMware

Save | Discard | Delete

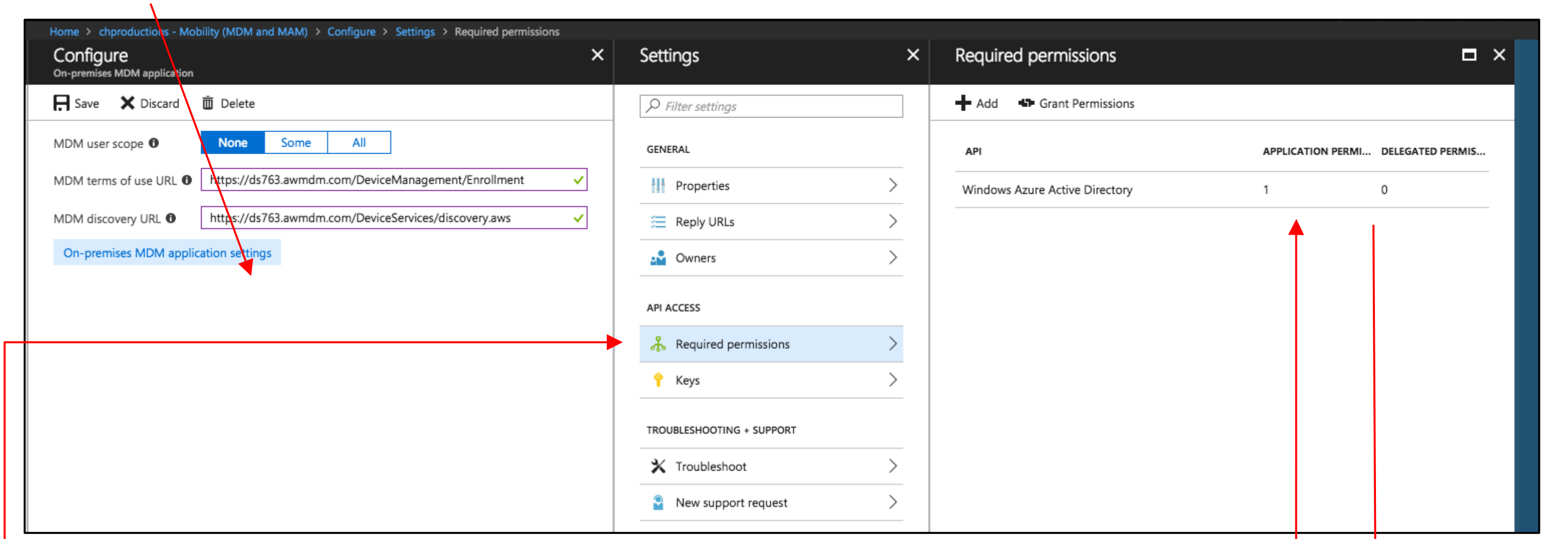
MDM user scope: **None** | Some | All

MDM terms of use URL: https://ds763.awmdm.com/devicemanagement/enrollment

MDM discovery URL: https://ds763.awmdm.com/deviceservices/discovery.aws

This application will have the same MDM terms of use and discovery URLs

We now need to configure the application.



Home > chproductions - Mobility (MDM and MAM) > Configure > Settings > Required permissions

Configure

On-premises MDM application

Save | Discard | Delete

MDM user scope: **None** | Some | All

MDM terms of use URL: https://ds763.awmdm.com/DeviceManagement/Enrollment

MDM discovery URL: https://ds763.awmdm.com/DeviceServices/discovery.aws

On-premises MDM application settings

Settings

Filter settings

GENERAL
- Properties
- Reply URLs
- Owners

API ACCESS
- Required permissions
- Keys

TROUBLESHOOTING + SUPPORT
- Troubleshoot
- New support request

Required permissions

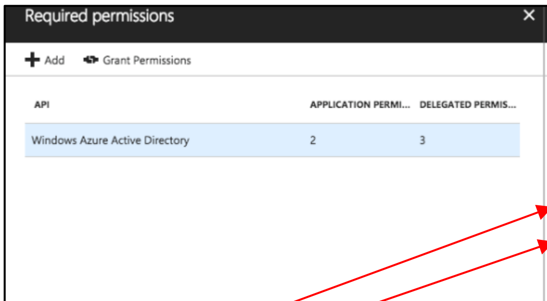
Add | Grant Permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	1	0

As the AirWatch Desktop Platform Guide States - We need to change the permissions of this application.
https://resources.air-watch.com/view/664yvcld3g7tm5jxzf6y/en

- Click on 'Required Permissions'
- Click on 'Windows Azure Active Directory'

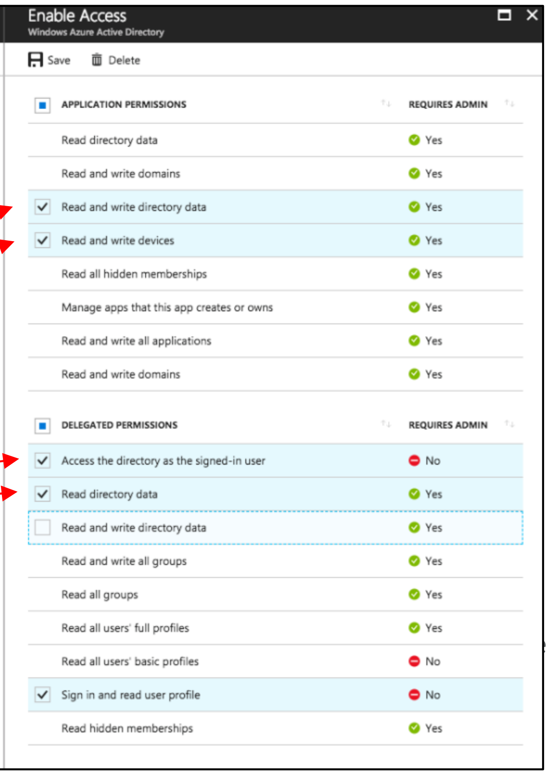
Make sure the permissions of the application are set the same as the Windows Desktop Platform guide states.



Required permissions

Add | Grant Permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	2	3



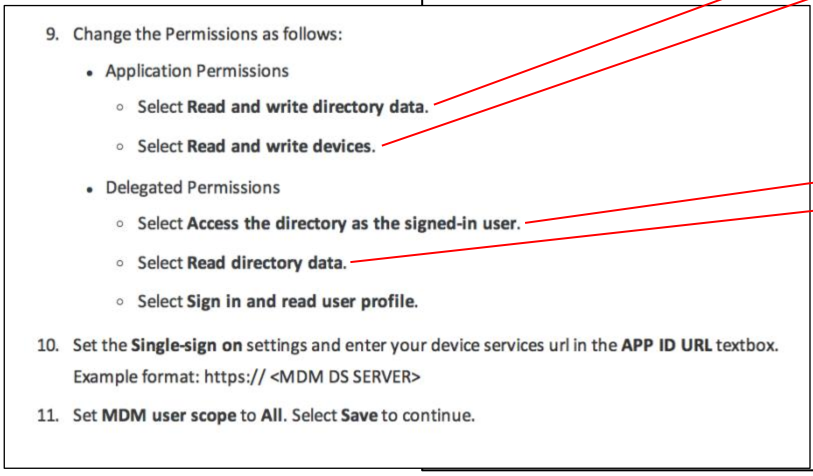
Enable Access

Windows Azure Active Directory

Save | Delete

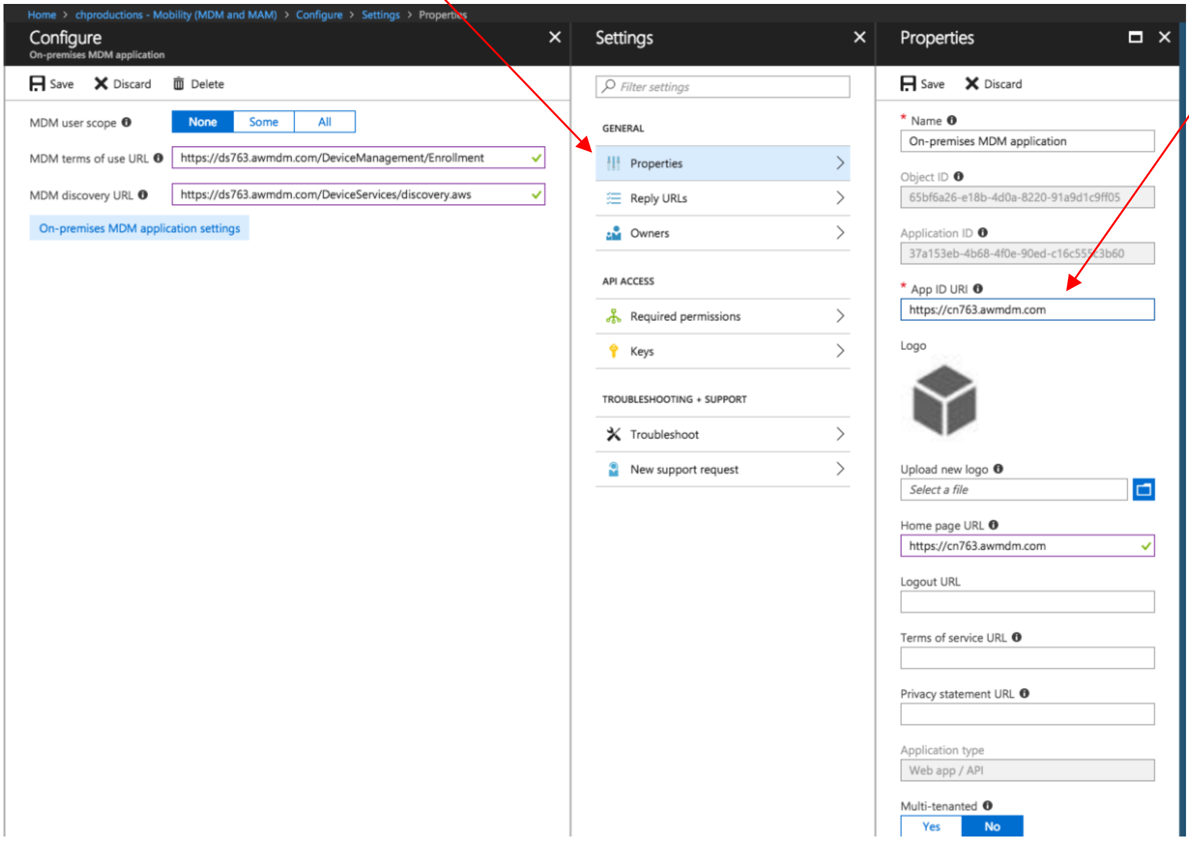
	APPLICATION PERMISSIONS	REQUIRES ADMIN
	Read directory data	✓ Yes
	Read and write domains	✓ Yes
☑	Read and write directory data	✓ Yes
☑	Read and write devices	✓ Yes
	Read all hidden memberships	✓ Yes
	Manage apps that this app creates or owns	✓ Yes
	Read and write all applications	✓ Yes
	Read and write domains	✓ Yes

	DELEGATED PERMISSIONS	REQUIRES ADMIN
☑	Access the directory as the signed-in user	⛔ No
☑	Read directory data	✓ Yes
□	Read and write directory data	✓ Yes
	Read and write all groups	✓ Yes
	Read all groups	✓ Yes
	Read all users' full profiles	✓ Yes
	Read all users' basic profiles	⛔ No
☑	Sign in and read user profile	⛔ No
	Read hidden memberships	✓ Yes



9. Change the Permissions as follows:
   - Application Permissions
     - Select **Read and write directory data**.
     - Select **Read and write devices**.
   - Delegated Permissions
     - Select **Access the directory as the signed-in user**.
     - Select **Read directory data**.
     - Select **Sign in and read user profile**.
10. Set the **Single-sign on** settings and enter your device services url in the **APP ID URL** textbox. Example format: https:// <MDM DS SERVER>
11. Set **MDM user scope** to **All**. Select **Save** to continue.

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



MDM user scope: None | Some | All (None selected)

MDM terms of use URL: https://ds763.awmdm.com/DeviceManagement/Enrollment

MDM discovery URL: https://ds763.awmdm.com/DeviceServices/discovery.aws

On-premises MDM application settings

* Name: On-premises MDM application

Object ID: 65bf6a26-e18b-4d0a-8220-91a9d1c9ff05

Application ID: 37a153eb-4b68-4f0e-90ed-c16c555c3b60

* App ID URI: https://cn763.awmdm.com

Logo

Upload new logo: Select a file

Home page URL: https://cn763.awmdm.com

Logout URL:

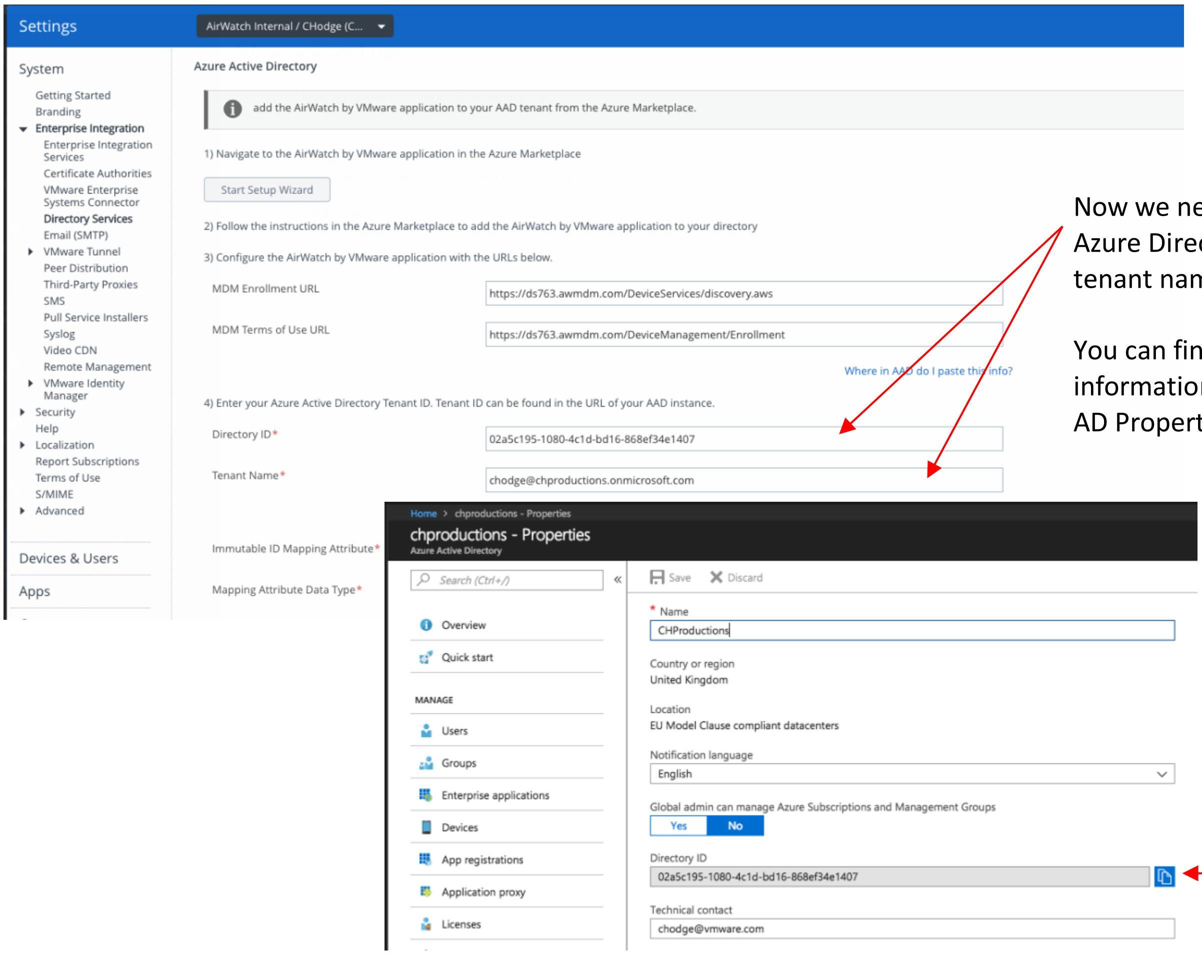
Terms of service URL:

Privacy statement URL:

Application type: Web app / API

Multi-tenanted: Yes | No (No selected)

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.



Azure Active Directory

add the AirWatch by VMware application to your AAD tenant from the Azure Marketplace.

1) Navigate to the AirWatch by VMware application in the Azure Marketplace

2) Follow the instructions in the Azure Marketplace to add the AirWatch by VMware application to your directory

3) Configure the AirWatch by VMware application with the URLs below.

MDM Enrollment URL: https://ds763.awmdm.com/DeviceServices/discovery.aws

MDM Terms of Use URL: https://ds763.awmdm.com/DeviceManagement/Enrollment

4) Enter your Azure Active Directory Tenant ID. Tenant ID can be found in the URL of your AAD instance.

Directory ID*: 02a5c195-1080-4c1d-bd16-868ef34e1407

Tenant Name*: chodge@chproductions.onmicrosoft.com

Immutable ID Mapping Attribute*

Mapping Attribute Data Type*

* Name: CHProductions

Country or region: United Kingdom

Location: EU Model Clause compliant datacenters

Notification language: English

Global admin can manage Azure Subscriptions and Management Groups: Yes | No (No selected)

Directory ID: 02a5c195-1080-4c1d-bd16-868ef34e1407

Technical contact: chodge@vmware.com

Now we need to fill in the Azure Directory ID and the tenant name.

You can find the tenant information from the Azure AD Properties (see below)