EUC: Advanced Integrations - 2019

LIVEFIRE SOLUTIONS

Table of Contents

Day 1

Getting Started - Workspace ONE Access & Workspace ONE UEM SaaS Instance

Part 1 Overview

The scenario you will be working with this week is a company called euc-livefire. They are a very dynamic organisation and have traditionally been on-premise but have recently moved into the cloud without truly understanding the challenges and would like a simple solution from an end-user perspective.

The organisation has key drivers around security, availability, mobility, and business continuity. They have an existing infrastructure with multiple authentication services such as OKTA and active Directory and would like to bring these together from the end-user perspective.

The organisation has recently started considering moving from office 2013 to Office 365 and sees this as another cloud resource the users would potentially need to connect to.

End-users require consumption of their applications across all platforms and recently have commented on how difficult it is to remember all the access portals and passwords.

As a consulting team our objective this week will be to integrate all existing resources both On-premise and SaaS into a singular simple solution for end users.

1. Overview of our On-premise and SaaS resources

On-premise resources

- The following resources in your lab environment are representative of what the EUC-Livefire organisation "On-premise' resources.
  1. Active Directory Domain Controller and DNS services.
     Server Name is **ControlCenter2** and the Active Directory Domain is **EUC-Livefire.com**
  2. **Citrix XenApp server.**
     We have a Citrix XenApp server with Storefront and legacy applications published to Citrix XenApp server name is Citrix.euc-livefire.com. A dedicated server for the integration broker called **Citrixbroker.euc-livefire.com**and a server called **citrixrdsh.euc-livefire.com**
  3. **Connector Server**
     A dedicated Windows server called **ws1.euc-livefire.com**, this is dedicated for the Workspace ONE Access connector which will have to be installed.

Cloud SaaS resources

As part of this story and part of the final solution you will register now in this section, with the following SaaS resources.

- A SaaS Instance of Workspace ONE Access (formerly known as VMware Identity Manager)
- A SaaS Instance of WorkspaceONE UEM (formerly known as VMware AirWatch)

In a later part of the labs you will register with the following SaaS services with a view to building a complete EUC solution.

- Office 365 tenant which will federate with Workspace ONE Access
- A Salesforce tenant with Workspace ONE Access

Part 2 : Registration of your SaaS Tenants for Workspace ONE Access and Workspace ONE UEM

This section takes you through the registration process for your lab resources. You will login to a SaaS tenant of Workspace ONE Access and Workspace ONE UEM.

In addition you will login and gain access to what will represent your on-premise components.

These include the Microsoft Windows Workspace ONE Access Connector, your Windows 10 Test Virtual machine and your Citrix Farm

1. **To Register for the course (Digital Workspace Livefire)** by clicking on the unique lab registration link found on www.vmware.com/go/euclivefire that takes your to **mylearn.vmware.com**

2. Click on **Start This Course**

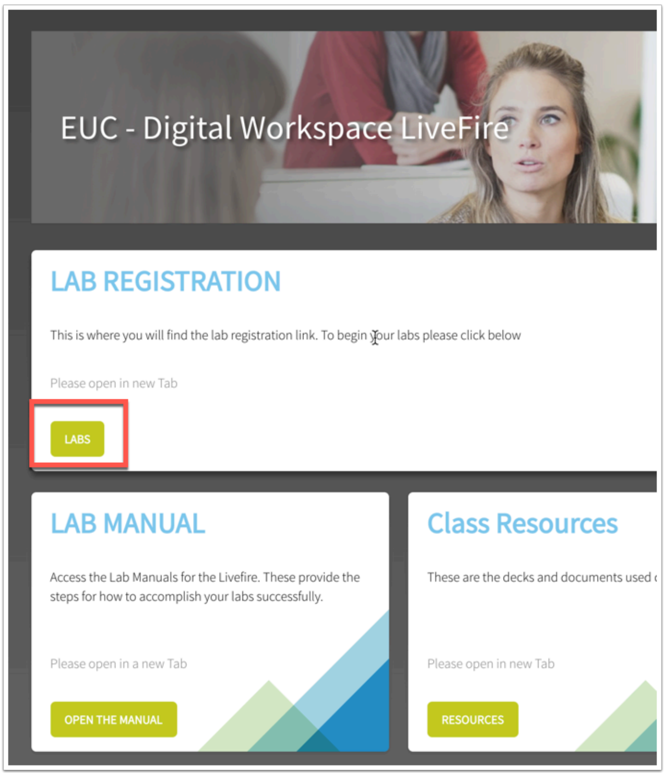
3. You will notice that a new Windows will open that allows you to Access the VLP (VMware Learning Platform) from which you will interact with your on-premises components. We will come back to these later in the lab.

4. At this time check your e-mail and you should have received an e-mail from **svc.labadmin@vmware.com**.

NOTE: Check your JUNK folder

5. This e-mail contains the unique tenant for your Workspace ONE Access SaaS instance. Click on the **TENANT URL** to launch the Workspace ONE Access Admin Console.

Use the credentials provided to login : Username: **Administrator** Password: **VMware1!**



EUC - Digital Workspace LiveFire

LAB REGISTRATION

This is where you will find the lab registration link. To begin your labs please click below

Please open in new Tab

LAB MANUAL

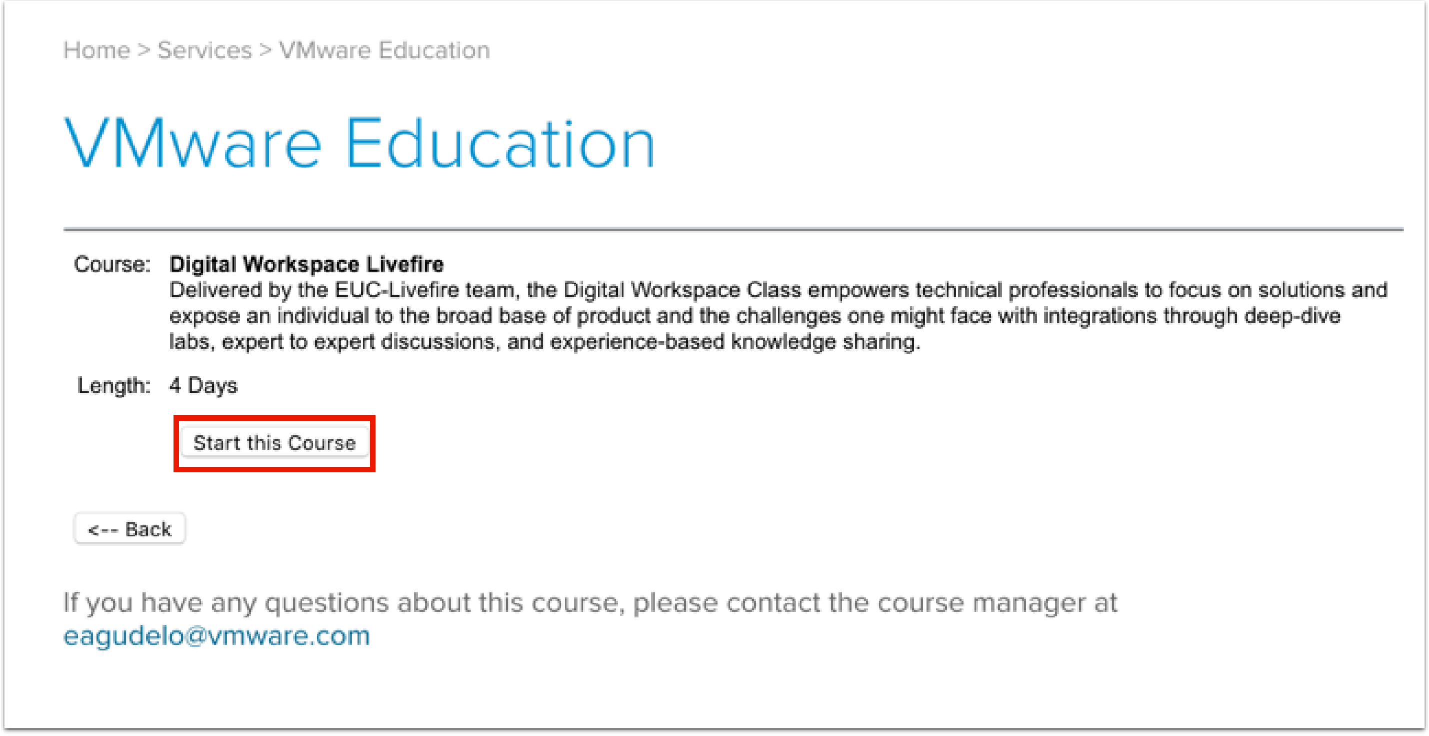
Access the Lab Manuals for the Livefire. These provide the steps for how to accomplish your labs successfully.

Please open in a new Tab

Class Resources

These are the decks and documents used

Please open in new Tab



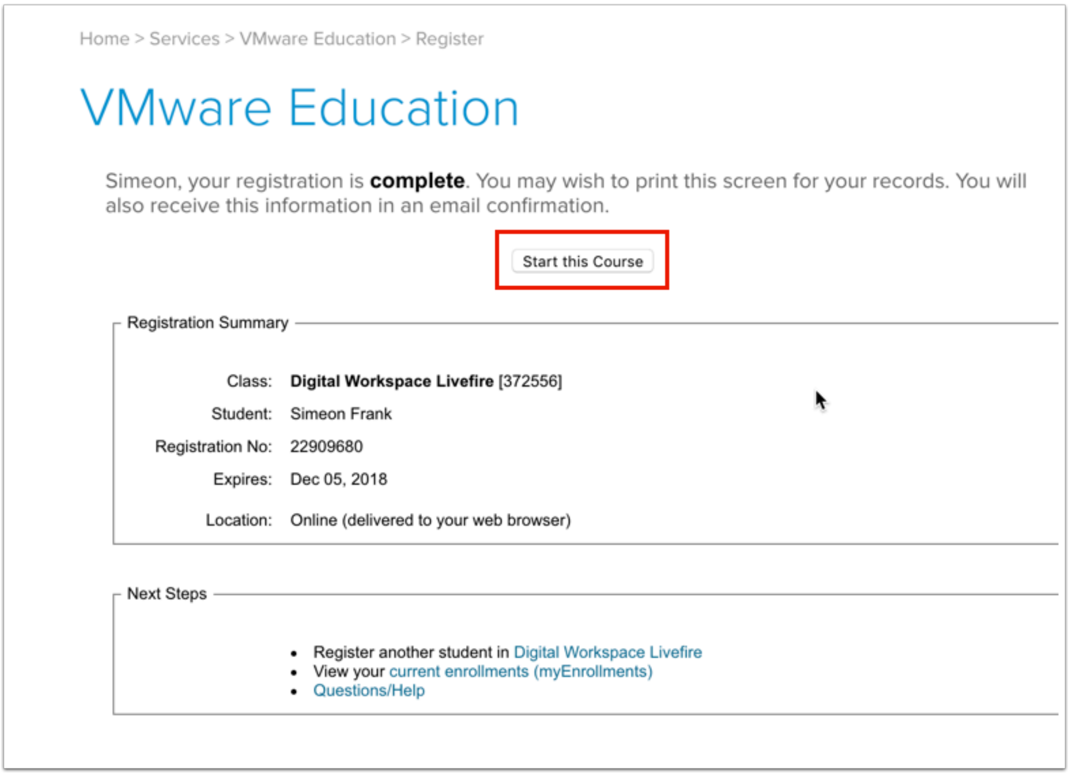
Home > Services > VMware Education

VMware Education

Course: **Digital Workspace Livefire**
Delivered by the EUC-Livefire team, the Digital Workspace Class empowers technical professionals to focus on solutions and expose an individual to the broad base of product and the challenges one might face with integrations through deep-dive labs, expert to expert discussions, and experience-based knowledge sharing.

Length: 4 Days

If you have any questions about this course, please contact the course manager at eagudelo@vmware.com



Home > Services > VMware Education > Register

VMware Education

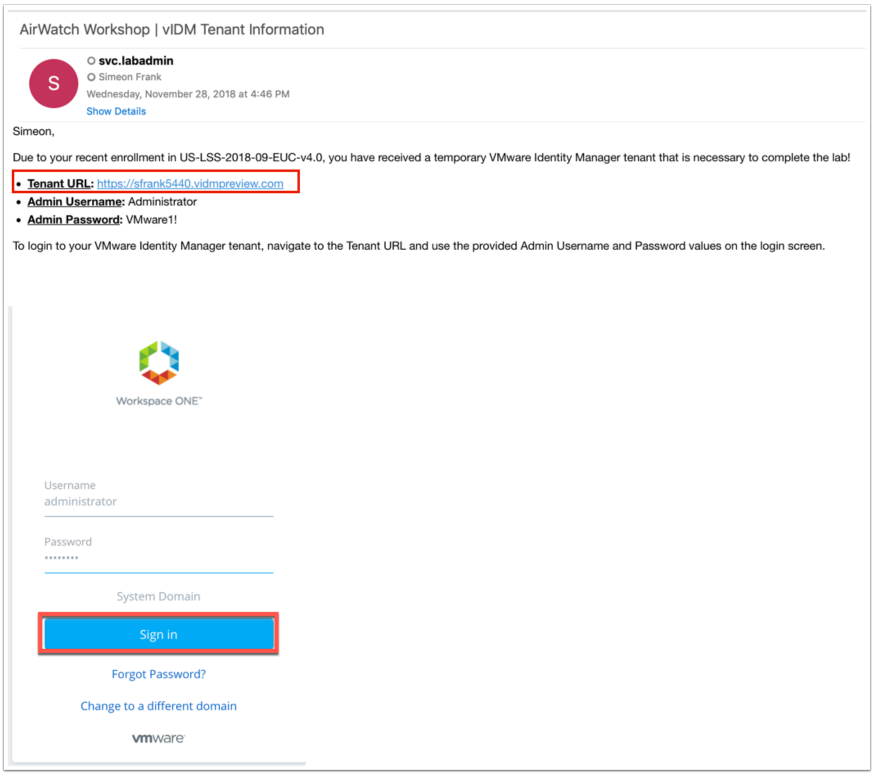
Simeon, your registration is **complete**. You may wish to print this screen for your records. You will also receive this information in an email confirmation.

Registration Summary

Class:	**Digital Workspace Livefire** [372556]
Student:	Simeon Frank
Registration No:	22909680
Expires:	Dec 05, 2018
Location:	Online (delivered to your web browser)

Next Steps

- Register another student in Digital Workspace Livefire
- View your current enrollments (myEnrollments)
- Questions/Help



AirWatch Workshop | vIDM Tenant Information

svc.labadmin
Simeon Frank
Wednesday, November 28, 2018 at 4:46 PM
Show Details

Simeon,

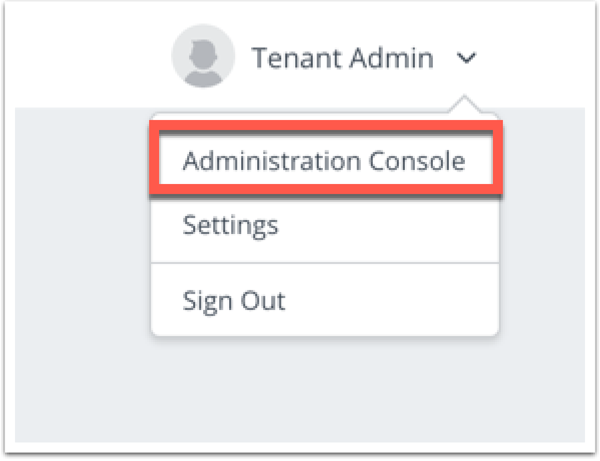
Due to your recent enrollment in US-LSS-2018-09-EUC-v4.0, you have received a temporary VMware Identity Manager tenant that is necessary to complete the lab!

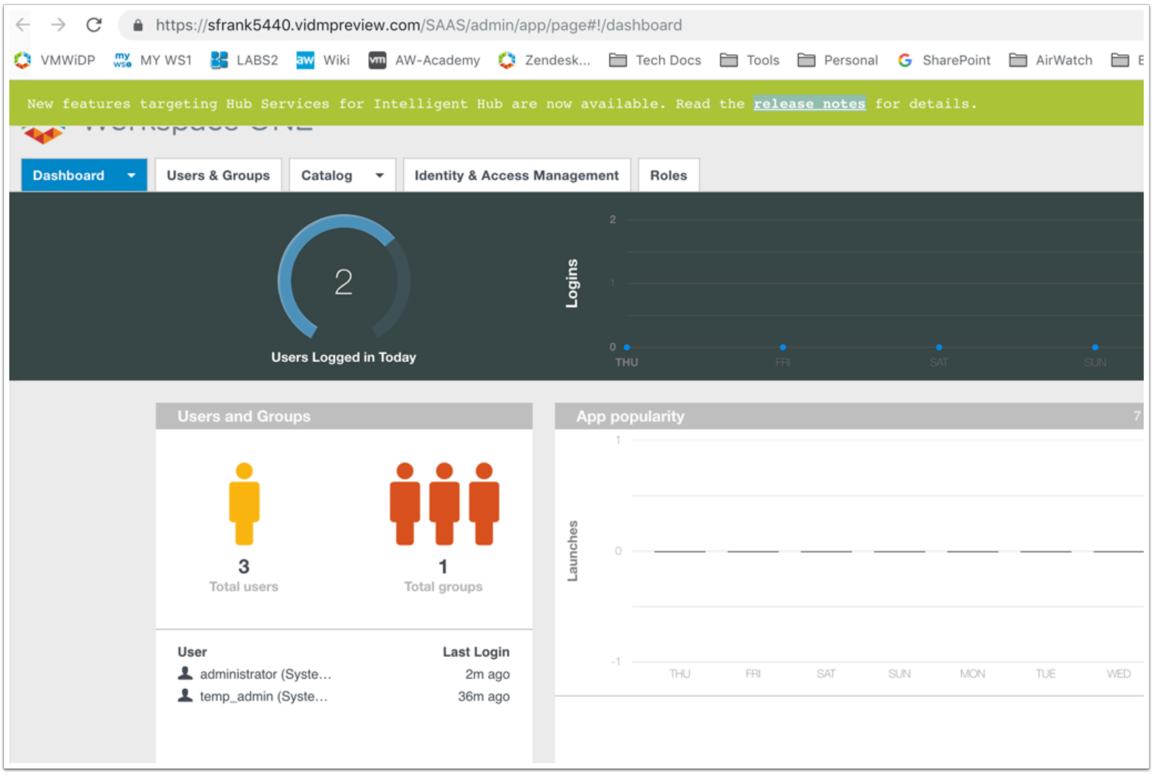
- **Tenant URL:** https://sfrank5440.vidmpreview.com
- **Admin Username:** Administrator
- **Admin Password:** VMware1!

To login to your VMware Identity Manager tenant, navigate to the Tenant URL and use the provided Admin Username and Password values on the login screen.

6. Now that you are signed in, change from the catalog view to the admin console by navigating to the top right and clicking on Tenant Admin and selecting Administration Console from the drop-down.

7. You should now see the Workspace ONE Access **Admin Console** to which we will return in a later lab.





New features targeting Hub Services for Intelligent Hub are now available. Read the release notes for details.

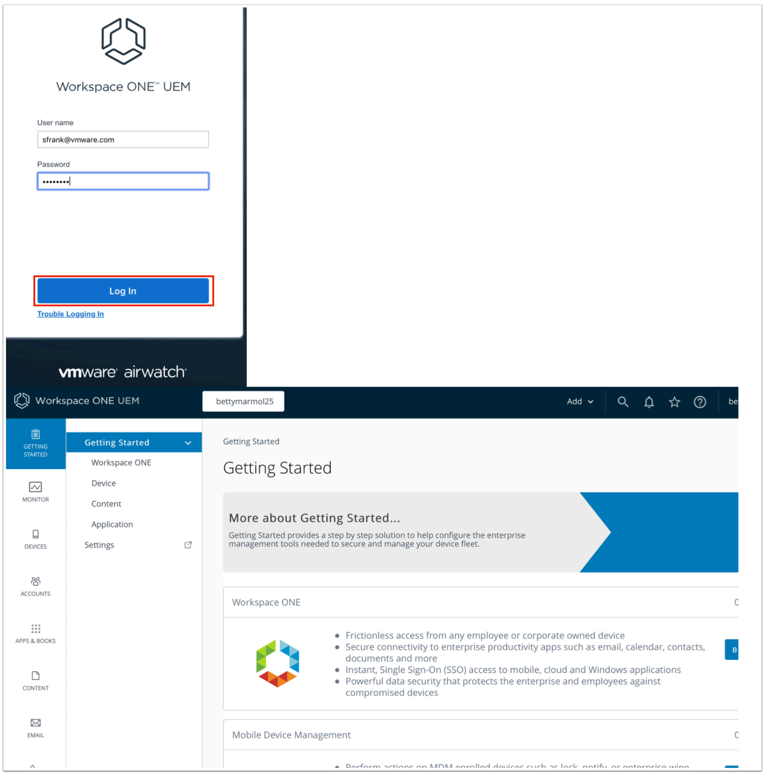
User	Last Login
administrator (Syste...	2m ago
temp_admin (Syste...	36m ago

8. Open a browser and navigate https://cn-livefire.awmdm.com

9. Use the e-mail address you signed up to the course with as the **User Name** (Eg sfrank@vmware.com) and the password: **VMware1!** Click **Log In**

10. Now set a security question and answer and a four digit Pin

11. You should now be on the Getting started window of the UEM console which is the default landing page.



User name: sfrank@vmware.com

Password: ••••••••

More about Getting Started...

Getting Started provides a step by step solution to help configure the enterprise management tools needed to secure and manage your device fleet.

- Frictionless access from any employee or corporate owned device
- Secure connectivity to enterprise productivity apps such as email, calendar, contacts, documents and more
- Instant, Single Sign-On (SSO) access to mobile, cloud and Windows applications
- Powerful data security that protects the enterprise and employees against compromised devices

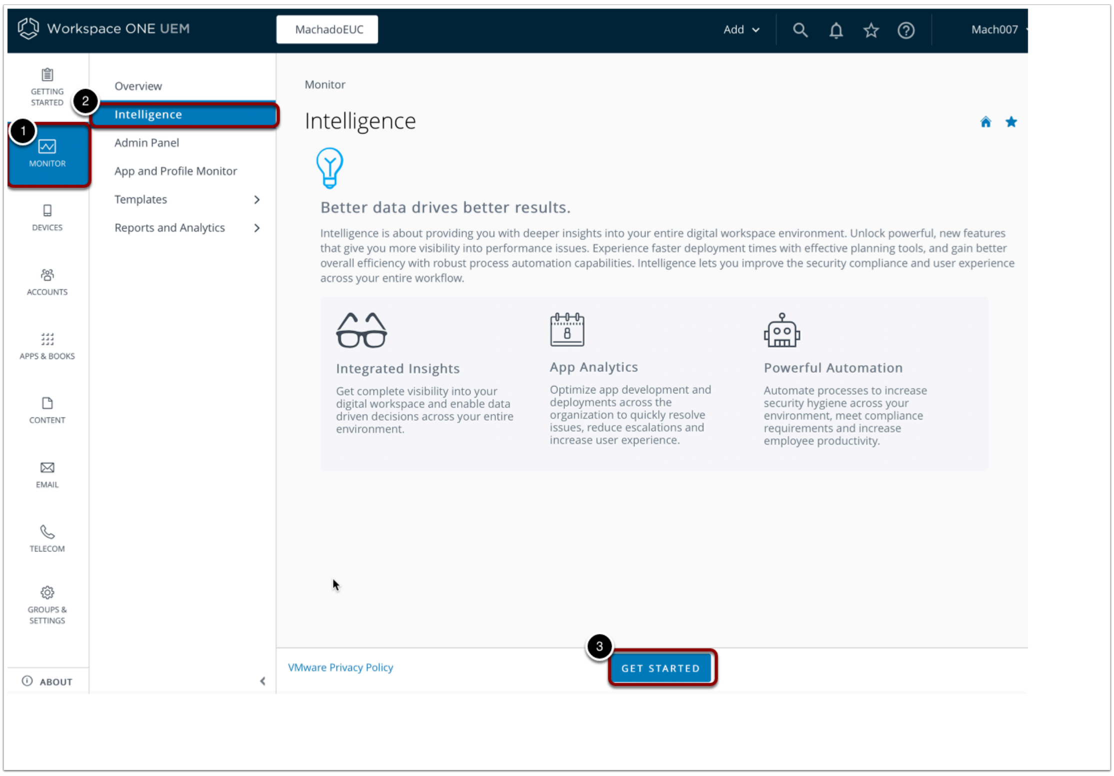
Part 3. Integrating with Workspace ONE Intelligence

This part of the lab will take you through how to activate your WorkspaceOne Intelligence Trial environment from the UEM console.

1. IF you aren't already, log into the Workspace ONE UEM console by opening a browser to https://cn-livefire.awmdm.com

2. Login using your **e-mail** as username and password: **VMware1!**

3. Select **Monitor** on your left of the Workspace ONE UEM pane and then select **Intelligence** and click **GET STARTED**



Intelligence

Better data drives better results.

Intelligence is about providing you with deeper insights into your entire digital workspace environment. Unlock powerful, new features that give you more visibility into performance issues. Experience faster deployment times with effective planning tools, and gain better overall efficiency with robust process automation capabilities. Intelligence lets you improve the security compliance and user experience across your entire workflow.

Integrated Insights

Get complete visibility into your digital workspace and enable data driven decisions across your entire environment.

App Analytics

Optimize app development and deployments across the organization to quickly resolve issues, reduce escalations and increase user experience.

Powerful Automation

Automate processes to increase security hygiene across your environment, meet compliance requirements and increase employee productivity.

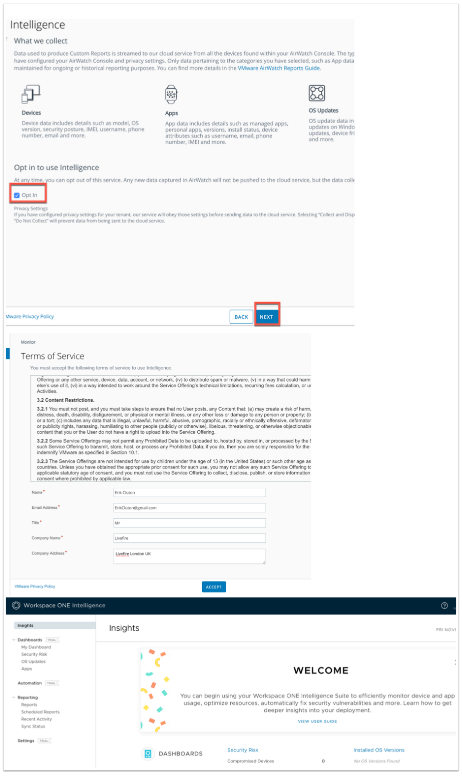
4. It will now give you the information as to what Intelligence will collect from your UEM environment.

Click the **check box** next to "**Opt In**" and select **Next** at the bottom of the page.

5. You will now need to **fill in your details** and select **ACCEPT.** Note: The form values can be fictitious.

6. You will now be re-directed to the Intelligence server.

You now have access to the WorkspaceOne Intelligence platform.



Intelligence

What we collect

Data used to produce Custom Reports is streamed to our cloud service from all the devices found within your AirWatch Console. The typ have configured your AirWatch Console and privacy settings. Only data pertaining to the categories you have selected, such as App data maintained for ongoing or historical reporting purposes. You can find more details in the VMware AirWatch Reports Guide.

Devices

Device data includes details such as model, OS version, security posture, IMEI, username, phone number, email and more.

Apps

App data includes details such as managed apps, personal apps, versions, install status, device attributes such as username, email, phone number, IMEI and more.

OS Updates

OS update data in updates on Windo updates, device fri and more.

Opt in to use Intelligence

At any time, you can opt out of this service. Any new data captured in AirWatch will not be pushed to the cloud service, but the data colle

☑ Opt In

Privacy Settings

If you have configured privacy settings for your tenant, our service will obey those settings before sending data to the cloud service. Selecting "Collect and Disp "Do Not Collect" will prevent data from being sent to the cloud service.

Terms of Service

You must accept the following terms of service to use Intelligence.

Offering or any other service, device, data, account, or network, (iv) to distribute spam or malware, (v) in a way that could harm else's use of it, (vi) in a way intended to work around the Service Offering's technical limitations, recurring fees calculation, or us Activities.

3.2 Content Restrictions.

3.2.1 You must not post, and you must take steps to ensure that no User posts, any Content that: (a) may create a risk of harm, distress, death, disability, disfigurement, or physical or mental illness, or any other loss or damage to any person or property; (b or a tort; (c) includes any data that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamator or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable content that you or the User do not have a right to upload into the Service Offering.

3.2.2 Some Service Offerings may not permit any Prohibited Data to be uploaded to, hosted by, stored in, or processed by the S such Service Offering to transmit, store, host, or process any Prohibited Data; if you do, then you are solely responsible for the indemnify VMware as specified in Section 10.1.

3.2.3 The Service Offerings are not intended for use by children under the age of 13 (in the United States) or such other age as countries. Unless you have obtained the appropriate prior consent for such use, you may not allow any such Service Offering to applicable statutory age of consent, and you must not use the Service Offering to collect, disclose, publish, or store information consent where prohibited by applicable law.

Name*	Erik Cluton
Email Address*	ErikCluton@gmail.com
Title*	Mr
Company Name*	Livefire
Company Address*	Livefire London UK

WELCOME

You can begin using your Workspace ONE Intelligence Suite to efficiently monitor device and app usage, optimize resources, automatically fix security vulnerabilities and more. Learn how to get deeper insights into your deployment.

Compromised Devices 0

No OS Versions Found

We will setup the WorkspaceOne Intelligence integration with Workspace ONE Access. this will allow us to begin aggregating information based on logins to Workspace ONE UEM and AppLaunch.

1. On the left of the pane, navigate to and select the dropdown next to **Settings** , and select **Integrations** select SET UP under **Workspace ONE Access**

2. Select **GET STARTED** on the the wizard page

3. On the **Authorize: Workspace ONE Access** page select **Provide Credentials** and next to **Tenant Domain*** type **your unique Workspace ONE Access tenant URL** for this course. e.g **https://aw-livefirerplaston.Workspace ONE Accesspreview.com**

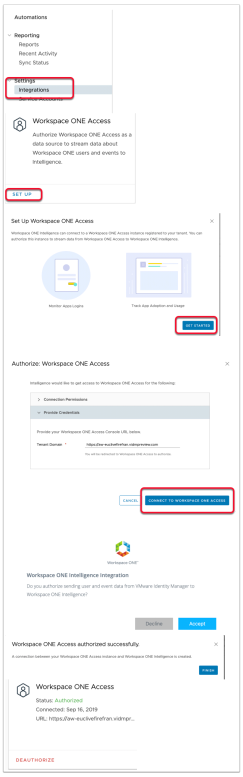
4. Select **CONNECT TO WORKSPACE ONE ACCESS**

5. On the **Workspace ONE Intelligence Integration** window select **ACCEPT**

6. On **Workspace ONE Access authorised successfully** window select **FINISH**

This concludes the the setup of our VMware WorkspaceOne tenants needed for the remainder of the labs.

You may now move on to the next lab



Workspace ONE Access

Authorize Workspace ONE Access as a data source to stream data about Workspace ONE users and events to Intelligence.

Set Up Workspace ONE Access

Workspace ONE Intelligence can connect to a Workspace ONE Access instance registered to your tenant. You can authorize this instance to stream data from Workspace ONE Access to Workspace ONE Intelligence.

Authorize: Workspace ONE Access

Intelligence would like to get access to Workspace ONE Access for the following:

Provide your Workspace ONE Access Console URL below.

Tenant Domain * https://aw-euclivefirefran.vidmpreview.com

You will be redirected to Workspace ONE Access to authorize.

Workspace ONE Intelligence Integration

Do you authorize sending user and event data from VMware Identity Manager to Workspace ONE Intelligence?

Workspace ONE Access authorized successfully.

A connection between your Workspace ONE Access instance and Workspace ONE Intelligence is created.

Workspace ONE Access

Status: Authorized

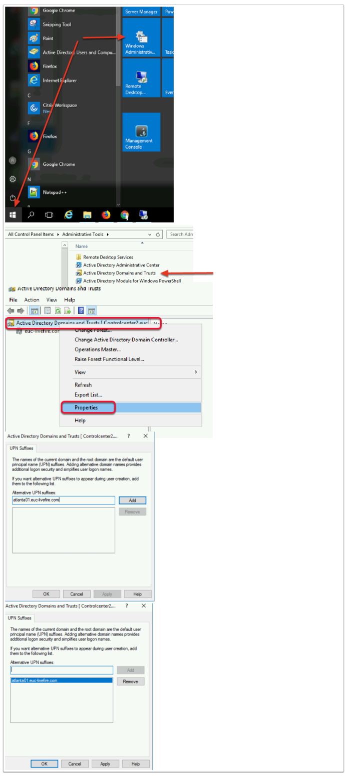
Connected: Sep 16, 2019

URL: https://aw-euclivefirefran.vidmpr...

Part 4. Configuring domain trust

1. On your **ControlCenter Desktop**, Select the **Start** Button to launch the **Start Menu** and select **Administrative Tools**

1. Select **Active Directory Domains and Trusts** shortcut
2. In **Active Directory Domain and Trusts mmc** select and right-click **Active Directory Domains and Trusts [ControlCenter2.euc-livefire.com]**
3. Select Properties
4. Under the **UPN Suffixes** Tab under **Alternative UPN suffixes** type ***your custom domain name***. the example we have in this lab is **tokyo01.euc-livefire.com**
5. Select **Add** , select **OK** to close the window, **close** the **Active Directory Domains and Trusts** Window.


Google Chrome
Snipping Tool
Paint
Active Directory Users and Compu...
Firefox
Internet Explorer
Citrix Workspace
Notepad++
Server Manager
Windows Administrativ...
Remote Desktop...
Management Console
Remote Desktop Services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
File Action View Help
Active Directory Domains and Trusts [Controlcenter2.euc
euc-livefire.com
Change Forest...
Change Active Directory Domain Controller...
Operations Master...
Raise Forest Functional Level...
View
Refresh
Export List...
Properties
Help
Active Directory Domains and Trusts [Controlcenter2....
UPN Suffixes
Add
Remove
OK
Cancel
Apply
Help

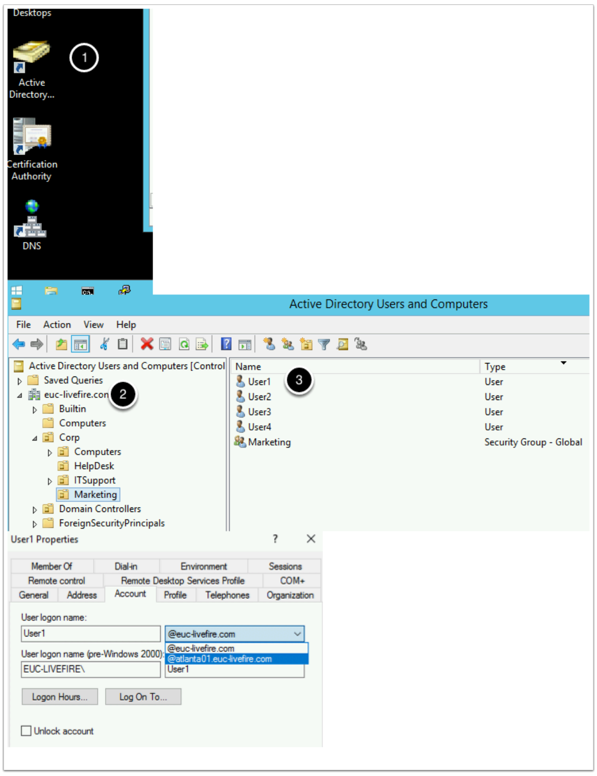
The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes: atlanta01.euc-livefire.com

2.

- On your **ControlCenter** Desktop **close** Active Directory Domain and trusts.
  1. In the **Administrative tools** folder select **Active Directory Users and Computers** shortcut and select **open**
  2. Under the euc-livefire.com domain, expand the **Corp** > **Marketing** Organisational Units
  3. You will notice we have **Users 1 to 4.** Select and right-click **User1** and select **Properties**
  4. Select the **Account** tab, to the right of **User logon name:** select the **drop down arrow** and select ***your custom domain***
  5. Repeat these tasks for all 4 users. **Close** the **Active Directory Users and Computers** window

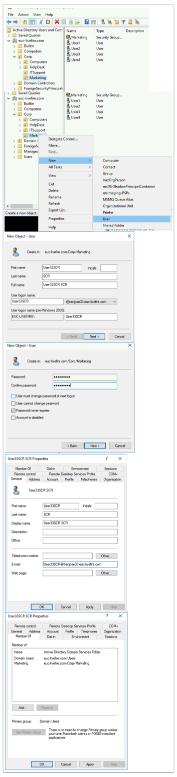


Part 5. Configuration of a Custom Test Account

In this part you'll be creating your test user for the salesforce lab.

1. Open **Active Directory User & Computers**. Expand the **EUC-livefire.com** domain, expand the **Corp OU** and expand the **Marketing OU**
2. On the **Marketing OU** select and right-click the **Marketing OU** and select **New User**. Fill in the unique user details,
   - **First Name:** User xxxxx {your student number + {the first letter of your city and country abbreviation}} eg {for San jose, Costa Rica User33SCR}
   - **Last Name:** {the first letter of your city and country abbreviation} eg. SCR
   - **Username:** FirstName@customdomain.euc-livefire.com, eg. User33SCR@Sanjose33.euc-livefire.com}

- Select **Next**
- In the **New Object - User**, type your **password** **VMware1!**
- select the **Password never expires** **checkbox**, select **Next,** select **Finish**
- Select your **custom user** and select and go to **properties**, on the **General** Tab type in the **email address** eg.**user35AK@utrecht35.euc-livefire.com**
- Select the **Member Of t**ab select **Add,** in the **Enter the object names** box type **Marketing** and select **Check Names,** select **OK**, select` **OK**



Name	Type	Description
Marketing	Security Group...	
User1	User	
User2	User	
User3	User	
User4	User	

New Object - User

Create in: euc-livefire.com/Corp/Marketing

First name: User33SCR Initials:

Last name: SCR

Full name: User33SCR SCR

User logon name: User33SCR @sanjose33.euc-livefire.com

User logon name (pre-Windows 2000): EUC-LIVEFIRE\ User33SCR

New Object - User

Create in: euc-livefire.com/Corp/Marketing

Password: ••••••••

Confirm password: ••••••••

□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

User33SCR SCR Properties

User33SCR SCR

First name: User33SCR Initials:

Last name: SCR

Display name: User33SCR SCR

Description:

Office:

Telephone number:

E-mail: User33SCR@Sanjose33.euc-livefire.com

Web page:

User33SCR SCR Properties

Member of:

Name	Active Directory Domain Services Folder
Domain Users	euc-livefire.com/Users
Marketing	euc-livefire.com/Corp/Marketing

Primary group: Domain Users

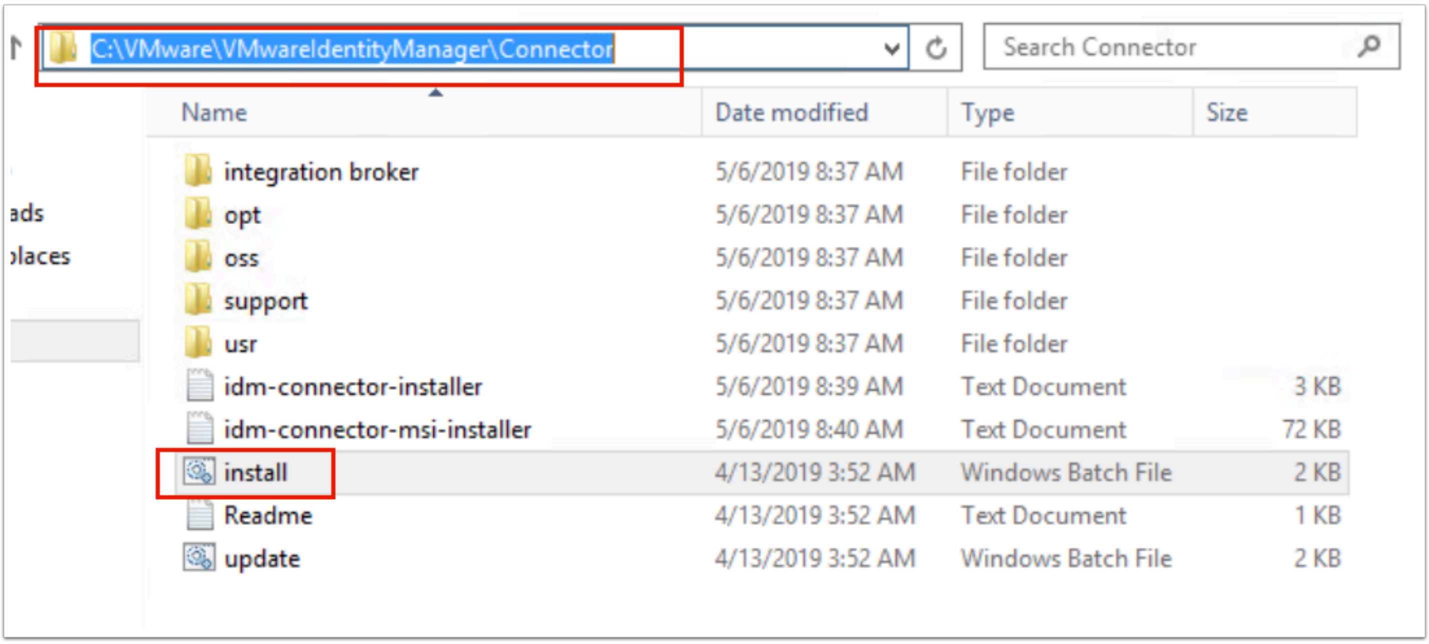
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Configuring the Workspace ONE Access Connector

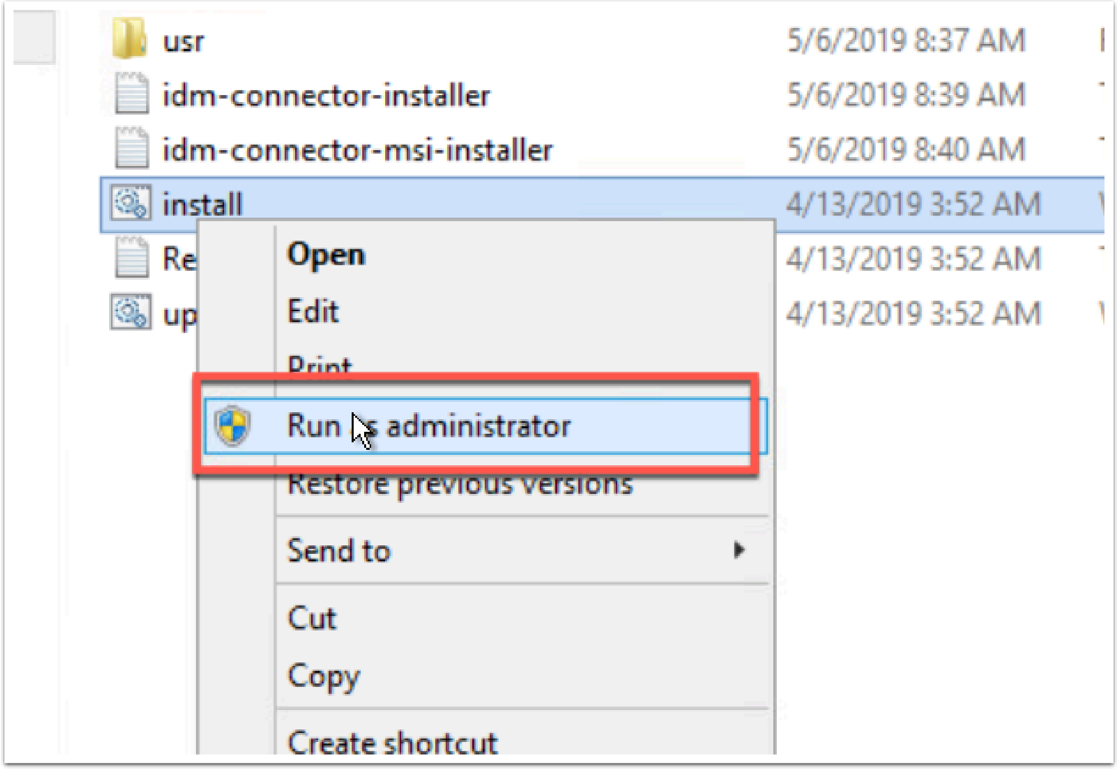
Part 1. Configuring the Workspace ONE Access Connector

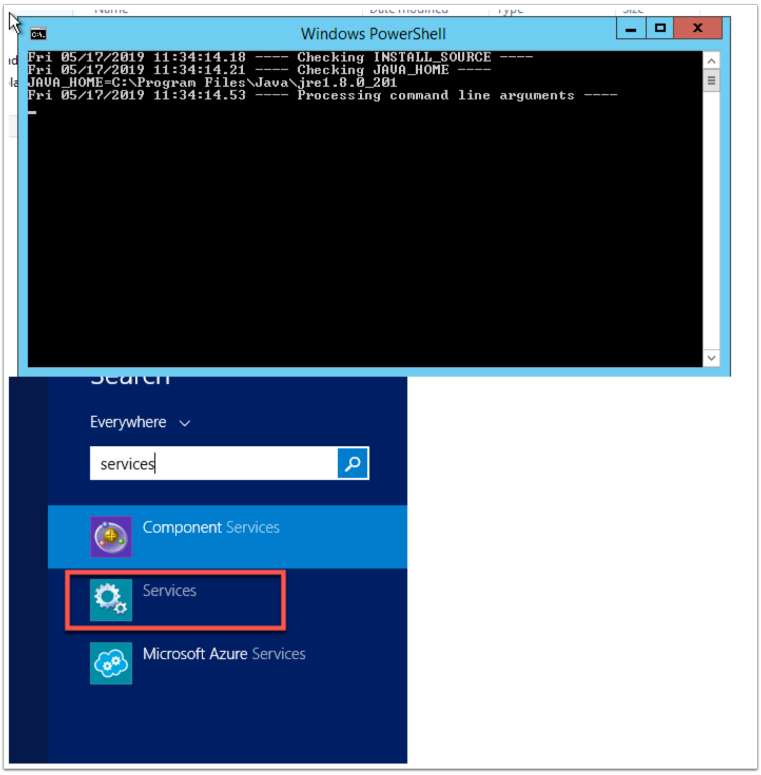
1. We have pre-installed the Workspace ONE Access Connector for you in the Lab environment. However since we have cloned the machine the connector is in an idle state and needs to be re-initiated.

- Log into your ControlCenter2 server with username **administrator@euc-livefire.com** and password **VMware1!**
    1. On your **ControlCenter2** server desktop select your **Remote Desktops** folder and select and launch your **WS1-Connector.RDP** shortcut.
    2. When prompted log in as username **administrator@euc-livefire.com** with the password **VMware1!**
    3. On the **WS1-Connector** server open the **File Explorer** to the following path **C:\VMware\VMwareidentityManager\Connector**
    4. Right Click the **install.bat** file and click **Run as Administrator**
    5. This will launch a PowerShell window that will clear out the state of the connector. Wait till the Powershell Window closes which confirms it has run successfully.
    6. Open **services.msc** and **start** the **VMware IDM Connector** service
    7. Wait for a few minutes till all the services have launched and move on to the next part of the lab.

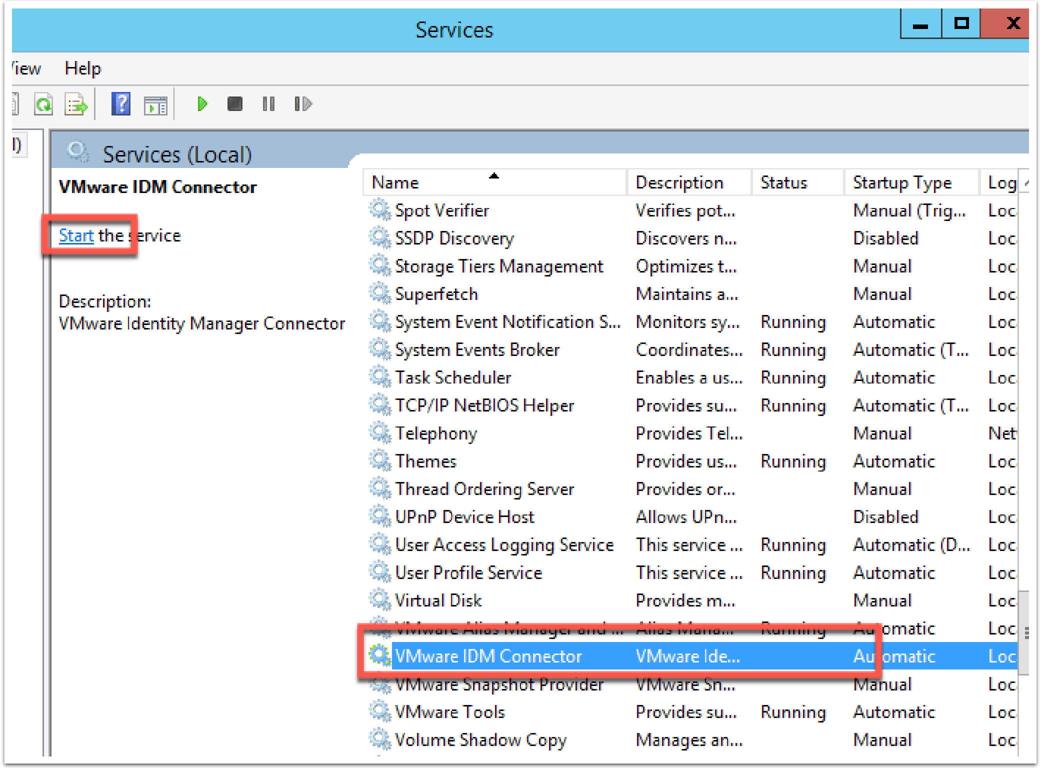


Name	Date modified	Type	Size
integration broker	5/6/2019 8:37 AM	File folder	
opt	5/6/2019 8:37 AM	File folder	
oss	5/6/2019 8:37 AM	File folder	
support	5/6/2019 8:37 AM	File folder	
usr	5/6/2019 8:37 AM	File folder	
idm-connector-installer	5/6/2019 8:39 AM	Text Document	3 KB
idm-connector-msi-installer	5/6/2019 8:40 AM	Text Document	72 KB
install	4/13/2019 3:52 AM	Windows Batch File	2 KB
Readme	4/13/2019 3:52 AM	Text Document	1 KB
update	4/13/2019 3:52 AM	Windows Batch File	2 KB





```
Fri 05/17/2019 11:34:14.18 ---- Checking INSTALL_SOURCE ----
Fri 05/17/2019 11:34:14.21 ---- Checking JAVA_HOME ----
JAVA_HOME=C:\Program Files\Java\jre1.8.0_201
Fri 05/17/2019 11:34:14.53 ---- Processing command line arguments ----
```



VMware IDM Connector

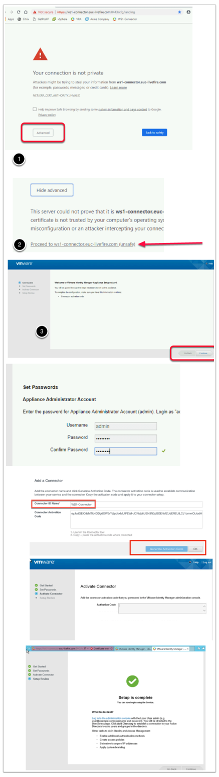
Start the service

Description:
VMware Identity Manager Connector

Name	Description	Status	Startup Type	Log
Spot Verifier	Verifies pot...		Manual (Trig...	Loc
SSDP Discovery	Discovers n...		Disabled	Loc
Storage Tiers Management	Optimizes t...		Manual	Loc
Superfetch	Maintains a...		Manual	Loc
System Event Notification S...	Monitors sy...	Running	Automatic	Loc
System Events Broker	Coordinates...	Running	Automatic (T...	Loc
Task Scheduler	Enables a us...	Running	Automatic	Loc
TCP/IP NetBIOS Helper	Provides su...	Running	Automatic (T...	Loc
Telephony	Provides Tel...		Manual	Net
Themes	Provides us...	Running	Automatic	Loc
Thread Ordering Server	Provides or...		Manual	Loc
UPnP Device Host	Allows UPn...		Disabled	Loc
User Access Logging Service	This service ...	Running	Automatic (D...	Loc
User Profile Service	This service ...	Running	Automatic	Loc
Virtual Disk	Provides m...		Manual	Loc
VMware Alias Manager and ...	Alias Mana...	Running	Automatic	Loc
VMware IDM Connector	VMware Ide...		Automatic	Loc
VMware Snapshot Provider	VMware Sn...		Manual	Loc
VMware Tools	Provides su...	Running	Automatic	Loc
Volume Shadow Copy	Manages an...		Manual	Loc

1. Our objective is to associate our on-premise connector instance with our SaaS instance of Workspace ONE Access.

- Log on to your **Control Center2** server in your Lab use your **Google Chrome browser**.
  1. On your chrome select the **WS1-connnector** shortcut or type **https://ws1-connector.euc-livefire.com:8443/cfg in the address bar**
  2. On the Your Connection is not private page, select **Advanced** and select **Proceed to ws1-connector.euc-livefire.comue.**
  3. On the **Get Started** Window select **Continue**
  4. In the **Set Passwords** section next to **Username** type **admin** next to **password** type **VMware1!** next to **Confirm Password** type **VMware1!** select **Continue** at the bottom of the page.
  5. On your browser, open up a **second Tab**, navigate to your unique **Workspace ONE Access Tenant** and if you have not done so login as **Administrator** with your **unique password**, that your received in your e-mail login
  6. Navigate to **Identity & Access Management** **>** **Setup** **>** **Connectors** Select **Add Connector**
  7. Next to **Connector ID Name:** type **WS1-Connector.** Next select **Generate Activation Code** . Next **copy** this code
  8. **Revert back** to your **WS1-Connector Server** setup: On the **activate connector page** **Paste** this code into the **Activation Code** box of your **Connector configuration** setup, select **Continue**
  9. You should get a **setup is complete** page inside the Workspace ONE Access Console.



Your connection is not private

Attackers might be trying to steal your information from **ws1-connector.euc-livefire.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **ws1-connector.euc-** certificate is not trusted by your computer's operating sy misconfiguration or an attacker intercepting your connec

Proceed to ws1-connector.euc-livefire.com (unsafe)

Welcome to VMware Identity Manager Appliance Setup wizard.

You will be guided through the steps necessary to set up the appliance.

To complete the configuration, make sure you have this information available

- Connector activation code

Set Passwords

Appliance Administrator Account

Enter the password for Appliance Administrator Account (admin). Login as "a

Username: admin
Password: ••••••••
Confirm Password: ••••••••

Add a Connector

Add the connector name and click Generate Activation Code. The connector activation code is used to establish communication between your service and the connector. Copy the activation code and apply it to your connector setup.

Connector ID Name*: WS1-Connector

Connector Activation Code: eyJvdGEiOiIzMTU4ODg5OW9rYjJpbloMUlFEWHJCNVp6UEN3N3pSOEhMZUdEREU... LCJ1cmwiOiJodH

1. Launch the Connector tool
2. Copy + paste the Activation code where prompted

Activate Connector

Add the connector activation code that you generated in the VMware Identity Manager administration console.

Activation Code:

Setup is complete

You can now begin using the Service.

What to do next?

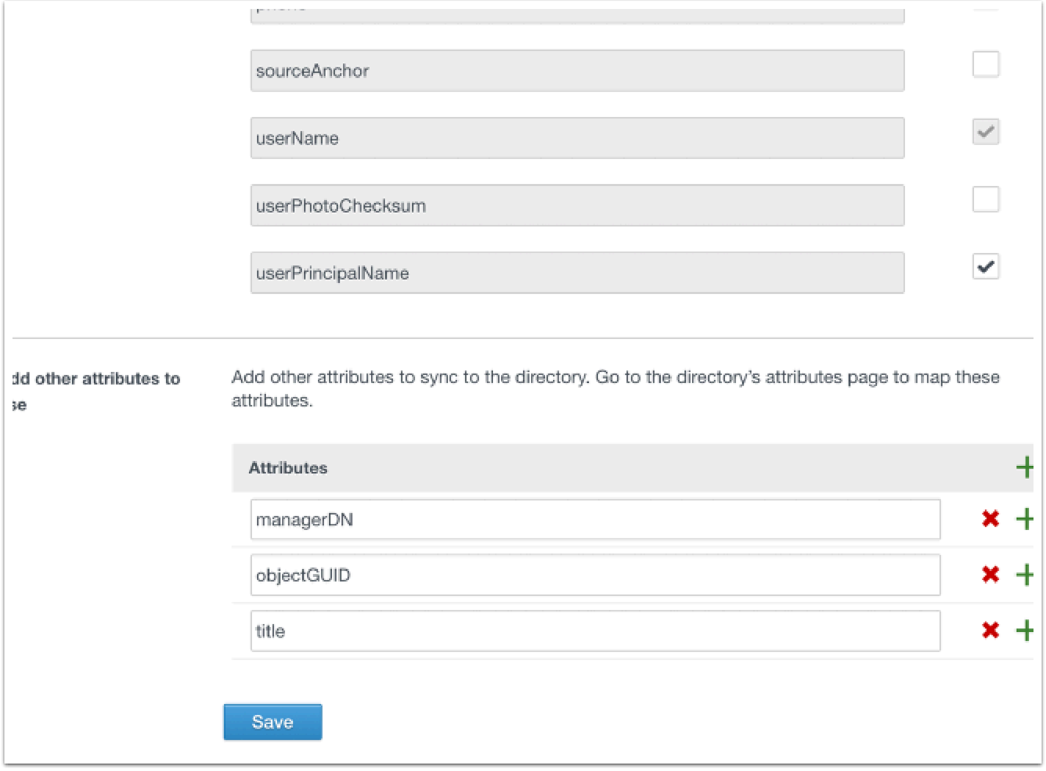
Log in to the administration console with the Local User admin (e.g. user@example.com) username and password. You will be directed to the Directories page. Click **Add Directory** to establish a connection to your Active Directory to sync users and groups to the directory.

Other tasks to do in Identity and Access Management

- Enable additional authentication methods
- Create access policies
- Set network range of IP addresses
- Apply custom branding

2. We will now configure and synchronise Active Directory to the Workspace ONE Access server using the external connector.

- First we will configure the Attributes. Note! Every organisation will need to research their requirements when deciding whether or not to set attributes to **required.** For specific applications where this needs to be considered, if the associated user object does not have the attribute, authentication might fail.
  1. Navigate to **Identity & Access Management** > **Setup** > **User Attributes**
     Notice the attributes that are available and the option available to set these to **Required**.
     IMPORTANT NOTE: The attributes set to required **cannot** be changed after a directory sync has taken place.
  2. Set the attribute **distinguishedName** and **userPrincipalName** to Required
  3. Under Attributes to the right select the **Green Plus** (+) Add the following additional attributes (case sensitive) :
     - **objectGUID**
     - **title**
     - **managerDN**
  4. Select **Save**



sourceAnchor	☐
userName	☑
userPhotoChecksum	☐
userPrincipalName	☑

dd other attributes to se

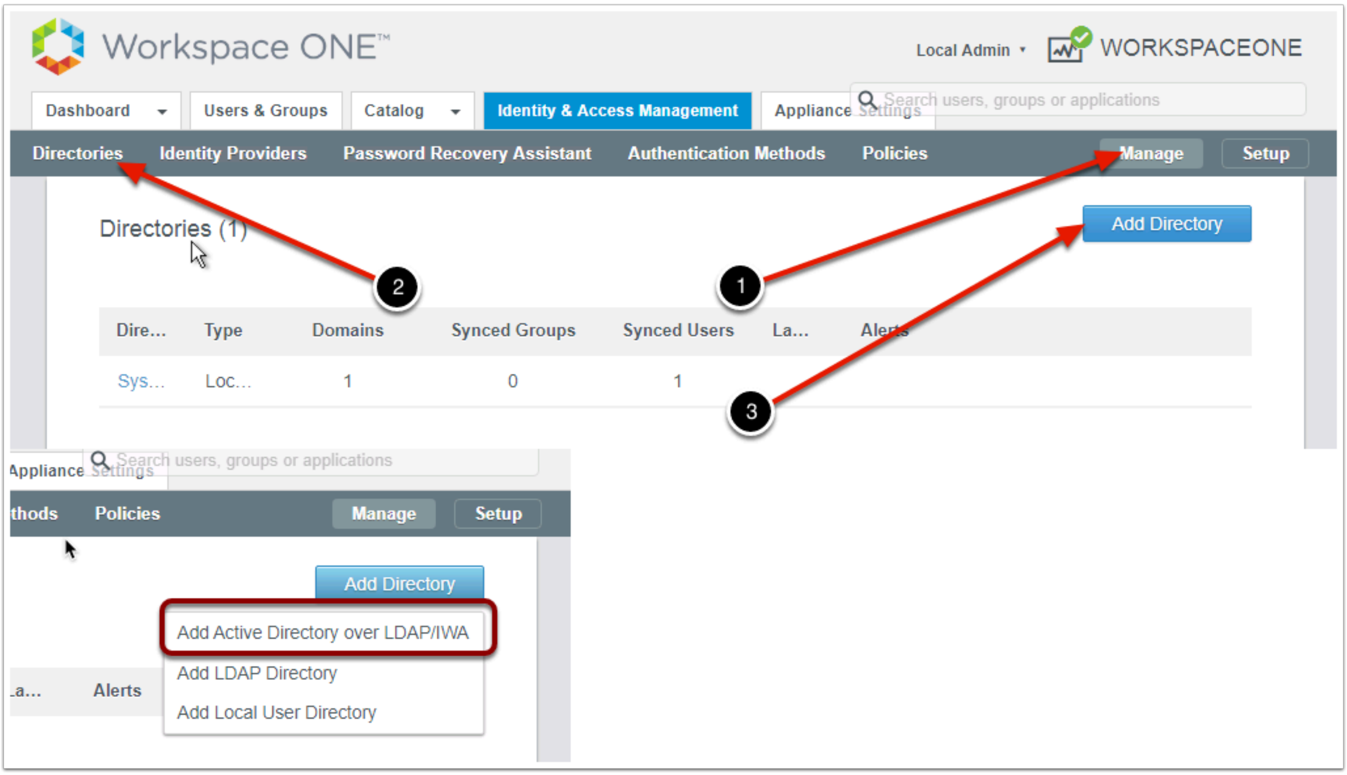
Add other attributes to sync to the directory. Go to the directory's attributes page to map these attributes.

Attributes	
managerDN	✖ +
objectGUID	✖ +
title	✖ +

Save

3. Configure our AD-sync configuration with Workspace ONE Access.

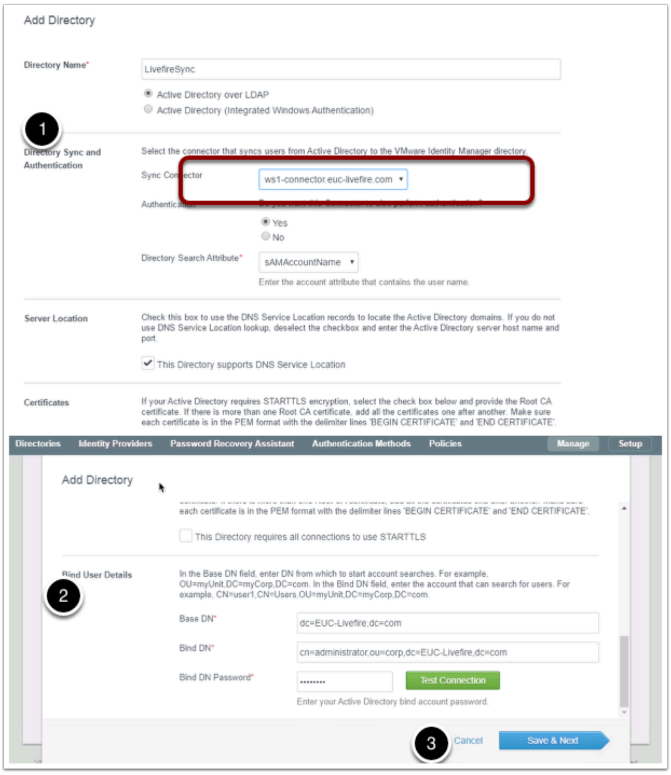
1. To the right of the screen select **Manage**, select **Directories**
2. Select **Add Directory** > **Add Active Directory over LDAP/IWA**



Dire...	Type	Domains	Synced Groups	Synced Users	La...	Alerts
Sys...	Loc...	1	0	1		

4. Configure our AD-sync configuration with Workspace ONE Access....continued

- In **Add Directory** Page, configure the following
  1. **Directory Name:** LivefireSync
  2. Ensure the **Active Directory over LDAP** **radio button** is selected
  3. The **Sync Connector** select the external connector **ws1-connector.euc-livefire.com**
  4. **Directory Search Attribute**: **sAMAccountName**
  5. **Base DN:** **dc=EUC-Livefire,dc=com**
  6. **Bind DN:** **cn=administrator,ou=corp,dc=EUC-Livefire,dc=com**
  7. **Bind DN Password:** **VMware1!**
  8. Select Test Connection
  9. Select **Save & Next**



Add Directory

Directory Name* LivefireSync

● Active Directory over LDAP
○ Active Directory (Integrated Windows Authentication)

Directory Sync and Authentication

Select the connector that syncs users from Active Directory to the VMware Identity Manager directory.

Sync Connector ws1-connector.euc-livefire.com

Authentication
● Yes
○ No

Directory Search Attribute* sAMAccountName

Enter the account attribute that contains the user name.

Server Location

Check this box to use the DNS Service Location records to locate the Active Directory domains. If you do not use DNS Service Location lookup, deselect the checkbox and enter the Active Directory server host name and port.

☑ This Directory supports DNS Service Location

Certificates

If your Active Directory requires STARTTLS encryption, select the check box below and provide the Root CA certificate. If there is more than one Root CA certificate, add all the certificates one after another. Make sure each certificate is in the PEM format with the delimiter lines 'BEGIN CERTIFICATE' and 'END CERTIFICATE'.

Add Directory

each certificate is in the PEM format with the delimiter lines 'BEGIN CERTIFICATE' and 'END CERTIFICATE'.

☐ This Directory requires all connections to use STARTTLS

Bind User Details

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

Base DN* dc=EUC-Livefire,dc=com

Bind DN* cn=administrator,ou=corp,dc=EUC-Livefire,dc=com

Bind DN Password* ••••••••

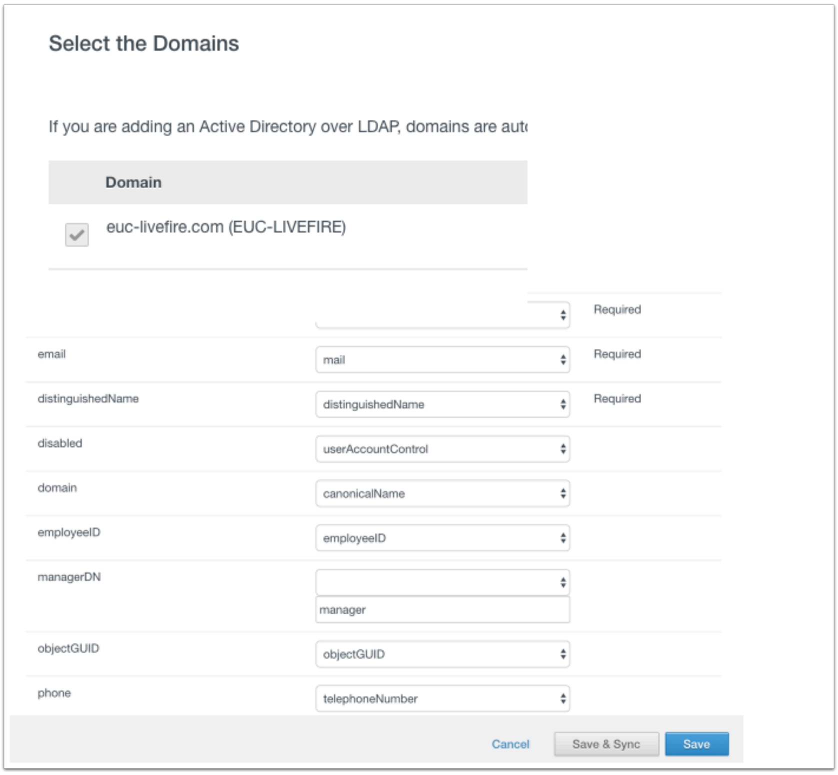
Enter your Active Directory bind account password.

5.

- Configure our AD-sync configuration with Workspace ONE Access....continued
  1. On the **Select the Domains** page, select **Next.** **euc-livefire.com** should be discovered.
  2. On the **Map User Attribute** page scroll down to **objectGuid** and select the **drop down** arrow select **objectGUID.**
     Since this is the attribute we setup earlier in User Attributes we will also need to map it to an AD attribute.
  3. Next to **managerDN** select ***custom input*** and type **manager** in the dropdown
  4. Next to **title** select **title** in the dropdown
  5. Select **Next**

Note of interest

From version **Workspace ONE Access 1903** of , an attribute has been added which is **sourceanchor** set this also to **ObjectGUID**. Sourceanchor is the attribute often used for when federating Azure. (Note: Some large customers may decide to use an alternative value such as ms-ds-consistenctguid for this attribute)



Select the Domains

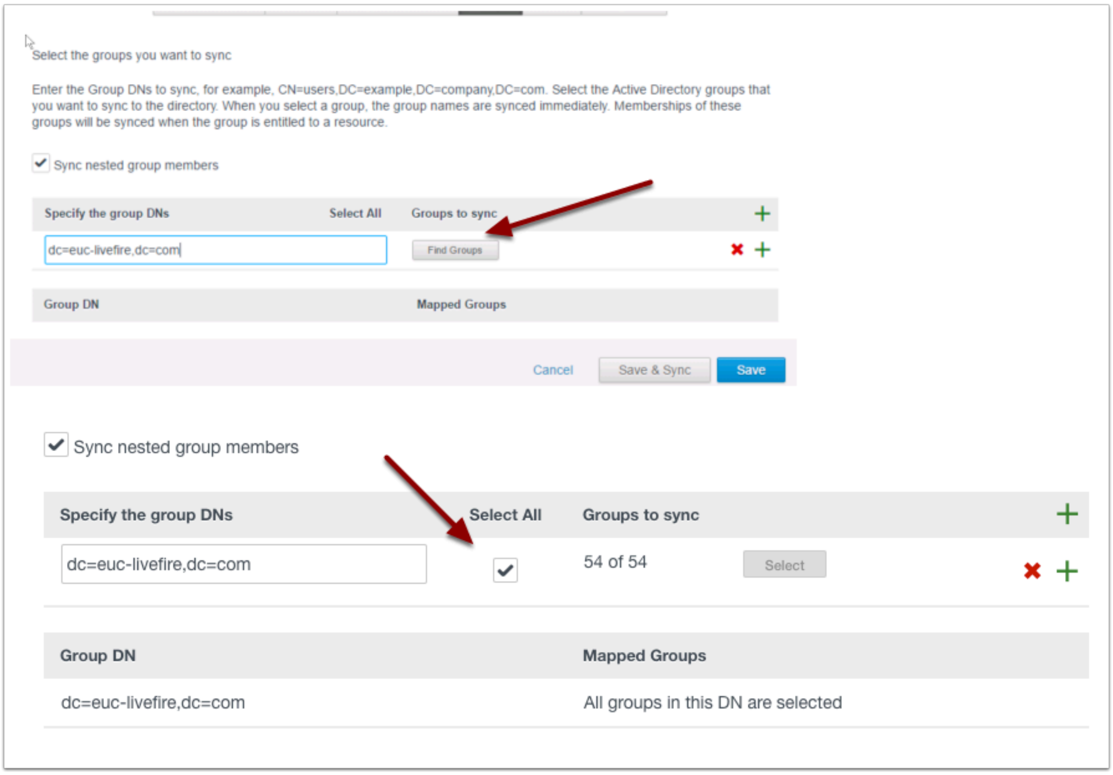
If you are adding an Active Directory over LDAP, domains are aut

	Domain
☑	euc-livefire.com (EUC-LIVEFIRE)

		Required
email	mail	Required
distinguishedName	distinguishedName	Required
disabled	userAccountControl	
domain	canonicalName	
employeeID	employeeID	
managerDN	 manager	
objectGUID	objectGUID	
phone	telephoneNumber	

6.

- Configure our AD-sync configuration with Workspace ONE Access....continued
  1. On the **Select the Groups you want to sync** page, select the green plus (+) to the right of the page,
  2. Under **Specify the group DNs** type the following **dc=euc-livefire,dc=com** next to the distinguished name you added, select Find Groups then the **Select All** check box
  3. select **Next**.



Select the groups you want to sync

Enter the Group DNs to sync, for example, CN=users,DC=example,DC=company,DC=com. Select the Active Directory groups that you want to sync to the directory. When you select a group, the group names are synced immediately. Memberships of these groups will be synced when the group is entitled to a resource.

☑ Sync nested group members

Specify the group DNs	Select All	Groups to sync
dc=euc-livefire,dc=com		Find Groups

Group DN	Mapped Groups

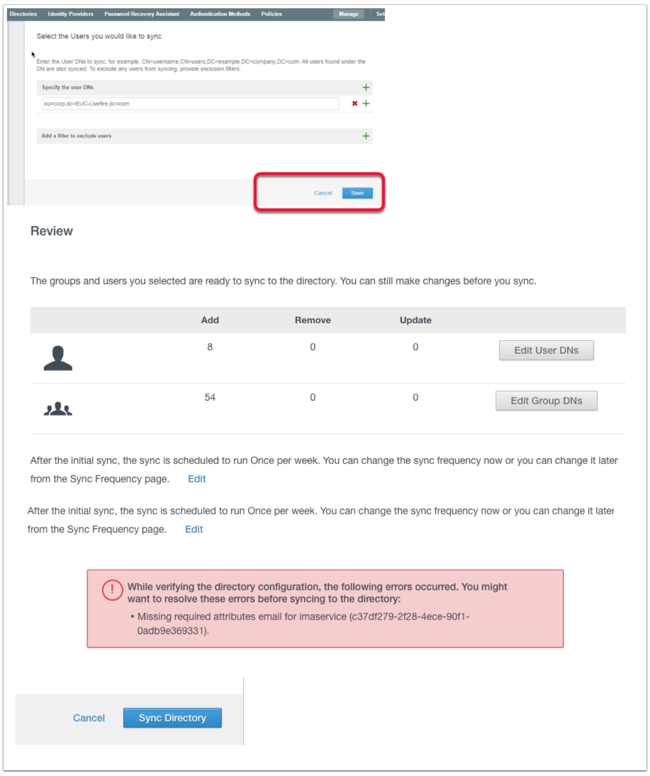
☑ Sync nested group members

Specify the group DNs	Select All	Groups to sync
dc=euc-livefire,dc=com	☑	54 of 54

Group DN	Mapped Groups
dc=euc-livefire,dc=com	All groups in this DN are selected

7.

- Configure our AD-sync configuration with Workspace ONE Access....continued
  1. On the **Select the Users you would like to sync page,** under **specify the user DNs** type **ou=corp,dc=EUC-Livefire,dc=com**
  2. Select **Next**, notice the objects to sync in the Review page.
  3. There may be an error, "Missing required attributes email for imaservice" Disregard this error. The sync will stil work.
  4. Select **Sync Directory**



Select the Users you would like to sync

Enter the User DNs to sync, for example, CN=username,CN=users,DC=example,DC=company,DC=com. All users found under the DN are also synced. To exclude any users from syncing, provide exclusion filters.

Specify the user DNs

ou=corp,dc=EUC-Livefire,dc=com

Add a filter to exclude users

Review

The groups and users you selected are ready to sync to the directory. You can still make changes before you sync.

	Add	Remove	Update	
👤	8	0	0	Edit User DNs
👥	54	0	0	Edit Group DNs

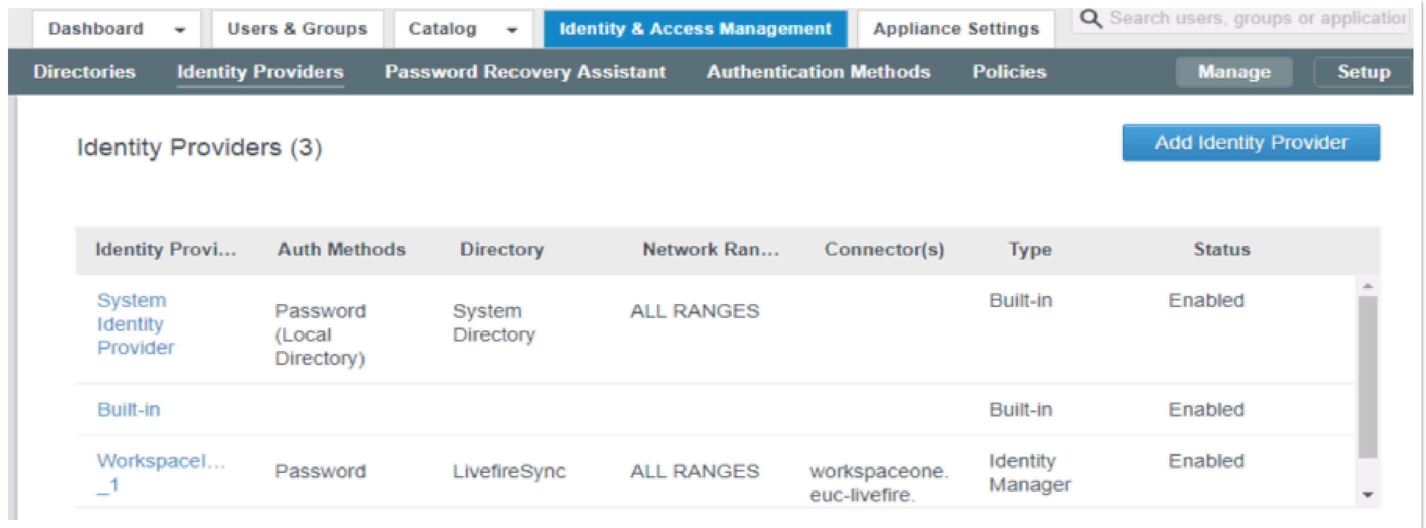
After the initial sync, the sync is scheduled to run Once per week. You can change the sync frequency now or you can change it later from the Sync Frequency page. Edit

After the initial sync, the sync is scheduled to run Once per week. You can change the sync frequency now or you can change it later from the Sync Frequency page. Edit

While verifying the directory configuration, the following errors occurred. You might want to resolve these errors before syncing to the directory:
- Missing required attributes email for imaservice (c37df279-2f28-4ece-90f1-0adb9e369331).

8. Configuring the Built-in IDP in Workspace ONE Access

- Navigate to and select **Identity & Access Management** > **Manage**, select **Identity Providers**. Notice you now have an additional Identity Provider which is a Workspace IDP called **WorkspaceIDP_1xxx** which is associated with the LiveFireSync directory we just created above. This is an automatic process whereby when the built in connector is associated with Active Directory this Identity Provider gets created.



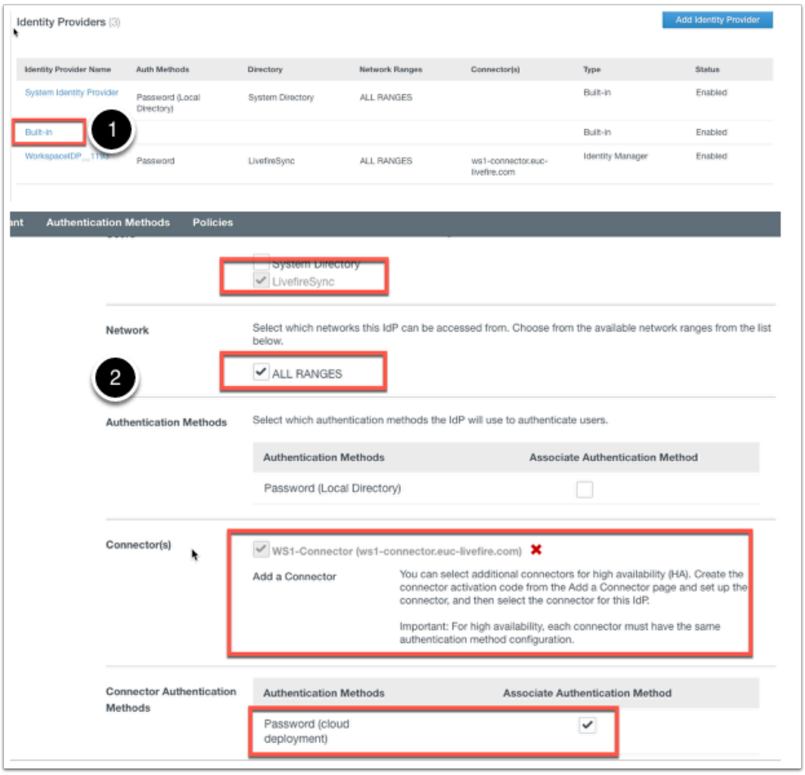
Identity Providers (3)

Identity Provi...	Auth Methods	Directory	Network Ran...	Connector(s)	Type	Status
System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Enabled
Built-in					Built-in	Enabled
WorkspaceI... _1	Password	LivefireSync	ALL RANGES	workspaceone.euc-livefire.	Identity Manager	Enabled

9. Configuring the Built-in IDP in Workspace ONE Access...continued

- Let's associate the Built-In iDP with the AD and the external connector to ensure **Password (Cloud Deployment)** can be used as an authentication method.

1. Select **Built-In.**
2. In the **Built-in IDP** windows select the following:
    1. Select **LivefireSync** under Users
    2. **All Ranges** under Network
    3. **Add** the **WS1-Connector.euc-livefire.com** to the connector section
        1. Click **Add Connector** to confirm
    4. Select **Password (Cloud Deployment)** **checkbox**
    5. Select **Save** at the bottom of the page.



Identity Providers (3)

Identity Provider Name	Auth Methods	Directory	Network Ranges	Connector(s)	Type	Status
System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Enabled
Built-in					Built-in	Enabled
WorkspaceIDP__1190	Password	LivefireSync	ALL RANGES	ws1-connector.euc-livefire.com	Identity Manager	Enabled

☐ System Directory
☑ LivefireSync

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

☑ ALL RANGES

Authentication Methods: Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Password (Local Directory)	☐

Connector(s): ☑ WS1-Connector (ws1-connector.euc-livefire.com) ✖

Add a Connector: You can select additional connectors for high availability (HA). Create the connector activation code from the Add a Connector page and set up the connector, and then select the connector for this IdP.

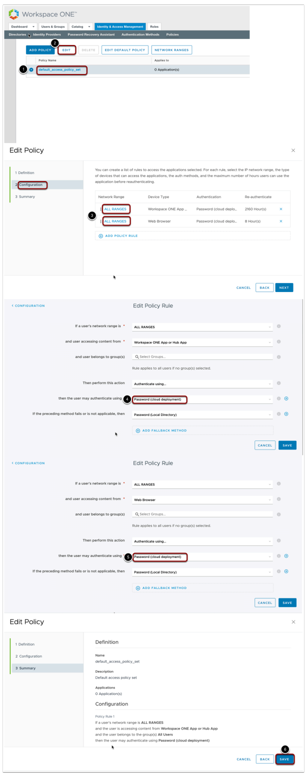
Important: For high availability, each connector must have the same authentication method configuration.

Connector Authentication Methods:

Authentication Methods	Associate Authentication Method
Password (cloud deployment)	☑

10. Configuring the Built-in IDP in Workspace ONE Access...continued

- We need to ensure that our default access policy has **Password (Cloud Deployment)** set as the authentication method for enrollment to work. Note, Workspace ONE enrollment uses this access policy.
    1. Navigate to **Identity & Access Management** > **Manage** > **Policies .** Select **dafault_access_policy_set** and select **EDIT** (this will edit the default Access Policy Set)
    2. Select **Configuration** on the left navigation and **Workspace One App Policy** and select **Password (Cloud Deployment)** as the first authentication form. Select **SAVE** at the bottom of the page.
        1. **NOTE**: Be sure to leave Password (Local Directory) as the fallback method as seen in the screen shot below.
    3. Now Select the **Web Browser** and do the same by changing the primary authentication method to **Password (Cloud Deployment)** and select **SAVE** at the bottom of the page.
        1. **NOTE**: Be sure to leave Password (Local Directory) as the fallback method
    4. Select **NEXT** on the **Policy Page** and **SAVE** on the final page of the wizard.



Policy Name	Applies to
default_access_policy_set	0 Application(s)

Edit Policy

1 Definition
2 Configuration
3 Summary

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
ALL RANGES	Workspace ONE App ...	Password (cloud deplo...	2160 Hour(s)
ALL RANGES	Web Browser	Password (cloud deplo...	8 Hour(s)

Edit Policy Rule

If a user's network range is * ALL RANGES
and user accessing content from * Workspace ONE App or Hub App
and user belongs to group(s) Select Groups...
Rule applies to all users if no group(s) selected.
Then perform this action Authenticate using...
then the user may authenticate using Password (cloud deployment)
If the preceding method fails or is not applicable, then Password (Local Directory)

Edit Policy Rule

If a user's network range is * ALL RANGES
and user accessing content from * Web Browser
and user belongs to group(s) Select Groups...
Rule applies to all users if no group(s) selected.
Then perform this action Authenticate using...
then the user may authenticate using Password (cloud deployment)
If the preceding method fails or is not applicable, then Password (Local Directory)

Edit Policy

Definition

Name
default_access_policy_set

Description
Default access policy set

Applications
0 Application(s)

Configuration

Policy Rule 1
If a user's network range is **ALL RANGES**
and the user is accessing content from **Workspace ONE App or Hub App**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **Password (cloud deployment)**

This section of the lab is completed. We will not install and configure the ACC as a later lab will look at SCIM provisioning users in the WorkspaceOne UEM.

Workspace ONE Access and Workspace ONE UEM Integration

Part 1: Workspace ONE UEM integration with Workspace ONE Access

In this section we will do the Workspace ONE UEM side of the configuration.

1. Switch back to the Workspace ONE UEM Admin console.

- Be sure to make these settings at the **company organisation group**, then navigate to Groups and Settings > All Settings > System > Enterprise Integration> VMware Identity Manager > Configuration

2. Click **CONFIGURE** under ***Server*** settings

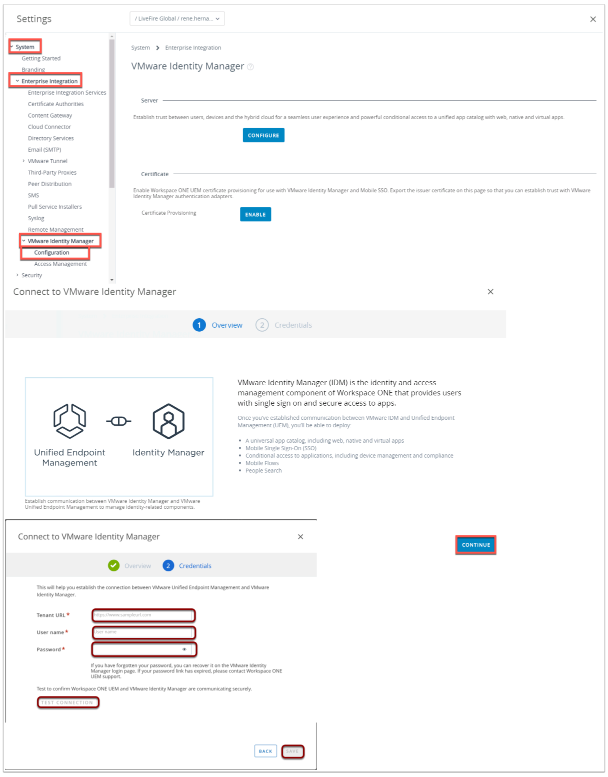
3. Click **CONTINUE**

On the Connect to **VMware Identity Manager** window enter the following:

1. **Tenant URL**: **Your Tenant** eg. https://aw-euclivefiret3rn.vidmpreview.com
2. **User Name: Your Tenant Admin account**
3. **Password: Your Tenant Password**

Select **TEST CONNECTION** to ensure Tenant configuration has been entered successfully.

4. Select **SAVE** and close the settings window



Establish trust between users, devices and the hybrid cloud for a seamless user experience and powerful conditional access to a unified app catalog with web, native and virtual apps.

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

VMware Identity Manager (IDM) is the identity and access management component of Workspace ONE that provides users with single sign on and secure access to apps.

Once you've established communication between VMware IDM and Unified Endpoint Management (UEM), you'll be able to deploy:

- A universal app catalog, including web, native and virtual apps
- Mobile Single Sign-On (SSO)
- Conditional access to applications, including device management and compliance
- Mobile Flows
- People Search

Establish communication between VMware Identity Manager and VMware Unified Endpoint Management to manage identity-related components.

This will help you establish the connection between VMware Unified Endpoint Management and VMware Identity Manager.

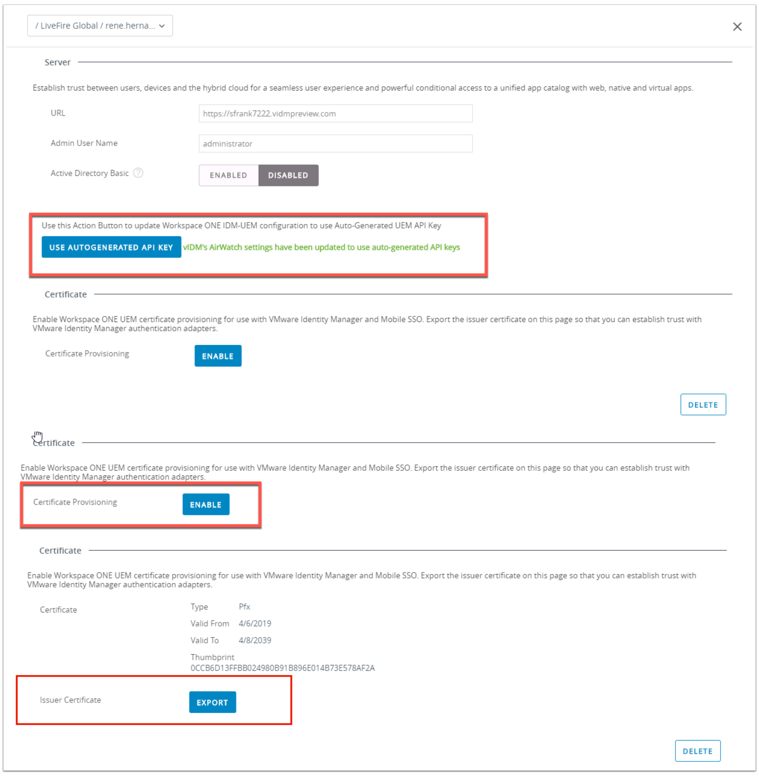
If you have forgotten your password, you can recover it on the VMware Identity Manager login page. If your password link has expired, please contact Workspace ONE UEM support.

Test to confirm Workspace ONE UEM and VMware Identity Manager are communicating securely.

1. Click "**Use Autogenerated API KEY**"

2. In the **Certificate** section, next to **Certificate Provisioning** click **ENABLE** - we will use this certificate later for Single-Sign-On with Windows 10

3. Now click **EXPORT** - we will use this certificate in a later exercise. leave this window open for the next part.



Server

Establish trust between users, devices and the hybrid cloud for a seamless user experience and powerful conditional access to a unified app catalog with web, native and virtual apps.

URL: https://sfrank7222.vidmpreview.com

Admin User Name: administrator

Active Directory Basic: DISABLED

Use this Action Button to update Workspace ONE IDM-UEM configuration to use Auto-Generated UEM API Key

vIDM's AirWatch settings have been updated to use auto-generated API keys

Certificate

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

Certificate Provisioning

Certificate

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

Certificate Provisioning

Certificate

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

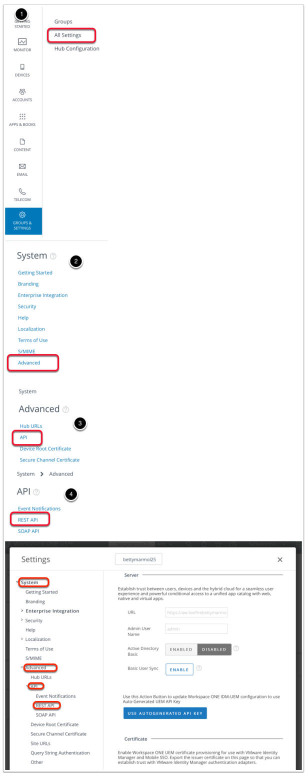
Certificate
Type Pfx
Valid From 4/6/2019
Valid To 4/8/2039
Thumbprint
0CCB6D13FFBB024980B91B896E014B73E578AF2A

Issuer Certificate

Part 1B. Creating a custom REST API Account

- We will configure this REST API Account in preparation for Part 2 of this Lab

1. If you closed the settings windows in the previous part navigate in the Workspace ONE UEM Admin Console to **Groups & Settings** > **All Settings**
2. Under **System** select **Advanced**
3. Under **Advanced** select **API**
4. Under **API** select **REST API**



Establish trust between users, devices and the hybrid cloud for a seamless user experience and powerful conditional access to a unified app catalog with web, native and virtual apps.

URL: https://aw-livefirebettymarmo

Admin User Name: admin

Active Directory Basic: ENABLED [✓ DISABLED]

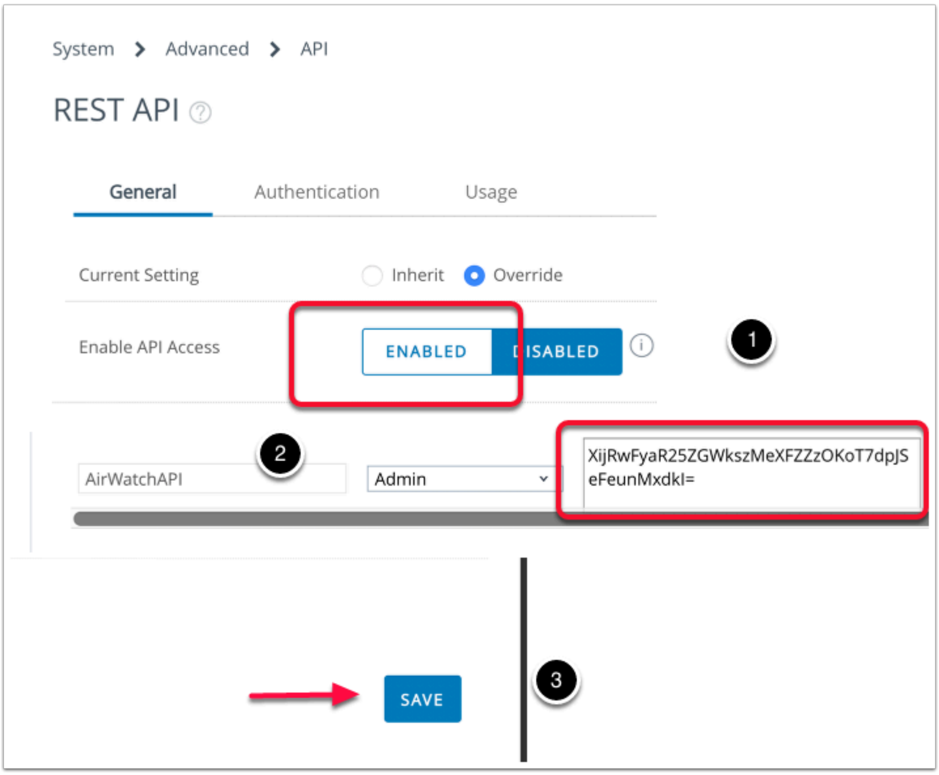
Basic User Sync

Use this Action Button to update Workspace ONE IDM-UEM configuration to use Auto-Generated UEM API Key

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

2. Part 1B. continued..

- Creating a custom REST API Account
  1. Under **REST API** under **General** next to **Current Setting** select the **Override** **radio button**. Next to **ENABLE API Access** ensure that **ENABLED** is selected.
  2. You will notice an **AirWatchAPI Admin** is automatically generated. **Copy the API Token and save to a text editor**
  3. Select **SAVE**
  4. After the settings have been save successfully select the **X** in the right corner to close the window



System > Advanced > API

REST API

General | Authentication | Usage

Current Setting ○ Inherit ● Override

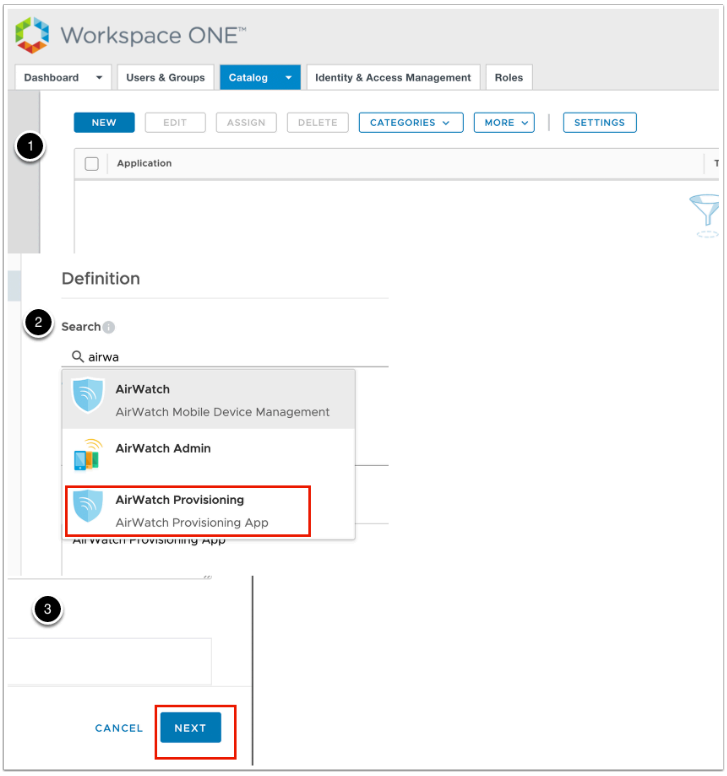
Enable API Access ENABLED DISABLED

AirWatchAPI | Admin | XijRwFyaR25ZGWkszMeXFZZzOKoT7dpJSeFeunMxdkI=

Part 2: Configuring the AirWatch Provisioning Adaptor in Workspace ONE Access for Workspace ONE UEM

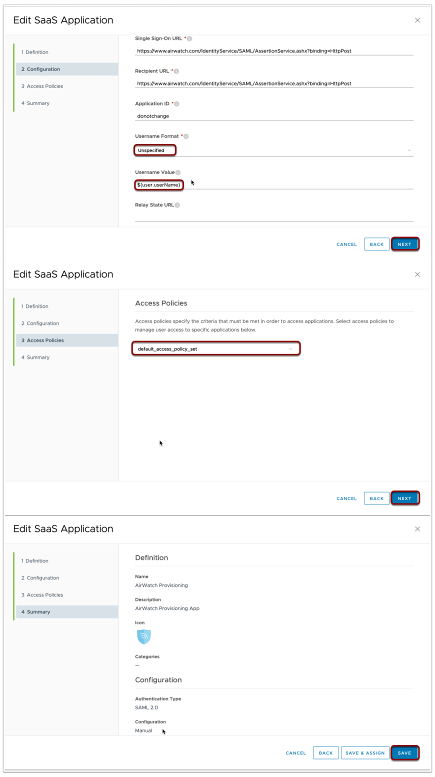
1. AirWatch Provisioning Adaptor

- This first section will be done in the **Workspace ONE Access** SaaS console
  1. In the **Admin Console** select the **Catalog** tab and select **NEW**
  2. On the **New Saas Application**, next to section **1.Definition** under **search** type **AirWa** and you should see **Airwatch Provisioning**. Select **AirWatch Provisioning**
  3. Select **Next**



2. AirWatch Provisioning Adaptor

- In the NEW Saas Application wizard continued...
  1. In Section **2.Configuration** ensure the following is configured:-
     - Under **Username Format** ensure **Unspecified** is selected, Under **Username Value** ensure ${user.userName} is selected and click **NEXT**
  2. In Section **3. Access Policies** accept the default and select **NEXT**
  3. In Section **4.Summary** select **SAVE**



Edit SaaS Application

Single Sign-On URL *
https://www.airwatch.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost

Recipient URL *
https://www.airwatch.com/IdentityService/SAML/AssertionService.ashx?binding=HttpPost

Application ID *
donotchange

Username Format *
Unspecified

Username Value
${user.userName}

Relay State URL

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

Edit SaaS Application

Definition

Name
AirWatch Provisioning

Description
AirWatch Provisioning App

Icon

Categories
—

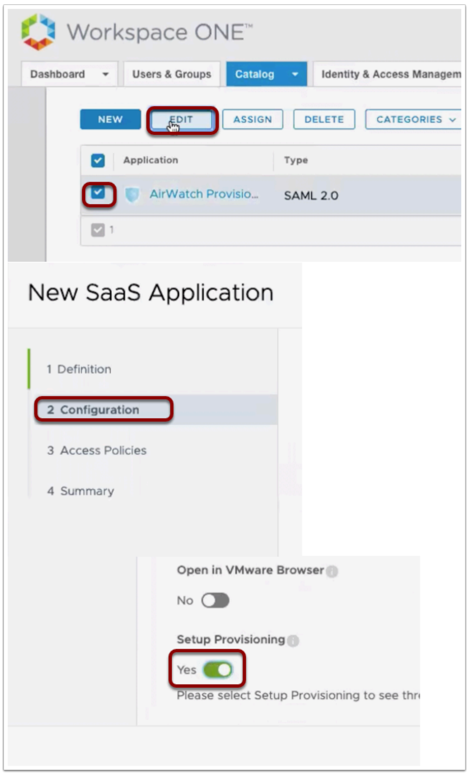
Configuration

Authentication Type
SAML 2.0

Configuration
Manual

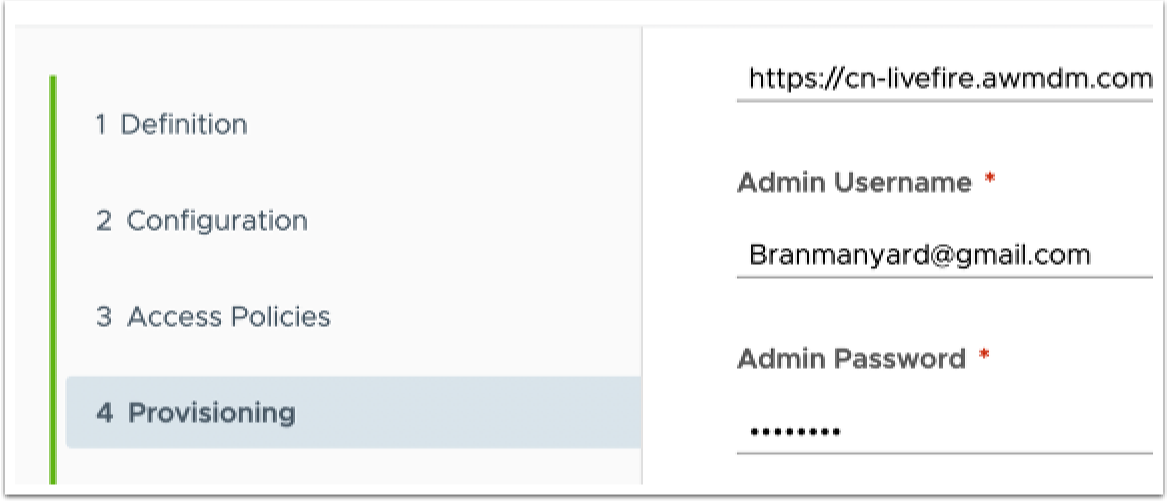
3. AirWatch Provisioning Adaptor

- Under the **Catalog tab**
  1. select the **check box** next to **Airwatch Provisioning** and select **EDIT**
  2. In the **Edit Saas Application** wizard in the left pane select **2 Configuration**
  3. In the Configuration section **scroll down**, expand **Advanced Properties** and change **Setup Provisioning toggle** from **No** to **Yes**



4. AirWatch Provisioning Adaptor

- In this section we will continue in the Workspace ONE Access console
  1. In the **Edit Saas Application** wizard select section **4 Provisioning**
  2. In the middle pane under **Airwatch Host** type : - **https://cn-livefire.awmdm.com**
     - Under **Admin Username** type your **custom Workspace ONE UEM Admin account**
     - Under **Admin Password** type your the **custom Admin password (should be VMware1!)**



https://cn-livefire.awmdm.com

Admin Username *

Branmanyard@gmail.com

Admin Password *

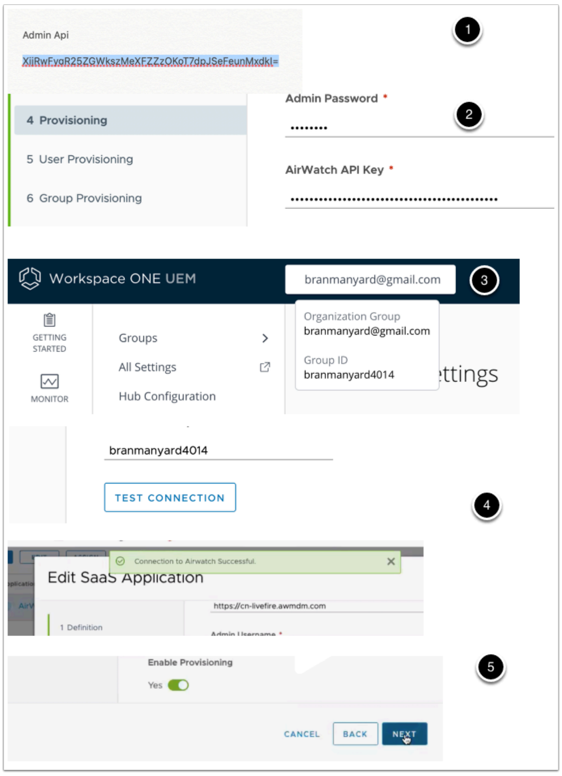
••••••••

5. AirWatch Provisioning Adaptor

- In this section we will continue in the Workspace ONE Access console

1. Launch your **text editor** where you have documented your Identity Manager admin Token and **copy the admin token**
2. Switch back to your **VIDM Edit Saas Application** wizard and under **AirWatch API Key** **paste the token**
3. Switch back to your **Workspace ONE UEM** console, at the top of the Workspace ONE UEM Console you will see your Organization Name, Expand your Organization Name and copy your Group ID
4. Switch back to your **VIDM Edit Saas Application** wizard
   - Under **AirWatch Group ID** type **YOUR Group ID**
   - Scroll down and under **Enable Provisioning** change the **toggle** from **No** to **Yes**
   - Above **Enable Provisioning** select **TEST CONNECTION**, you should notice a **Connection to Airwatch Succesful** message

5. At the bottom of the **VIDM Edit Saas Application** wizard select **NEXT**



Admin Api
XjiRwFyqR25ZGWkszMeXFZZzOKoT7dpJSeFeunMxdkI=

Admin Password *
••••••••

AirWatch API Key *
••

Organization Group
branmanyard@gmail.com

Group ID
branmanyard4014

branmanyard4014

Connection to Airwatch Successful.

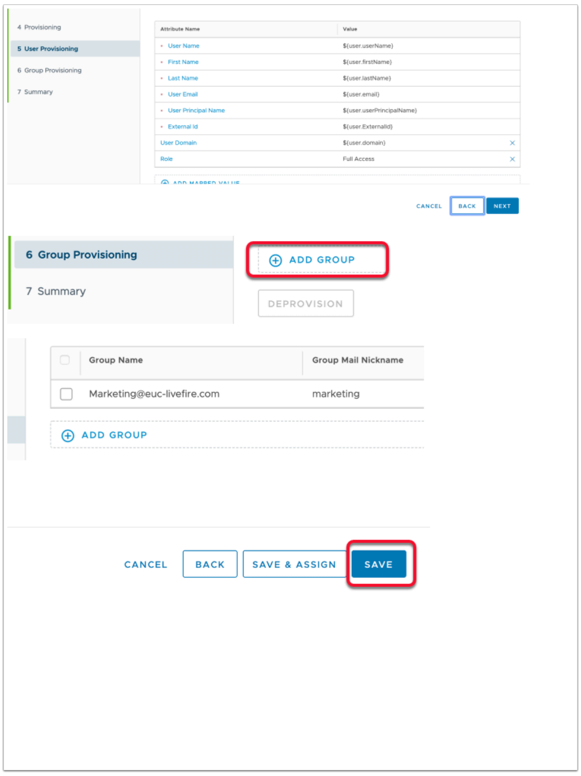
Edit SaaS Application

https://cn-livefire.awmdm.com

Enable Provisioning
Yes

6. AirWatch Provisioning Adaptor

- In this section you will continue with the **VIDM Edit Saas Application** wizard
  1. In section **5 User Provisioning,** accept the default and select **NEXT**
  2. in section **6 Group Provisioning**, select **ADD GROUP**
  3. Under **Group Name** type **mark** and select **Marketing@euc-livefire.com,** under **Nickname** type **Marketing** and select **SAVE**
  4. On the **Group Provisioning** page select **NEXT**
  5. On section **7 Summary** select **SAVE**

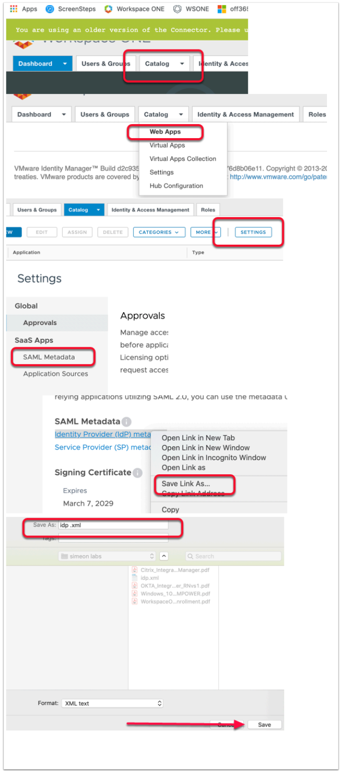


Attribute Name	Value
User Name	${user.userName}
First Name	${user.firstName}
Last Name	${user.lastName}
User Email	${user.email}
User Principal Name	${user.userPrincipalName}
External Id	${user.ExternalId}
User Domain	${user.domain}
Role	Full Access

Group Name	Group Mail Nickname
Marketing@euc-livefire.com	marketing

7. AirWatch Provisioning Adaptor

- In this section we will continue on the **Workspace ONE Access Admin Console** and download an .XML file:-
  1. If you are not there already, navigate to **Catalog** > **Web Apps**
  2. To the right select **SETTINGS**
  3. Under **Settings** > **SaaS Apps** select **SAML Metadata**
  4. Under **SAML Metadata** select **Identity Provider (IdP) metadata** right click and select **Save Link As**
  5. In the **SAVE as** window select **Save,** you will notice the file name is **idp.xml**



You are using an older version of the Connector. Please u

VMware Identity Manager™ Build d2c935 ... 76d8b06e11. Copyright © 2013-20 ... treaties. VMware products are covered by ... http://www.vmware.com/go/pate

Approvals

Manage acce: before applic: Licensing opti request acces

relying applications utilizing SAML 2.0, you can use the metadata u

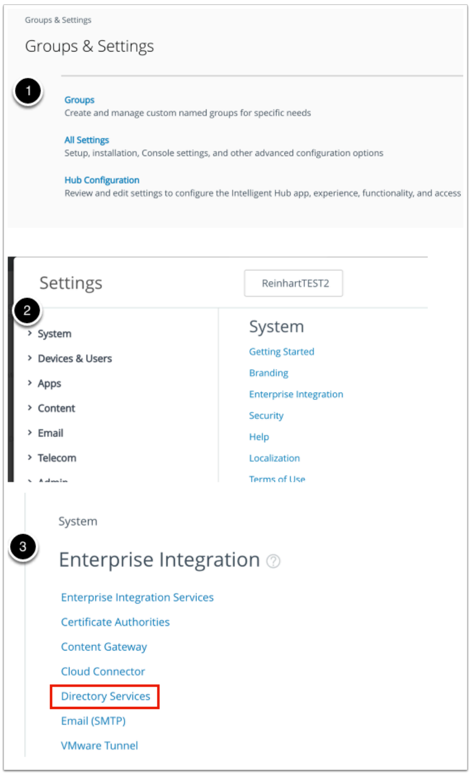
Expires: March 7, 2029

Save As: idp .xml

Format: XML text

8. AirWatch Provisioning Adaptor

- In this section we will switch to the **Workspace ONE UEM** console
  1. Go to **Groups & SETTINGS** > **ALL SETTINGS**
  2. In the **Settings** window under **System** select **Enterprise Integration**
  3. Under **Enterprise Integration** select **Directory Services**



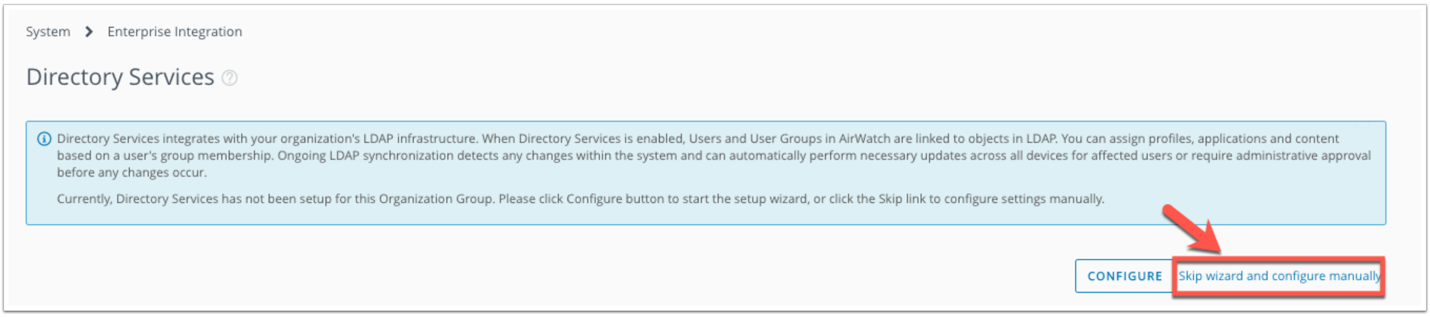
Groups: Create and manage custom named groups for specific needs

All Settings: Setup, installation, Console settings, and other advanced configuration options

Hub Configuration: Review and edit settings to configure the Intelligent Hub app, experience, functionality, and access

9. AirWatch Provisioning Adaptor

1. In the **Directory Services** interface click **"Skip wizard and configure manually"**
2. Under the **Server** tab (default) next to **Current Setting** ensure the **Override radio button** is selected
3. Under **LDAP** next **Directory Type** change this from **Active Directory** to **None**
4. Under **LDAP** next to **Use SAML for Authentication** select the **ENABLED** box

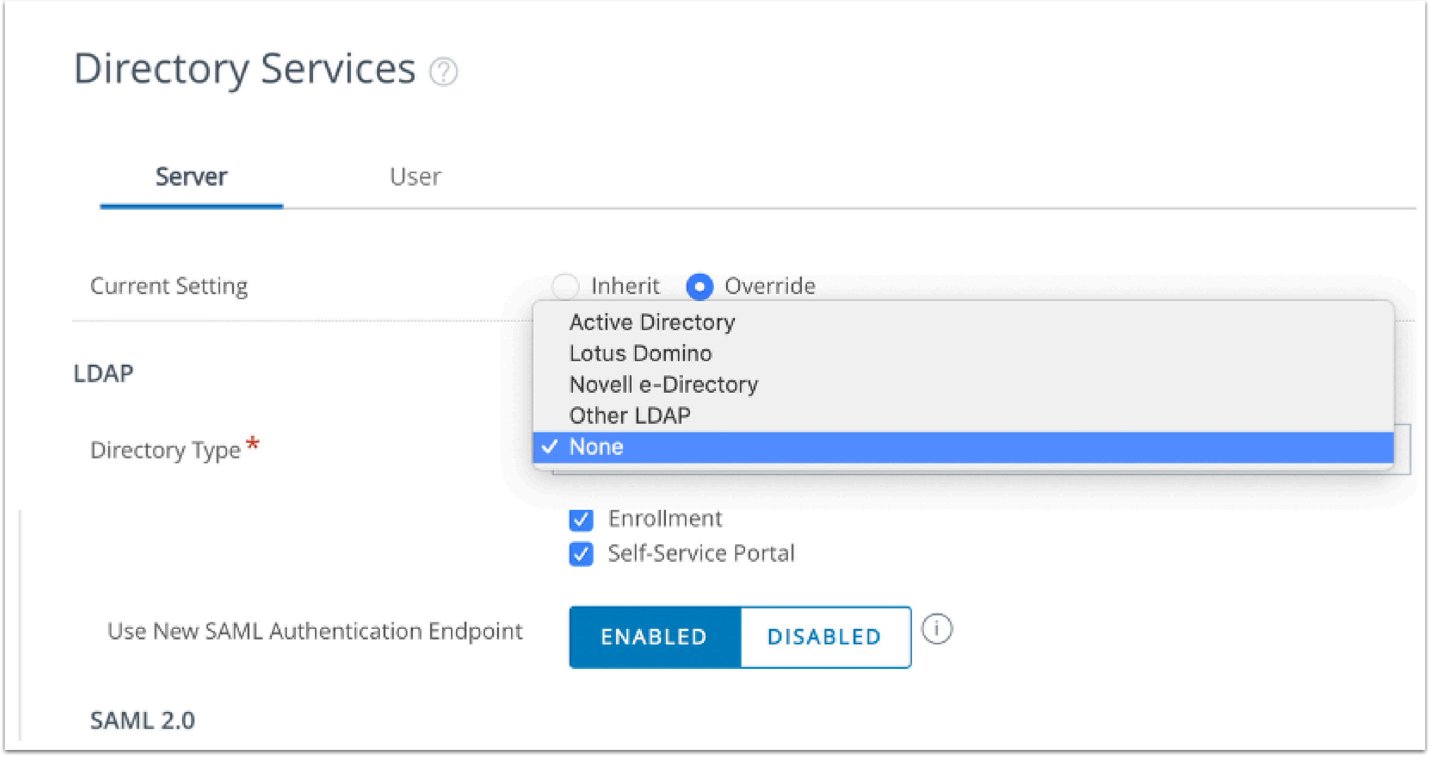


System > Enterprise Integration

Directory Services

Directory Services integrates with your organization's LDAP infrastructure. When Directory Services is enabled, Users and User Groups in AirWatch are linked to objects in LDAP. You can assign profiles, applications and content based on a user's group membership. Ongoing LDAP synchronization detects any changes within the system and can automatically perform necessary updates across all devices for affected users or require administrative approval before any changes occur.

Currently, Directory Services has not been setup for this Organization Group. Please click Configure button to start the setup wizard, or click the Skip link to configure settings manually.



Directory Services

Current Setting ○ Inherit ● Override

LDAP

Directory Type*

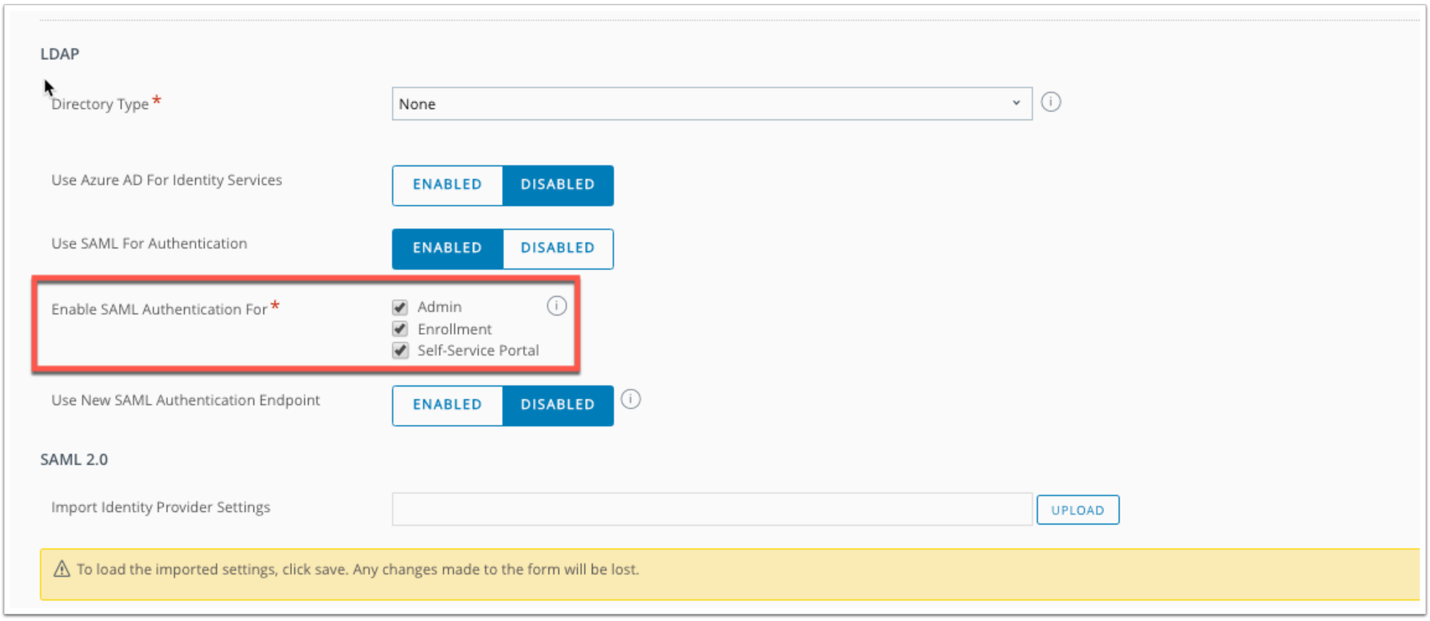
☑ Enrollment
☑ Self-Service Portal

Use New SAML Authentication Endpoint [✓ ENABLED] DISABLED

SAML 2.0

10. AirWatch Provisioning Adaptor

1. Next to **Enable SAML Authentication For** put a check next to **Admin, Enrollment** and Self-Service Portal
2. Next to Use New SAML Authentication Endpoint select **Enabled**
3. Under **SAML 2.0** next to **Import Identity Provider Settings** select **UPLOAD** and choose your xml file.
4. At the bottom of the window select **SAVE**
5. Next to **Request Binding Type** select the POST radio button,
6. Next to **Response Binding Type** select the POST radio button, scroll down and select **SAVE**
7. Close the Settings window by selecting **X** to the right of the window



LDAP

Directory Type * None

Use Azure AD For Identity Services ENABLED [✓ DISABLED]

Use SAML For Authentication [✓ ENABLED] DISABLED

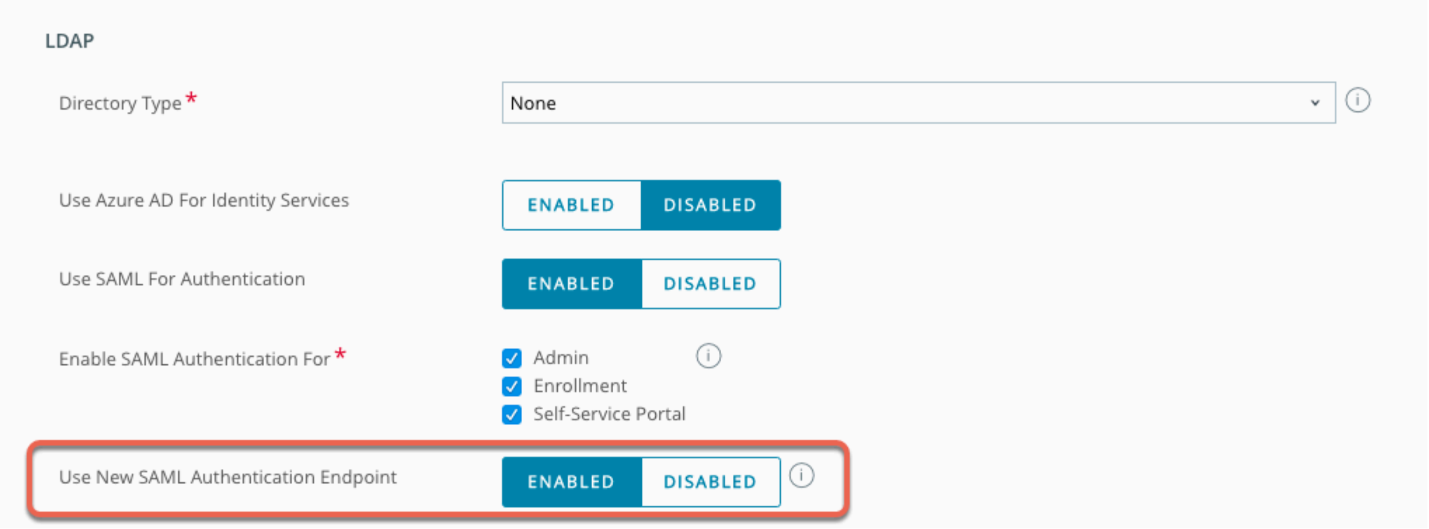
Enable SAML Authentication For * ☑ Admin ☑ Enrollment ☑ Self-Service Portal

Use New SAML Authentication Endpoint ENABLED [✓ DISABLED]

SAML 2.0

Import Identity Provider Settings UPLOAD

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



LDAP

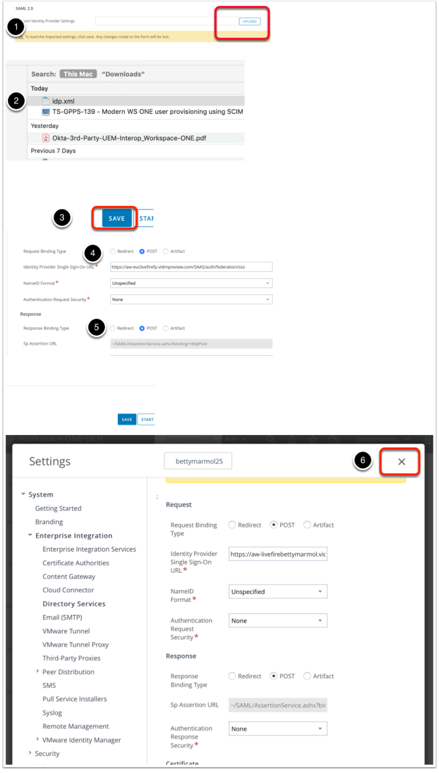
Directory Type * None

Use Azure AD For Identity Services ENABLED [✓ DISABLED]

Use SAML For Authentication [✓ ENABLED] DISABLED

Enable SAML Authentication For * ☑ Admin ☑ Enrollment ☑ Self-Service Portal

Use New SAML Authentication Endpoint [✓ ENABLED] DISABLED



SAML 2.0

1 ...ort Identity Provider Settings UPLOAD

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

2 Search: This Mac "Downloads"

Today
- idp.xml
- TS-GPPS-139 - Modern WS ONE user provisioning using SCIM

Yesterday
- Okta-3rd-Party-UEM-Interop_Workspace-ONE.pdf

Previous 7 Days

3 SAVE STAR

Request Binding Type 4 ○ Redirect ● POST ○ Artifact

Identity Provider Single Sign-On URL * https://aw-euclivefirefp.vidmpreview.com/SAAS/auth/federation/sso

NameID Format * Unspecified

Authentication Request Security * None

Response

Response Binding Type 5 ○ Redirect ● POST ○ Artifact

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

SAVE START

Settings bettymarmol25 6 ×

Request

Request Binding Type ○ Redirect ● POST ○ Artifact

Identity Provider Single Sign-On URL * https://aw-livefirebettymarmol.vic

NameID Format * Unspecified

Authentication Request Security * None

Response

Response Binding Type ○ Redirect ● POST ○ Artifact

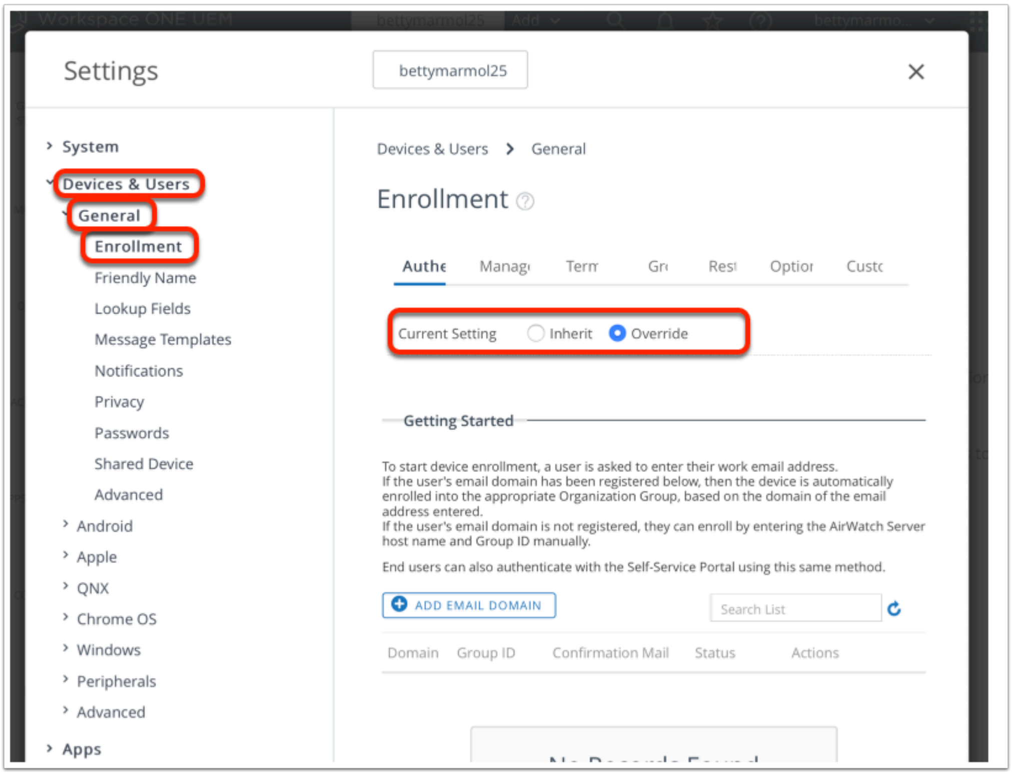
Sp Assertion URL ~/SAML/AssertionService.ashx?bir

Authentication Response Security * None

Certificate

11. AirWatch Provisioning Adaptor

- In this section we will work **Workspace ONE UEM Admin Console,** Under **Groups and settings** > **All** Settings > **Devices & Users** > **General** **>** **Enrollment**
  1. Next to **Current Settings** Click **Override**
  2. Next to **Authentication Mode(s)** ensure the **Directory** **checkbox** is enabled
  3. Next to **Source of Authentication for Intelligent Hub.** Select **VMWARE IDENTITY MANAGER**
     NOTE: If SAML 2.0 is enabled as above it will still use Workspace ONE Access for authentication even if **WORKSPACE ONE UEM** is selected, but **People Search** and **Notifications** will only be enabled in **HUB** if **VMWARE IDENTITY MANAGER** is select here.
  4. Select **SAVE**



Settings

bettymarmol25

- System
- Devices & Users
  - General
    - Enrollment
    - Friendly Name
    - Lookup Fields
    - Message Templates
    - Notifications
    - Privacy
    - Passwords
    - Shared Device
    - Advanced
  - Android
  - Apple
  - QNX
  - Chrome OS
  - Windows
  - Peripherals
  - Advanced
- Apps

Devices & Users > General

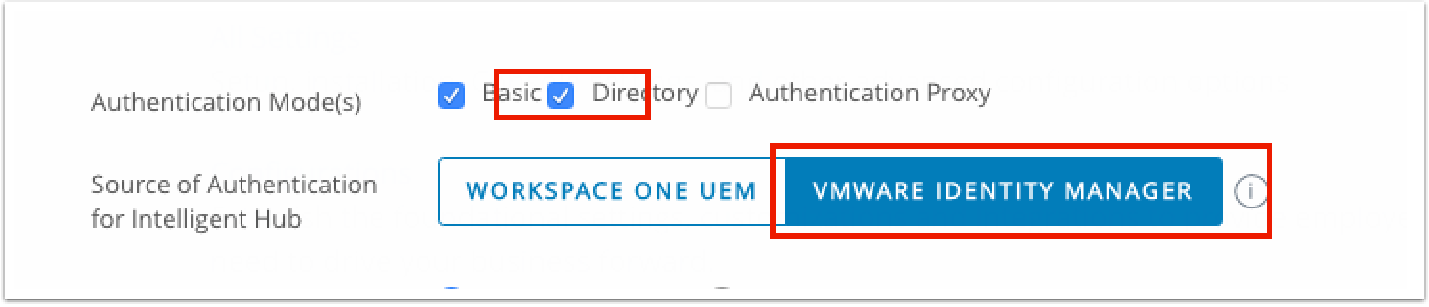
Enrollment

Current Setting ○ Inherit ● Override

Getting Started

To start device enrollment, a user is asked to enter their work email address.
If the user's email domain has been registered below, then the device is automatically enrolled into the appropriate Organization Group, based on the domain of the email address entered.
If the user's email domain is not registered, they can enroll by entering the AirWatch Server host name and Group ID manually.
End users can also authenticate with the Self-Service Portal using this same method.

Domain	Group ID	Confirmation Mail	Status	Actions



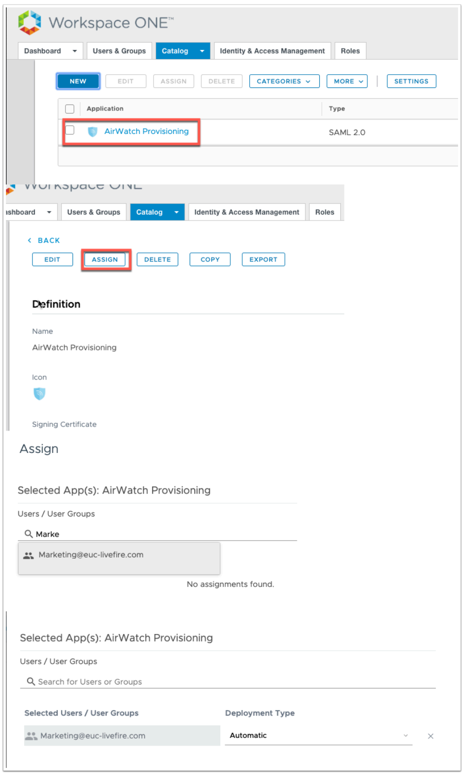
Authentication Mode(s) ☑ Basic ☑ Directory □ Authentication Proxy

Source of Authentication for Intelligent Hub: WORKSPACE ONE UEM / VMWARE IDENTITY MANAGER

12. AirWatch Provisioning Adaptor

- Switch back to the **Workspace ONE Access Admin console**
  1. Select Catalog and select the checkbox next to **AirWatch Provisioning** Application Select ASSIGN
  2. In the Assign window under **Users / User Groups** type Marketing, select Marketing@euc-livefire.com
  3. Under **Deployment Type** change **User-Activated** to Automatic and SAVE
  4. The users should now be provisioned into **WorkspaceOne UEM**. You can check this by going into the **WorkspaceONE UEM console** select Accounts > Users > List View

Note! It could take up to 10 minutes for provisioning to work.



Application	Type
AirWatch Provisioning	SAML 2.0

Definition

Name
AirWatch Provisioning

Icon

Signing Certificate

Assign

Selected App(s): AirWatch Provisioning

Users / User Groups

Marke

Marketing@euc-livefire.com

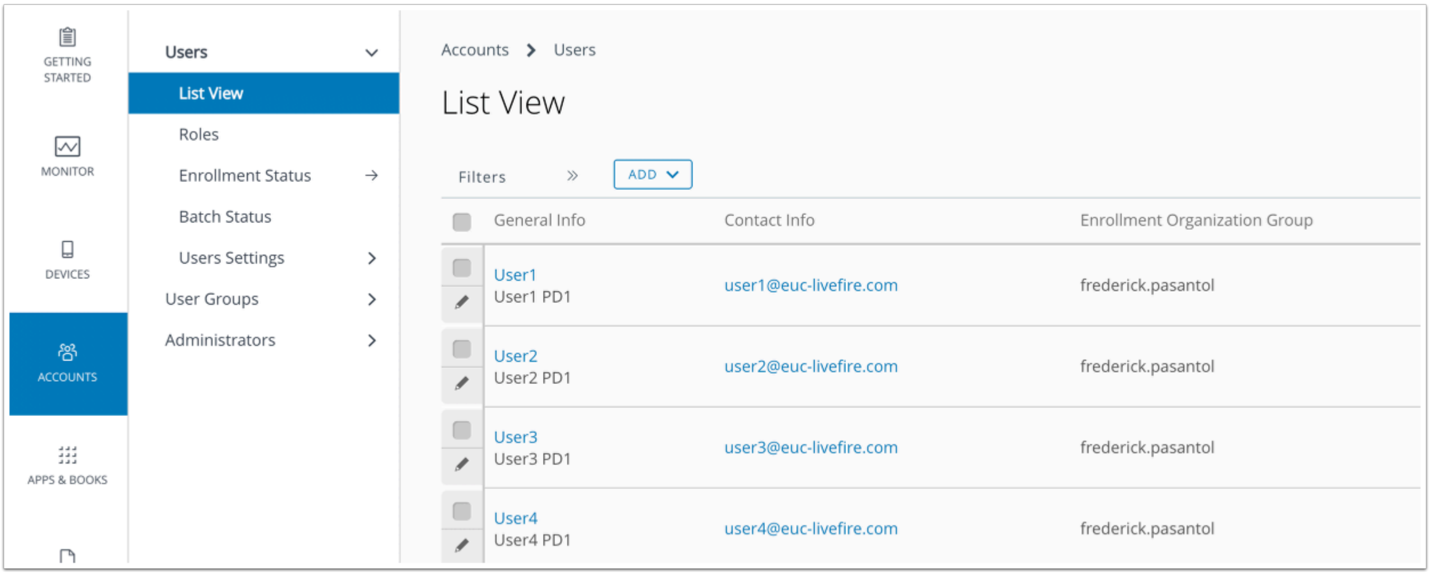
No assignments found.

Selected App(s): AirWatch Provisioning

Users / User Groups

Search for Users or Groups

Selected Users / User Groups	Deployment Type
Marketing@euc-livefire.com	Automatic



List View

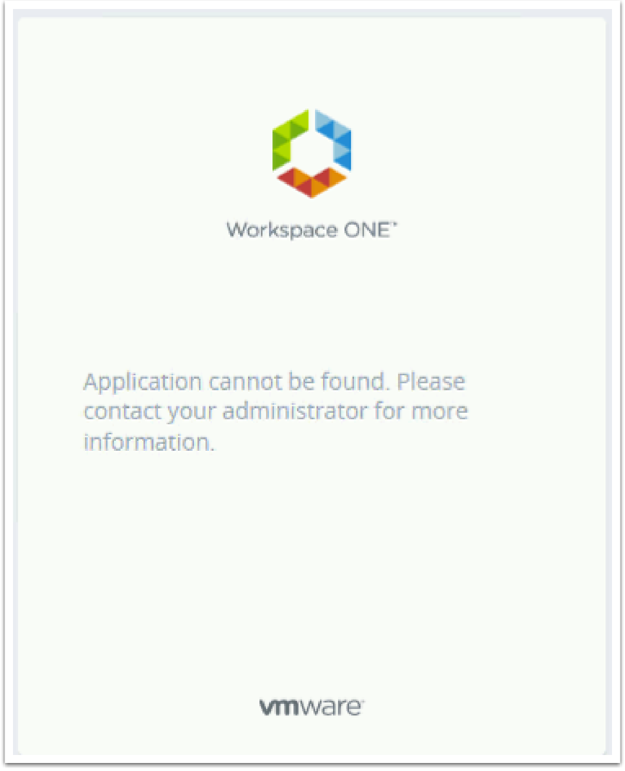
General Info	Contact Info	Enrollment Organization Group
User1 User1 PD1	user1@euc-livefire.com	frederick.pasantol
User2 User2 PD1	user2@euc-livefire.com	frederick.pasantol
User3 User3 PD1	user3@euc-livefire.com	frederick.pasantol
User4 User4 PD1	user4@euc-livefire.com	frederick.pasantol

Part 3: Completing full SAML configuration in Workspace ONE Access of Workspace ONE UEM

The AirWatch Provisioning Adaptor is a new way to configure User and Group Provisioning. One of the steps we followed was to copy Workspace ONE Access Metadata into Workspace ONE UEM. What we have learned in our troubleshooting is that if we were to leave configuration as it is, enrollment of devices will fail. In testing with Windows 10 and Android based enrollment we got a common error message which looked as follows. Application cannot be found.

With extensive collaboration with the PSO team in our Atlanta USA office we were able to establish the cause.

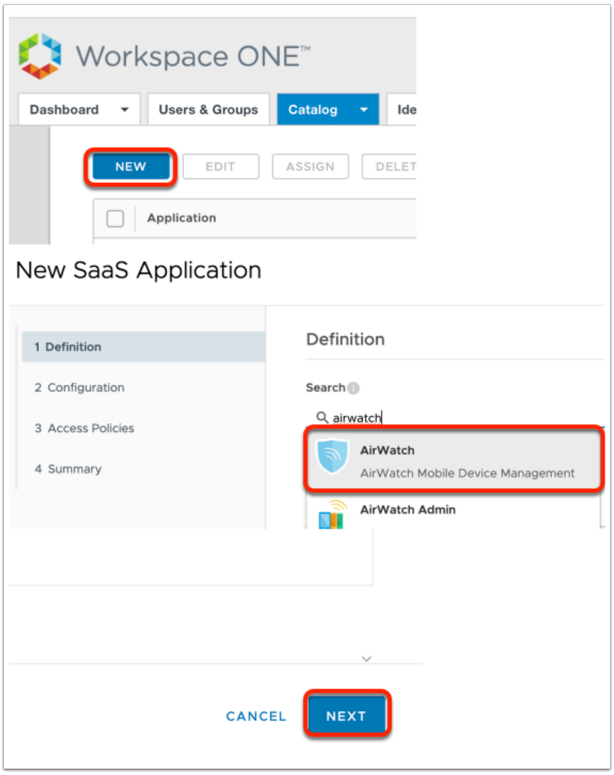
We required full SAML configuration on both services that being Workspace ONE UEM and Workspace ONE Access. Up till now we have only configure SAML integration of Workspace ONE Access in Workspace ONE UEM. We will now configure SAML integration in Workspace ONE Access of Workspace ONE UEM.



Application cannot be found. Please contact your administrator for more information.

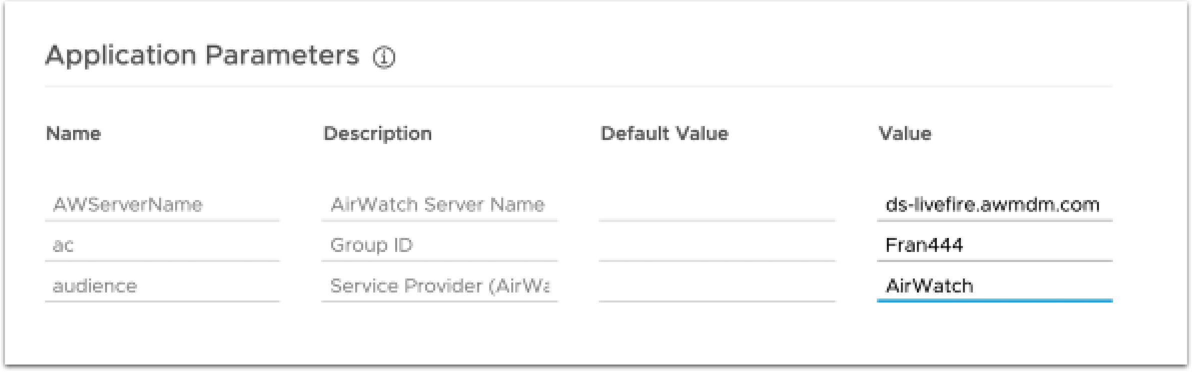
1. SAML integration Configuration (Part 4)

- Switch to your **Workspace ONE Access** Console
  1. Select **Catalog** > **Web Apps** and then select **NEW**
  2. In the **New Saas Application** under **Search** type **airwatch** and select **AirWatch Mobile Device Management**
  3. Scroll down to the bottom of the page and select **NEXT**



2. SAML integration Configuration (Part 4)

- Step 2 of the New Saas Application wizard
  1. In the **New Saas Application** wizard, step **2 Configuration**, scroll down to **Application Parameters** and configure the following:- next to :
     1. **AWServerName** under **Value** type : **ds-livefire.awmdm.com**
     2. **AC** type your Group ID under **Value** : **eg. Plaston444**
     3. **Audience** under **Value: AirWatch**
     4. Scroll down and move the **toggle** under **Show in User Portal** to **No**
     5. Select **NEXT**
  2. In step **3 Access Policies** select **NEXT**
  3. In step **4 Summary** select **SAVE**



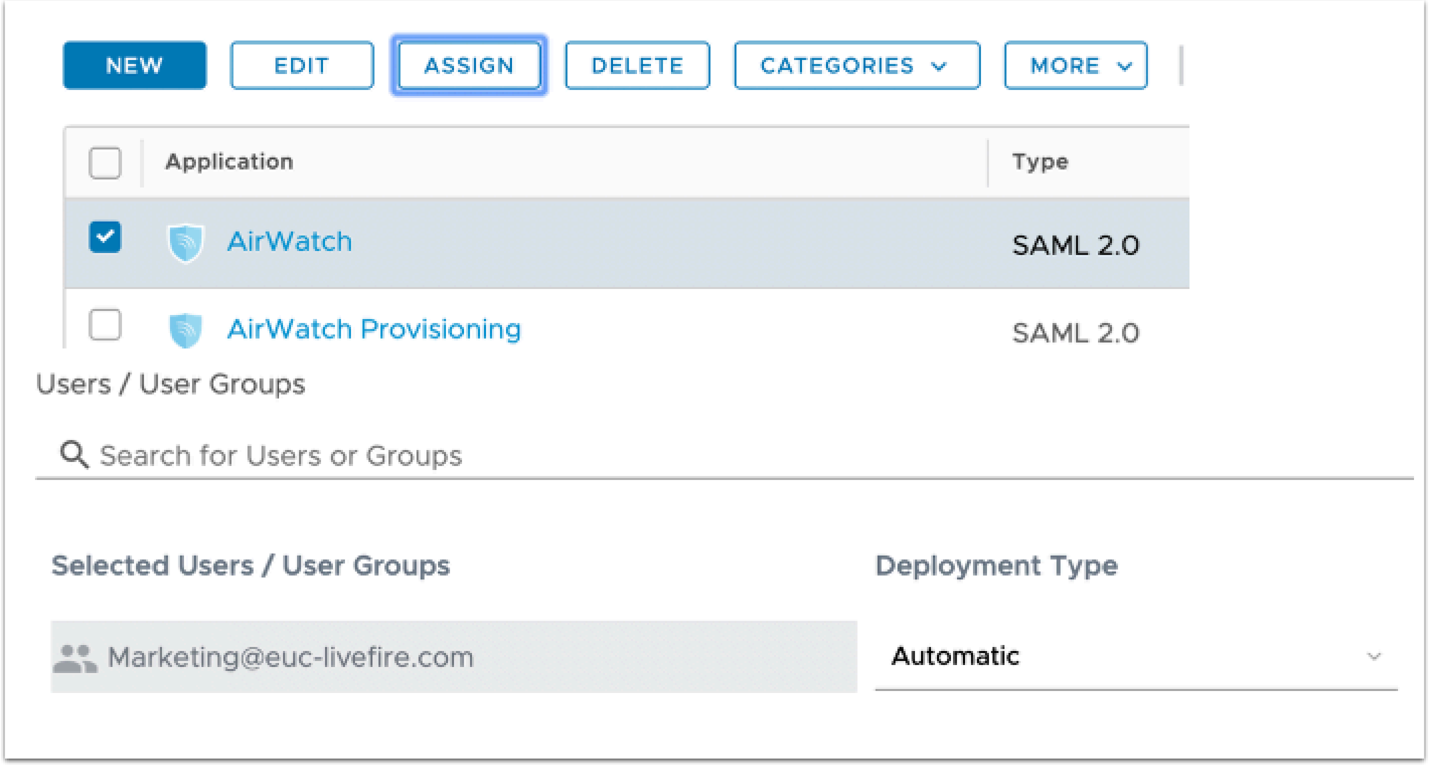
Application Parameters ⓘ

Name	Description	Default Value	Value
AWServerName	AirWatch Server Name		ds-livefire.awmdm.com
ac	Group ID		Fran444
audience	Service Provider (AirWa		AirWatch

5. SAML integration Configuration (Part 4)

- Select the **checkbox** next to **AirWatch** application and select **Assign**

1. In the **Assign** window under **Users** in the search type **Mark** and add **marketing@euc-livefire.com,** set the **Deployment Type** to **Automatic** and select **SAVE**



☐	Application	Type
☑	AirWatch	SAML 2.0
☐	AirWatch Provisioning	SAML 2.0

Users / User Groups

Search for Users or Groups

Selected Users / User Groups	Deployment Type
Marketing@euc-livefire.com	Automatic

Federating AZURE with Workspace ONE Access and Office 365 as a service

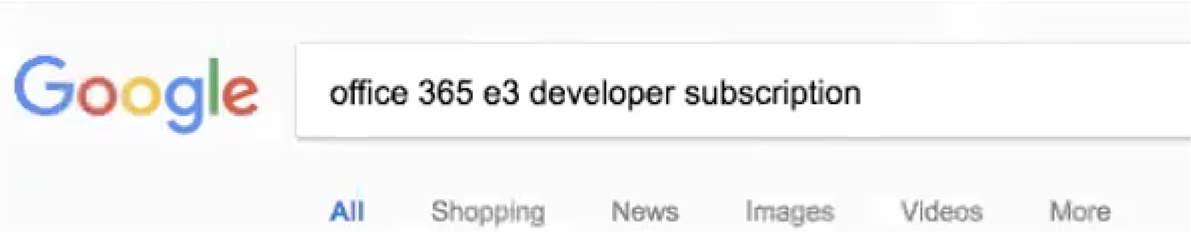
Part 1: Setting Up a Developer Account

One needs to setup an **Office 365 E3 Developer** subscription account to be able to integrate with Workspace ONE. In this section we will walk through and setup the required developer subscription that allows you a 12 -month free trial.

An Important NOTE!

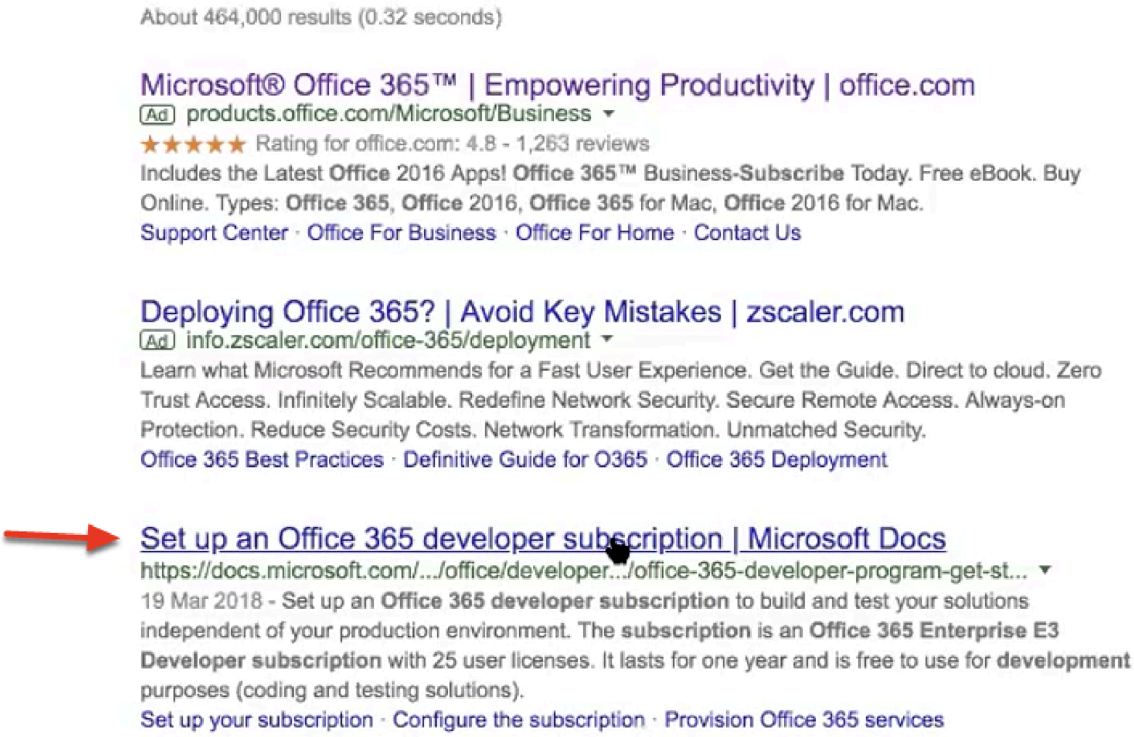
- Be sure to to take notes and document your configurations immediately.
- Be 100% clear from your document what your assigned domain name is.

1. Open a browser and go to **Google Chrome search engine** and type **office 365 e3 developer subscription.**



office 365 e3 developer subscription

2. Find the option that says **Set up an Office 365 developer subscription** and **select**



About 464,000 results (0.32 seconds)

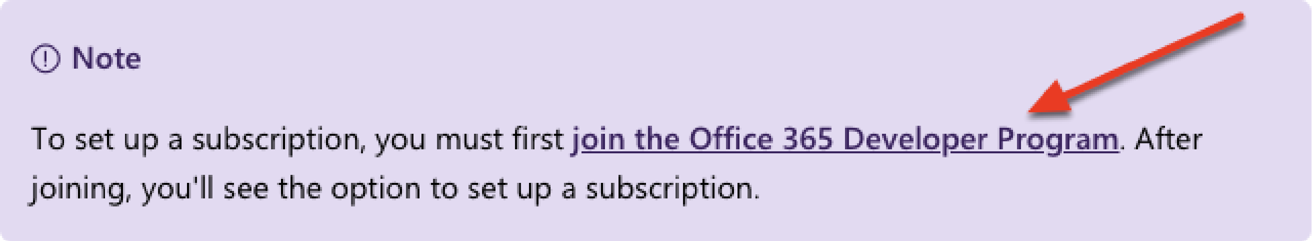
Microsoft® Office 365™ | Empowering Productivity | office.com
Ad products.office.com/Microsoft/Business
★★★★★ Rating for office.com: 4.8 - 1,263 reviews
Includes the Latest Office 2016 Apps! Office 365™ Business-Subscribe Today. Free eBook. Buy Online. Types: Office 365, Office 2016, Office 365 for Mac, Office 2016 for Mac.
Support Center · Office For Business · Office For Home · Contact Us

Deploying Office 365? | Avoid Key Mistakes | zscaler.com
Ad info.zscaler.com/office-365/deployment
Learn what Microsoft Recommends for a Fast User Experience. Get the Guide. Direct to cloud. Zero Trust Access. Infinitely Scalable. Redefine Network Security. Secure Remote Access. Always-on Protection. Reduce Security Costs. Network Transformation. Unmatched Security.
Office 365 Best Practices · Definitive Guide for O365 · Office 365 Deployment

Set up an Office 365 developer subscription | Microsoft Docs
https://docs.microsoft.com/.../office/developer.../office-365-developer-program-get-st...
19 Mar 2018 - Set up an Office 365 developer subscription to build and test your solutions independent of your production environment. The subscription is an Office 365 Enterprise E3 Developer subscription with 25 user licenses. It lasts for one year and is free to use for development purposes (coding and testing solutions).
Set up your subscription · Configure the subscription · Provision Office 365 services

3. On the **Set up an Office 365 developer subscription** page under **Set up your subscription** Under **! Note**

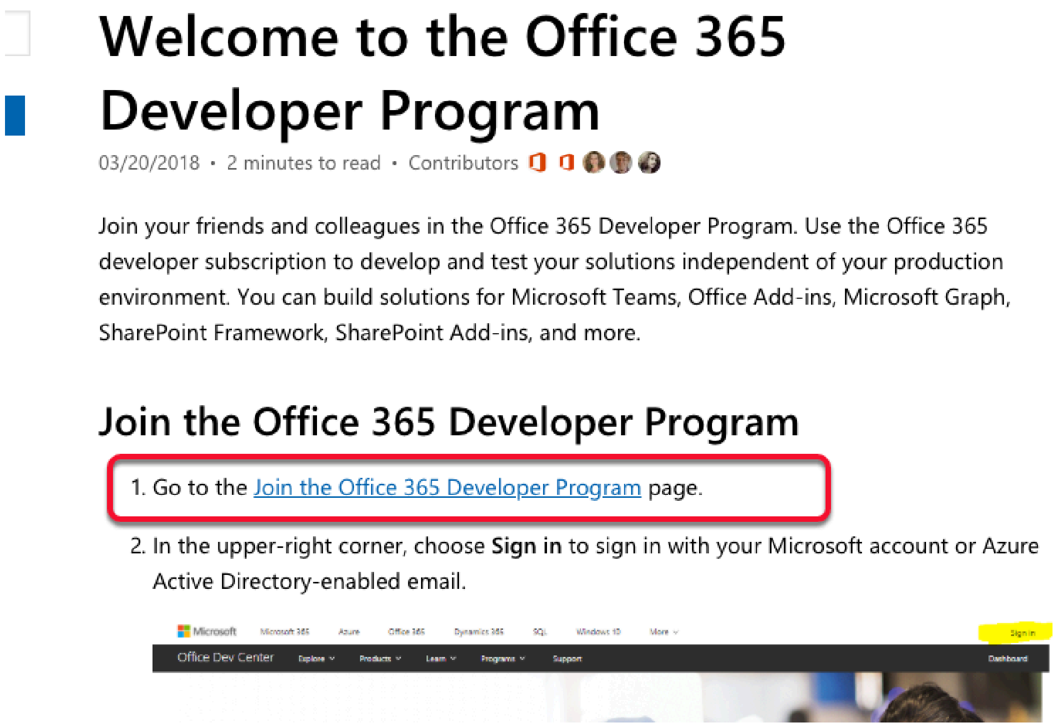
Select the **join the Office 365 Developer Program** hyperlink



ⓘ Note

To set up a subscription, you must first join the Office 365 Developer Program. After joining, you'll see the option to set up a subscription.

4. On the **Welcome to theOffice 365 Developer Program** page select the **Join the Office 365 Developer Program** page



Welcome to the Office 365 Developer Program

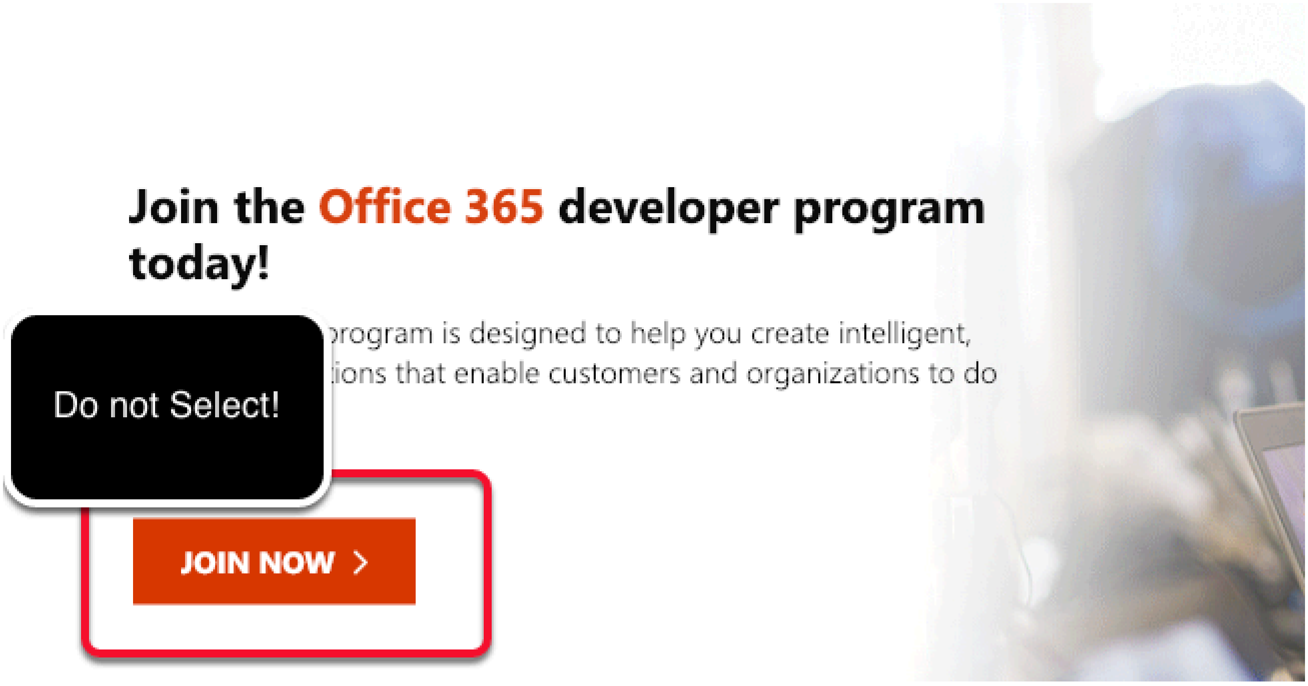
03/20/2018 • 2 minutes to read • Contributors

Join your friends and colleagues in the Office 365 Developer Program. Use the Office 365 developer subscription to develop and test your solutions independent of your production environment. You can build solutions for Microsoft Teams, Office Add-ins, Microsoft Graph, SharePoint Framework, SharePoint Add-ins, and more.

Join the Office 365 Developer Program

1. Go to the Join the Office 365 Developer Program page.
2. In the upper-right corner, choose **Sign in** to sign in with your Microsoft account or Azure Active Directory-enabled email.

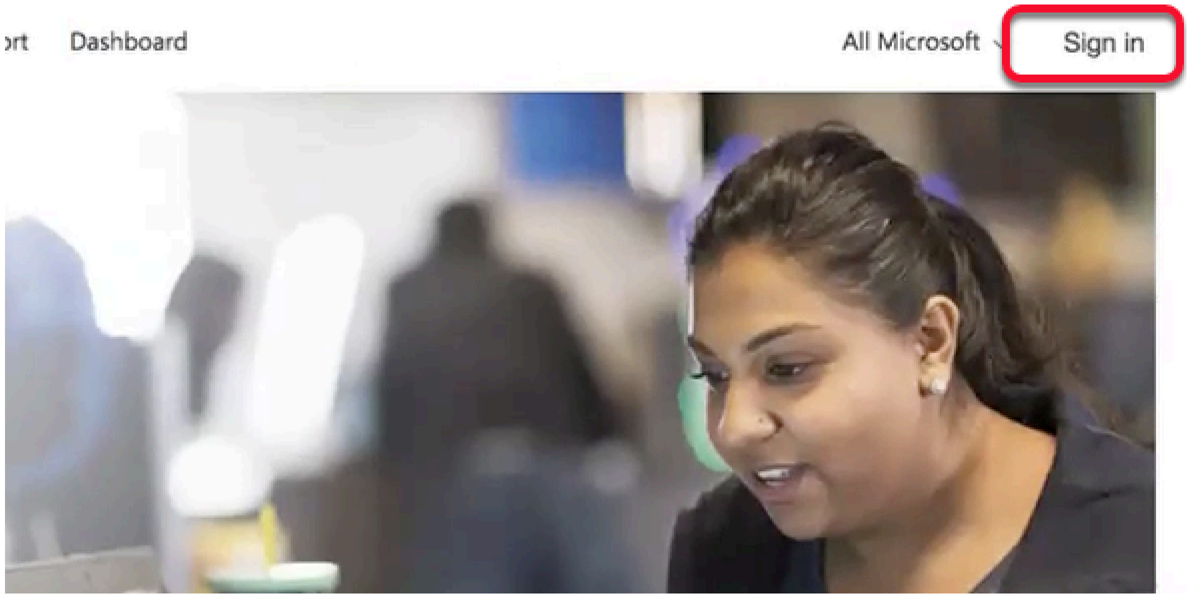
5. You will now be re-directed a 3rd time to the **Join the Office 365 developer program today!** Do not select JOIN NOW



Join the Office 365 developer program today!

...program is designed to help you create intelligent, ...ions that enable customers and organizations to do

6. To the right of the page first select **Sign In**



7. On **Microsoft Sign in Page** type in the **email address** of an account you own (NB! If this account is already associated with an office 365 account you will have to create a new account)

7.1 Alternatively next to **NO account?** select **Create one!**

7.2 On the **Create account** page type your **custom email address**

7.3 Select **Next**

7.4 On the **Create a password** window type a unique **password** and select Next

7.5 On the **Create account** page type in your **country** and **Birthdate** and select **Next**

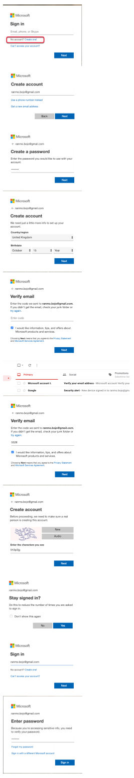
7.6 On the **Verify email** page notice you *need to enter a code*, log into your gmail account and select the email and find the code and then **enter the code** in the **Enter Code** area and select **Next**

7.7 On the **Create account**, page enter the **custom security** letters for your login

7.8 On the **Stay Signed** in page, select **Yes**

7.9 On the **Sign in** page type in your custom **email address** and select **Next**

7.10 On the **Enter password** page, type in your **password** and select **Sign in**



Microsoft

Sign in

Email, phone, or Skype

No account? Create one!

Can't access your account?

Next

Microsoft

Create account

ranmo.bojo@gmail.com

Use a phone number instead

Get a new email address

Back Next

Microsoft

← ranmo.bojo@gmail.com

Create a password

Enter the password you would like to use with your account.

••••••••

Next

Microsoft

← ranmo.bojo@gmail.com

Create account

We need just a little more info to set up your account.

Country/region: United Kingdom

Birthdate: October 15 Year

Next

Microsoft

← ranmo.bojo@gmail.com

Verify email

Enter the code we sent to **ranmo.bojo@gmail.com**. If you didn't get the email, check your junk folder or try again.

Enter code

☑ I would like information, tips, and offers about Microsoft products and services.

Choosing **Next** means that you agree to the Privacy Statement and Microsoft Services Agreement.

Next

☐ ☆ **Microsoft account t.** **Verify your email address** - Microsoft account Verify you

☐ ☆ **Google** **Security alert** - New device signed in to ranmo.bojo@gm

Microsoft

← ranmo.bojo@gmail.com

Verify email

Enter the code we sent to **ranmo.bojo@gmail.com**. If you didn't get the email, check your junk folder or try again.

5528

☑ I would like information, tips, and offers about Microsoft products and services.

Choosing **Next** means that you agree to the Privacy Statement and Microsoft Services Agreement.

Next

Microsoft

← ranmo.bojo@gmail.com

Create account

Before proceeding, we need to make sure a real person is creating this account.

New

Audio

Enter the characters you see: 5h3p3jg

Next

Microsoft

ranmo.bojo@gmail.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again

No Yes

Microsoft

Sign in

ranmo.bojo@gmail.com

No account? Create one!

Can't access your account?

Next

Microsoft

ranmo.bojo@gmail.com

Enter password

Because you're accessing sensitive info, you need to verify your password.

••••••••

Forgot my password

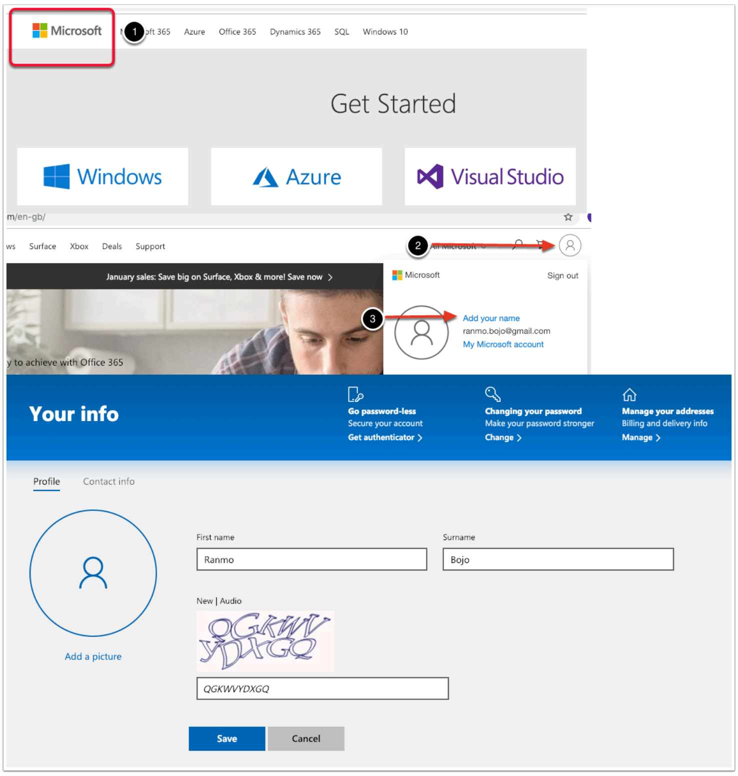
Sign in with a different Microsoft account

Sign in

8.1 To the left of the page, select the **Microsoft icon**

8.2 Then look to the right of the page and select your **account Icon**, next select **Add your name**

8.3 On the **Your info** page under **First name** type your custom **name** and under **Surname** type your custom **Surname**, type in the **matching security letters** and select **Save**



First name: Ranmo

Surname: Bojo

QGKWVYDXGQ

9.0 Open an Incognito browser session with Google Chrome and copy the following url in the Browser address bar,

https://developer.microsoft.com/en-us/office/dev-program

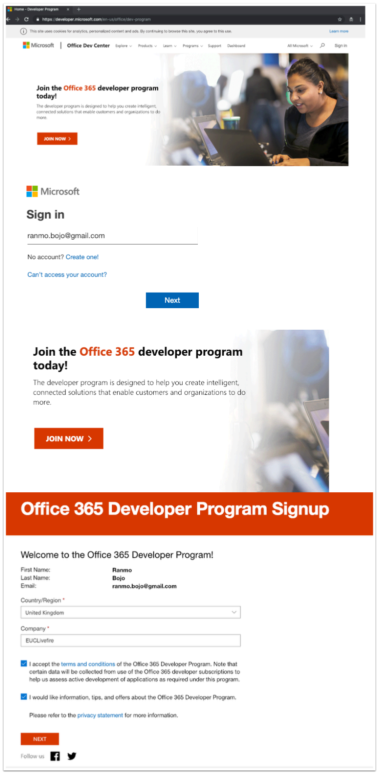
9.1 To the right select **Sign In**, On the **Sign In** page type in your **custom email address** and select **Next**

9.2 On the **Enter password** window, type the **custom password** you created and select **Sign in**

9.3 On the **Stay signed in?** window select **Yes**

9.4 On the **Join Office 365 Developer program today** page select **JOIN NOW>**

9.5 On the **Office 365 Developer Program Signup** page select your **Country/Region** and type in the **name of your Company** and select the **two checkboxes** for **terms and conditions** and **information** and select **NEXT**



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

Join the Office 365 developer program today!

The developer program is designed to help you create intelligent, connected solutions that enable customers and organizations to do more.

JOIN NOW >

Microsoft

Sign in

ranmo.bojo@gmail.com

No account? Create one!

Can't access your account?

Next

Join the Office 365 developer program today!

The developer program is designed to help you create intelligent, connected solutions that enable customers and organizations to do more.

JOIN NOW >

Office 365 Developer Program Signup

Welcome to the Office 365 Developer Program!

First Name:	Ranmo
Last Name:	Bojo
Email:	ranmo.bojo@gmail.com

Country/Region *

United Kingdom

Company *

EUCLivefire

☑ I accept the terms and conditions of the Office 365 Developer Program. Note that certain data will be collected from use of the Office 365 developer subscriptions to help us assess active development of applications as required under this program.

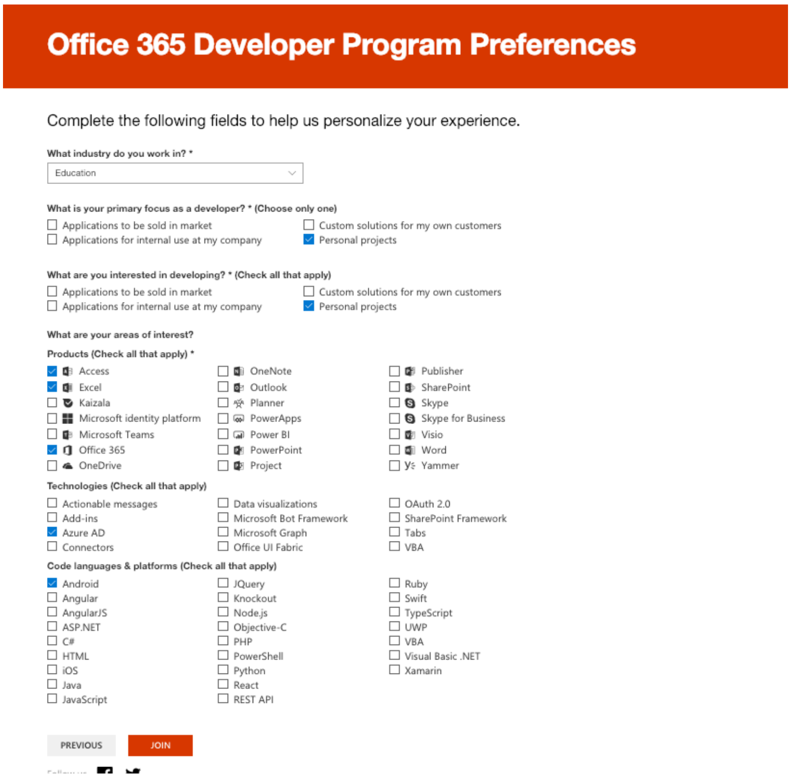
☑ I would like information, tips, and offers about the Office 365 Developer Program.

Please refer to the privacy statement for more information.

NEXT

Follow us

10. On the **Office 365 Developer Program Preferences** page select **enough check box and options** to make sure the **Join** button becomes available and the select **JOIN**


Office 365 Developer Program Preferences

Complete the following fields to help us personalize your experience.

What industry do you work in? *

Education

What is your primary focus as a developer? * (Choose only one)

□ Applications to be sold in market
□ Applications for internal use at my company
□ Custom solutions for my own customers
☑ Personal projects

What are you interested in developing? * (Check all that apply)

□ Applications to be sold in market
□ Applications for internal use at my company
□ Custom solutions for my own customers
☑ Personal projects

What are your areas of interest?

Products (Check all that apply) *

☑ Access
☑ Excel
□ Kaizala
□ Microsoft identity platform
□ Microsoft Teams
☑ Office 365
□ OneDrive
□ OneNote
□ Outlook
□ Planner
□ PowerApps
□ Power BI
□ PowerPoint
□ Project
□ Publisher
□ SharePoint
□ Skype
□ Skype for Business
□ Visio
□ Word
□ Yammer

Technologies (Check all that apply)

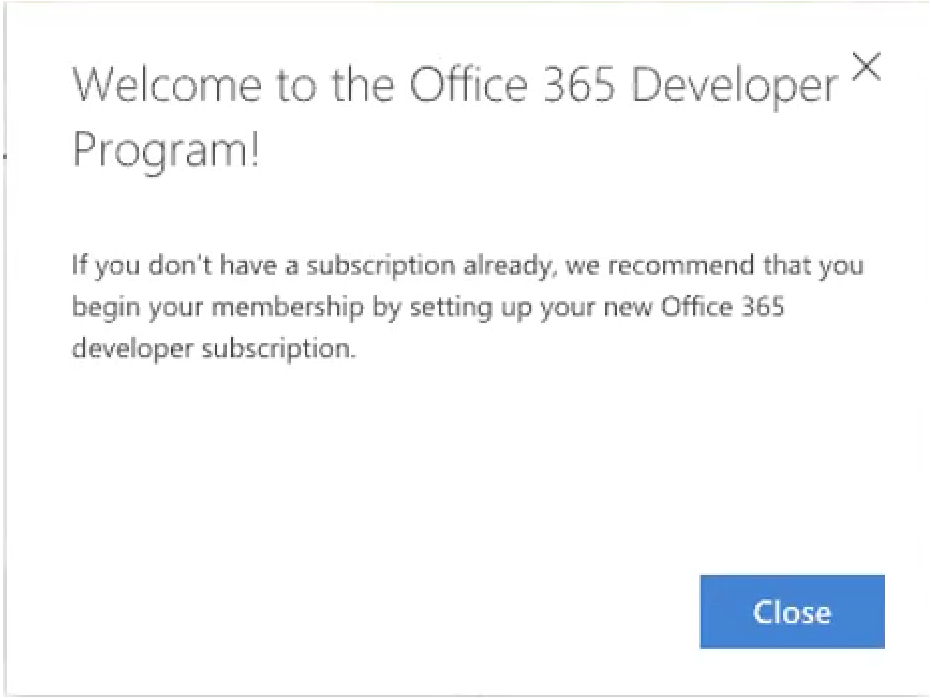
□ Actionable messages
□ Add-ins
☑ Azure AD
□ Connectors
□ Data visualizations
□ Microsoft Bot Framework
□ Microsoft Graph
□ Office UI Fabric
□ OAuth 2.0
□ SharePoint Framework
□ Tabs
□ VBA

Code languages & platforms (Check all that apply)

☑ Android
□ Angular
□ AngularJS
□ ASP.NET
□ C#
□ HTML
□ iOS
□ Java
□ JavaScript
□ JQuery
□ Knockout
□ Node.js
□ Objective-C
□ PHP
□ PowerShell
□ Python
□ React
□ REST API
□ Ruby
□ Swift
□ TypeScript
□ UWP
□ VBA
□ Visual Basic .NET
□ Xamarin

PREVIOUS JOIN

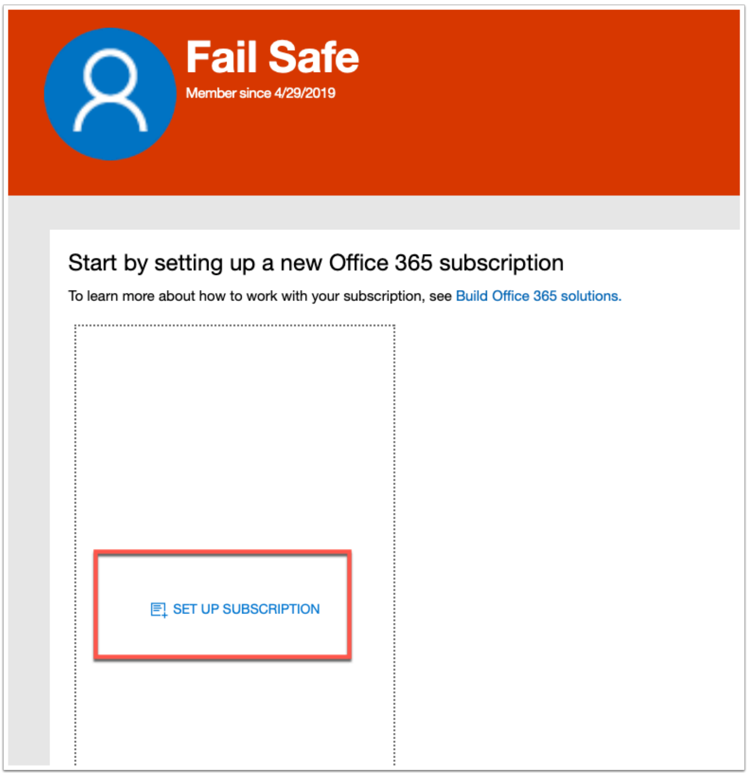
11. Close the **Welcome to the Office 365 Developer Program!** Window by selecting **Close**



Welcome to the Office 365 Developer Program!

If you don't have a subscription already, we recommend that you begin your membership by setting up your new Office 365 developer subscription.

12. On the **Office 365 Developer** Page select **SET UP SUBSCRIPTION**



Start by setting up a new Office 365 subscription

To learn more about how to work with your subscription, see Build Office 365 solutions.

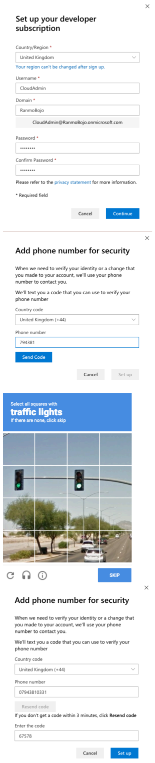
13. In the **Setup your developer subscription** window, create a unique admin account , for example, your username could be CloudAdmin and your **Domain** could be your firstname and surname

NB! Ensure you document these credentials

14. When you are done select **Continue**

15. On the **Add phone number for security** windows type in your **Country Code** and your **phone number**

16. Select **SEND** code , follow through on the **security picture block** selecting your **relevant pictures**, and select **Next** Enter the Code from your phone and select Set up



Set up your developer subscription

Country/Region *
United Kingdom
Your region can't be changed after sign up.

Username *
CloudAdmin

Domain *
RanmoBojo
CloudAdmin@RanmoBojo.onmicrosoft.com

Password *
••••••••

Confirm Password *
••••••••

Please refer to the privacy statement for more information.

* Required field

Add phone number for security

When we need to verify your identity or a change that you made to your account, we'll use your phone number to contact you.

We'll text you a code that you can use to verify your phone number

Country code
United Kingdom (+44)

Phone number
794381

Select all squares with
traffic lights
If there are none, click skip

Add phone number for security

When we need to verify your identity or a change that you made to your account, we'll use your phone number to contact you.

We'll text you a code that you can use to verify your phone number

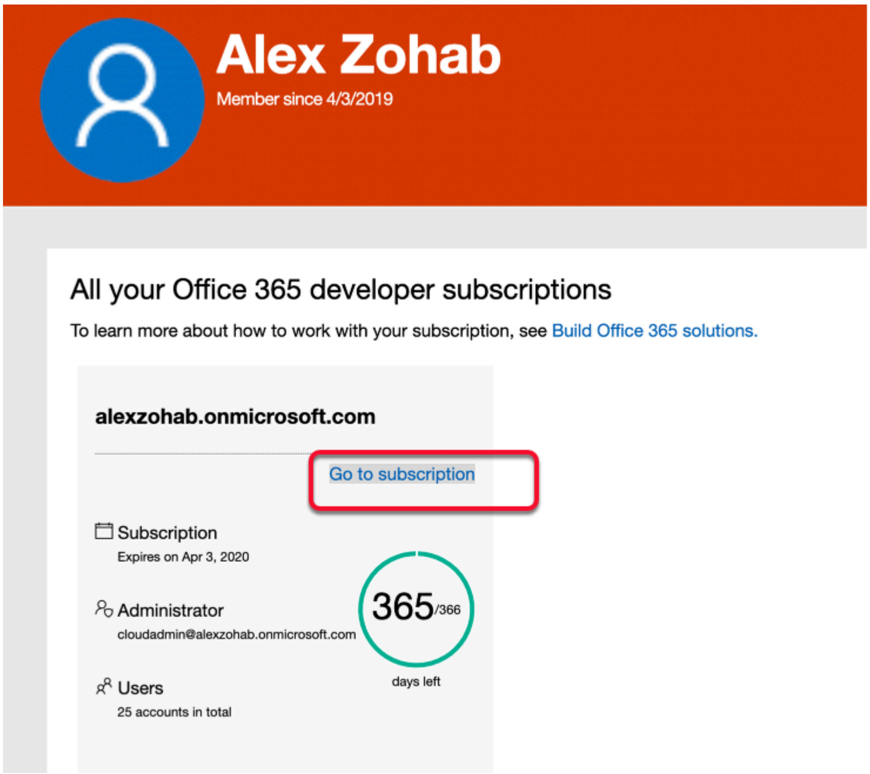
Country code
United Kingdom (+44)

Phone number
07943810331

If you don't get a code within 3 minutes, click **Resend code**

Enter the code
67578

17. Once **your** registration is complete you can login in using your new ADMIN account. On the your **Office 365 Subscription** page select and right click the **Go to subscription** hyper link and select Open Link in New Tab



Alex Zohab

Member since 4/3/2019

All your Office 365 developer subscriptions

To learn more about how to work with your subscription, see Build Office 365 solutions.

alexzohab.onmicrosoft.com

Go to subscription

Subscription

Expires on Apr 3, 2020

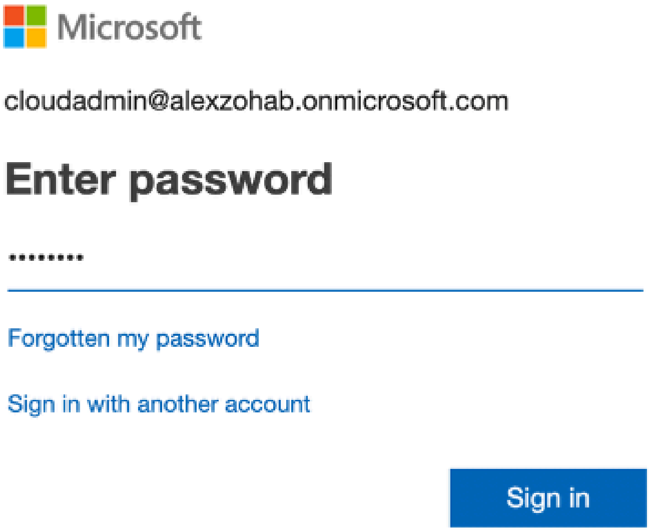
Administrator

cloudadmin@alexzohab.onmicrosoft.com

Users

25 accounts in total

18. On the **Sign In window** , Enter your **password** and select **Sign in**



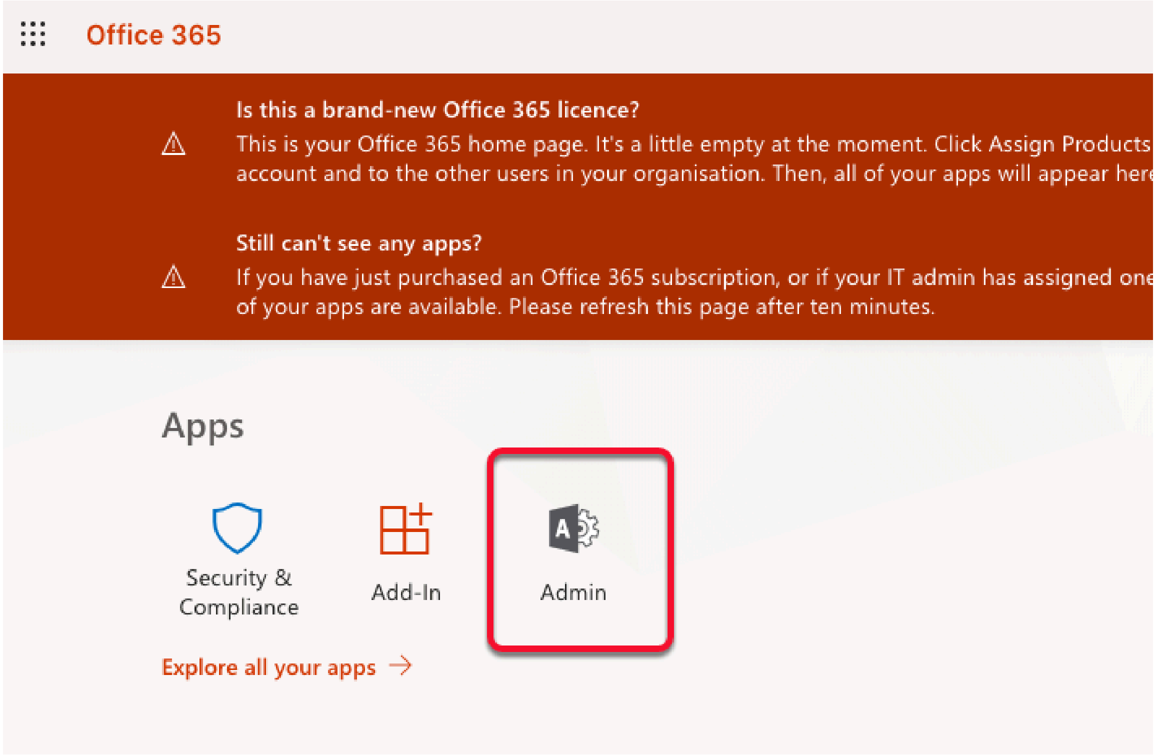
Microsoft

cloudadmin@alexzohab.onmicrosoft.com

Enter password

••••••••

19. On the **Office 365 Page** almost in the middle select **Admin**



Office 365

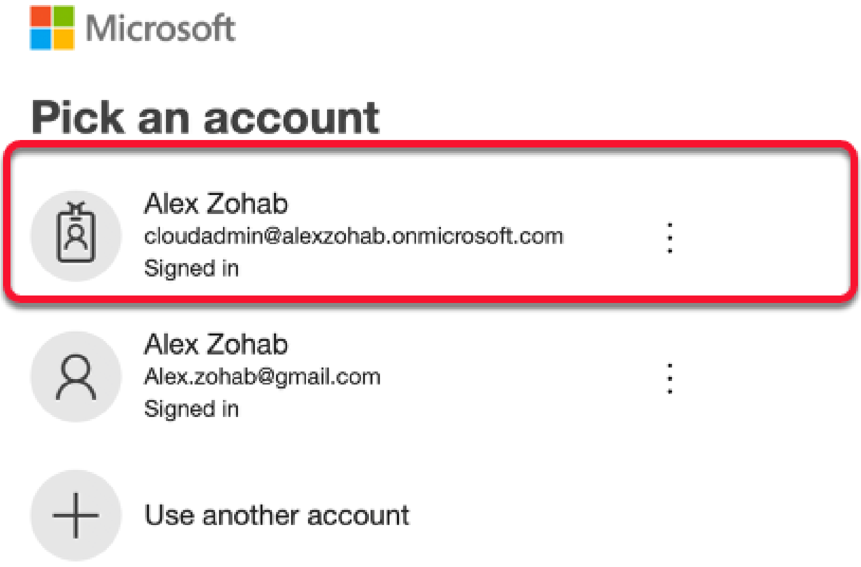
Is this a brand-new Office 365 licence?

⚠ This is your Office 365 home page. It's a little empty at the moment. Click Assign Products account and to the other users in your organisation. Then, all of your apps will appear here

Still can't see any apps?

⚠ If you have just purchased an Office 365 subscription, or if your IT admin has assigned one of your apps are available. Please refresh this page after ten minutes.

20. On the **sign in** page pick your new **CloudAdmin** account



Microsoft

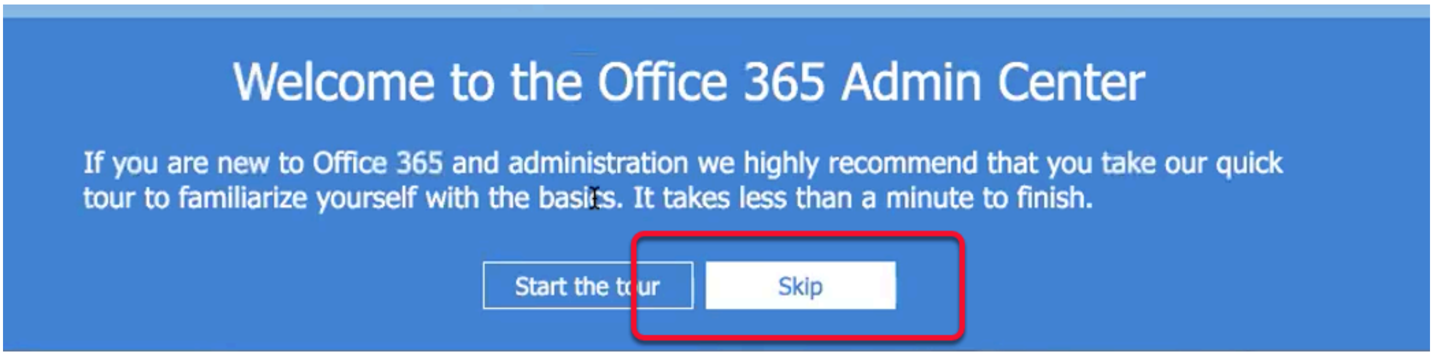
Pick an account

Alex Zohab
cloudadmin@alexzohab.onmicrosoft.com
Signed in

Alex Zohab
Alex.zohab@gmail.com
Signed in

Use another account

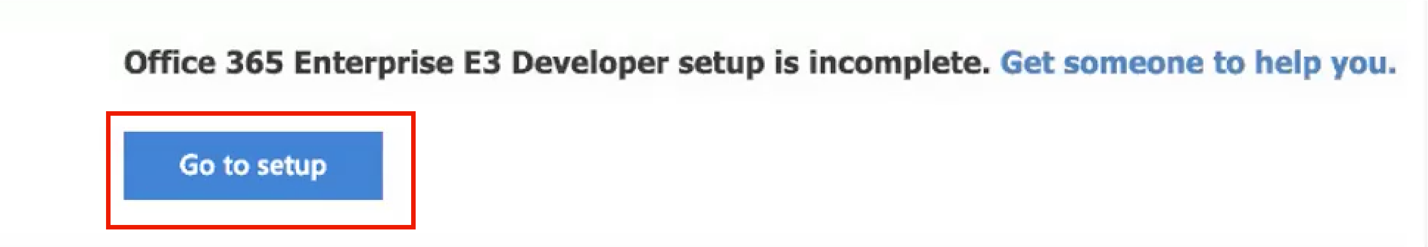
21. **If** you get prompted with a Welcome to **Office 365 Admin Center** Page select **Skip**



Welcome to the Office 365 Admin Center

If you are new to Office 365 and administration we highly recommend that you take our quick tour to familiarize yourself with the basics. It takes less than a minute to finish.

22. Notice the **Office 365 E3 Developer Setup is incomplete**. Select **Go to Setup box**



Office 365 Enterprise E3 Developer setup is incomplete. Get someone to help you.

23. **NB!** Before moving onto the next section, ensure that you are **100% clear** what **YOUR** registered Domain will be.

In the course lab we will use a Domain naming convention based on the location we are delivering at.

For example if this training session was being delivered in Atlanta , your domain name might be **atlanta01.euc-livefire.com** for ***student number 1***. If we have 18 attendees there will be 18 different registered Domain names using the above mentioned naming convention. we have automated the dns configuration for this lab, so we will use a **vrealize automation self service portal** to configure your dns zone.

On the **Microsoft 365 admin center** ensure the **Connect a domain you already own** radio button is selected and below ***type your registered Domain name*** (this example in the screenshot is only for demo purposes) select **Next**

❗ Note when registering your own domain name with Office 365, there are several approaches. The most seamless and trouble free approach is to register your own Domain Name with GODADDY. This provides a seamless experience and the verification takes seconds once you have your own domain name from GODADDY. GODADDY is an example of a name provider that seamlessly integrates with Microsoft's Office 365. If one chose this option your name that you use would belong to you for however long you choose to use your Office 365 Tenant

Another approach is to do this manually. EUC Livefire already owns a domain name which is hosted in AWS Route53. In the Office 365 setup wizard you will notice there is a step by step guide on how to setup your zone in AWS Route53 manually. We have chosen to automate this process for the sake of time.

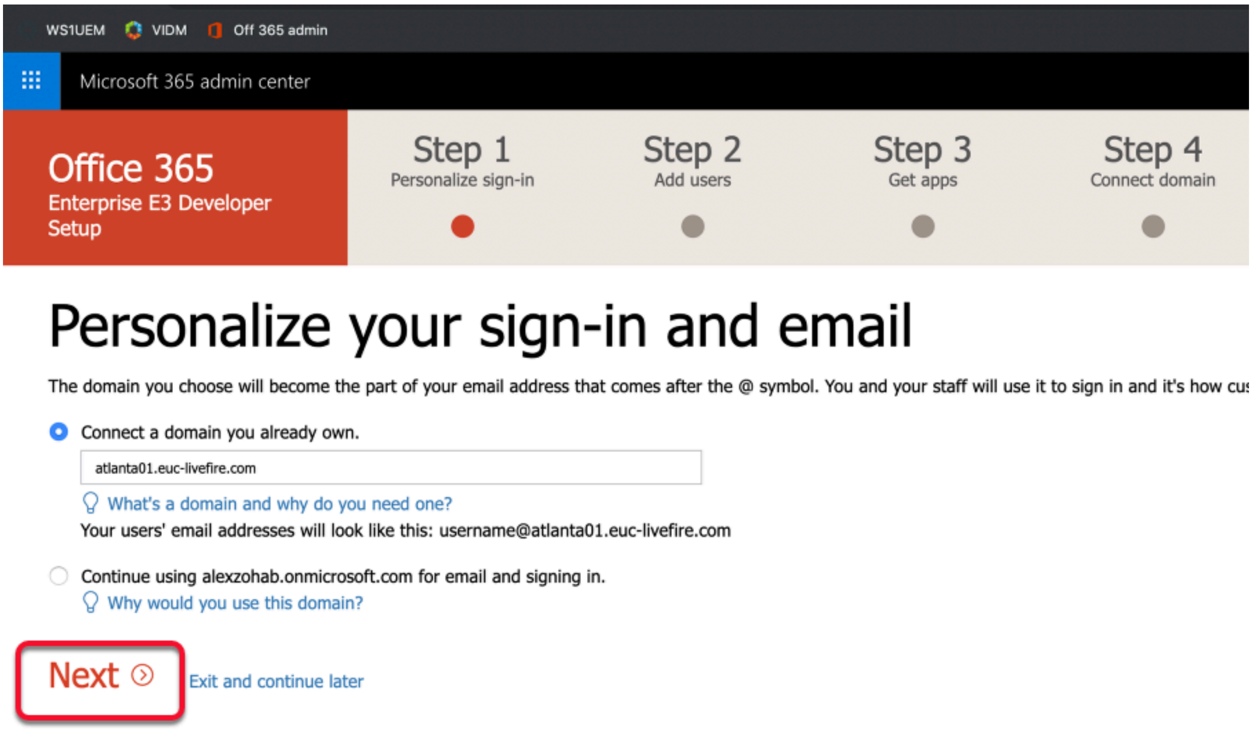
If you choose this option the zone provided to you by Livefire associated with your tenant will possibly only be active for a maximum of a month and you will then have to find your own Domain name.

If you choose to follow the Livefire option, we have automated this process for your convenience using VMware VRA. Generally DNS name configuration in AWS Area 53 is a completely Manual process. We have automated more than 98% of this process. You will however interface with VMware vRealize Automation for 2 configurations.

1. **MS record** modification

2. **MX record** modification

You do not have Access to AWS AREA53. You will be using VMware vRealize Automation to facilitate the edit of these records



Personalize your sign-in and email

The domain you choose will become the part of your email address that comes after the @ symbol. You and your staff will use it to sign in and it's how cus

● Connect a domain you already own.

atlanta01.euc-livefire.com

What's a domain and why do you need one?

Your users' email addresses will look like this: username@atlanta01.euc-livefire.com

○ Continue using alexzohab.onmicrosoft.com for email and signing in.

Why would you use this domain?

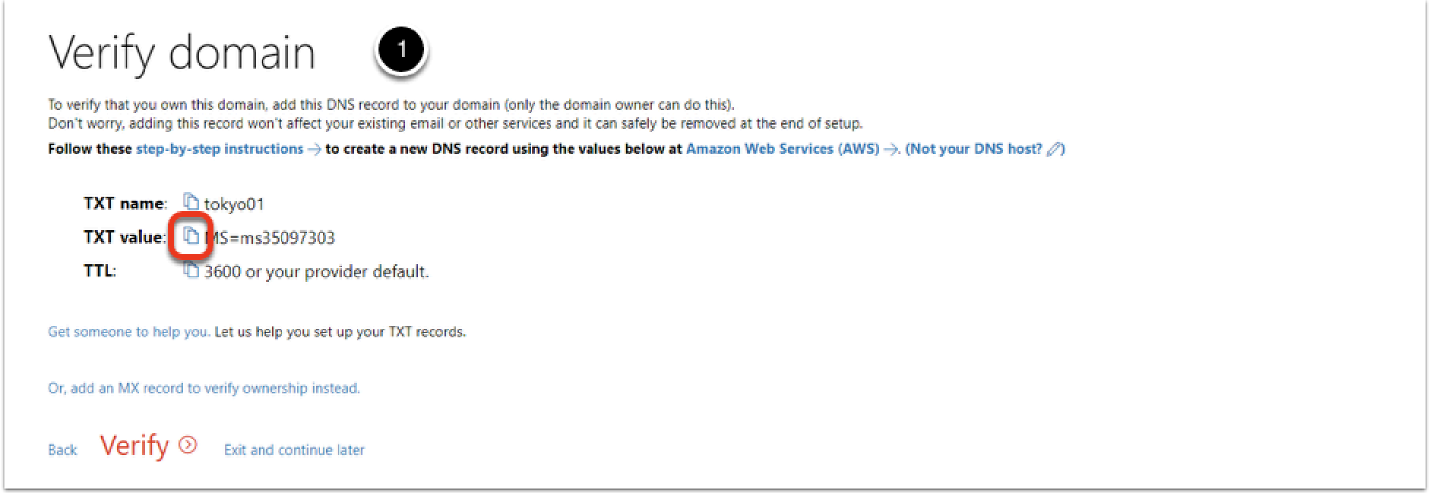
24. On the **Verify domain** page notice there are step-by-step instructions to follow,

Notice that there are DNS records called **TXT name**, **TXT value** and **TTL**

- Note!. We have our Hosted DNS service in called AREA53 on AWS. We have our own euc-livefire.com Zone. Each of you have your own registered Zone Database, that is part of the EUC-Livefire.com namespace. eg. Tokyo01.euc-livefire.com. Your Office 365 instance will need to be verified with this namespace .To do this will require to modify your DNS subzone, working with the vrealize automation portal in a different browser tab while your doing your o365 tenant.

1. Click on the **copy** icon next to your MS record
2. Select **Verify** at the bottom of the screen

NB! At this point ignore any error messages !



Verify domain

To verify that you own this domain, add this DNS record to your domain (only the domain owner can do this).
Don't worry, adding this record won't affect your existing email or other services and it can safely be removed at the end of setup.
Follow these step-by-step instructions → to create a new DNS record using the values below at Amazon Web Services (AWS) →. (Not your DNS host?)

TXT name: tokyo01
TXT value: MS=ms35097303
TTL: 3600 or your provider default.

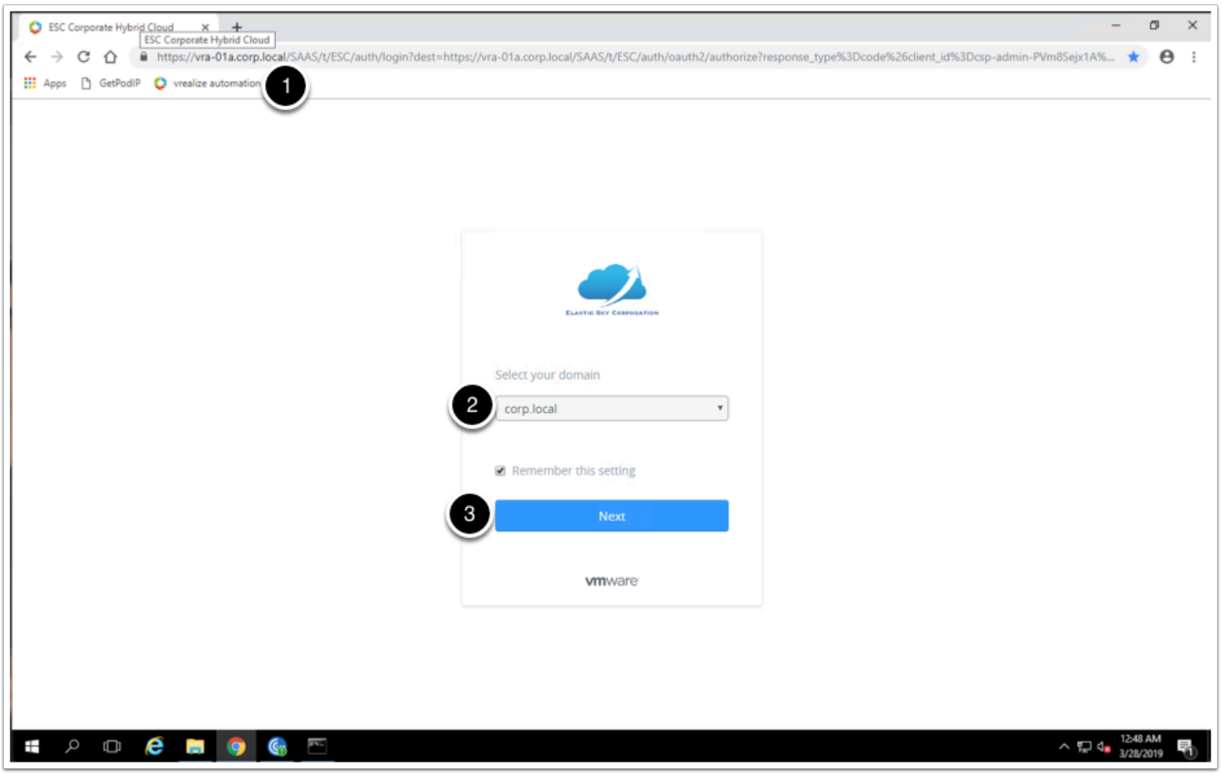
Get someone to help you. Let us help you set up your TXT records.

Or, add an MX record to verify ownership instead.

25

- On your **Controlcenter2 desktop**, from your task bar open your **FireFox Browser**

1. Next to the bookmarks bar open **vrealize automation**
2. Next to the "**Select your domain**" dropdown menu select **corp.local**
3. Select Next



https://vra-01a.corp.local/SAAS/t/ESC/auth/login?dest=https://vra-01a.corp.local/SAAS/t/ESC/auth/oauth2/authorize?response_type%3Dcode%26client_id%3Dcsp-admin-PVm8Sejx1A%...

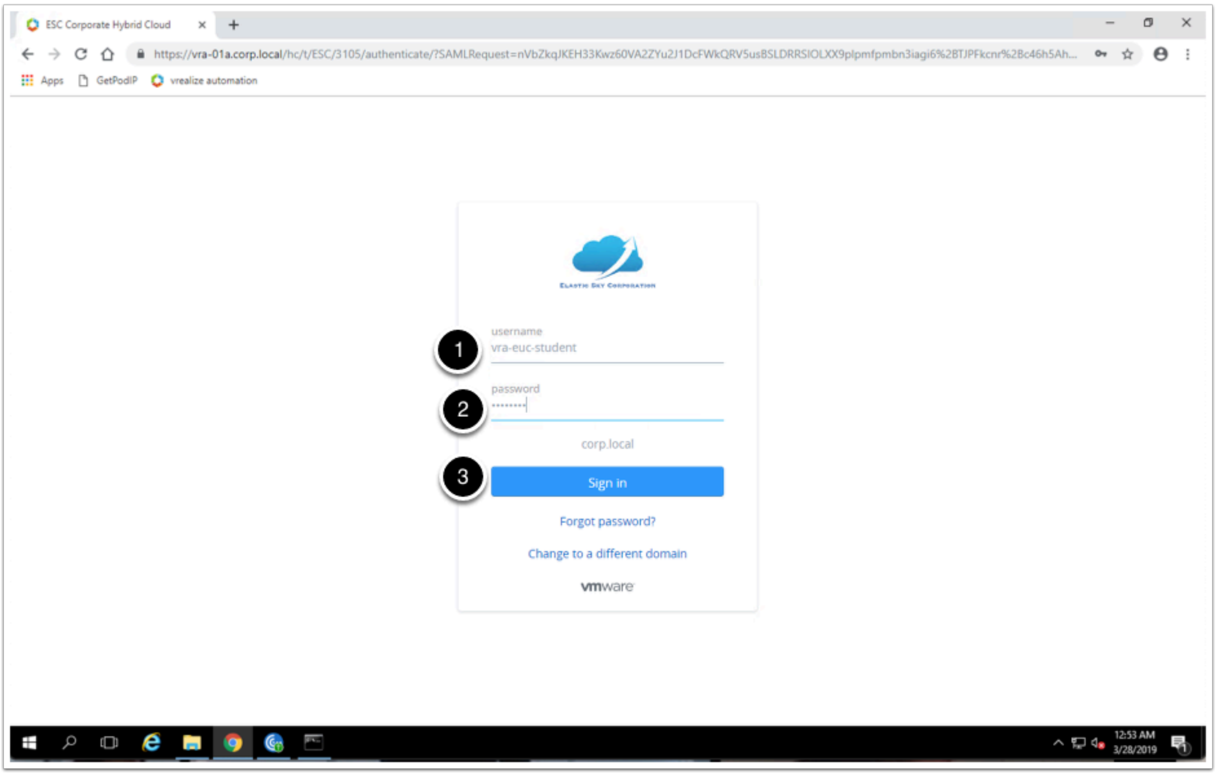
Select your domain

corp.local

☑ Remember this setting

26.

- VRA automation continued ...
  1. In the **username** field type **vra-euc-student**
  2. In the **password** field type **VMware1!**
  3. select **Sign in**



https://vra-01a.corp.local/hc/t/ESC/3105/authenticate/?SAMLRequest=nVbZkqJKEH33Kwz60VA2ZYu2J1DcFWkQRV5usBSLDRRSIOLXX9plpmfpmbn3iagi6%2BTJPFkcnr%2Bc46h5Ah...

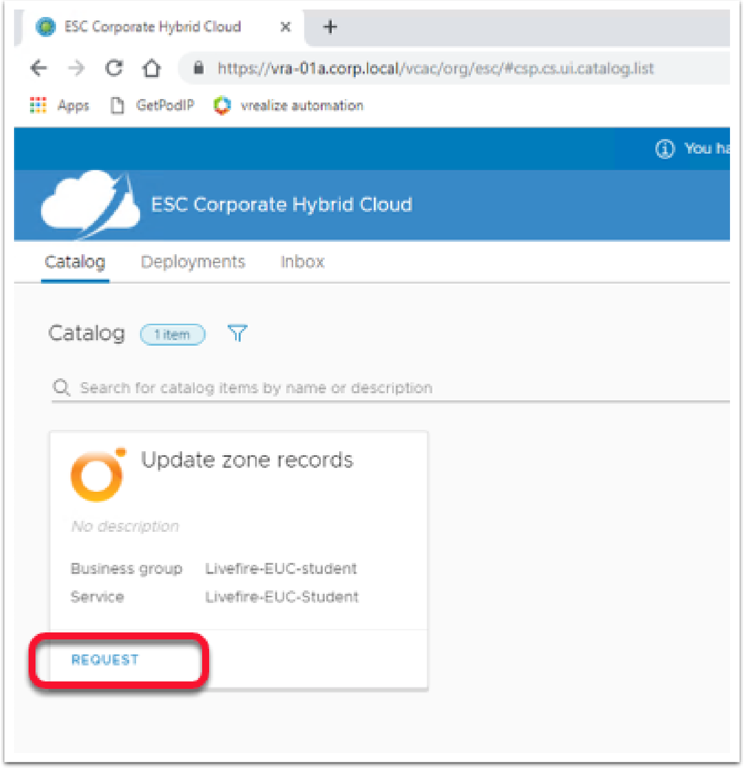
username
vra-euc-student

password
••••••••

corp.local

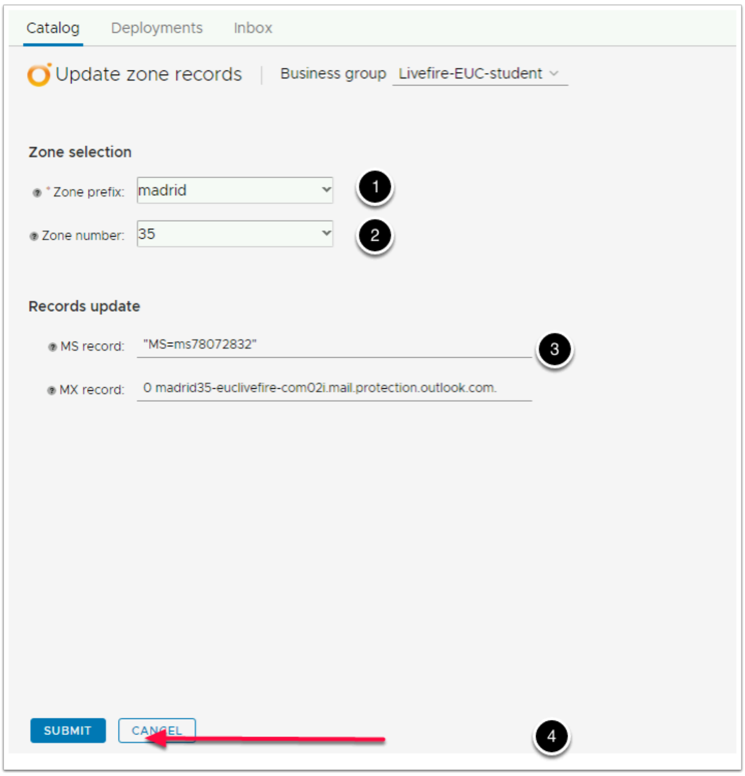
27. VRA automation continued ...

- In the **update zone records** catalog object, select **Request**



27.

- VRA automation continued ...
  1. Next to **zone prefix** dropdown menu select the **city corresponding to your current location**.
  2. Next to **zone number** drop down menu select **your dns zone number** as described in your information sheet
  3. Under **Records update** next to **MS record** replace the existing record your MS record and Paste your **MS record,**
     NOTE ensure that your MS record is enclosed in Quotation Marks
  4. Select **Submit**



Catalog Deployments Inbox

Update zone records | Business group Livefire-EUC-student

Zone selection

* Zone prefix: madrid

Zone number: 35

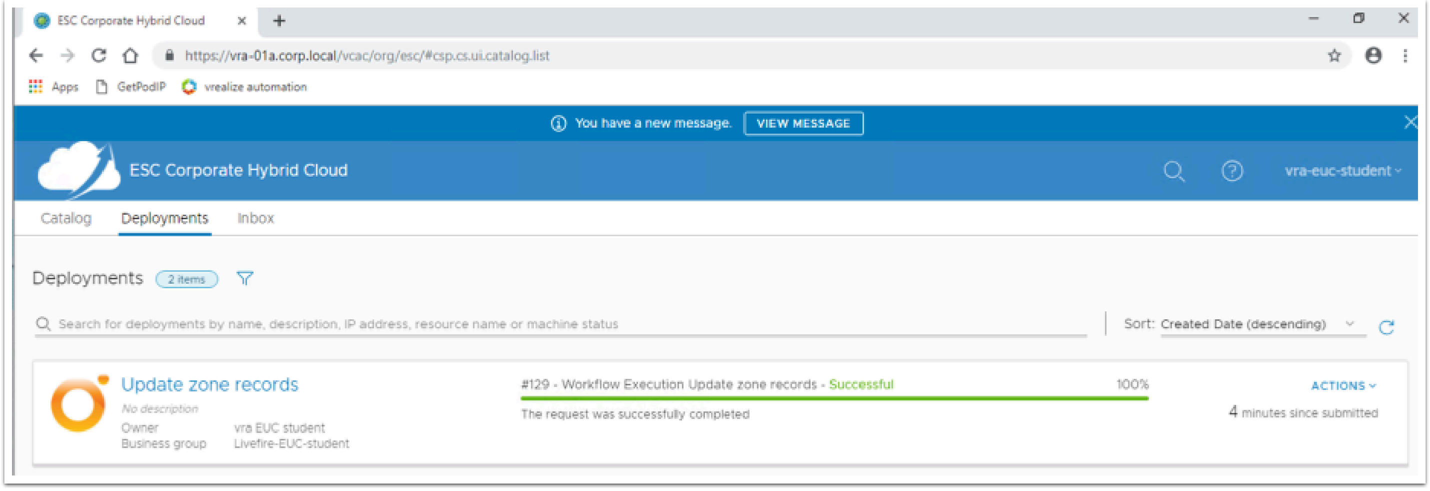
Records update

MS record: "MS=ms78072832"

MX record: 0 madrid35-euclivefire-com02i.mail.protection.outlook.com.

SUBMIT CANCEL

28. Wait until the progress shows 100% and continue with your lab. you might need to refresh your browser if you see no progress bar.



https://vra-01a.corp.local/vcac/org/esc/#csp.cs.ui.catalog.list

You have a new message. VIEW MESSAGE

ESC Corporate Hybrid Cloud

Catalog Deployments Inbox

Deployments 2 items

Search for deployments by name, description, IP address, resource name or machine status

Sort: Created Date (descending)

Update zone records

No description

Owner vra EUC student

Business group Livefire-EUC-student

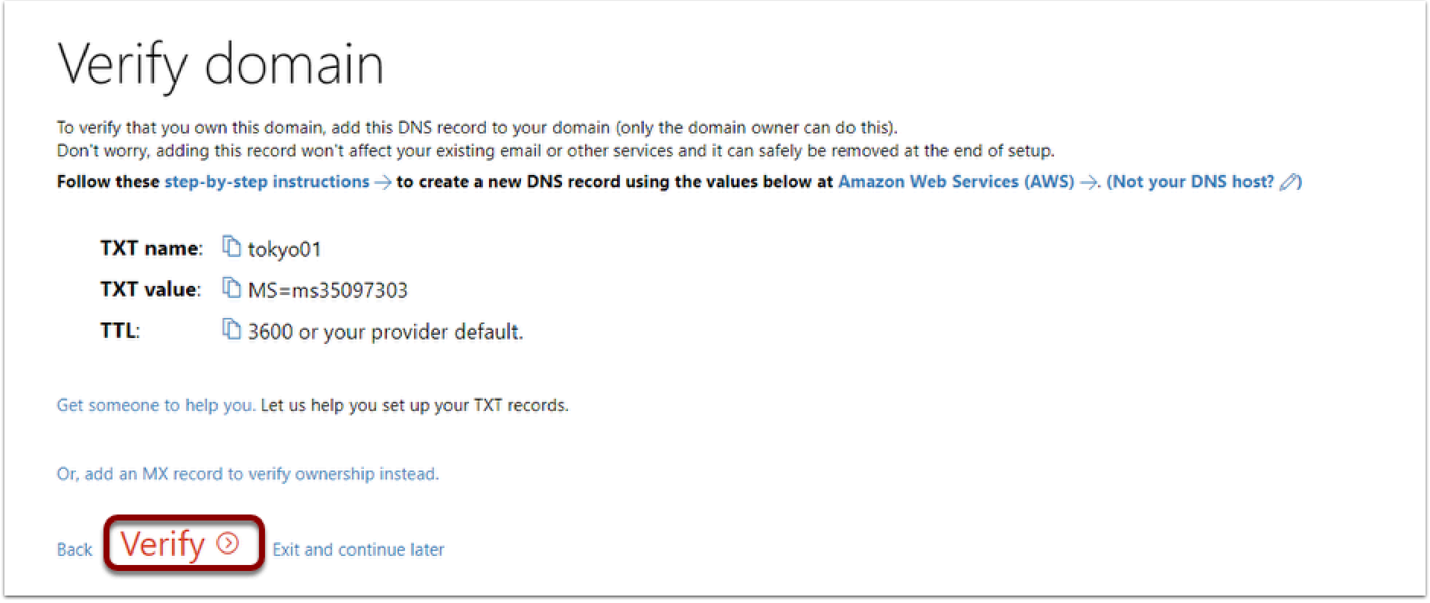
#129 - Workflow Execution Update zone records - Successful 100%

The request was successfully completed

ACTIONS

4 minutes since submitted

29 .Go back to your o365 domain configuration and click on **verify**. it might give you an error because of the time it takes to replicate DNS configurations and it might require you to click on verify a couple more times.



Verify domain

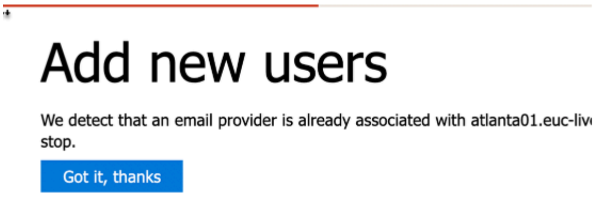
To verify that you own this domain, add this DNS record to your domain (only the domain owner can do this).
Don't worry, adding this record won't affect your existing email or other services and it can safely be removed at the end of setup.
Follow these step-by-step instructions → **to create a new DNS record using the values below at** Amazon Web Services (AWS) →. (Not your DNS host?)

TXT name: tokyo01
TXT value: MS=ms35097303
TTL: 3600 or your provider default.

Get someone to help you. Let us help you set up your TXT records.

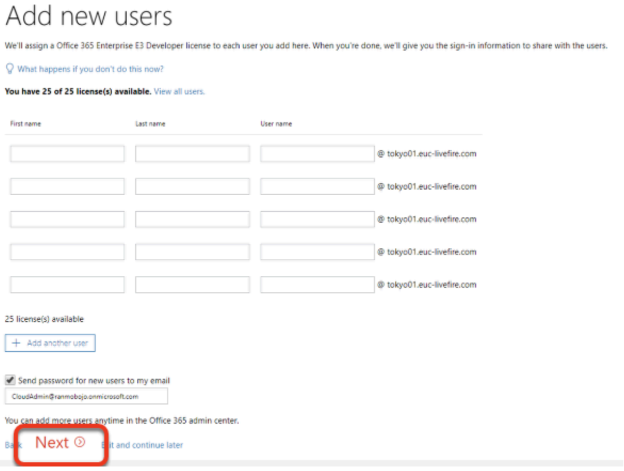
Or, add an MX record to verify ownership instead.

30. On **Add new users** window select **Got it, thanks,** select Next



Add new users

We detect that an email provider is already associated with atlanta01.euc-live
stop.



Add new users

We'll assign a Office 365 Enterprise E3 Developer license to each user you add here. When you're done, we'll give you the sign-in information to share with the users.

What happens if you don't do this now?

You have 25 of 25 license(s) available. View all users.

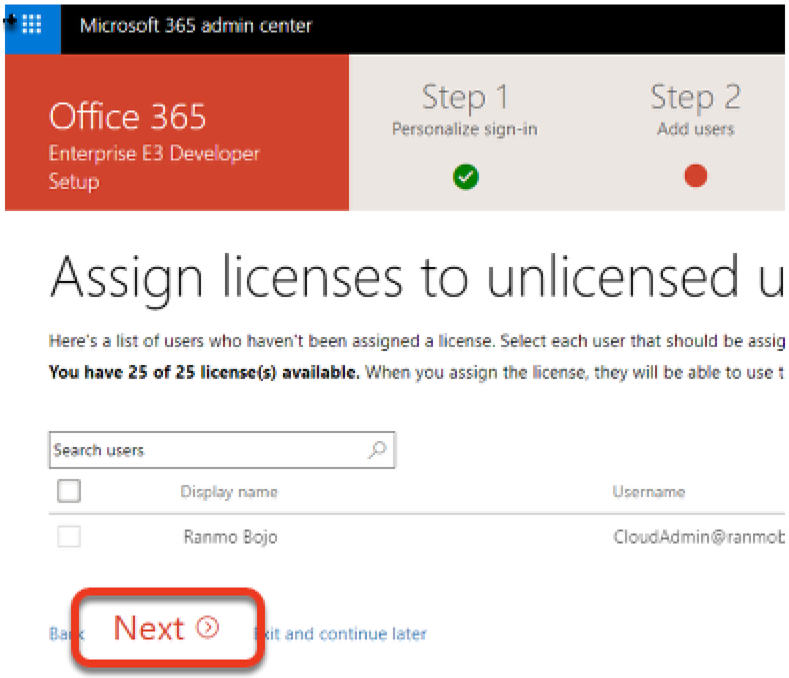
First name	Last name	User name
		@ tokyo01.euc-livefire.com
		@ tokyo01.euc-livefire.com
		@ tokyo01.euc-livefire.com
		@ tokyo01.euc-livefire.com
		@ tokyo01.euc-livefire.com

25 license(s) available

☑ Send password for new users to my email
CloudAdmin@ranmobojo.onmicrosoft.com

You can add more users anytime in the Office 365 admin center.

31. On the **Assign licenses to unlicensed users** page select **Next**



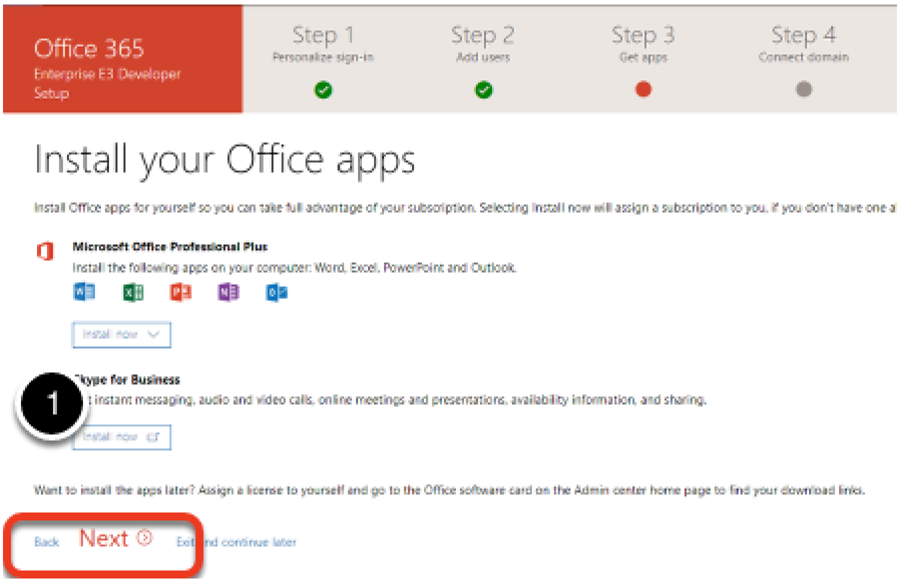
Assign licenses to unlicensed u

Here's a list of users who haven't been assigned a license. Select each user that should be assig

You have 25 of 25 license(s) available. When you assign the license, they will be able to use t

□	Display name	Username
□	Ranmo Bojo	CloudAdmin@ranmob

32. On **Install your Office apps** page select **Next**



Install your Office apps

Install Office apps for yourself so you can take full advantage of your subscription. Selecting Install now will assign a subscription to you. If you don't have one a

Microsoft Office Professional Plus

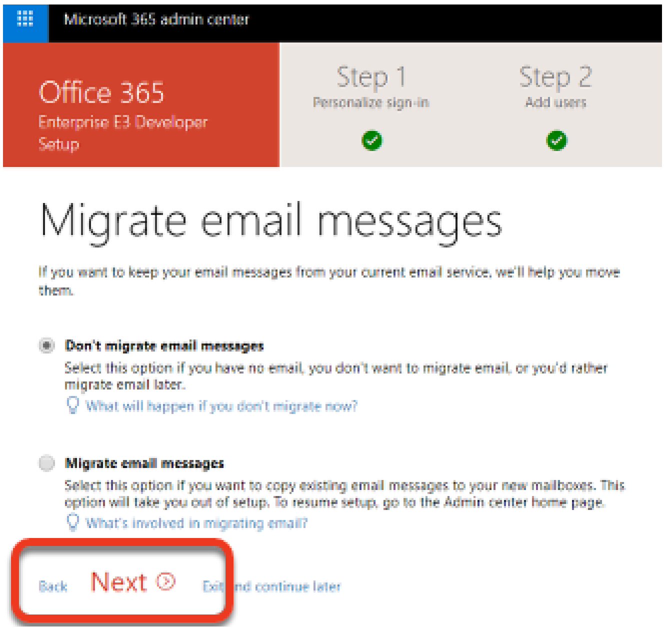
Install the following apps on your computer: Word, Excel, PowerPoint and Outlook.

Skype for Business

t instant messaging, audio and video calls, online meetings and presentations, availability information, and sharing.

Want to install the apps later? Assign a license to yourself and go to the Office software card on the Admin center home page to find your download links.

33. On the **Migrate email messages** page leave the default **Don't migrate email messages** radio button and select **Next**



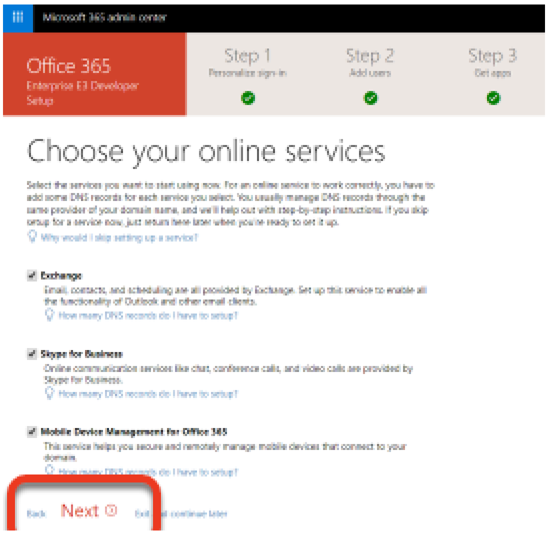
Migrate email messages

If you want to keep your email messages from your current email service, we'll help you move them.

● **Don't migrate email messages**
Select this option if you have no email, you don't want to migrate email, or you'd rather migrate email later.
What will happen if you don't migrate now?

○ **Migrate email messages**
Select this option if you want to copy existing email messages to your new mailboxes. This option will take you out of setup. To resume setup, go to the Admin center home page.
What's involved in migrating email?

34. On the **Choose your online services** page, ensure that **Exchange, Skype for Business** and **Mobile Device Management for Office 365 checkboxes** are selected and select **Next**



Choose your online services

Select the services you want to start using now. For an online service to work correctly, you have to add some DNS records for each service you select. You usually manage DNS records through the same provider of your domain name, and we'll help out with step-by-step instructions. If you skip setup for a service now, just return here later when you're ready to set it up.
Why would I skip setting up a service?

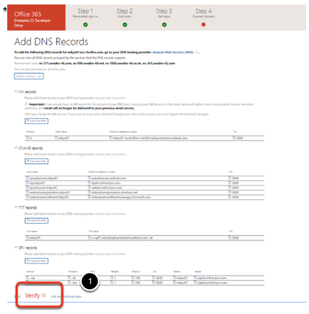
☑ **Exchange**
Email, contacts, and scheduling are all provided by Exchange. Set up this service to enable all the functionality of Outlook and other email clients.
How many DNS records do I have to setup?

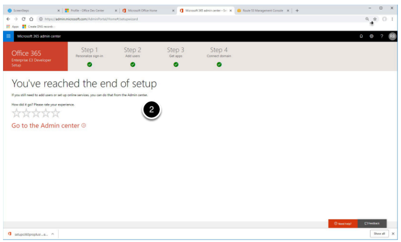
☑ **Skype for Business**
Online communication services like chat, conference calls, and video calls are provided by Skype for Business.
How many DNS records do I have to setup?

☑ **Mobile Device Management for Office 365**
This service helps you secure and remotely manage mobile devices that connect to your domain.
How many DNS records do I have to setup?

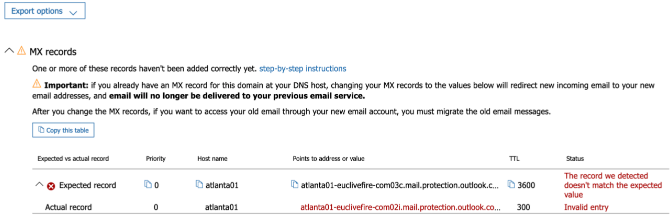
35.

- On the **Add DNS Records** page.
  1. When ready select **Verify** at the bottom of the **Add DNS Records** window. If there is a failure on any records reach out to the EUC-livefire instructor team to get the records fixed and select
     Verify again. Note you might have to give a few minutes for the records to update in DNS before selecting **Verify**
  2. Notice that when **Verify** is successful the **you just configured your Office 365 Tenant successfully** will show and you are ask to provide feedback related to your experience.
- However, If Verify is Not successful and its MX related in the message go to the next step in this exercise.





You've reached the end of setup



MX records

One or more of these records haven't been added correctly yet. step-by-step instructions

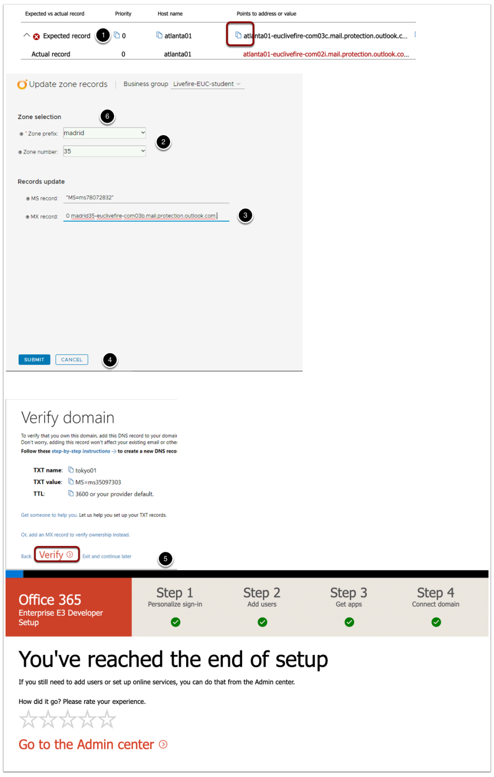
⚠ **Important:** if you already have an MX record for this domain at your DNS host, changing your MX records to the values below will redirect new incoming email to your new email addresses, and **email will no longer be delivered to your previous email service.**

After you change the MX records, if you want to access your old email through your new email account, you must migrate the old email messages.

Expected vs actual record	Priority	Host name	Points to address or value	TTL	Status
Expected record	0	atlanta01	atlanta01-euclivefire-com03c.mail.protection.outlook.c...	3600	The record we detected doesn't match the expected value
Actual record	0	atlanta01	atlanta01-euclivefire-com02i.mail.protection.outlook.co...	300	Invalid entry

36

- If you get an error mentioning your **MX records** follow these steps:
  1. Click on the the **copy** icon next to **Expected record**
  2. On your **ControlCenter2** server, Go back to the **update zone records tool,** select **REQUEST**
  3. Get to your zone and paste the **MX records**,
     - NOTE the example, there is a zero in front MX record, this is a priority field and should not be deleted.
  4. Select **SUBMIT**
  5. Go to your 0365 domain configuration and **Verify** the domain again.
  6. You should get a message saying You've reached the end of the setup



Expected vs actual record	Priority	Host name	Points to address or value
Expected record	0	atlanta01	atlanta01-euclivefire-com03c.mail.protection.outlook.c...
Actual record	0	atlanta01	atlanta01-euclivefire-com02i.mail.protection.outlook.co...

Update zone records | Business group Livefire-EUC-student

Zone selection

* Zone prefix: madrid

Zone number: 35

Records update

MS record: "MS=ms78072832"

MX record: 0 madrid35-euclivefire-com03b.mail.protection.outlook.com

SUBMIT CANCEL

Verify domain

To verify that you own this domain, add this DNS record to your domai
Don't worry, adding this record won't affect your existing email or othe
Follow these step-by-step instructions → to create a new DNS reco

TXT name: tokyo01
TXT value: MS=ms35097303
TTL: 3600 or your provider default.

Get someone to help you. Let us help you set up your TXT records.

Or, add an MX record to verify ownership instead.

Back Verify Exit and continue later

Office 365
Enterprise E3 Developer
Setup

Step 1 Personalize sign-in ✓
Step 2 Add users ✓
Step 3 Get apps ✓
Step 4 Connect domain ✓

You've reached the end of setup

If you still need to add users or set up online services, you can do that from the Admin center.

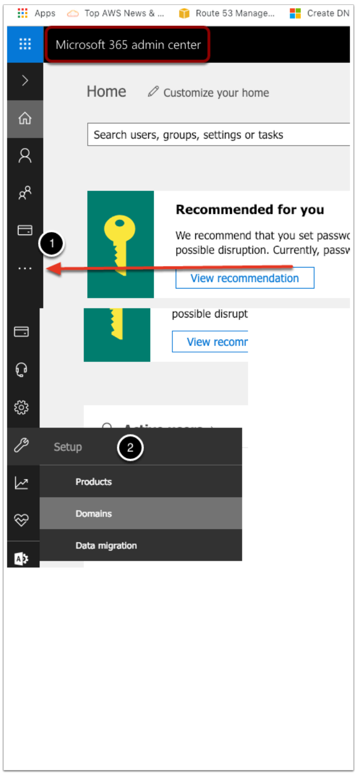
How did it go? Please rate your experience.

☆☆☆☆☆

Go to the Admin center

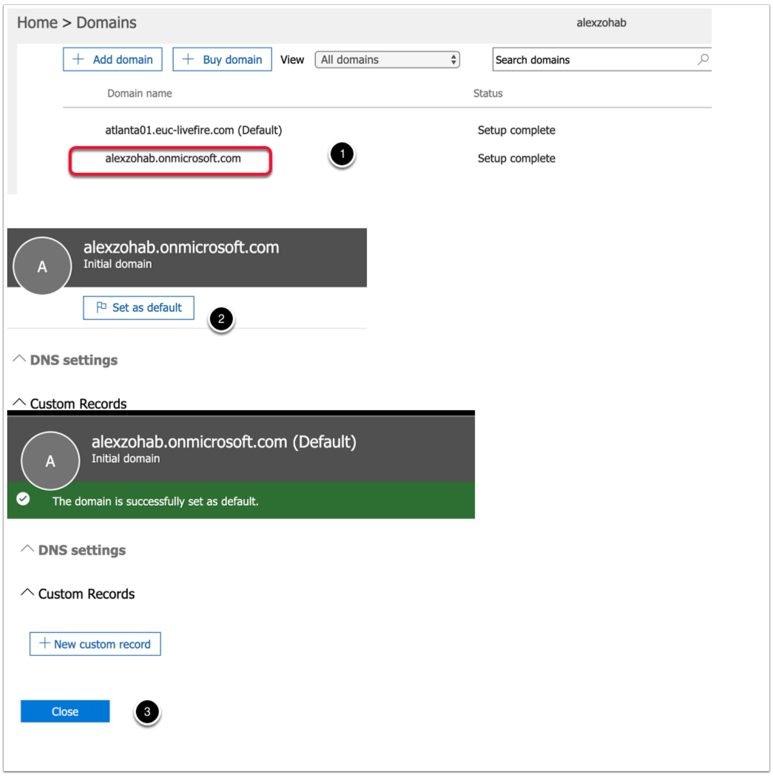
37. Select **Microsoft 365 Admin center** next to the **9 dot blue square** in the top left corner.

- In your Microsoft 365 Admin center,
  1. Select the 3 parallel dots in the black bar to the left of the console, this will expand the console
  2. Select the Spanner icon for **Setup** and select **Domains**



38.

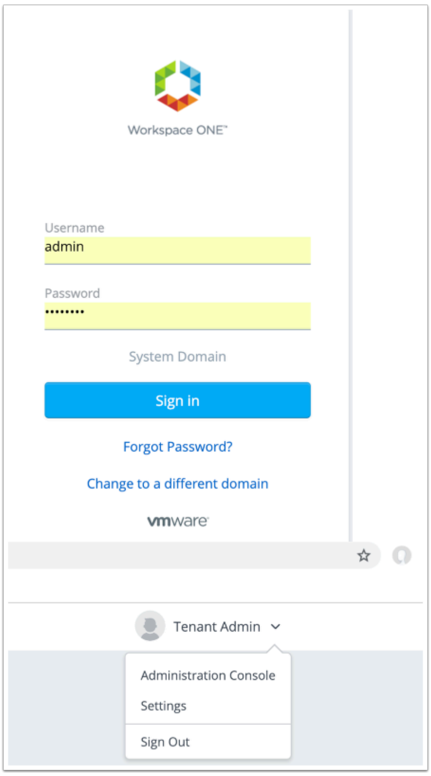
- In the **Home** > **Domains** interface, check to see if your namespace you have associated with your Office 365 setup has a **(Default)** next to it. If this is the case do the following.
  1. Select your **account name** that is not set to default :
  2. Select **Set as default**
  3. Your custom domain cannot be the default domain when federating with Workspace ONE Access. Select **Close.** Check to see that you have a corresponding configuration in the domain portion of your setup as the screenshot.



Part 2: Federating Office 365 with Workspace ONE Access.

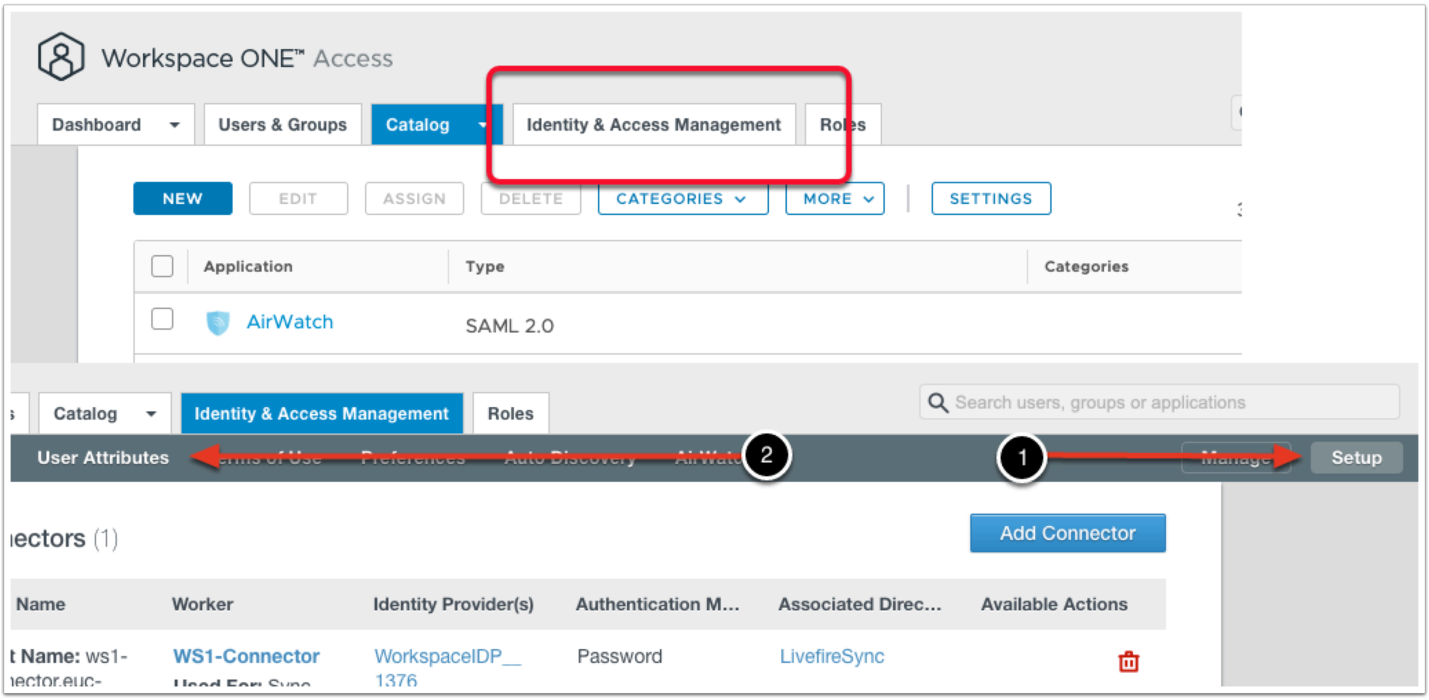
In Part 2 of this lab session we will now federate our Office 365 Tenant with a Workspace ONE Access SAAS tenant.

1. Using your **Tenant Admin** credentials, login into your **SAAS Workspace ONE Access** Tenant.
   1. To the right of the **Workspace ONE Access** console under **Tenant Admin** select **Administration Console**



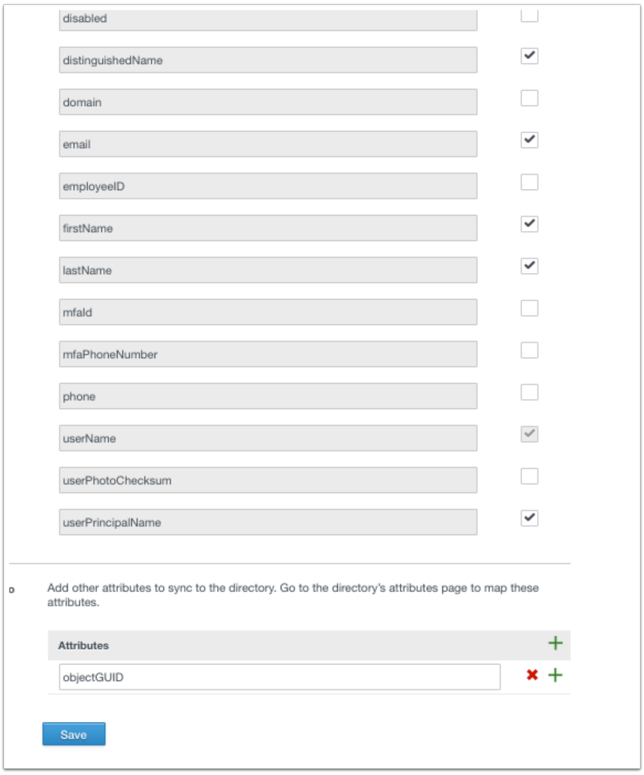
2. Select the **Identity & Access Management** tab

- To the right in the **Identity & Access Management** tab select **Setup** > **User Attributes**



3. In the **User Attributes** interface notice you have already set **userPrincipalName** and **distinguishedName** to **Required** and you have already created the **objectGUID** attribute.

These are pre-req requirements for Federating Office 365 with Workspace ONE Access.



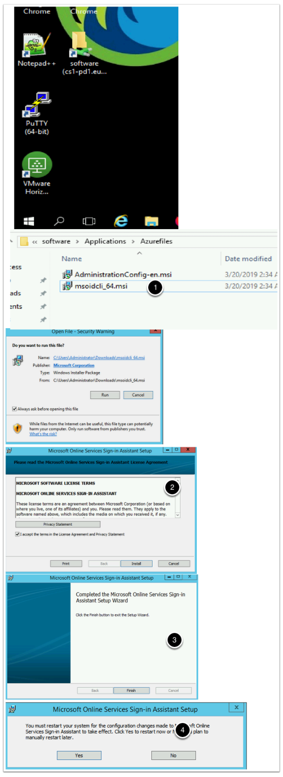
disabled	□
distinguishedName	☑
domain	□
email	☑
employeeID	□
firstName	☑
lastName	☑
mfaId	□
mfaPhoneNumber	□
phone	□
userName	☑
userPhotoChecksum	□
userPrincipalName	☑

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

Attributes
objectGUID

4.

- On your **ControlCenter2** desktop server select your **Software** shortcut and open the path to the **Applications** folder. In the **Applications** folder open the **Azurefiles** folder.
  1. **Open** the **msoidcli_64.msi** installer and when prompted select **Run**
  2. On the **Microsoft Online Services Sign-in Assistant Setup** page select the **I accept the terms in the Licence agreement**... **checkbox.** Select **Install**,
  3. When the installer is done select **Finish**
  4. **If** prompted to **restart** then do so and login as administrator


Chrome
Chrome
Notepad++
software (cs1-pd1.eu...
PuTTY (64-bit)
VMware Horiz...
software › Applications › Azurefiles
Name
Date modified
AdministrationConfig-en.msi
3/20/2019 2:34
msoidcli_64.msi
3/20/2019 2:34
1
Open File - Security Warning
Run
Cancel
What's the risk?
Microsoft Online Services Sign-in Assistant Setup
2
Privacy Statement
Print
Back
Install
Cancel
Microsoft Online Services Sign-in Assistant Setup
3
Back
Finish
Cancel
Microsoft Online Services Sign-in Assistant Setup
4
Yes
No

Do you want to run this file?

Name: C:\Users\Administrator\Downloads\msoidcli_64.msi
Publisher: Microsoft Corporation
Type: Windows Installer Package
From: C:\Users\Administrator\Downloads\msoidcli_64.msi

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.

Please read the Microsoft Online Services Sign-in Assistant License Agreement

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT ONLINE SERVICES SIGN-IN ASSISTANT

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any.

☑ I accept the terms in the License Agreement and Privacy Statement

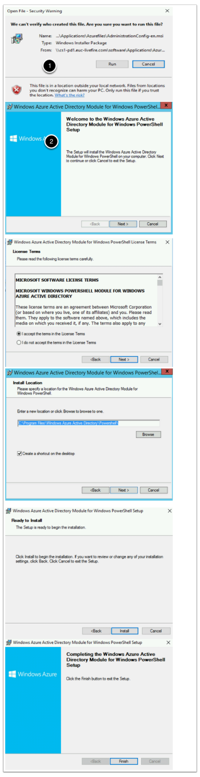
Completed the Microsoft Online Services Sign-in Assistant Setup Wizard

Click the Finish button to exit the Setup Wizard.

You must restart your system for the configuration changes made to ft Online Services Sign-in Assistant to take effect. Click Yes to restart now or plan to manually restart later.

5.

- Under the same **Azurefiles** folder,
  1. Select and launch the **AdministrationConfig-en.msi ,** select **Run**. **On the Open File - Security Warning** window select Run
  2. On the **Windows Azure Active Directory Module for Windows Powershell Setup** window select **Next**
  3. On the **License Terms** window , ensure the **I accept the terms radio button** is selected and select **Next**
  4. On the **Install Location** window, select **Next**
  5. On the **Ready to Install** window select **Install**
  6. Select **Finish**



Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

Name: ...\Applications\Azurefiles\AdministrationConfig-en.msi
Type: Windows Installer Package
From: \\cs1-pd1.euc-livefire.com\software\Applications\Azur...

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only run this file if you trust the location. What's the risk?

Windows Azure Active Directory Module for Windows PowerShel...

Welcome to the Windows Azure Active Directory Module for Windows PowerShell Setup

The Setup will install the Windows Azure Active Directory Module for Windows PowerShell on your computer. Click Next to continue or click Cancel to exit the Setup.

Windows Azure Active Directory Module for Windows PowerShell License Terms

License Terms
Please read the following license terms carefully.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS POWERSHELL MODULE FOR WINDOWS AZURE ACTIVE DIRECTORY

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any

● I accept the terms in the License Terms
○ I do not accept the terms in the License Terms

Windows Azure Active Directory Module for Windows PowerShel...

Install Location
Please specify a location for the Windows Azure Active Directory Module for Windows PowerShell.

Enter a new location or click Browse to browse to one.

C:\Program Files\Windows Azure Active Directory\Powershell\

☑ Create a shortcut on the desktop

Windows Azure Active Directory Module for Windows PowerShell Setup

Ready to Install
The Setup is ready to begin the installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the Setup.

Windows Azure Active Directory Module for Windows PowerShell Setup

Completing the Windows Azure Active Directory Module for Windows PowerShell Setup

Click the Finish button to exit the Setup.

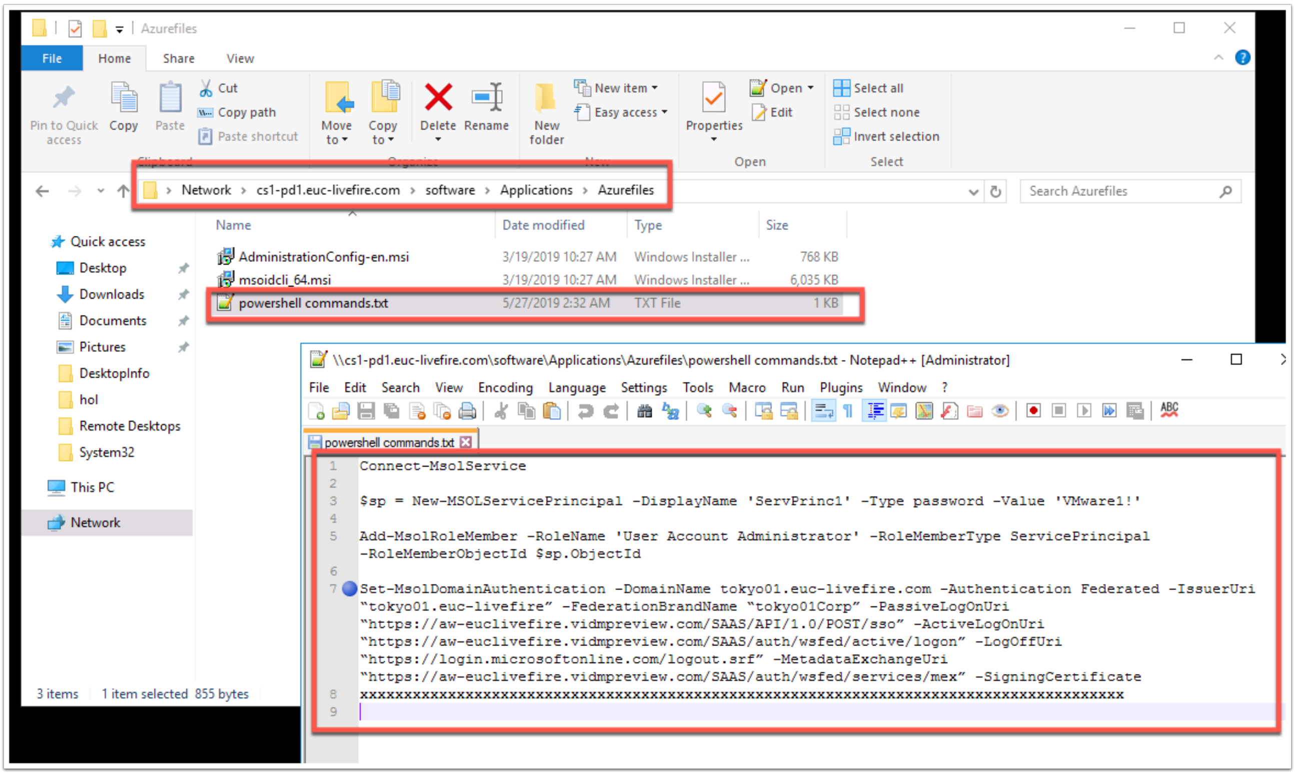
6.

- On your **ControlCenter** server desktop, you will notice a **Windows Azure Active Directory for Powershell** Shortcut.
  1. Right click the **Windows Powershell** and select **Run as administrator**
  2. For your convenience we have added all the powershell commands to a TXT file that is available in the software folder on the desktop.You can copy the commands from the file directly into the powershell. **Please note some of the commands require editing**
  3. Simply browse to **\\cs1-pd1.euc-livefire.com\software\Applications\Azurefiles** where you will find the file **powershell commands.txt**
  4. In the Powershell Console type the following

     ```
     Connect-MsolService
     ```

1. When prompted for **User name** and **Password**, use your Cloud Admin account e.g. ***cloudadmin@ranmobojo.onmicrosoft.com***
2. Next we have to create a Service Principal account type in the powershell

   ```
   $sp = New-MSOLServicePrincipal -DisplayName 'ServPrinc1' -Type password
   -Value 'VMware1!'
   ```
3. Next we are going to assign a role to the ServPrinc1 user
   ```
   Add-MsolRoleMember -RoleName 'User Account Administrator'
   -RoleMemberType ServicePrincipal -RoleMemberObjectId $sp.ObjectId
   ```



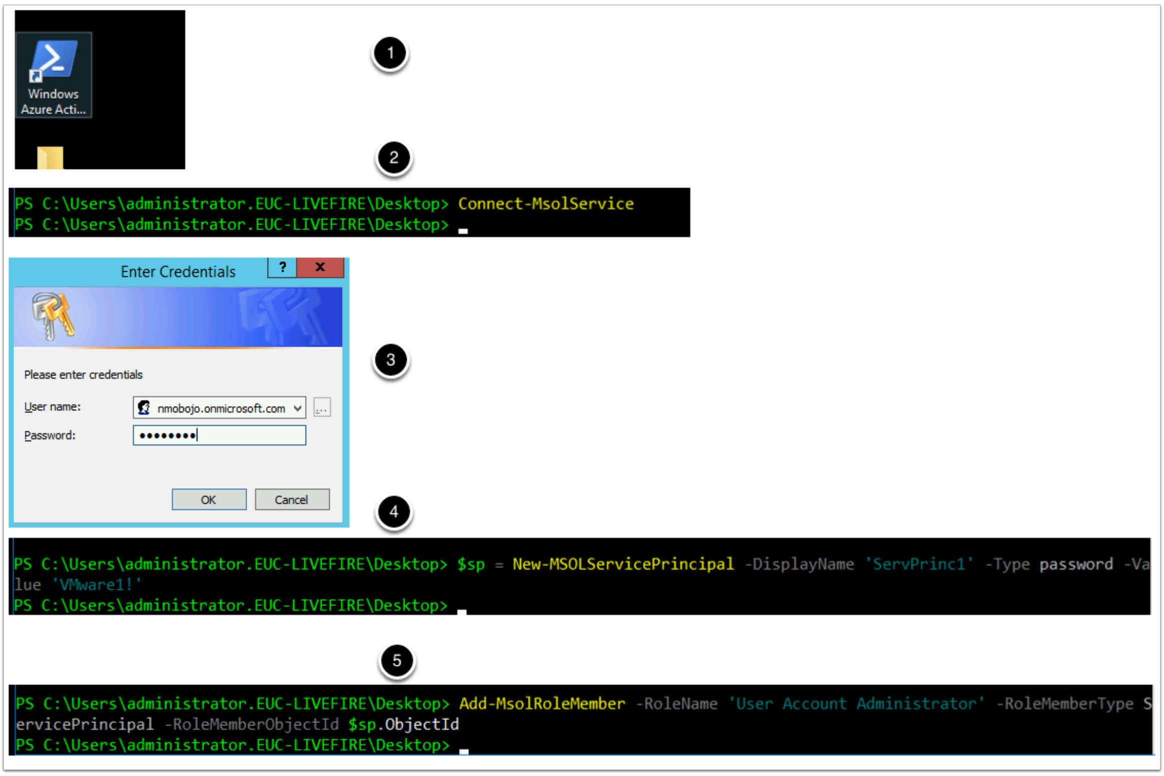
Network › cs1-pd1.euc-livefire.com › software › Applications › Azurefiles

Name	Date modified	Type	Size
AdministrationConfig-en.msi	3/19/2019 10:27 AM	Windows Installer ...	768 KB
msoidcli_64.msi	3/19/2019 10:27 AM	Windows Installer ...	6,035 KB
powershell commands.txt	5/27/2019 2:32 AM	TXT File	1 KB

3 items   1 item selected 855 bytes

\\cs1-pd1.euc-livefire.com\software\Applications\Azurefiles\powershell commands.txt - Notepad++ [Administrator]

```
Connect-MsolService

$sp = New-MSOLServicePrincipal -DisplayName 'ServPrinc1' -Type password -Value 'VMware1!'

Add-MsolRoleMember -RoleName 'User Account Administrator' -RoleMemberType ServicePrincipal
-RoleMemberObjectId $sp.ObjectId

Set-MsolDomainAuthentication -DomainName tokyo01.euc-livefire.com -Authentication Federated -IssuerUri
"tokyo01.euc-livefire" -FederationBrandName "tokyo01Corp" -PassiveLogOnUri
"https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/POST/sso" -ActiveLogOnUri
"https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/active/logon" -LogOffUri
"https://login.microsoftonline.com/logout.srf" -MetadataExchangeUri
"https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/services/mex" -SigningCertificate
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

```



1

2

```
PS C:\Users\administrator.EUC-LIVEFIRE\Desktop> Connect-MsolService
PS C:\Users\administrator.EUC-LIVEFIRE\Desktop> _
```

3

Please enter credentials

User name: nmobojo.onmicrosoft.com

Password: ••••••••

4

```
PS C:\Users\administrator.EUC-LIVEFIRE\Desktop> $sp = New-MSOLServicePrincipal -DisplayName 'ServPrinc1' -Type password -Va
lue 'VMware1!'
PS C:\Users\administrator.EUC-LIVEFIRE\Desktop> _
```

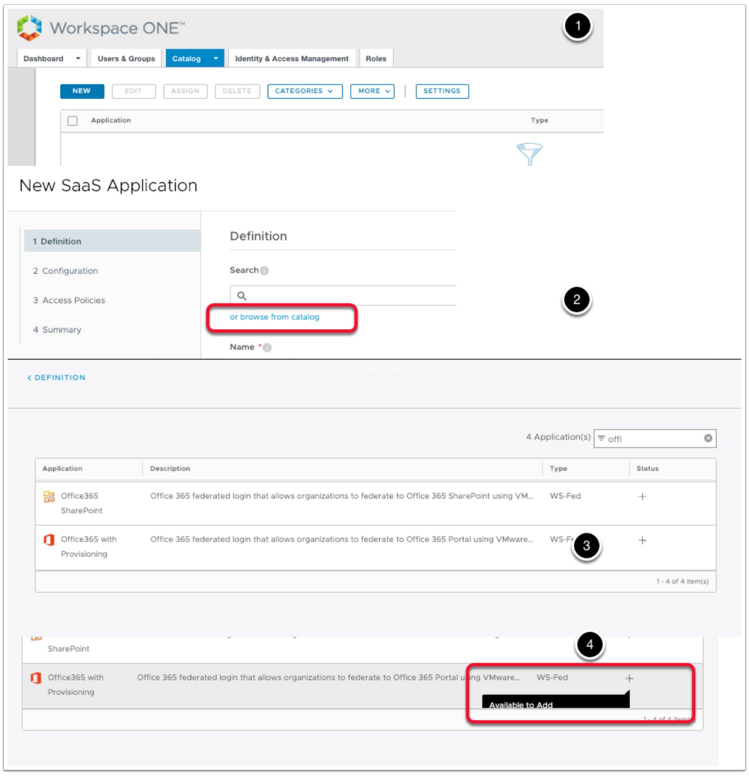
5

```
PS C:\Users\administrator.EUC-LIVEFIRE\Desktop> Add-MsolRoleMember -RoleName 'User Account Administrator' -RoleMemberType S
ervicePrincipal -RoleMemberObjectId $sp.ObjectId
PS C:\Users\administrator.EUC-LIVEFIRE\Desktop> _
```

7

- Revert back to your Workspace ONE Access SAAS Tenant Admin Console
  1. Select the Catalog Tab in the **Admin Console**, select NEW
  2. In the **New SaaS Application** window under **Definition** select **or browse from catalog**
  3. In the **DEFINITION** window to the right in the **search** area type **off**

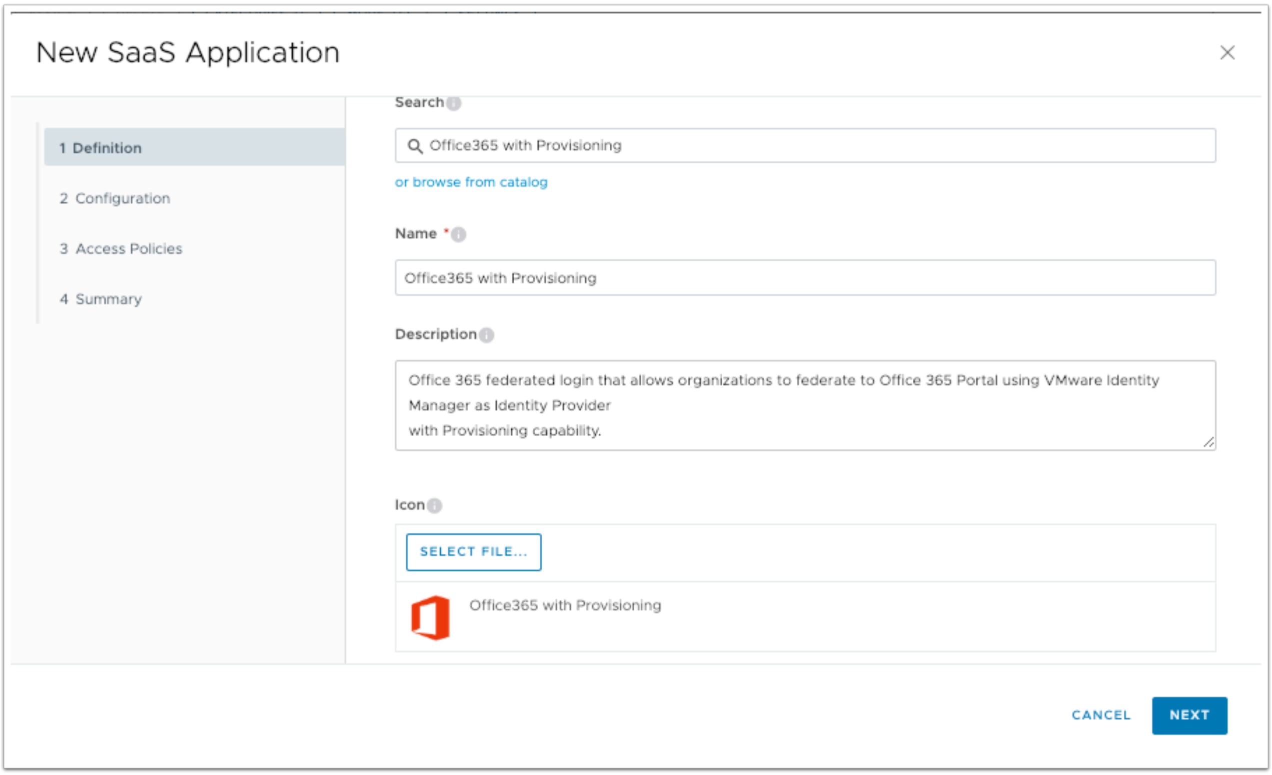
4. Select **Office365 with Provisioning** by selecting the + sign to the right



Application	Description	Type	Status
Office365 SharePoint	Office 365 federated login that allows organizations to federate to Office 365 SharePoint using VM...	WS-Fed	+
Office365 with Provisioning	Office 365 federated login that allows organizations to federate to Office 365 Portal using VMware...	WS-Fed	+

1 - 4 of 4 item(s)

8 On the New SAAS Application window select **Next**



Search: Office365 with Provisioning

Name *: Office365 with Provisioning

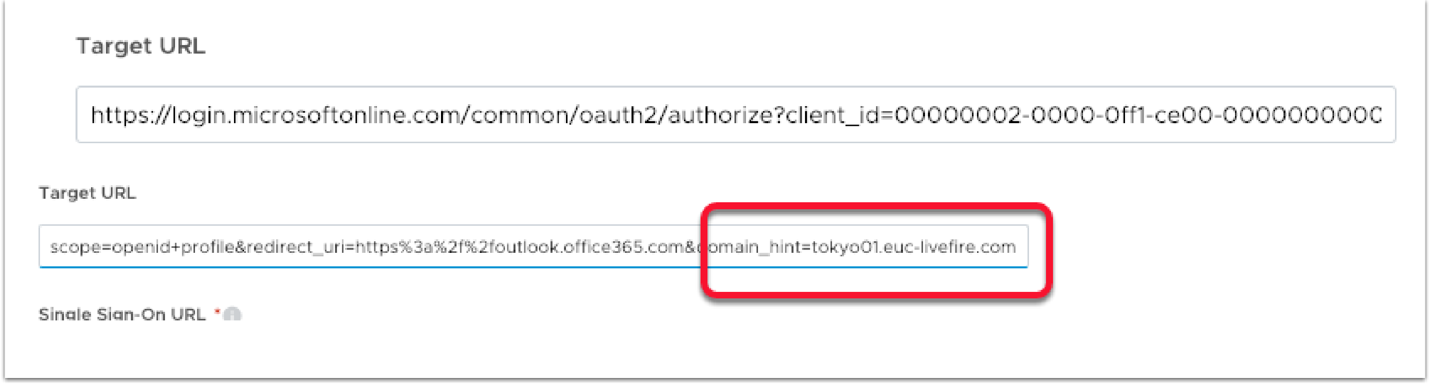
Description: Office 365 federated login that allows organizations to federate to Office 365 Portal using VMware Identity Manager as Identity Provider
with Provisioning capability.

Icon: Office365 with Provisioning

9. In the **New Saas Application** window, in the **Configuration** section add the following:

- Under **Target URL** add the following. Actual text to copy to edit into the configuration is in **BLUE**
- **edit the last area** after hint= ....domain_hint=tokyo01.euc-livefire.com

```
https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-
ce00-000000000000&response_mode=form_post&response_type=code+id_token&
scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&
domain_hint=tokyo01.euc-livefire.com
```



Target URL

https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-00000000C

Target URL

scope=openid+profile&redirect_uri=https%3a%2f%2foutlook.office365.com&domain_hint=tokyo01.euc-livefire.com

Single Sign-On URL *

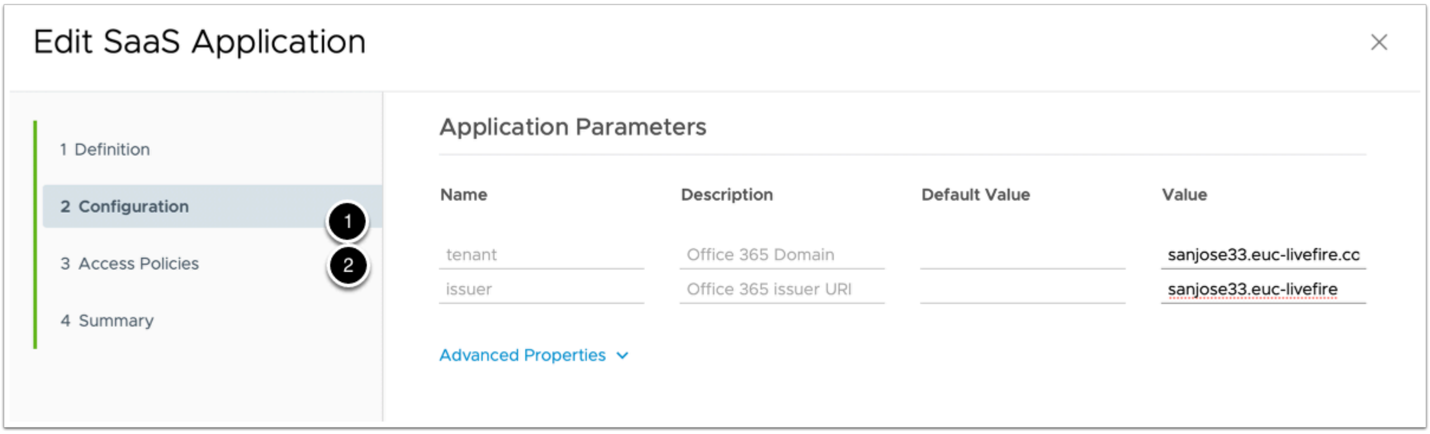
10

- In the **New Saas Application** window, in the **Configuration** section leave the following default:

  -Single Sign-On URL / **Application ID** / **Username Format / Username Value**

1. Add the following: under **Application Parameters** in the ***tenant*** line under **Value** add ***YOUR*** custom Fully Qualified Domain Name ie **tokyo01.euc-livefire.com**
2. Under **Application Parameters** in the ***issuer*** line under **Value** add your custom domain name (without the .com part) ie **tokyo01.euc-livefire**

Make sure there are no hidden carriage returns if you paste this in



Edit SaaS Application

Application Parameters

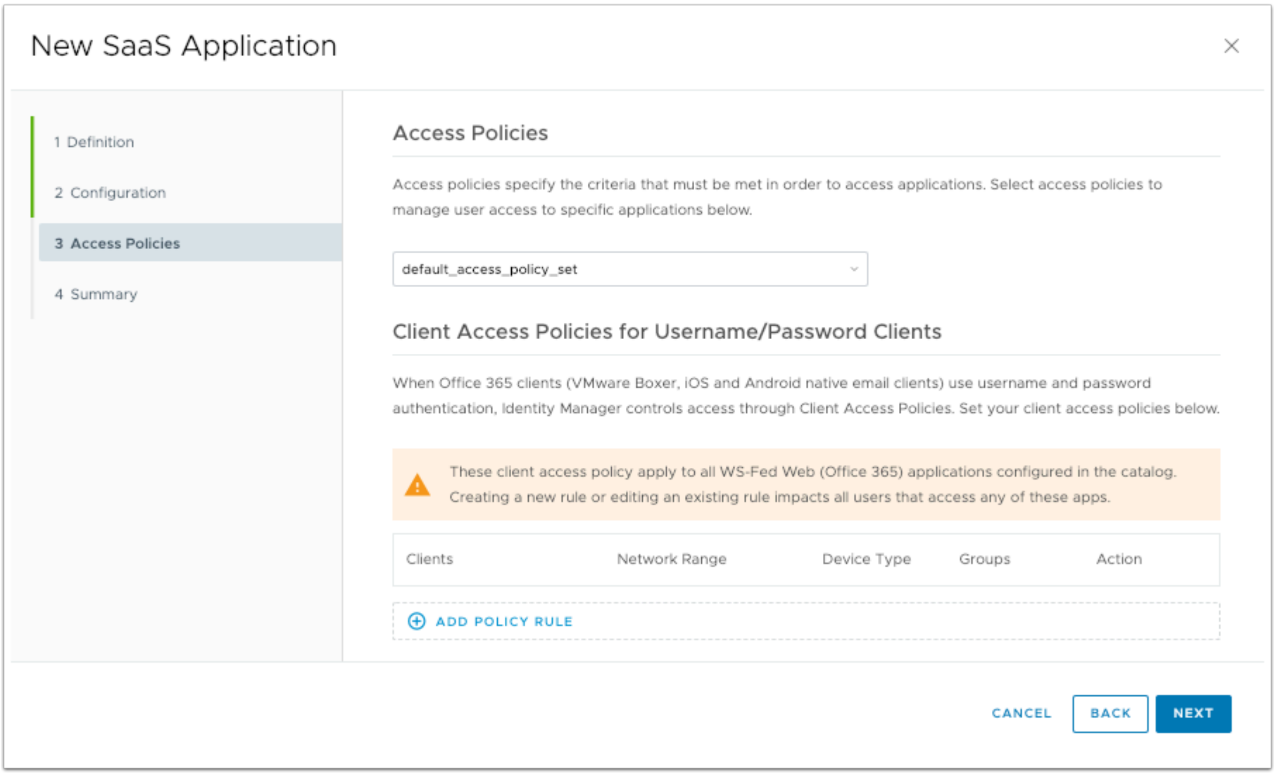
Name	Description	Default Value	Value
tenant	Office 365 Domain		sanjose33.euc-livefire.cc
issuer	Office 365 issuer URI		sanjose33.euc-livefire

11. In the **New Saas Application** window, in the **Configuration** section under **Advanced Properties** ***leave the following default:***

-**Enable Multiple O365 Email Domains** / **Credential Verification** / **Signature Algorithm / Digest Algorithm / Assertion Time**
-Under Custom Attribute Mapping in the *UPN* and ImmutableID keep the values default

- In the **New Saas Application** window, in the **Access Policies** section select **NEXT**

.



New SaaS Application

1 Definition
2 Configuration
3 Access Policies
4 Summary

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

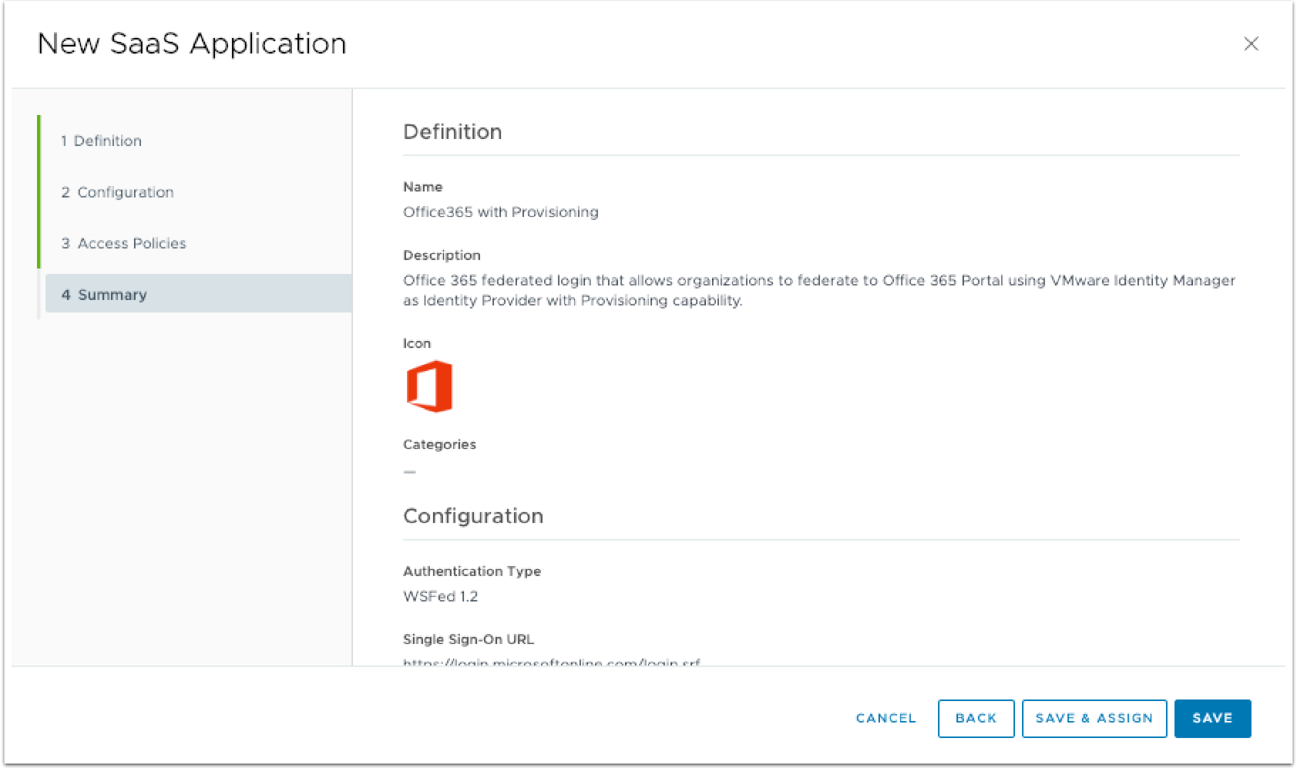
Client Access Policies for Username/Password Clients

When Office 365 clients (VMware Boxer, iOS and Android native email clients) use username and password authentication, Identity Manager controls access through Client Access Policies. Set your client access policies below.

These client access policy apply to all WS-Fed Web (Office 365) applications configured in the catalog. Creating a new rule or editing an existing rule impacts all users that access any of these apps.

Clients	Network Range	Device Type	Groups	Action

12. In the **New Saas Application** window, in the **Summary** section select **SAVE**



New SaaS Application

Definition

Name
Office365 with Provisioning

Description
Office 365 federated login that allows organizations to federate to Office 365 Portal using VMware Identity Manager as Identity Provider with Provisioning capability.

Icon

Categories
—

Configuration

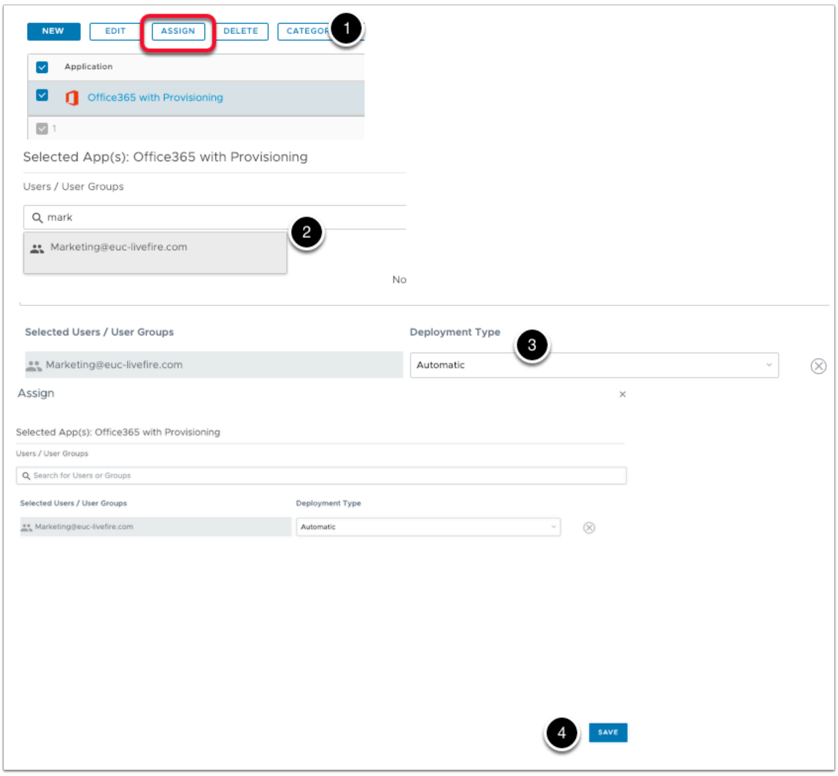
Authentication Type
WSFed 1.2

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

13

- We will now do the Entitlement configuration of the User

1. In the **Catalog** for Web Apps select the **Office 365 with Provisioning** and select **Assign**
2. In the **Assign** wizard type Mark in the **search area** under **Users / User Groups,** select **Marketing@euc-livefire.com**
3. Under **Deployment Type**, select the **drop down arrow** change the **Deployment Type** to **Automatic**
4. In the **Assign** wizard, review your configuration, in the bottom right hand corner select **SAVE**



NEW
EDIT
ASSIGN
DELETE
CATEGOR
1
Application
Office365 with Provisioning
1
Selected App(s): Office365 with Provisioning
Users / User Groups
mark
2
Marketing@euc-livefire.com
No
Selected Users / User Groups
Deployment Type
3
Marketing@euc-livefire.com
Automatic
Assign
Selected App(s): Office365 with Provisioning
Users / User Groups
Search for Users or Groups
Selected Users / User Groups
Deployment Type
Marketing@euc-livefire.com
Automatic
4
SAVE

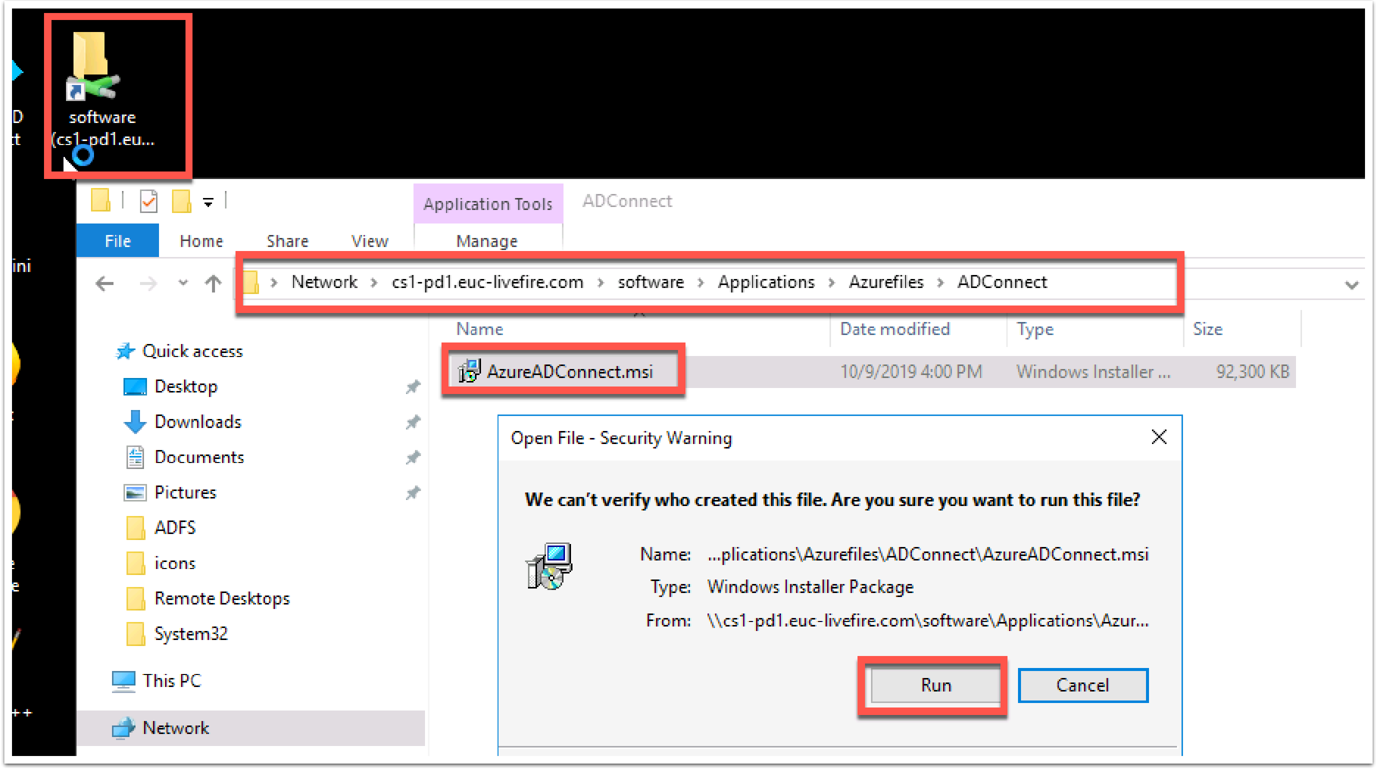
Part 3: Using Azure ADconnect for user provision to Azure AD

In this part we are goin to install Azure AD Connect tool to provision users to azure AD from on premise Active Directory.

Please note: It is best practice to use Azure AD connect tool but not a requirement. You can also provision users to Azure AD from Workspace ONE Access using Office365 with Provision application with Setup Provisioning ENABLED.

1. From your **Controlcenter** machine desktop, open the **Software** shortcut on your desktop and navigate to the **Applications > Azurefiles >ADconnect** folder.

2. Double- click on **AzureADConnect.msi** and click **run** on the security warning



Name	Date modified	Type	Size
AzureADConnect.msi	10/9/2019 4:00 PM	Windows Installer ...	92,300 KB

Open File - Security Warning

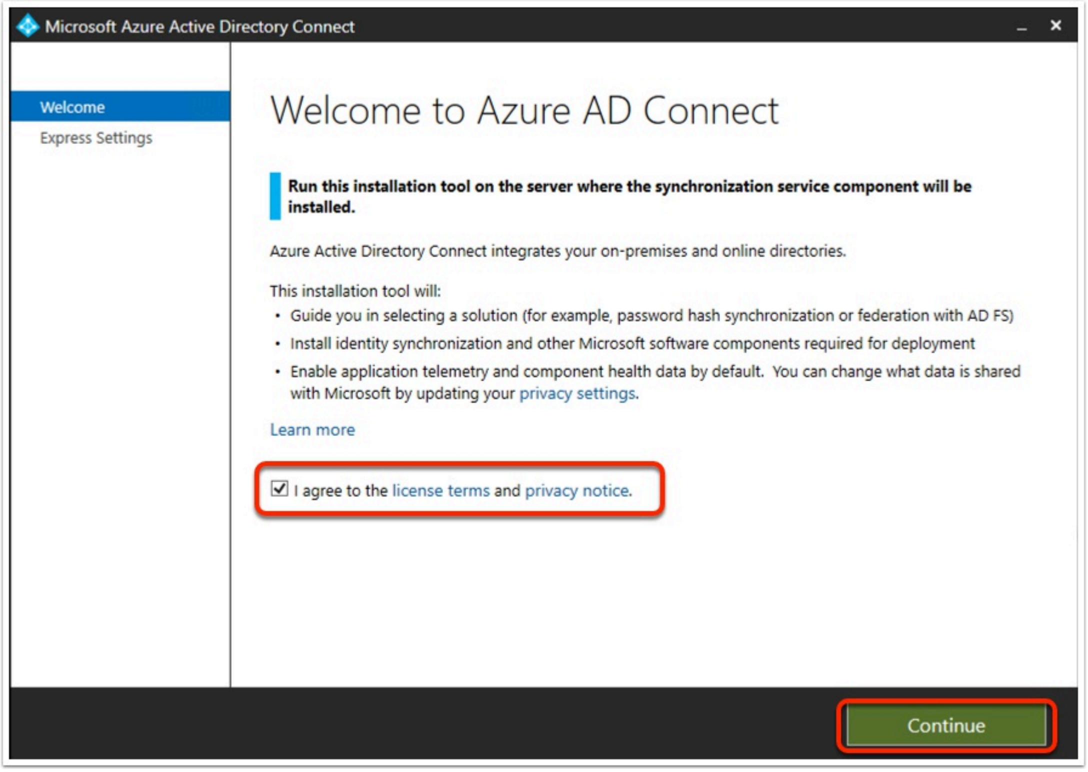
We can't verify who created this file. Are you sure you want to run this file?

Name: ...plications\Azurefiles\ADConnect\AzureADConnect.msi

Type: Windows Installer Package

From: \\cs1-pd1.euc-livefire.com\software\Applications\Azur...

3. On the **Welcome to Azure AD Connect** window check the box next to **"I agree to the license terms and privacy notice"** and click **Continue**



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

Azure Active Directory Connect integrates your on-premises and online directories.

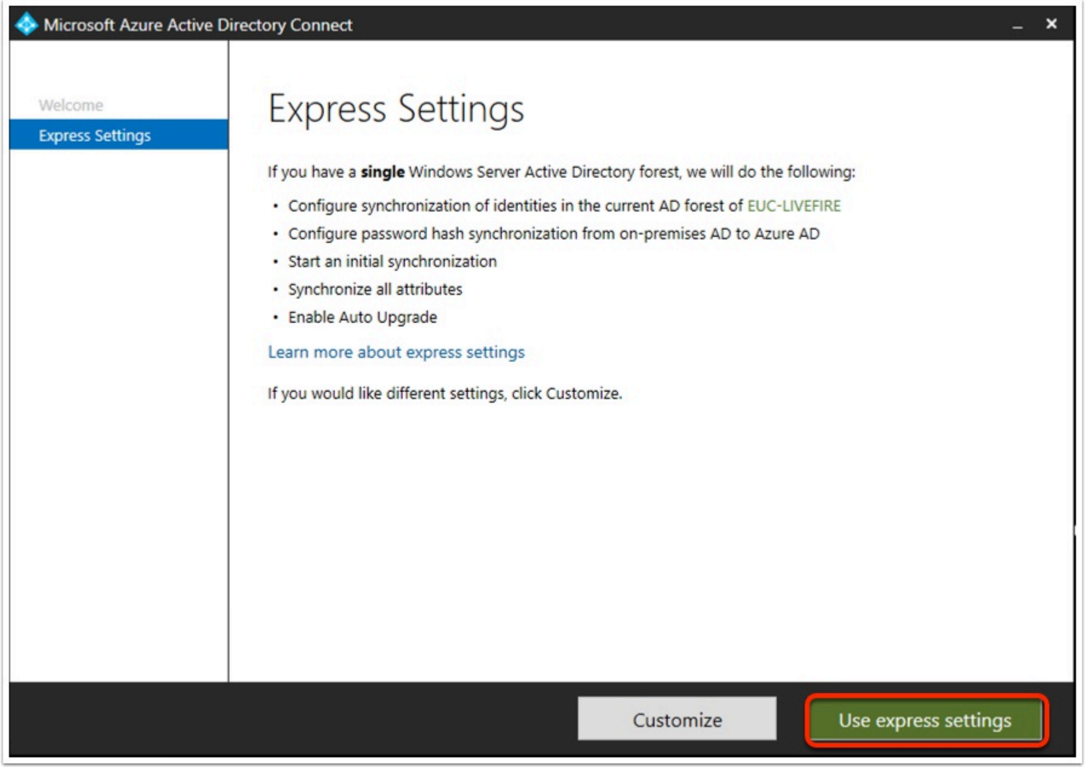
This installation tool will:

- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your privacy settings.

Learn more

☑ I agree to the license terms and privacy notice.

4. In the **Express Settings** window click on **"Use express settings"**


Microsoft Azure Active Directory Connect

Express Settings

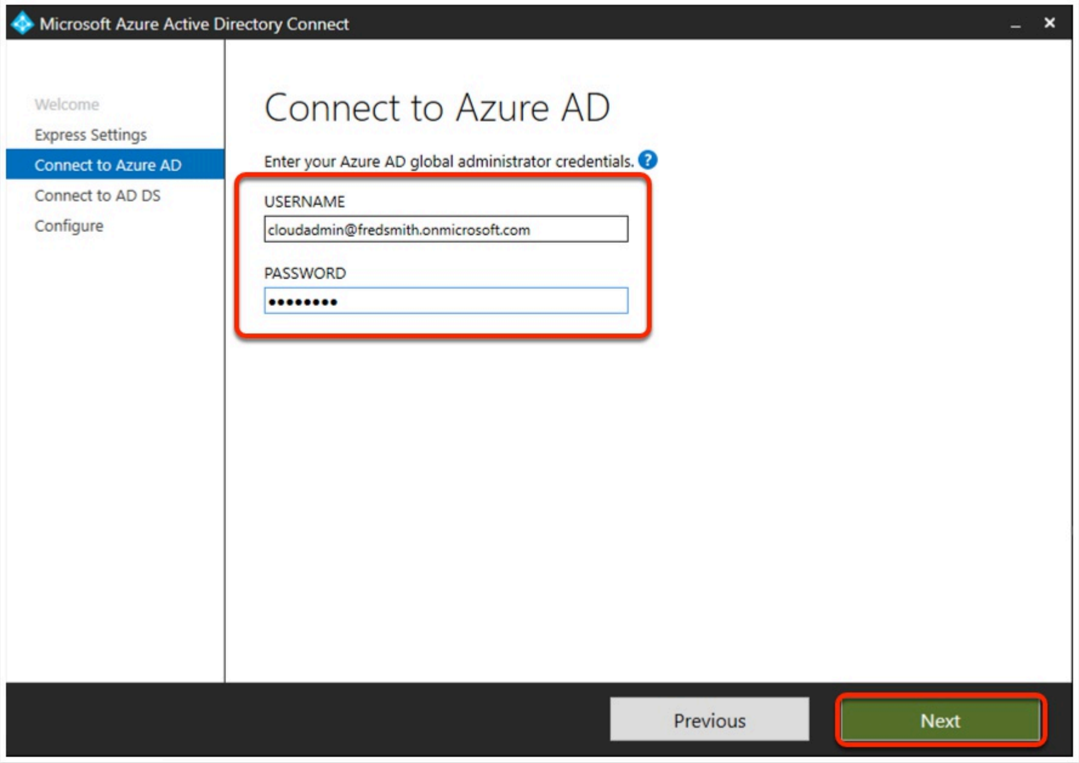
If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of EUC-LIVEFIRE
- Configure password hash synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

5. On the **"Connect to Azure AD"** window, **fill in your credentials** for your microsoft account and click **Next**


Microsoft Azure Active Directory Connect

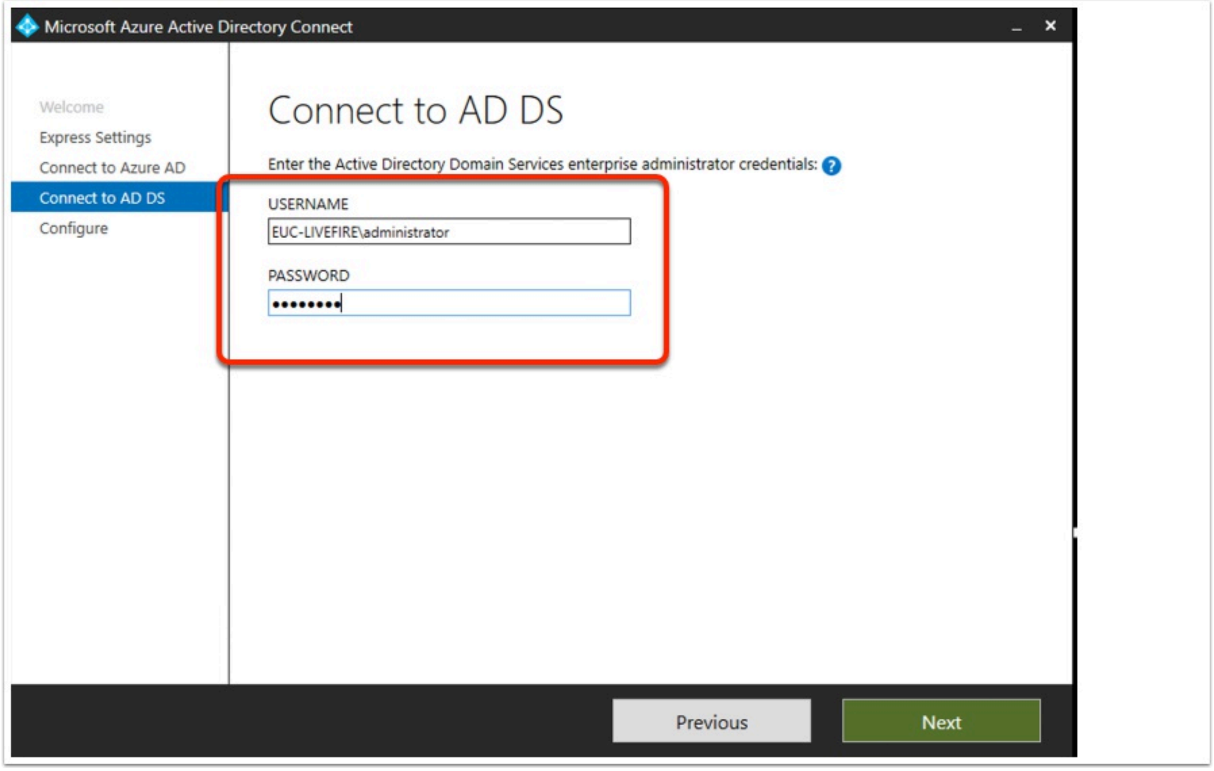
Connect to Azure AD

Enter your Azure AD global administrator credentials.

USERNAME: cloudadmin@fredsmith.onmicrosoft.com

PASSWORD: ••••••••

6. In the "**Connect to AD DS**" window fill in your domain credentials, **USERNAME:** EUC-LIVEFIRE\ADMINISTRATOR, PASSWORD: VMware1!



Connect to AD DS

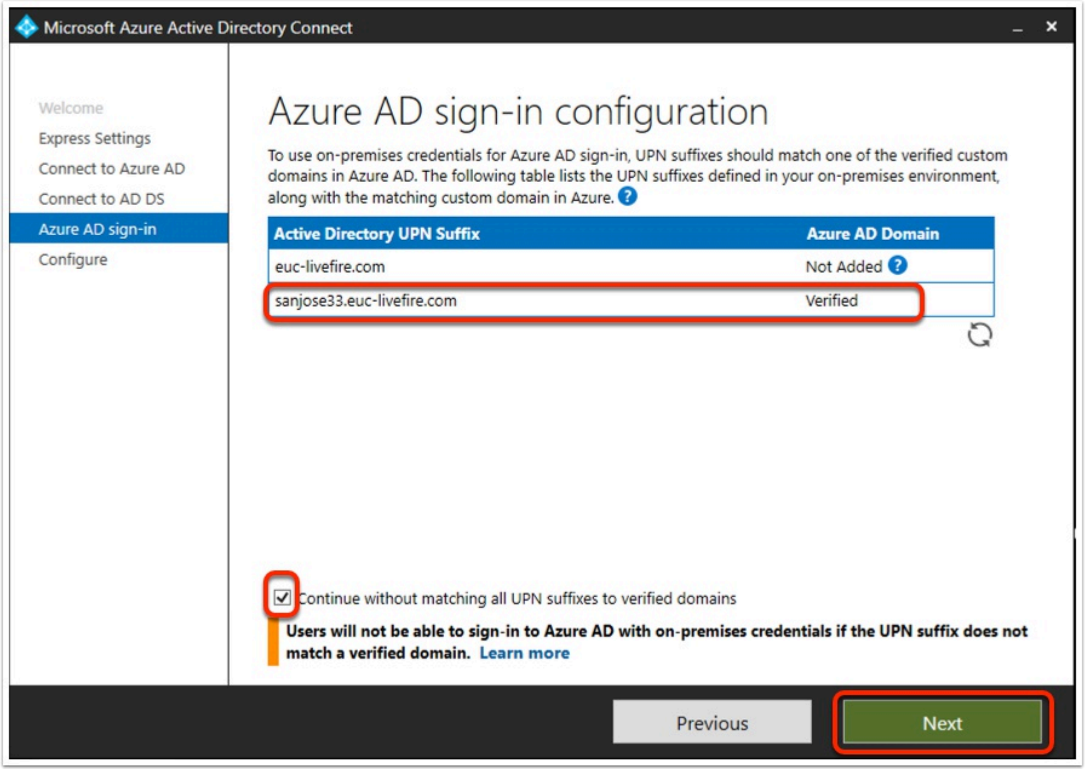
Enter the Active Directory Domain Services enterprise administrator credentials:

USERNAME: EUC-LIVEFIRE\administrator

PASSWORD: ••••••••

7. Verify your custom domain is verified

8. **Check the box** next to **"Continue without matching all UPN suffixes to verified domains"** and click **Next**



Azure AD sign-in configuration

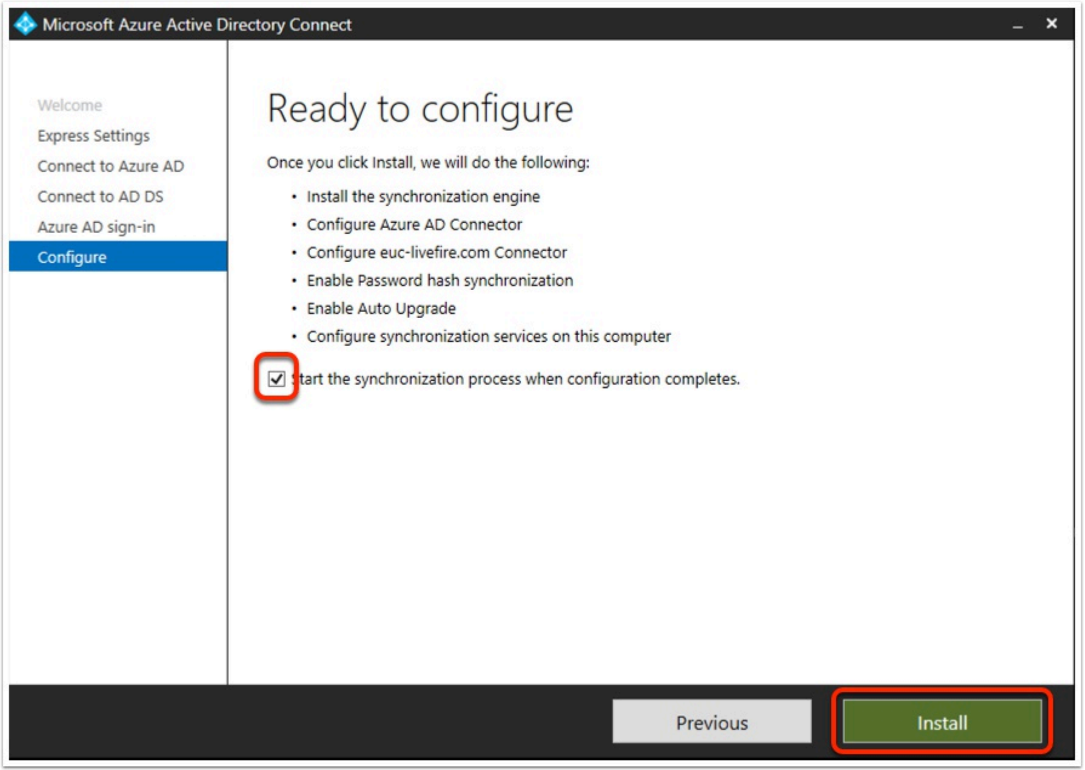
To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.

Active Directory UPN Suffix	Azure AD Domain
euc-livefire.com	Not Added
sanjose33.euc-livefire.com	Verified

☑ Continue without matching all UPN suffixes to verified domains

Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. Learn more

9. On the **"Ready to configure"** windowmake sure the box next to **"Start synchronization process when configuration completes"** is checked and click **Install.** Getting to the following step should take a couple of minutes.



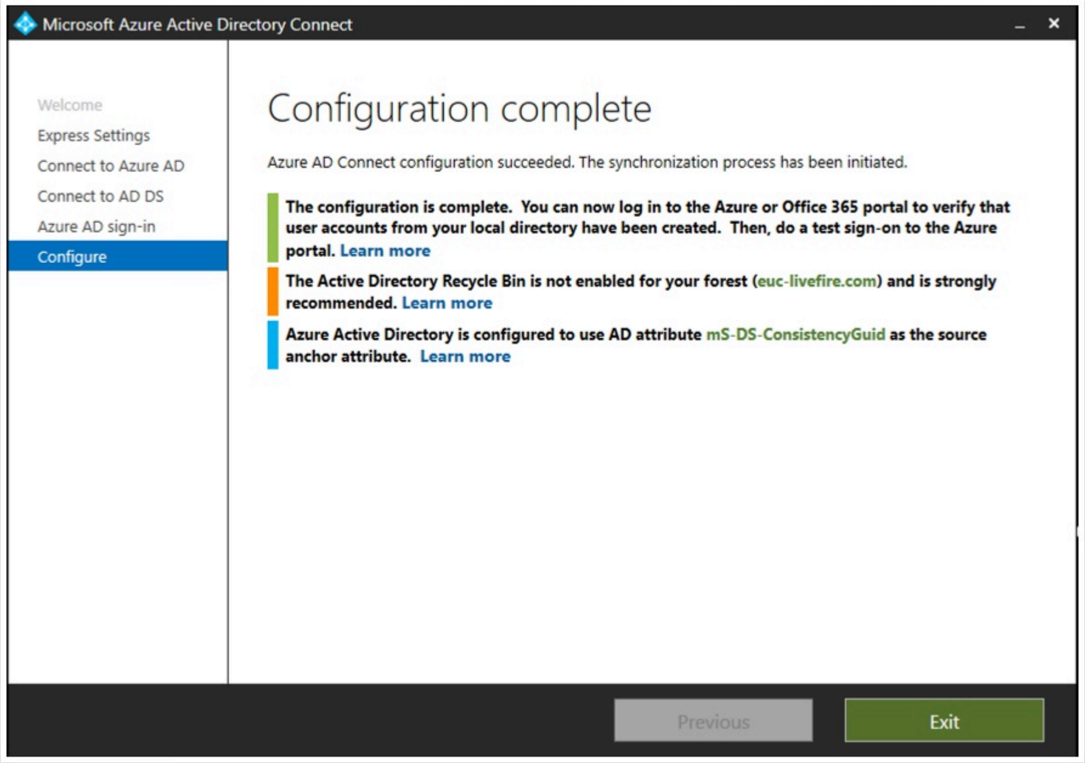
Ready to configure

Once you click Install, we will do the following:

- Install the synchronization engine
- Configure Azure AD Connector
- Configure euc-livefire.com Connector
- Enable Password hash synchronization
- Enable Auto Upgrade
- Configure synchronization services on this computer

☑ Start the synchronization process when configuration completes.

10. In the **"Configuration complete"** window click **"Exit"**



Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

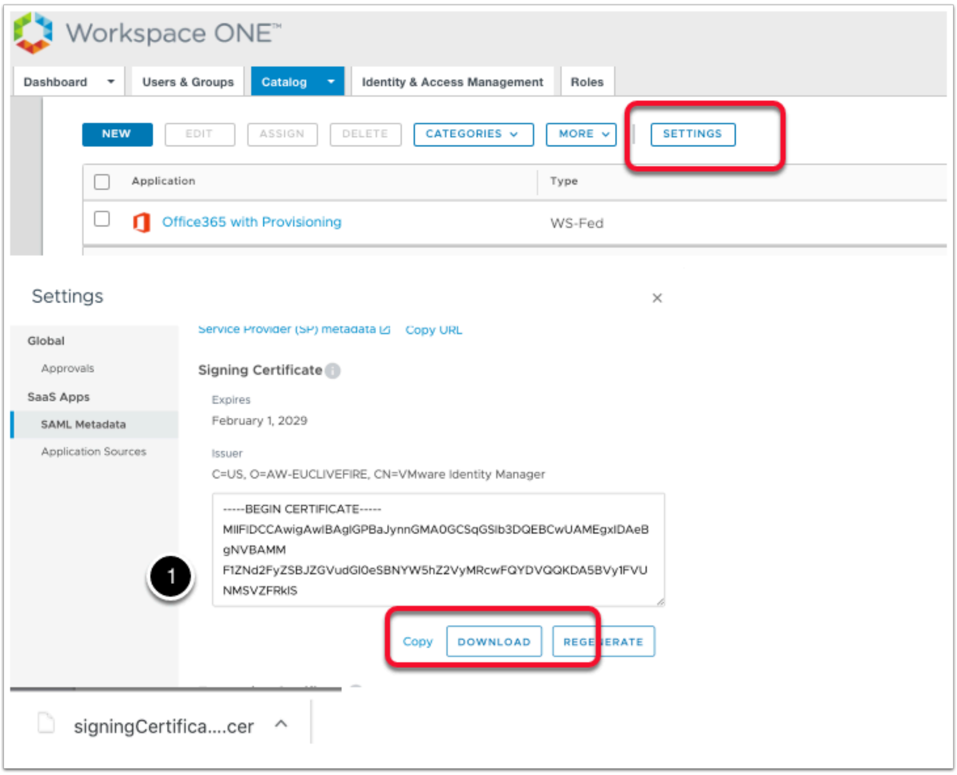
The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more

The Active Directory Recycle Bin is not enabled for your forest (euc-livefire.com) and is strongly recommended. Learn more

Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute. Learn more

Part 4: Setting up the SAML between Workspace ONE Access and Office 365

1. Ensure you do the next section on your **ControlCenter2** server .
    1. Login to your to the **Workspace ONE Access** Admin Console, as **Admin**, under the **Catalog > Web Apps** tab to the right select **SETTINGS**
    2. In the **Settings** window under **SaaS Apps**, select **SAML Metadata**, in the right hand pane under the **SAML Metadata** heading select **DOWNLOAD** under **Signing Certificate**
    3. Using Notepad++ Open the **signingCertificate.cer** from your default download location .



Application	Type
Office365 with Provisioning	WS-Fed

Signing Certificate

Expires
February 1, 2029

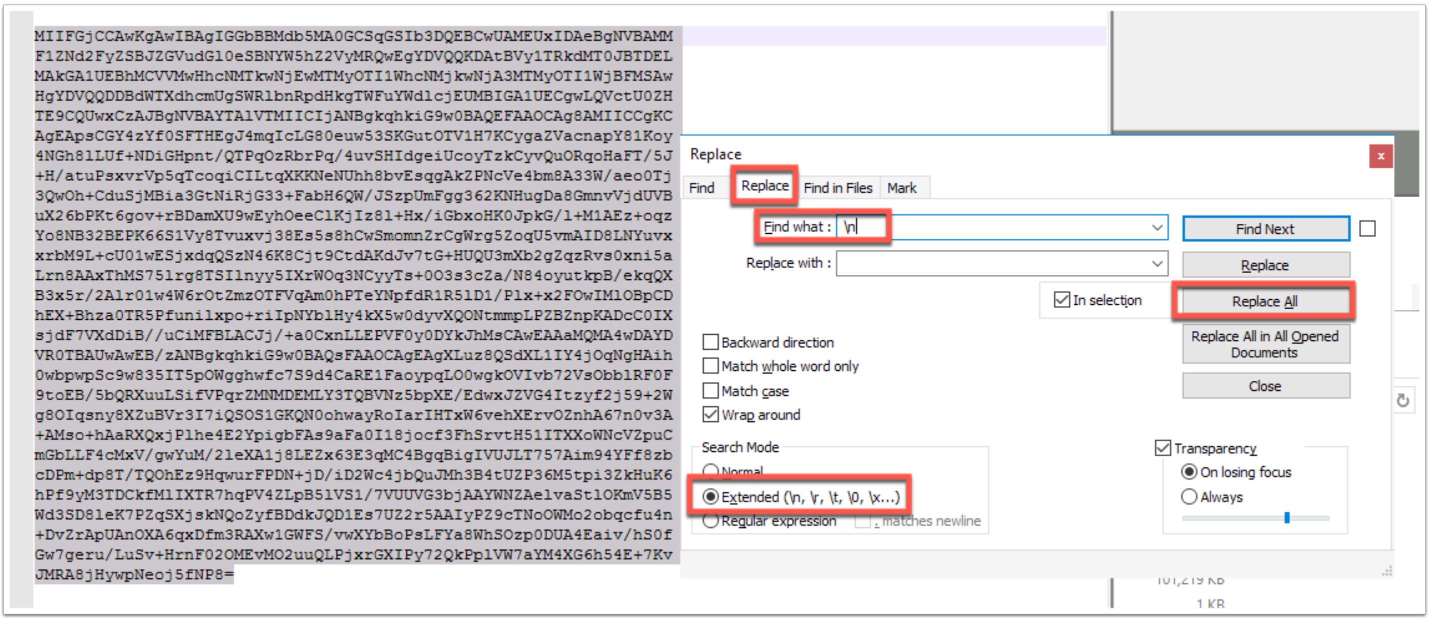
Issuer
C=US, O=AW-EUCLIVEFIRE, CN=VMware Identity Manager

```
-----BEGIN CERTIFICATE-----
MIIFIDCCAwigAwIBAgIGPBaJynnGMA0GCSqGSIb3DQEBCwUAMEgxIDAeB
gNVBAMM
F1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMRcwFQYDVQQKDA5BVy1FVU
NMSVZFRkIS
```

2. In the **signingCertificate.cer** we will remove all carriage returns the document

Do this with Notepad++ on your **ControlCenter server**. Any hidden carriage returns will cause this exercise to FAIL

1. Remove the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines from the certificate.
2. Then select the certificate portion of the file and click **ctrl** + **F** in the **Replace** tab at the top type **\n** in the Find what field.Leave the Replace with field empty. Make sure the Search Mode at the bottom is **Extended**. Then click on **Replace All**.
3. Your certificate should now no longer have carriage returns. Notepad++ will tell you how many instances were replaced and your certificate will look different.



```
MIIFGjCCAwKgAwIBAgIGGbBBMdb5MA0GCSqGSIb3DQEBCwUAMEUxIDAeBgNVBAMM
F1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMRQwEgYDVQQKDAtBVy1TRkdMT0JBTDEL
MAkGA1UEBhMCVVMwHhcNMTkwNjEwMTMyOTI1WhcNMjkwNjA3MTMyOTI1WjBFMSAw
HgYDVQQDDBdWTXdhcmUgSWRlbnRpdHkgTWFuYWdlcjEUMBIGA1UECgwLQVctU0ZH
TE9CQUwxCzAJBgNVBAYTAlVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC
AgEApsCGY4zYf0SFTHEgJ4mqIcLG80euw53SKGutOTV1H7KCygaZVacnapY81Koy
4NGh81LUf+NDiGHpnt/QTPqOzRbrPq/4uvSHIdgeiUcoyTzkCyvQuORqoHaFT/5J
+H/atuPsxvrVp5qTcoqiCILtqXKKNeNUhh8bvEsqgAkZPNcVe4bm8A33W/aeo0Tj
3QwOh+CduSjMBia3GtNiRjG33+FabH6QW/JSzpUmFgg362KNHugDa8GmnvVjdUVB
uX26bPKt6gov+rBDamXU9wEyhOeeClKjIz81+Hx/iGbxoHK0JpkG/l+M1AEz+oqz
Yo8NB32BEPK66S1Vy8Tvuxvj38Es5s8hCwSmomnZrCgWrg5ZoqU5vmAID8LNYuvx
xrbM9L+cU01wESjxdqQSzN46K8Cjt9CtdAKdJv7tG+HUQU3mXb2gZqzRvs0xni5a
Lrn8AAxThMS75lrg8TSIlnyy5IXrWOq3NCyyTs+0O3s3cZa/N84oyutkpB/ekqQX
B3x5r/2Alr01w4W6rOtZmzOTFVqAm0hPTeYNpfdR1R5lD1/Plx+x2FOwIMlOBpCD
hEX+Bhza0TR5Pfunilxpo+riIpNYblHy4kX5w0dyvXQONtmmpLPZBZnpKADcC0IX
sjdF7VXdDiB//uCiMFBLACJj/+a0CxnLLEPVF0y0DYkJhMsCAwEAAaMQMA4wDAYD
VR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAgXLuz8QSdXL1IY4jOqNgHAih
0wbpwpSc9w835IT5pOWgghwfc7S9d4CaRE1FaoypqLO0wgkOVIvb72VsObblRF0F
9toEB/5bQRXuuLSifVPqrZMNMDEMLY3TQBVNz5bpXE/EdwxJZVG4Itzyf2j59+2W
g8OIqsny8XZuBVr3I7iQSOS1GKQN0ohwayRoIarIHTxW6vehXErvOZnhA67n0v3A
+AMso+hAaRXQxjPlhe4E2YpigbFAs9aFa0I18jocf3FhSrvtH51ITXXoWNcVZpuC
mGbLLF4cMxV/gwYuM/2leXA1j8LEZx63E3qMC4BgqBigIVUJLT757Aim94YFf8zb
cDPm+dp8T/TQOhEz9HqwurFPDN+jD/iD2Wc4jbQuJMh3B4tUZP36M5tpi3ZkHuK6
hPf9yM3TDCkfMlIXTR7hqPV4ZLpB5lVS1/7VUUVG3bjAAYWNZAelvaStlOKmV5B5
Wd3SD8leK7PZqSXjskNQoZyfBDdkJQD1Es7UZ2r5AAIyPZ9cTNoOWMo2obqcfu4n
+DvZrApUAnOXA6qxDfm3RAXw1GWFS/vwXYbBoPsLFYa8WhSOzp0DUA4Eaiv/hS0f
Gw7geru/LuSv+HrnF02OMEvMO2uuQLPjxrGXIPy72QkPplVW7aYM4XG6h54E+7Kv
JMRA8jHywpNeoj5fNP8=
```

Replace

Find what : \n

Replace with :

☑ In selection

☐ Backward direction

☐ Match whole word only

☐ Match case

☑ Wrap around

Search Mode

○ Normal

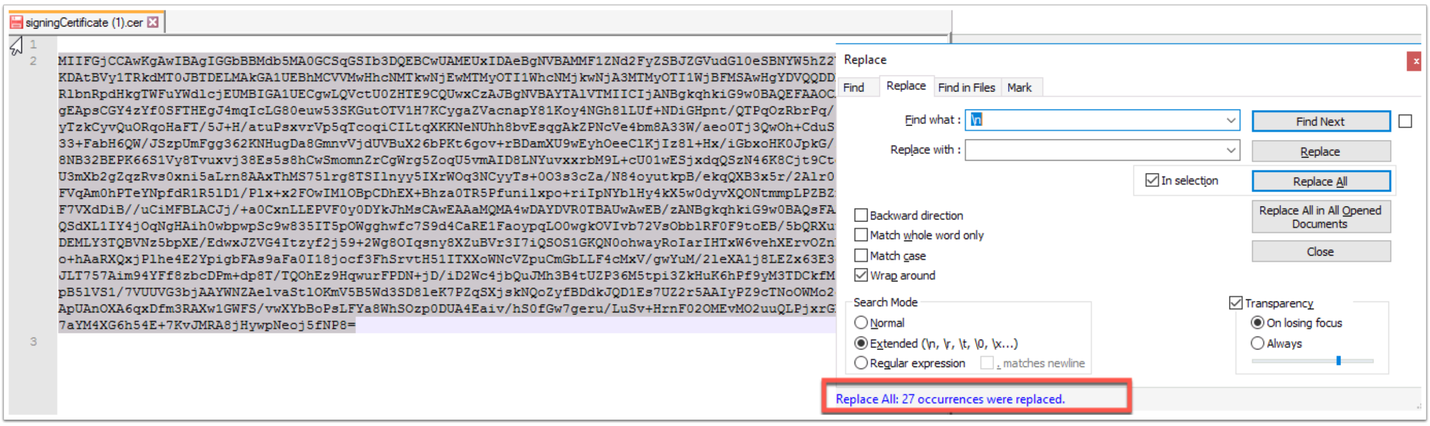
● Extended (\n, \r, \t, \0, \x...)

○ Regular expression ☐ . matches newline

☑ Transparency

● On losing focus

○ Always



```
MIIFGjCCAwKgAwIBAgIGGbBBMdb5MA0GCSqGSIb3DQEBCwUAMEUxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2
KDAtBVy1TRkdMT0JBTDELMAkGA1UEBhMCVVMwHhcNMTkwNjEwMTMyOTI1WhcNMjkwNjA3MTMyOTI1WjBFMSAwHgYDVQQDD
RlbnRpdHkgTWFuYWdlcjEUMBIGA1UECgwLQVctU0ZHTE9CQUwxCzAJBgNVBAYTAlVTMIICIjANBgkqhkiG9w0BAQEFAAOC
gEApsCGY4zYf0SFTHEgJ4mqIcLG80euw53SKGutOTV1H7KCygaZVacnapY81Koy4NGh81LUf+NDiGHpnt/QTPqOzRbrPq/
yTzkCyvQuORqoHaFT/5J+H/atuPsxvrVp5qTcoqiCILtqXKKNeNUhh8bvEsqgAkZPNcVe4bm8A33W/aeo0Tj3QwOh+CduS
33+FabH6QW/JSzpUmFgg362KNHugDa8GmnvVjdUVBuX26bPKt6gov+rBDamXU9wEyhOeeClKjIz81+Hx/iGbxoHK0JpkG/
8NB32BEPK66S1Vy8Tvuxvj38Es5s8hCwSmomnZrCgWrg5ZoqU5vmAID8LNYuvxxrbM9L+cU01wESjxdqQSzN46K8Cjt9Ct
U3mXb2gZqzRvs0xni5aLrn8AAxThMS75lrg8TSIlnyy5IXrWOq3NCyyTs+0O3s3cZa/N84oyutkpB/ekqQXB3x5r/2Alr0
FVqAm0hPTeYNpfdR1R5lD1/Plx+x2FOwIMlOBpCDhEX+Bhza0TR5Pfunilxpo+riIpNYblHy4kX5w0dyvXQONtmmpLPZBZ
F7VXdDiB//uCiMFBLACJj/+a0CxnLLEPVF0y0DYkJhMsCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFA
QSdXL1IY4jOqNgHAih0wbpwpSc9w835IT5pOWgghwfc7S9d4CaRE1FaoypqLO0wgkOVIvb72VsObblRF0F9toEB/5bQRXu
DEMLY3TQBVNz5bpXE/EdwxJZVG4Itzyf2j59+2Wg8OIqsny8XZuBVr3I7iQSOS1GKQN0ohwayRoIarIHTxW6vehXErvOZn
o+hAaRXQxjPlhe4E2YpigbFAs9aFa0I18jocf3FhSrvtH51ITXXoWNcVZpuCmGbLLF4cMxV/gwYuM/2leXA1j8LEZx63E3
JLT757Aim94YFf8zbcDPm+dp8T/TQOhEz9HqwurFPDN+jD/iD2Wc4jbQuJMh3B4tUZP36M5tpi3ZkHuK6hPf9yM3TDCkfM
pB5lVS1/7VUUVG3bjAAYWNZAelvaStlOKmV5B5Wd3SD8leK7PZqSXjskNQoZyfBDdkJQD1Es7UZ2r5AAIyPZ9cTNoOWMo2
ApUAnOXA6qxDfm3RAXw1GWFS/vwXYbBoPsLFYa8WhSOzp0DUA4Eaiv/hS0fGw7geru/LuSv+HrnF02OMEvMO2uuQLPjxrG
7aYM4XG6h54E+7KvJMRA8jHywpNeoj5fNP8=
```

Replace

Find what : \n

Replace with :

☑ In selection

☐ Backward direction

☐ Match whole word only

☐ Match case

☑ Wrap around

Search Mode

○ Normal

● Extended (\n, \r, \t, \0, \x...)

○ Regular expression ☐ . matches newline

☑ Transparency

● On losing focus

○ Always

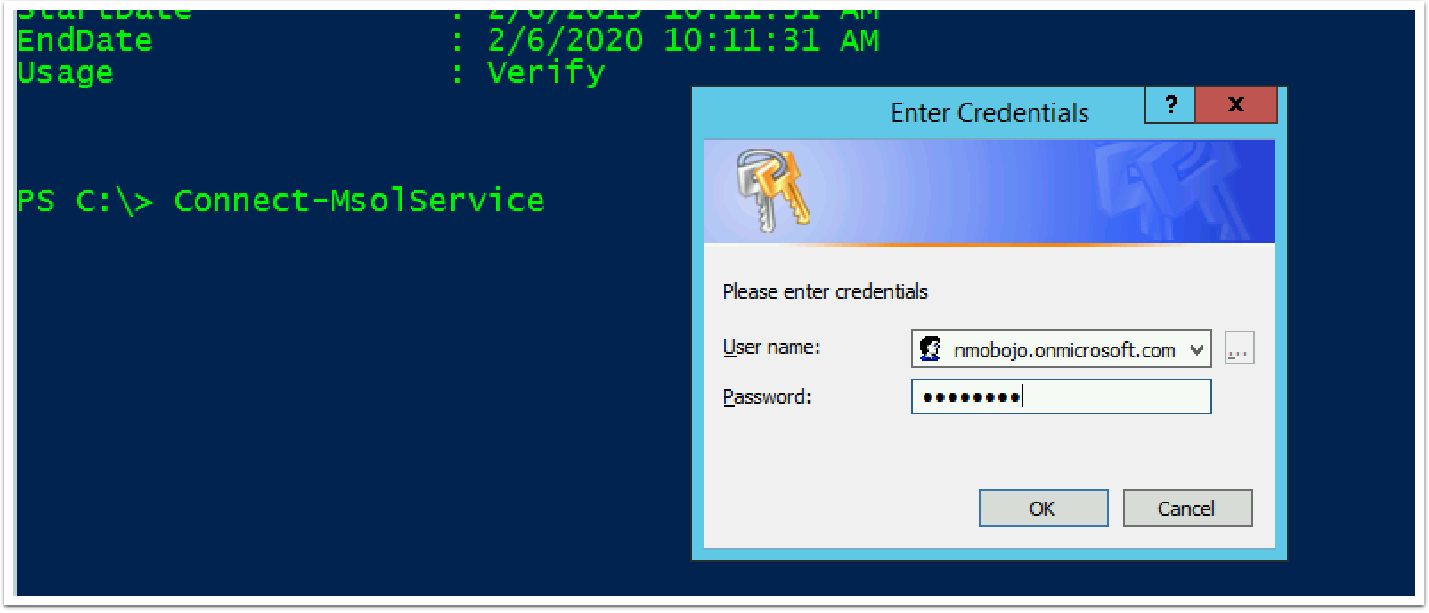
Replace All: 27 occurrences were replaced.

3. On the **ControlCenter2** server and open the existing **Powershell** interface we were working with earlier (from the shortcut on your desktop). please copy, edit and paste the commands from the text file called powershell comands, located in your Software folder (linked in your control center desktop), in the \Applications\Azurefiles folder.

Run the following command:

Connect-MsolService

- In the **Powershell Console** type the following using your **Cloudadmin** credentials. The example we use is **cloudadmin@ranmobojo.onmicrosoft.com** and your password



```
StartDate                    : 2/6/2019 10:11:31 AM
EndDate                      : 2/6/2020 10:11:31 AM
Usage                        : Verify


PS C:\> Connect-MsolService
```

4. Next we edit the following Powershell commands for our environment and include the certificate string as part of this command.

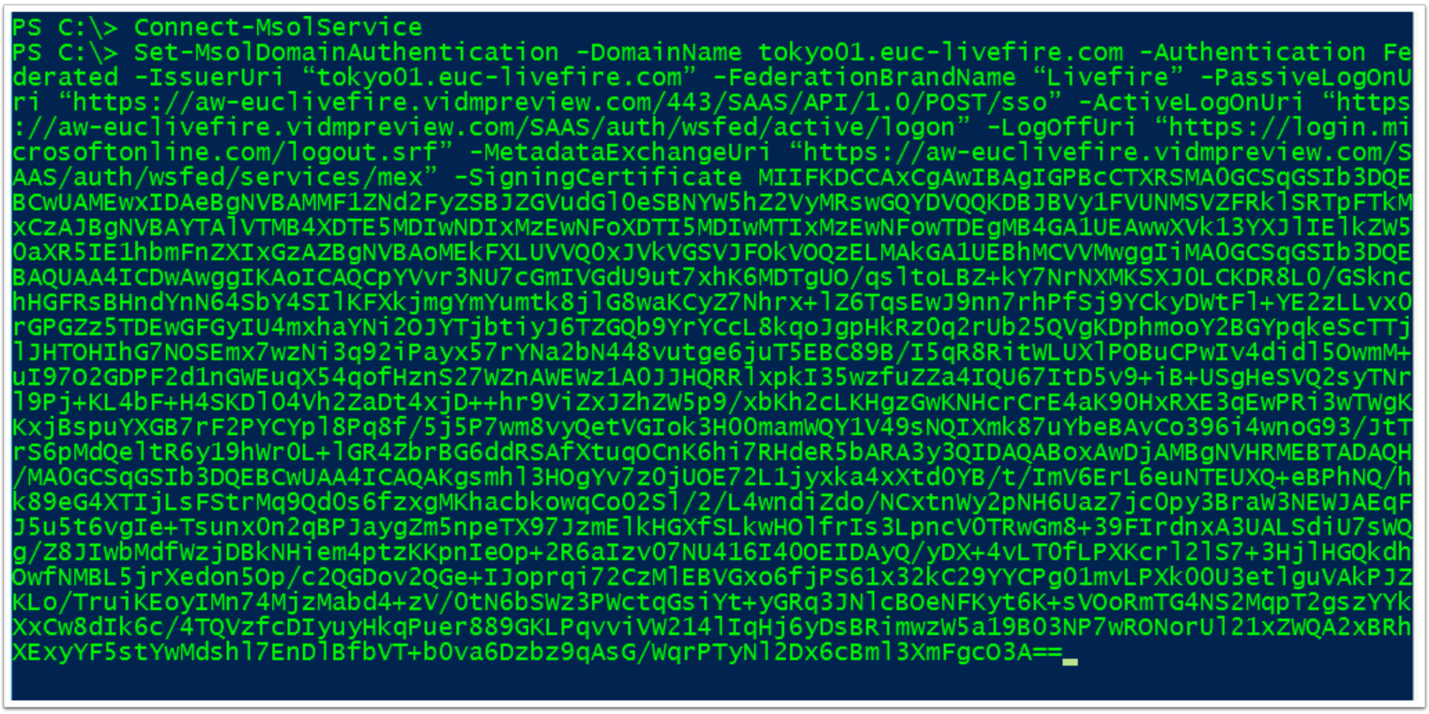
1. Edit the sample string by replacing any instance of **tokyo01** with the city and number from *YOUR CUSTOM Fully Qualified Domain name, i.e. london08*
2. Edit the sample string by replacing **aw-euclivefire.vidmpreview.com** with ***YOUR CUSTOM SAAS Workspace ONE Access Tenant Fully Qualified Domain name***

   example 1 is the string without the certificate|
   example 2 is the string with the certificate which you will have to append without introducing any hidden returns into Powershell

```
Set-MsolDomainAuthentication -DomainName tokyo01.euc-livefire.com -Authentication
Federated -IssuerUri “tokyo01.euc-livefire” -FederationBrandName “tokyo01Corp” -
PassiveLogOnUri “https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/POST/sso” -
ActiveLogOnUri “https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/active/logon” -
LogOffUri “https://login.microsoftonline.com/logout.srf” -MetadataExchangeUri
“https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/services/mex” -
SigningCertificate
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
Set-MsolDomainAuthentication -DomainName tokyo01.euc-livefire.com -Authentication
Federated -IssuerUri “tokyo01.euc-livefire” -FederationBrandName “tokyo01Corp” -
PassiveLogOnUri “https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/POST/sso” -
ActiveLogOnUri “https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/active/logon” -
LogOffUri “https://login.microsoftonline.com/logout.srf” -MetadataExchangeUri
“https://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/services/mex” -
SigningCertificate
MIIFIDCCAwigAwIBAgIGPBaJynnGMA0GCSqGSIb3DQEBCwUAMEgxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBN
YW5hZ2VyMRcwFQYDVQQKDA5BVy1FVUNMSVZFRklSRTELMAkGA1UEBhMCVVMwHhcNMTkwMjA0MjEzMTAyWhcNMjkw
```

```
MjAxMjEzMTAyWjBIMSAwHgYDVQQDDBdWTXdhcmUgSWRlbnRpdHkgTWFuYWdlcjEXMBUGA1UECgwOQVctRVVDTElW
RUZJUkUxCzAJBgNVBAYTAlVTMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEApWfE7UfEG9iupk538HEU
rqfAKb5VlcnsGrQCz9+Hb1QrDba8vvPWNp+H3MhkZ1RZS43mvy+3JVFEuEsCIqHyRrKsJVIswPda2eQKW/
Y7jd3RHZFoxoqbvF4kOyJq5+k38xI/
8t8Olkv2ruYYHwUZ+SDJpWdxFqbrpcBAFac5IYj7lPoPlOv9na+lZ7V8ddWQCrsNydKfndUPeBiUj389Xer0ckzH
TcYjeGG82X9NHDXVsmbiMFrDnP0ZbMCD21CMOGyZ8wKFzbx3toStDuqyF6MbXv3tpVCnF/
sELJaJNxbfdoslNGfbyNWiv/UQ7h8XDOywqpzMZkZkch/Bl6Ny1cS3UDW6GYgYuJHkmRu9Pgqv/
98QpFueBrrR71+9WTLocSVxgbBCdyrgwVOHAJK1+yZOrYuiLIGcdJfhjczOaN/
8dJnzYspxgW9tIxZ2SmQQDTy9zscvad2rplOZFqj9MQbDUmdanr52ksQ85jboArLW9B5TVmxefDtoPMiK6GKsR/
Q+ygEplsyDT1S6eGzXaVBOQFGjjAFQ3c0wOQtZ0Q6+JJRk3KO4X2F5arDRZKTCfEyzH8VYwaJ04BJBmlkPQs14IK
zAhwR/cqBzKnSFUxbeqm5U/
YLeyaO03NKEYimHqoW7cEB9sPQnO7YUuZOG0KqHrC0S8dVt6dk5adfa0LECAwEAAaMQMA4wDAYDVR0TBAUwAwEB/
zANBgkqhkiG9w0BAQsFAAOCAgEAiadCYNp2OVfFIlD3I3iQhLCvmc1hVKMEzz1FJNEAMZ3JZgwBEYLHL7d8kiRjI
7c4hvZ62P2eQ2bC6z3lzqGVK8GNyUPGMKKgcFOgjJrK+roP4s740cbn4hQX3j3cOLCuQKQ2NkzwF0+5qGU26vOvl
wnE8SONR4OxgScW2Bu55E5NOQj+Tu45Pt2KYZpSv9ZP9KJj75AqwmfkynomDBYZXT4WbSft5HDt7VXkFS6OPz41i
32yqDTtHePLKbJ83LcXEETDVfyfigS1m1VWwcDp9sLfbqA4yEIoGFNO5KMssHOkVeCFCjzCs06B1pVHoWYqqNOg0
gMU0vpX+gFcj7tHJklhbHUcqQpnYs/
AJyL0pEroVZTBJS3UgK9vMEage9P+hoVqiX9g+Csd0GjRLExlpkm3uFKt0su05UQ0E9PrYpOS74YbmuRFEUJ5R5P
zxSAWErG/
SxPWNtGKzKdGjJzBmErOgShODflleURanuL18FDqBR7KXGOnNWDNk5GKVcB2LWqmmz6AmCkFee9oPju6hT+Y4M3O
6mmP6dxjTILPUAddObZUUFhhX8fyjpTDUjTzKWdPaf5G4/
ISfSqa0CoCFaNGTeEhoR9NtjYlabENZMuD2OoVDacMQvRMN1IbtilDF9ISROG3jzVJDNtFvwkuRzUJ5QyUEAuBZ6
xpVEt/8Do=
```

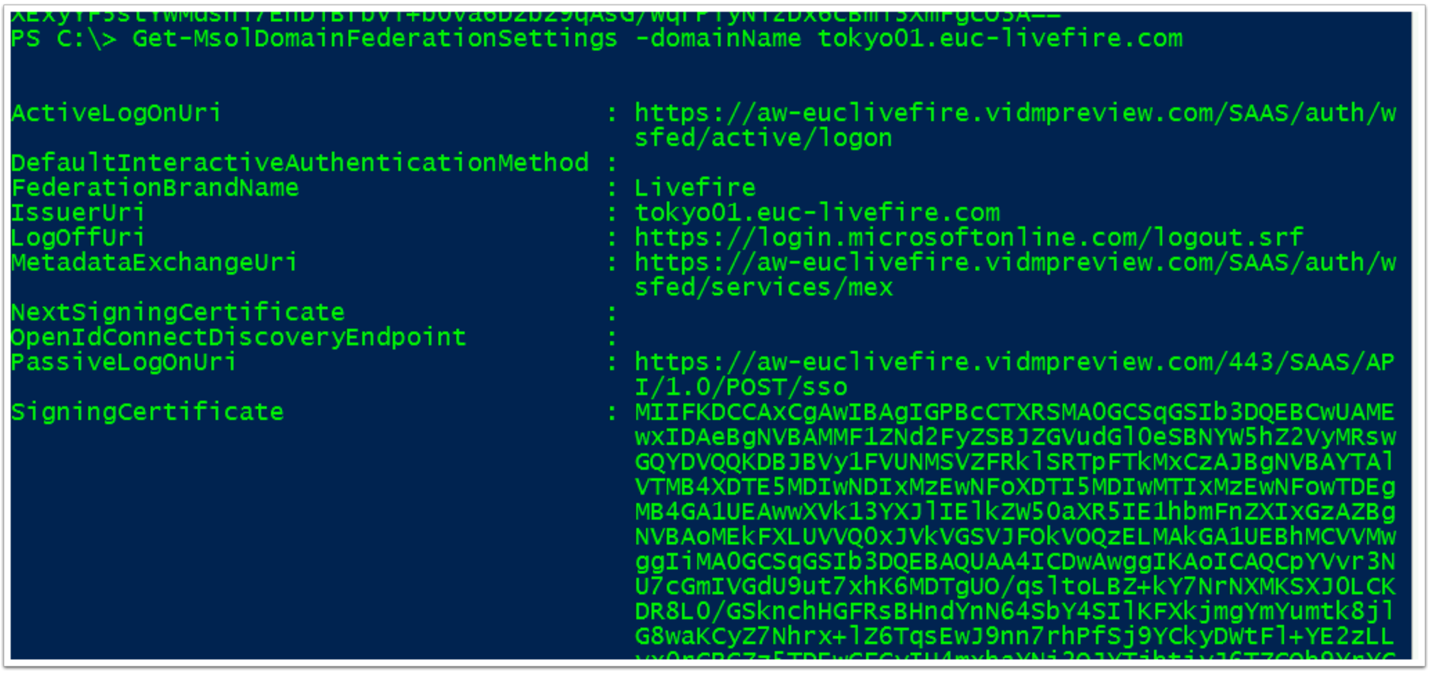


```
PS C:\> Connect-MsolService
PS C:\> Set-MsolDomainAuthentication -DomainName tokyo01.euc-livefire.com -Authentication Fe
derated -IssuerUri “tokyo01.euc-livefire.com” -FederationBrandName “Livefire” -PassiveLogOnU
ri “https://aw-euclivefire.vidmpreview.com/443/SAAS/API/1.0/POST/sso” -ActiveLogOnUri “https
://aw-euclivefire.vidmpreview.com/SAAS/auth/wsfed/active/logon” -LogOffUri “https://login.mi
crosoftonline.com/logout.srf” -MetadataExchangeUri “https://aw-euclivefire.vidmpreview.com/S
AAS/auth/wsfed/services/mex” -SigningCertificate MIIFKDCCAxCgAwIBAgIGPBcCTXRSMA0GCSqGSIb3DQE
BCwUAMEwxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMRswGQYDVQQKDBJBVy1FVUNMSVZFRklSRTpFTkM
xCzAJBgNVBAYTAlVTMB4XDTE5MDIwNDIxMzEwNFoXDTI5MDIwMTIxMzEwNFowTDEgMB4GA1UEAwwXVk13YXJlIElkZW5
0aXR5IE1hbmFnZXIxGzAZBgNVBAoMEkFXLUVVQ0xJVkVGSVJFOkVOQzELMAkGA1UEBhMCVVMwggIiMA0GCSqGSIb3DQE
BAQUAA4ICDwAwggIKAoICAQCpYVvr3NU7cGmIVGdU9ut7xhK6MDTgUO/qsltoLBZ+kY7NrNXMKSXJ0LCKDR8L0/GSknc
hHGFRsBHndYnN64SbY4SIlKFXkjmgYmYumtk8jlG8waKCyZ7Nhrx+lZ6TqsEwJ9nn7rhPfSj9YCkyDWtFl+YE2zLLvx0
rGPGZz5TDEwGFGyIU4mxhaYNi2OJYTjbtiyJ6TZGQb9YrYCcL8kqoJgpHkRz0q2rUb25QVgKDphmooY2BGYpqkeScTTj
lJHTOHIhG7NOSEmx7wzNi3q92iPayx57rYNa2bN448vutge6juT5EBC89B/I5qR8RitWLUXlPOBuCPwIv4didl5OwmM+
uI97O2GDPF2d1nGWEuqX54qofHznS27WZnAWEWz1AOJJHQRRlxpkI35wzfuZZa4IQU67ItD5v9+iB+USgHeSVQ2syTNr
l9Pj+KL4bF+H4SKDl04Vh2ZaDt4xjD++hr9ViZxJZhZW5p9/xbKh2cLKHgzGwKNHcrCrE4aK9OHxRXE3qEwPRi3wTWgK
KxjBspuYXGB7rF2PYCYpl8Pq8f/5j5P7wm8vyQetVGIok3H0OmamWQY1V49sNQIXmk87uYbeBAvCo396i4wnoG93/JtT
rS6pMdQeltR6y19hWr0L+lGR4ZbrBG6ddRSAfXtuqOCnK6hi7RHdeR5bARA3y3QIDAQABoxAwDjAMBgNVHRMEBTADAQH
/MA0GCSqGSIb3DQEBCwUAA4ICAQAKgsmhl3HOgYv7z0jUOE72L1jyxka4xXtd0YB/t/ImV6ErL6euNTEUXQ+eBPhNQ/h
k89eG4XTIjLsFStrMq9Qd0s6fzxgMKhacbkowqCoO2Sl/2/L4wndiZdo/NCxtnWy2pNH6Uaz7jc0py3BraW3NEWJAEqF
J5u5t6vgIe+Tsunx0n2qBPJaygZm5npeTX97JzmElkHGXfSLkwHOlfrIs3LpncVOTRwGm8+39FIrdnxA3UALSdiU7sWQ
g/Z8JIwbMdfWzjDBkNHiem4ptzKKpnIeOp+2R6aIzv07NU416I40OEIDAyQ/yDX+4vLT0fLPXKcrl21S7+3HjlHGQkdh
OwfNMBL5jrXedon5Op/c2QGDov2QGe+IJoprqi72CzMlEBVGxo6fjPS61x32kC29YYCPg01mvLPXk00U3etlguVAkPJZ
KLo/TruiKEoyIMn74MjzMabd4+zV/0tN6bSWz3PWctqGsiYt+yGRq3JNlcBOeNFKyt6K+sVOoRmTG4NS2MqpT2gszYYk
XxCw8dIk6c/4TQVzfcDIyuyHkqPuer889GKLPqvviVW214lIqHj6yDsBRimwzW5a19B03NP7wRONorUl21xZWQA2xBRh
XExyYF5stYwMdshl7EnDlBfbVT+b0va6Dzbz9qAsG/WqrPTyNl2Dx6cBml3XmFgcO3A==
```

5. We will now check the federation with the following command in the powershell

Get-MsolDomainFederationSettings -domainName tokyo01.euc-livefire.com

The settings will return output regarding the settings that make up this federation.

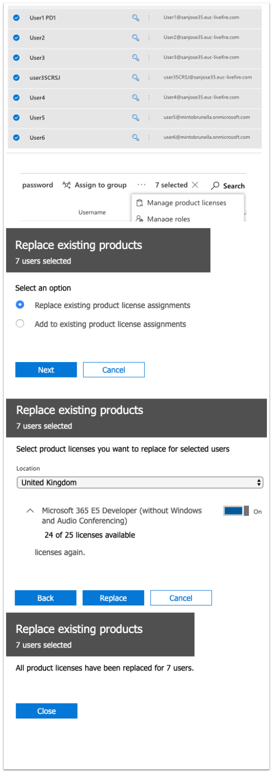


```
PS C:\> Get-MsolDomainFederationSettings -domainName tokyo01.euc-livefire.com


ActiveLogOnUri                         : https://aw-euclivefire.vidmpreview.com/SAAS/auth/w
                                         sfed/active/logon
DefaultInteractiveAuthenticationMethod :
FederationBrandName                    : Livefire
IssuerUri                              : tokyo01.euc-livefire.com
LogOffUri                              : https://login.microsoftonline.com/logout.srf
MetadataExchangeUri                    : https://aw-euclivefire.vidmpreview.com/SAAS/auth/w
                                         sfed/services/mex
NextSigningCertificate                 :
OpenIdConnectDiscoveryEndpoint         :
PassiveLogOnUri                        : https://aw-euclivefire.vidmpreview.com/443/SAAS/AP
                                         I/1.0/POST/sso
SigningCertificate                     : MIIFKDCCAxCgAwIBAgIGPBcCTXRSMA0GCSqGSIb3DQEBCwUAME
                                         wxIDAeBgNVBAMMF1ZNd2FyZSBJZGVudGl0eSBNYW5hZ2VyMRsw
                                         GQYDVQQKDBJBVy1FVUNMSVZFRklSRTpFTkMxCzAJBgNVBAYTAl
                                         VTMB4XDTE5MDIwNDIxMzEwNFoXDTI5MDIwMTIxMzEwNFowTDEg
                                         MB4GA1UEAwwXVk13YXJlIElkZW50aXR5IE1hbmFnZXIxGzAZBg
                                         NVBAoMEkFXLUVVQ0xJVkVGSVJFOkVOQzELMAkGA1UEBhMCVVMw
                                         ggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCpYVvr3N
                                         U7cGmIVGdU9ut7xhK6MDTgUO/qsltoLBZ+kY7NrNXMKSXJ0LCK
                                         DR8L0/GSknchHGFRsBHndYnN64SbY4SIlKFXkjmgYmYumtk8jl
                                         G8waKCyZ7Nhrx+lZ6TqsEwJ9nn7rhPfSj9YCkyDWtFl+YE2zLL
```

Part 5: In this part, we will now start testing the federation to see and ensure it it working properly

1.

- Login back to your **office 365 Tenant** with your office Admin account with this url https://admin.microsoft.com/Adminportal/Home?source=applauncher#/homepage and use your **cloudadmin account**
  1. In the left-hand pane under **Home**, select **Users** > **Active users.** Notice that Marketing group **Users 1 - 8** has been automatically provisioned with the unique suffix appended for the user principle name. Also notice that your users are Unlicensed. Select users 1-8
  2. Select the **radio buttons** next to **User 1 to User 8**. This is includes your **Custom User**
  3. Next to **Assign to group** select the **3 dots** which will expand the menu and select **Manage product licenses**
  4. In the **Manage Product licenses** window select **Next**
  5. On the **Replace existing products** window under **Location,** select a location ie United Kingdom.
  6. Next to **Microsoft E5 Developer (without Windows and Audio Conferencing),** turn the **slider bar** to **On**
  7. **Scroll down** and select **Replace** select **Close.**
  8. **NB!** - Validate that your **Cloudadmin** account is licensed as well. This will depend on whether you started off with a custom Outlook account or used another email in the beginning of the course labs. If not re-apply to the licensing to this account and then ensure that you can open the Cloudadmin mailbox. This requirement must be done before starting your OKTA lab.



User1 PD1	User1@sanjose35.euc-livefire.com
User2	User2@sanjose35.euc-livefire.com
User3	User3@sanjose35.euc-livefire.com
user35CRSJ	user35CRSJ@sanjose35.euc-livefire.com
User4	User4@sanjose35.euc-livefire.com
User5	user5@mintobrunella.onmicrosoft.com
User6	user6@mintobrunella.onmicrosoft.com

Replace existing products
7 users selected

Select an option

● Replace existing product license assignments

○ Add to existing product license assignments

Replace existing products
7 users selected

Select product licenses you want to replace for selected users

Location: United Kingdom

Microsoft 365 E5 Developer (without Windows and Audio Conferencing) — On

24 of 25 licenses available

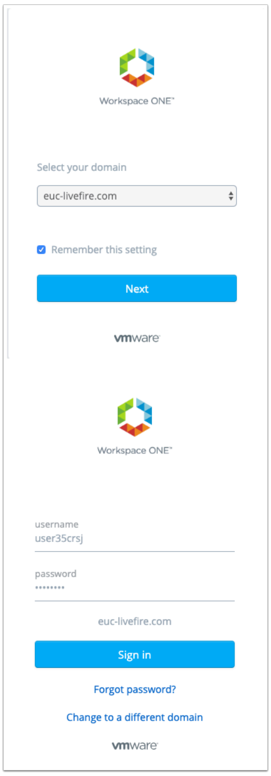
licenses again.

Replace existing products
7 users selected

All product licenses have been replaced for 7 users.

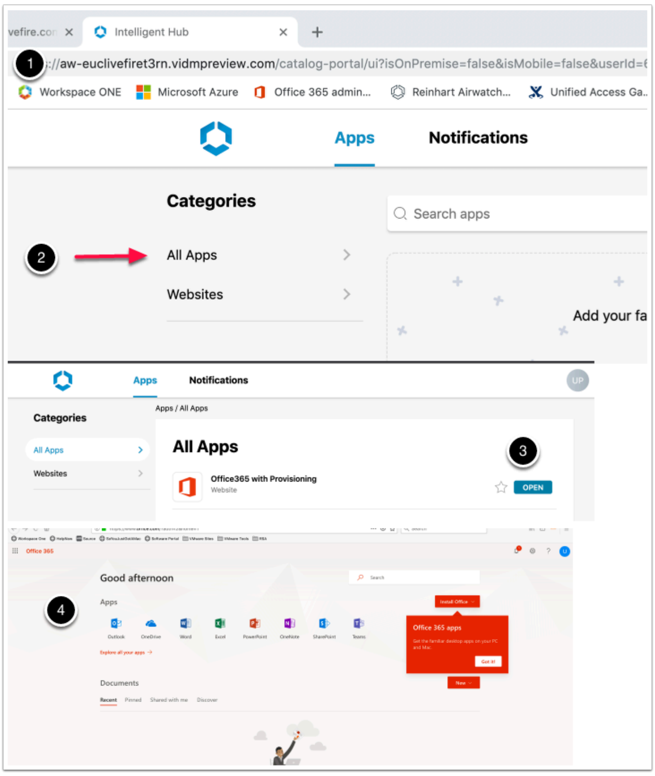
2.

- Open up an **Incognito** session of your browser and connect to your SAAS instance of Workspace ONE Access.
  1. On the login window ensure that on the select your domain window, **euc-livefire.com** is selected, select Next
  2. In the **username** section, use your custom **username ie** **user35scr** and the **password** **VMware1!** select **Sign in**



3.

- In the **Workspace ONE** console
  1. Under **Apps** select **All Apps**
  2. Next **Office 365 with Provisioning** select **Open**
  3. You should now see the Microsoft Office365 console

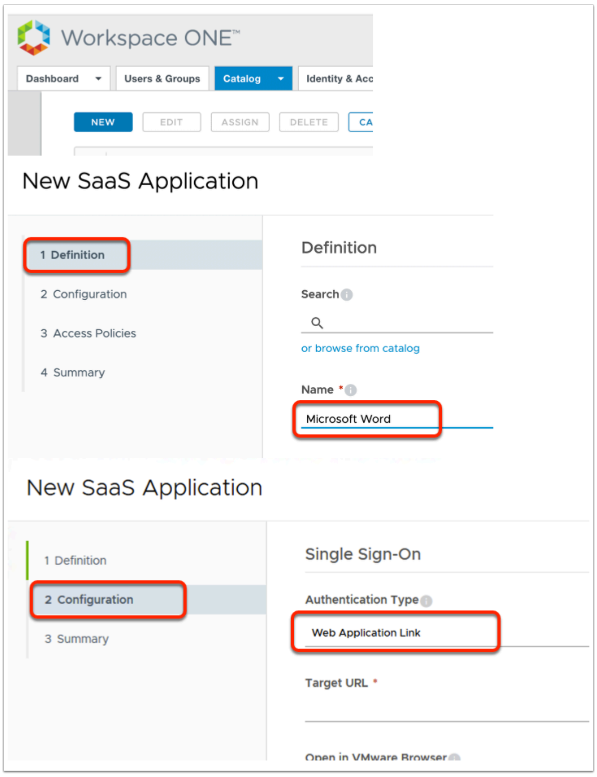


Part 6: Inserting Office 365 Deep Links into Workspace ONE Access

Having a Portal to Portal single sign-on experience very rarely excites a customer. In this section we will insert Deep Links within Workspace ONE Access to enhance the user experience.

1. Inserting Office 365 Deep links

- On your **Controlcenter** server. **Log in** to your to your Workspace ONE Access Console as Admin and select the **Catalog** tab > **Web Apps**
  1. Select **NEW**
  2. In the **New SaaS Application** window under **Name** type **Microsoft Word**
  3. Under Icon, click on **browse,** search for the software link on your desktop, and navigate to \Applications\Azurefiles\icons. select your **Word.png** Icon and select **Open.** At the bottom right select **NEXT**
  4. On **2. Configuration** in the **Single Sign-On** section under **Authentication type** to the right select the **drop down** and then select **Web Application Link**

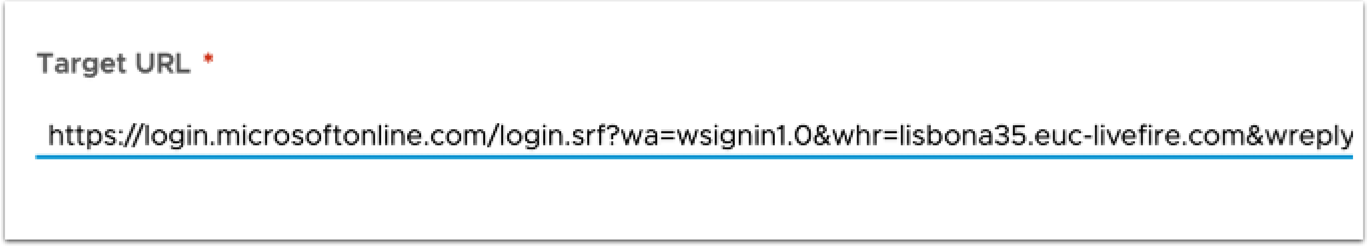


Name * Microsoft Word

Authentication Type Web Application Link

2. Inserting Office 365 Deep links (Part 5)

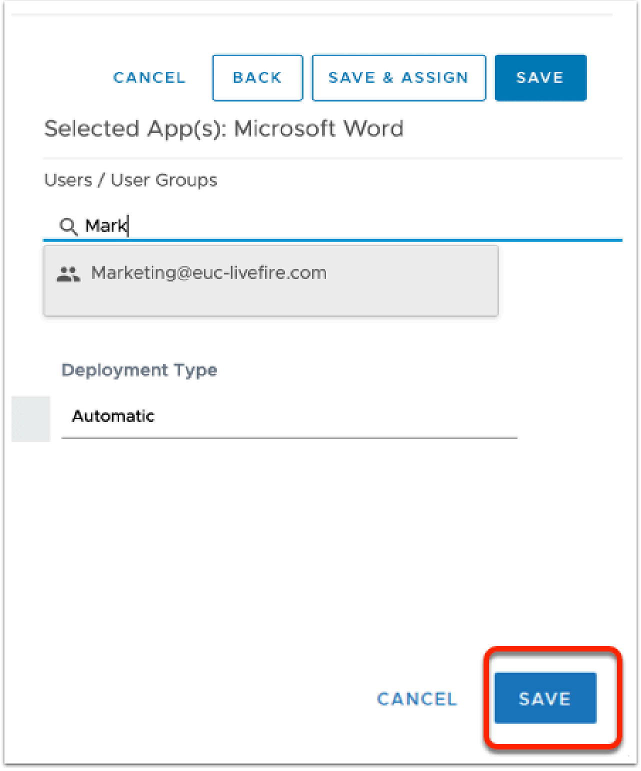
- Copy the URL below and edit in **Notepad++** the following in Blue with **your assigned domain suffix** and then **copy** the edited URL and Paste under the **Target URL**
  - **https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=EXAMPLEDOMAIN.euc-livefire.com&wreply=https://office.live.com/start/Word.aspx?auth=2**


Target URL *

https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=lisbona35.euc-livefire.com&wreply

3. Inserting Office 365 Deep links (Part 5)

- Select **NEXT** > **SAVE & ASSIGN**
  1. Under **Users / User Groups** in the **Search** area type **Mark**, select **Marketing@euc-livefire.com**
  2. Under **Deployment Type** select **Automatic** and select **SAVE**



Selected App(s): Microsoft Word

Users / User Groups

Mark

Marketing@euc-livefire.com

Deployment Type

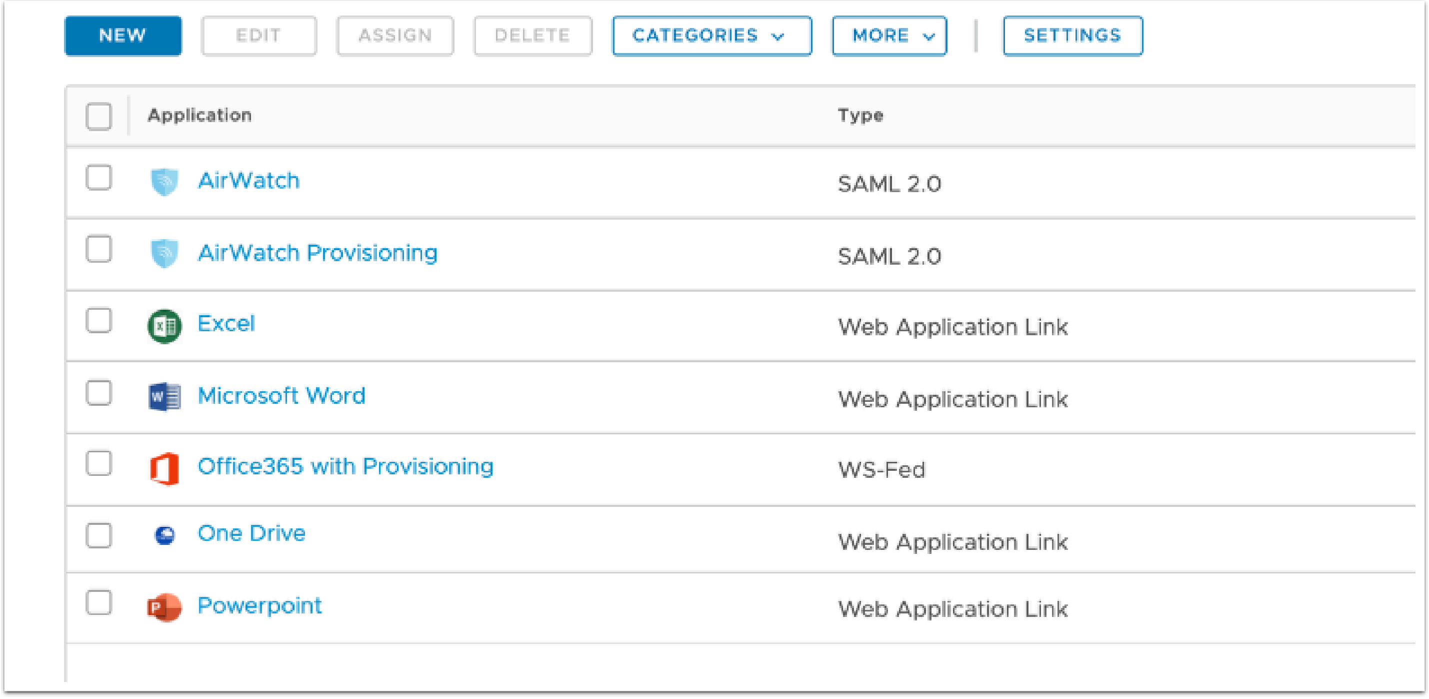
Automatic

4. Inserting Office 365 Deep links (Part 5)

- Repeat the above steps for
  1. **OneDrive**
     - https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=**lisbonb35**.euc-livefire.com&wreply=https://zingaramanwell-my.sharepoint.com
     - Replace **Lisbonb** with your domain
     - Replace **zingaramanwell** with your unique Office 365 domain name. eg in this example the domain name is cloudadmin@**zingaramanwell**.onmicrosoft .com, **zingaramanwell** is the domain name
  2. **Excel**

- https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=**lisbonb35**.euc-livefire.com&wreply=https://www.office.com/launch/excel?auth=2&home=1

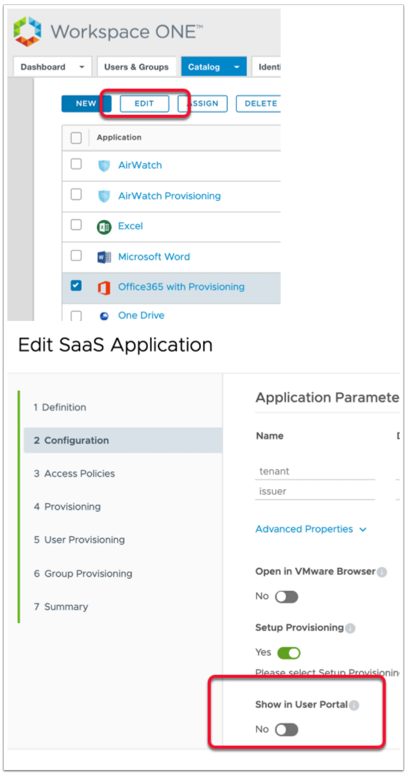
3. **PowerPoint**
   - https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=**lisbonb35**.euc-livefire.com&wreply=https://www.office.com/launch/powerpoint?auth=2
4. **Outlook**
   - https://login.microsoftonline.com/common/oauth2/authorize?client_id=00000002-0000-0ff1-ce00-000000000000&response_mode=form_post&
     livefire.com



☐ Application	Type
☐ AirWatch	SAML 2.0
☐ AirWatch Provisioning	SAML 2.0
☐ Excel	Web Application Link
☐ Microsoft Word	Web Application Link
☐ Office365 with Provisioning	WS-Fed
☐ One Drive	Web Application Link
☐ Powerpoint	Web Application Link

5. Inserting Office 365 Deep links (Part 5)

- The Office 365 application has been assigned to Marketing. It has to remain assigned to Marketing for the Deep links to work. However, we do not necessarily want this to be visible to the End-User. We will now solve this issue as part of a well thought out solution.
  1. In the **Catalog**, select the **Check-box** next to **Office365 with Provisioning**, select **EDIT**
  2. in the **Edit SaaS Application** window, select step **2 Configuration** and scroll down to the bottom. Change **Show in the User Portal** toggle from **Yes** to **No**
  3. Select **NEXT** > **NEXT** > **NEXT** > **NEXT** > **SAVE**



☐ AirWatch
☐ AirWatch Provisioning
☐ Excel
☐ Microsoft Word
☑ Office365 with Provisioning
☐ One Drive

Edit SaaS Application

tenant
issuer

Open in VMware Browser: No

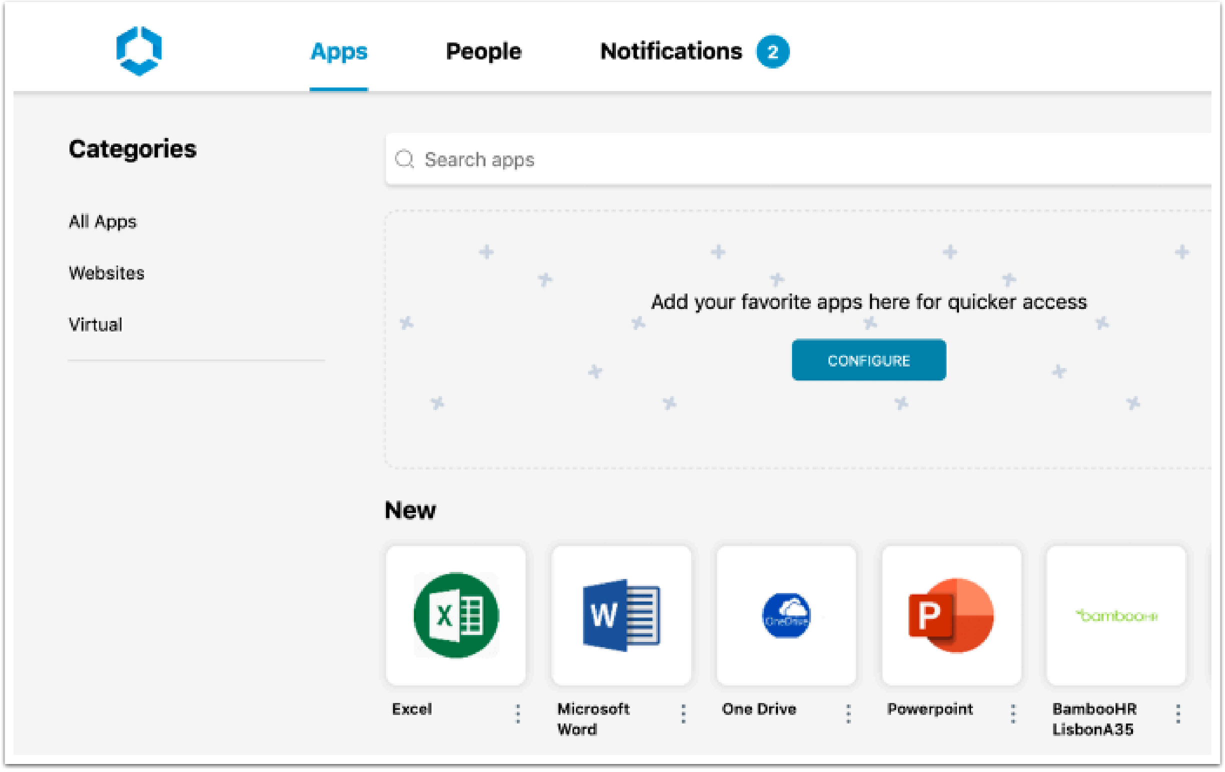
Setup Provisioning: Yes

Please select Setup Provisionin

Show in User Portal: No

6. Inserting Office 365 Deep links (Part 5)

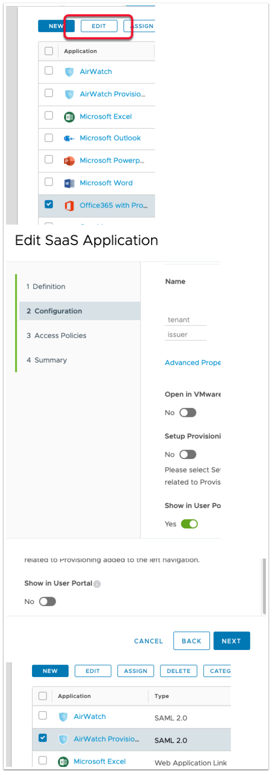
- Switch to a Browser in Incognito Mode . Using your Workspace ONE Access URL login as User1 with the password VMware1!
- Test your individual links for office 365



7. Tidying up the Catalog in Workspace ONE Access for a better User Experience

- Switch back to your **Workspace ONE Access Admin** Console and select the **Catalog** tab

1. In the **Catalog** next to **Office 365 with Provisioning** select the **check box** and then at the top select **EDIT**
2. In the **Edit SaaS Application** wizard select **2 Configuration** and **scroll down** to the bottom,
3. Change the **toggle** under **Show in User Portal** from **Yes** to **No** and select **NEXT** > **NEXT** > **SAVE**
4. Repeat the exact same process and validate that that the **AirWatch** and **AirWatch Provisioning** applications do not show in the User Portal



Federating a SAML application with Workspace ONE Access

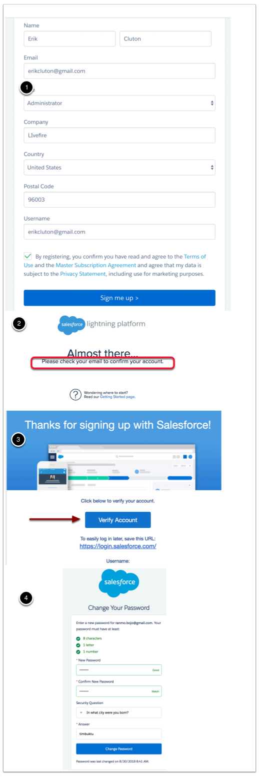
VMware Identity Manager SaaS application

Part 1. SFDC Pre-Requisites Setup

This lab is intended to prepare those federating SaaS applications for authentication via Workspace ONE Access. As SAML is a standard authentication type, this example is just one of many documented integrations. See here for more examples: **https://www.vmware.com/support/pubs/Workspace ONE Access_webapp_sso.html**

1.1 First we will sign up for a SFDC developer trial account.

- Open your Browser on the Control Center VM
  1. Navigate to **https://developer.salesforce.com/signup** for a free account.
     - Fill in your details using a personal e-mail address. Please ensure this e-mail address has not previously been used with SFDC
  2. *Go to your **email** and confirm your registration*. Select Verify Account. This will take you to the **Change Your Password** Site.
  3. **Set a password of your choosing** and provide a security question and answer
  4. Select **Change Password** to save and you will be redirected automatically to the Setup Home page.



Name
Erik | Cluton

Email
erikcluton@gmail.com

Administrator

Company
LIvefire

Country
United States

Postal Code
96003

Username
erikcluton@gmail.com

☑ By registering, you confirm you have read and agree to the Terms of Use and the Master Subscription Agreement and agree that my data is subject to the Privacy Statement, including use for marketing purposes.

Sign me up >

Almost there...
Please check your email to confirm your account.

Wondering where to start?
Read our Getting Started page.

Thanks for signing up with Salesforce!

Click below to verify your account.

Verify Account

To easily log in later, save this URL:
https://login.salesforce.com/

Username:

Change Your Password

Enter a new password for ranmo.bojo@gmail.com. Your password must have at least:
✓ 8 characters
✓ 1 letter
✓ 1 number

* New Password
········· Good

* Confirm New Password
········· Match

Security Question
In what city were you born?

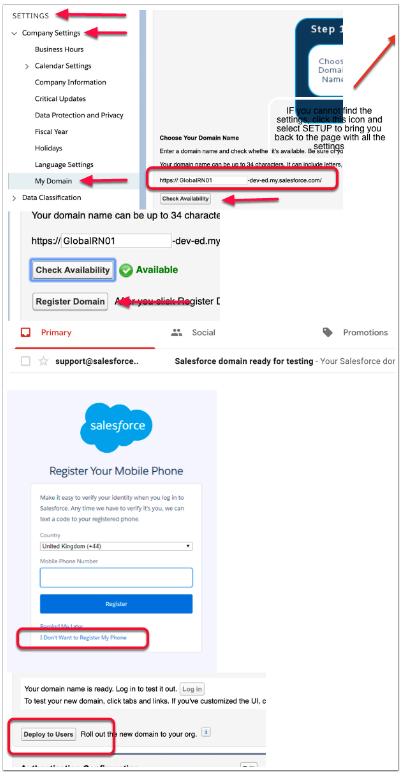
* Answer
timbuktu

Change Password

Password was last changed on 8/30/2018 8:41 AM.

1.2 You should still be automatically logged in with the user that you have created above, if not navigate to https://login.salesforce.com and login with the details for your account.

- **NOTE**: Salesforce has two Web Interfaces and this can get quite confusing. Please be sure to use the **lightning experience** interface rather than the classic interface. **You will now register a unique domain name for you SFDC dev account**
  1. On the Home page **Navigate to Settings** > **Company Settings** > **My Domain**
  2. Enter a **unique domain name** under "**Choose Your Domain Name" - first letter of first name plus last name plus livefire** - ***For example*** - globalrn01
  3. Click **check availability**, If available select **Register Domain**. *This process usually takes about 5 to 10 minutes.* (SalesForce has to publish that unique domain name) You can move on to "**Establish SAML Trust**" Section below come back to this section once you get asked to login to your unique URL.
  4. You will receive an e-mail to the address specified in your developer's account once it has successfully registered. **Click the link provided** in the **e-mail** to confirm your domain registration and login using the credentials you created above. **NOTE: at this point it might prompt you for a phone number. You can easily select I don't want to register my phone. Then it will just use your e-mail address as the second factor authentication.**
  5. Now Navigate back to **Settings** > **Company Settings** > **My Domain** and select the **Deploy to users** and confirm the pop-up.



IF you cannot find the settings, click this icon and select SETUP to bring you back to the page with all the settings

Choose Your Domain Name

Enter a domain name and check whethe it's available. Be sure of yo

Your domain name can be up to 34 characters. It can include letters,

https:// GlobalRN01 -dev-ed.my.salesforce.com/

Your domain name can be up to 34 characte

https:// GlobalRN01 -dev-ed.my

After you click Register D

support@salesforce.. Salesforce domain ready for testing - Your Salesforce dor

Register Your Mobile Phone

Make it easy to verify your identity when you log in to Salesforce. Any time we have to verify it's you, we can text a code to your registered phone.

Country: United Kingdom (+44)

Mobile Phone Number

Your domain name is ready. Log in to test it out.

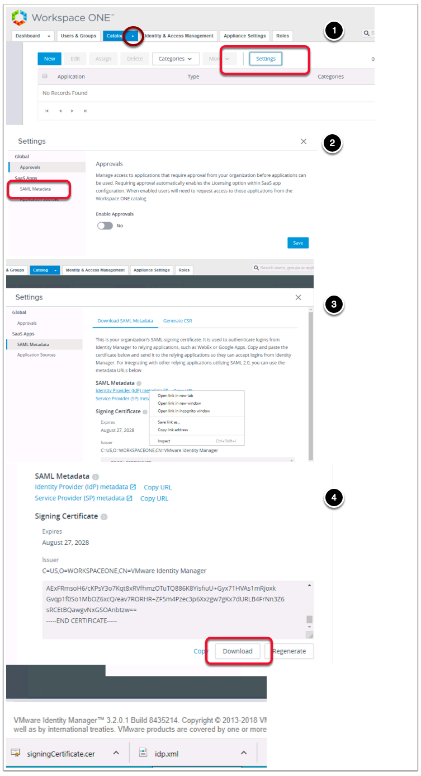
To test your new domain, click tabs and links. If you've customized the UI, c

Roll out the new domain to your org.

Part 2. Establish SAML Trust

2.1

- Now we will download the identity provider Signing certificate from Workspace ONE Access and upload it into SFDC to create the trust relationship for authentication.
  1. Login to your Saas Workspace ONE Access as sysadmin
  2. Select the **Catalog** tab and select **Settings**
  3. Select **Settings** select SAML Metadata
  4. Right click on **Identity Provider (Idp) metadata** and select **save link as**, this will open your **Save As** window. Leave the **Downloads** folder as default and the name as **idp.xml** and select **Save**
  5. Go to the **Signing Certificate** area and select **Download** , you should now have a **signingCertificate.cer** and a **idp.xml** in the **Downloads** folder



Approvals

Manage access to applications that require approval from your organization before applications can be used. Requiring approval automatically enables the Licensing option within SaaS app configuration. When enabled users will need to request access to those applications from the Workspace ONE catalog.

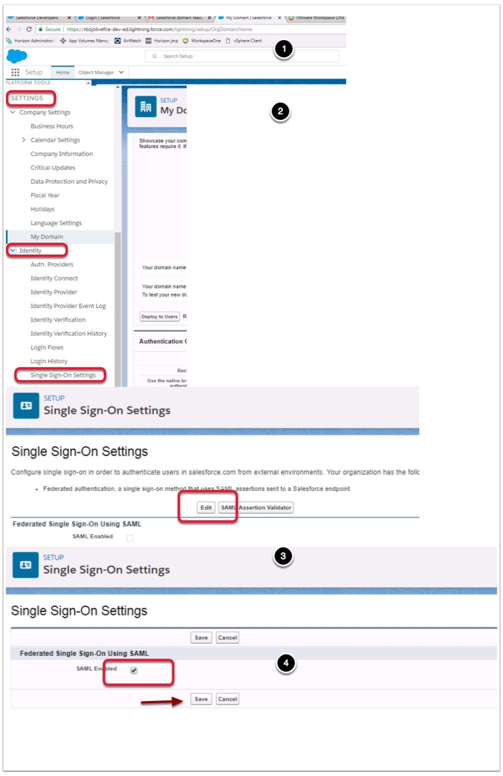
This is your organization's SAML-signing certificate. It is used to authenticate logins from Identity Manager to relying applications, such as WebEx or Google Apps. Copy and paste the certificate below and send it to the relying applications so they can accept logins from Identity Manager. For integrating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

```
AExFRmsoH6/cKPsY3o7Kqt8xRVfhmzOTuTQ886K8YisfiuU+Gyx71HVAs1mRjoxk
Gvqp1f0So1MbOZ6xcQ/eav7RORHR+ZF5m4Pzec3p6Xxzgw7gKx7dURLB4FrNn3Z6
sRCEtBQawgvNxGSOAnbtzw==
-----END CERTIFICATE-----
```

VMware Identity Manager™ 3.2.0.1 Build 8435214. Copyright © 2013-2018 VM
well as by international treaties. VMware products are covered by one or more

2.2

- Navigate back to your SalesForce site where you should now be able to login with your unique registered domain ***-dev-ed.lightning.force.com**
  1. On the home page for the admin user you will find **Settings** > **Identity** > **Single Sign-On Settings** **NOTE:** if you can't locate these options on the initials login page select the cog wheel in the top right hand side of the page and select setup and it will take you to the correct configuration page.
  2. On the **Single Sign-On Settings** Page next **SAML Assertion Validator** select **Edit**, below **Federated Single Sign-on Using SAML**, select the **SAML Enabled** **checkbox**. Select **Save.**



Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the follc

- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

Federated Single Sign-On Using SAML

SAML Enabled □

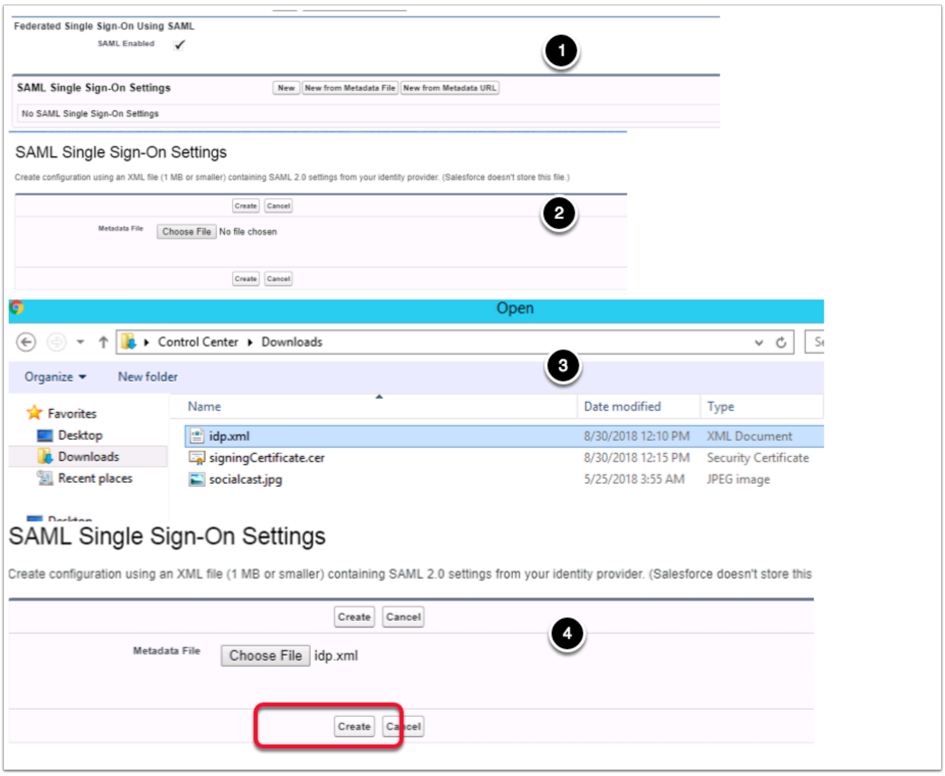
Single Sign-On Settings

Federated Single Sign-On Using SAML

SAML Enabled ☑

2.3

- Now select **New From Metadata File** just underneath where the SAML settings have been enabled.
  1. This will take you to the **SAML Single Sign-On Settings** page where it will request the SAML metadata**.**
  2. Click **Choose File** that you have downloaded into the **Downloads** Folder from Workspace ONE Access named **idm.xml** (created in step 5). select the **idp.xml** and select **Open** select **Create.**



SAML Single Sign-On Settings

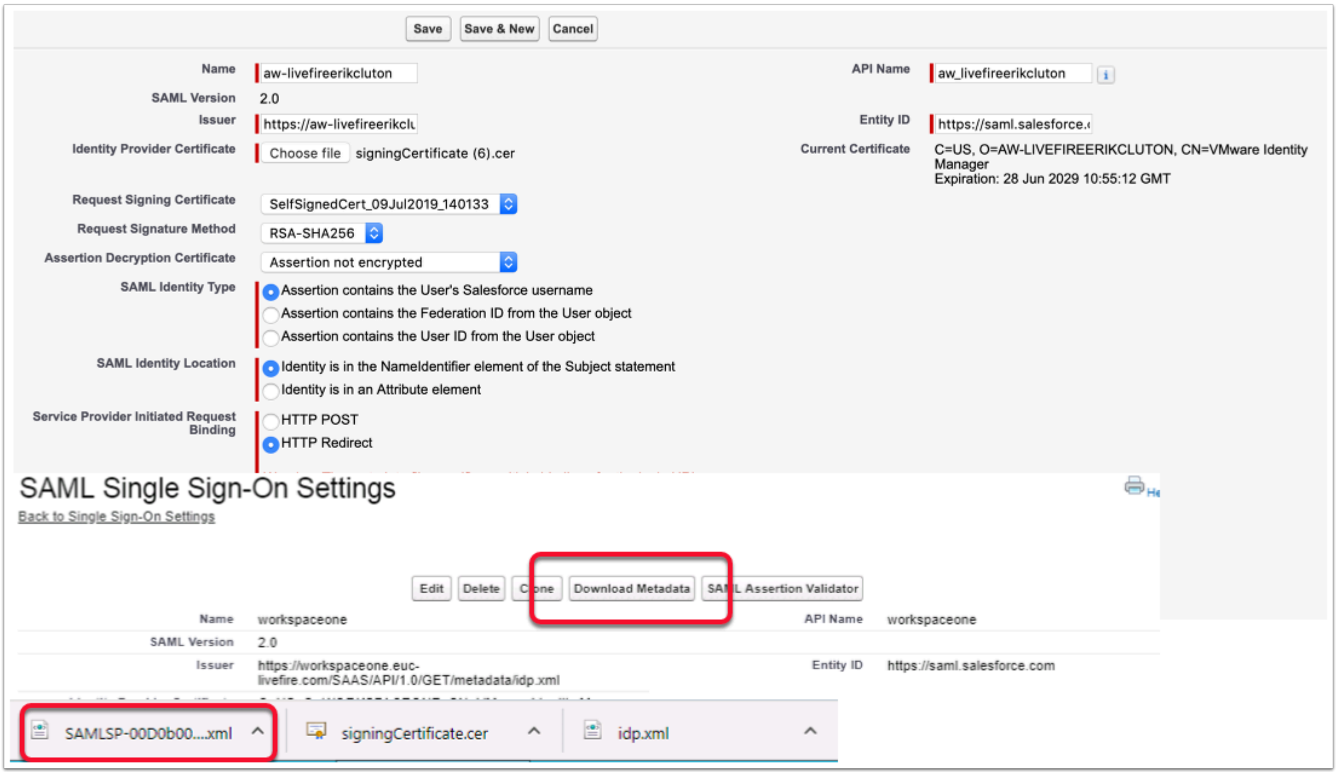
Create configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't store this file.)

Name	Date modified	Type
idp.xml	8/30/2018 12:10 PM	XML Document
signingCertificate.cer	8/30/2018 12:15 PM	Security Certificate
socialcast.jpg	5/25/2018 3:55 AM	JPEG image

2.4

- Notice now that the fields have been auto populated with the correct data from Workspace ONE Access

1. Ensure the Following are correct in the settings:
   - Next to **NAME:** *leave as default*
   - Next to **ISSUER:** *leave as default*, This is the XML that is provided for the Metadata -
   - Next to **Provider Certificate**: Upload the signingCertificate.cer into this field (this was created in step 5)
   - Next to **SAML Identity Type:** leave as default "Assertion contains the User's Salesforce username
   - Next to **SAML Identity Location**: *leave as default* "Identity is in the NameIdentifier element of the Subject statement
   - Next to **API Name:** *leave as default*
   - Next to **Entity ID:** Change to **https://saml.salesforce.com**
   - Next to **Identity Provider Login URL:** *l*eave as default
   - Next to **Custom Logout URL:** **your Workspace ONE Access URL**
     - **e.g.** https://aw-livefireerikcluton.vidmpreview.com
   - Ensure the check box from **Single Logout Enabled** is **removed.**
2. Select **Save**.
3. On the **SAML Single Sign-On Settings** page select **Download Metadata**.
   - **NOTE:** *Download metadata* is not available in the **edit view** you have to click on the policy This will **download an xml** file beginning with **SAMLSP.....xml**



Name: aw-livefireerikcluton
API Name: aw_livefireerikcluton
SAML Version: 2.0
Issuer: https://aw-livefireerikclu
Entity ID: https://saml.salesforce.
Identity Provider Certificate: Choose file signingCertificate (6).cer
Current Certificate: C=US, O=AW-LIVEFIREERIKCLUTON, CN=VMware Identity Manager
Expiration: 28 Jun 2029 10:55:12 GMT
Request Signing Certificate: SelfSignedCert_09Jul2019_140133
Request Signature Method: RSA-SHA256
Assertion Decryption Certificate: Assertion not encrypted
SAML Identity Type:
● Assertion contains the User's Salesforce username
○ Assertion contains the Federation ID from the User object
○ Assertion contains the User ID from the User object
SAML Identity Location:
● Identity is in the NameIdentifier element of the Subject statement
○ Identity is in an Attribute element
Service Provider Initiated Request Binding:
○ HTTP POST
● HTTP Redirect

SAML Single Sign-On Settings

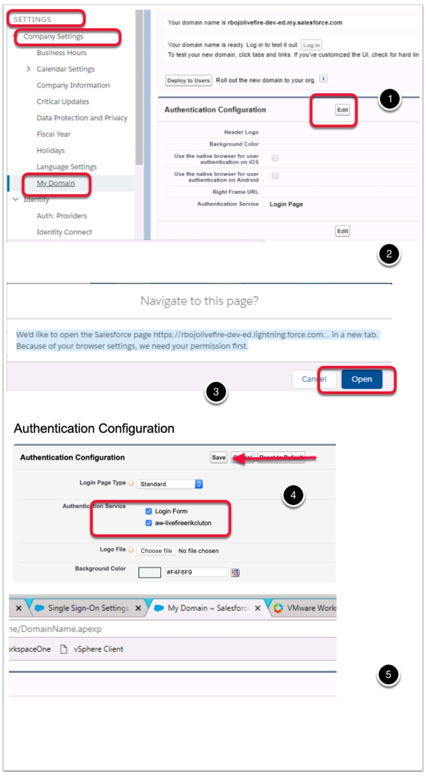
Back to Single Sign-On Settings

Name: workspaceone
API Name: workspaceone
SAML Version: 2.0
Issuer: https://workspaceone.euc-livefire.com/SAAS/API/1.0/GET/metadata/idp.xml
Entity ID: https://saml.salesforce.com

2.5

- On the SalesForce admin console
  1. Navigate to **Settings** > Company Settings > My Domain
  2. In the **Authentication Configuration** section select **edit,** this will open a new tab. Ensure that you observe Pop-up Blocker in your browser and select the radio button **to Always allow pop-ups.**...,
  3. Select **Done,** and then on the **Navigate to this page?** window select **Open**
  4. Under **Authentication Configuration** page next to **Authentication Service** select the **check box** that has **"YOUR Saas Workspace ONE Access"** and select **Save**
     - **NB! Notice that this pop-up window opened up in a new window on a new TAB.**

Revert back by selecting the original window Single Sign-On Settings tab to the left of your current window



Your domain name is rbojolivefire-dev-ed.my.salesforce.com

Your domain name is ready. Log in to test it out.
To test your new domain, click tabs and links. If you've customized the UI, check for hard lin

Roll out the new domain to your org.

Authentication Configuration

Header Logo
Background Color
Use the native browser for user authentication on iOS □
Use the native browser for user authentication on Android □
Right Frame URL
Authentication Service: Login Page

Navigate to this page?

We'd like to open the Salesforce page https://rbojolivefire-dev-ed.lightning.force.com... in a new tab. Because of your browser settings, we need your permission first.

Authentication Configuration

Authentication Configuration

Login Page Type: Standard
Authentication Service: ☑ Login Form ☑ aw-livefireerikcluton
Logo File: No file chosen
Background Color: #F4F6F9

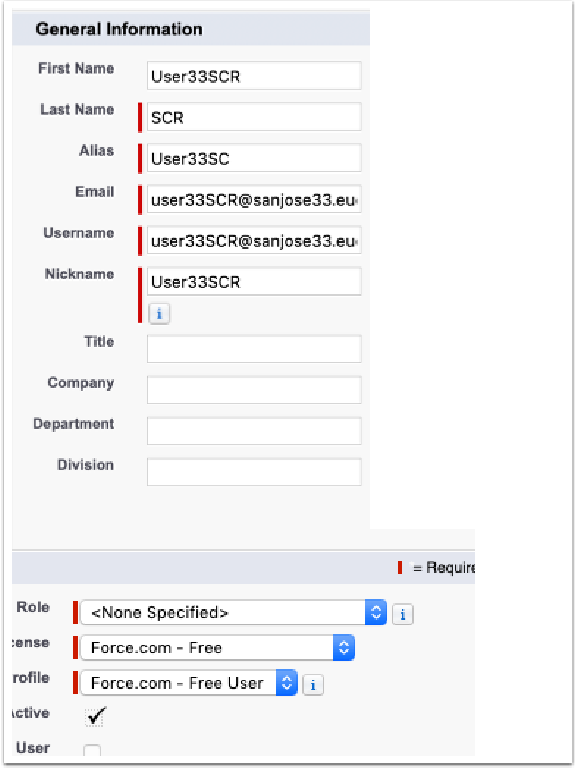
2.6

- Creating a unique user for your SalesForce environment.

NB! This has to be an Identical account to what you created at the beginning of the course

1. Navigate to **Administration** > **Users** > **Users** > click Select **New User**
2. Fill in the unique user details,
   - **First Name:** User xxxxx {your student number + {the first letter of your city and country abbreviation}} eg {for San jose, Costa Rica User33SCR}
   - **Last Name:** {the first letter of your city and country abbreviation} eg. SCR
   - **Alias:{same as your first name}**
   - **Email:{FirstName@customsuffix.euc-livefire.com}** (For Example: user33SCR@sanjose33.euc-livefire.com)
   - **Username:{FirstName@*customsuffix*.euc-livefire.com}** (For Example: user33SCR@sanjose33.euc-livefire.com)
   - **Nickname: {same as your FirstName}**
   - **Role: <None Specified >**
   - **User License: Force.com - Free**
   - **Profile:Force.com - Free User**
3. Click **Save**

This will be the user we will use to test the authentication



General Information

First Name	User33SCR
Last Name	SCR
Alias	User33SC
Email	user33SCR@sanjose33.eu
Username	user33SCR@sanjose33.eu
Nickname	User33SCR
Title	
Company	
Department	
Division	

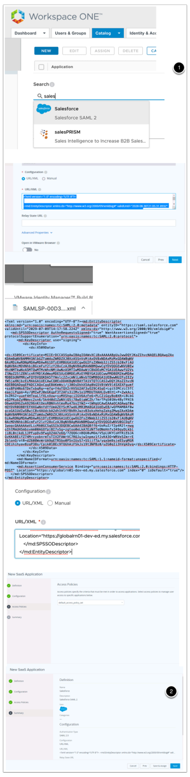
= Require

Role	<None Specified>
:ense	Force.com - Free
rofile	Force.com - Free User
ıctive	✓
User	□

2.7

- Navigate back to your **Workspace ONE Access console from your Controlcenter machine**

1. Select the **Catalog** tab, select **New**
2. On the **New Saas Application** window, in the search type **sales** and select **Salesforce**, select **Next**,
3. Under the **Single Sign-On** section under **Configuration**, select the **URL/XML radio** button.
4. Open **file Explorer** window and browse to Downloads. Right click and open the **metadata file** you downloaded from **Sales force** that was called **SAMLSP....xml**
5. Open in **Notepad.** In the Notepad select all or press **CTRL + A** and copy with **CTRL + C.** Now **paste** the **Metadata** in the XML field in **Single Sign-On** page under **URL/XML.**
6. On the **Single Sign-On** page select **Next**, on the **default Access policies** page accept the default select **Next** and select Save

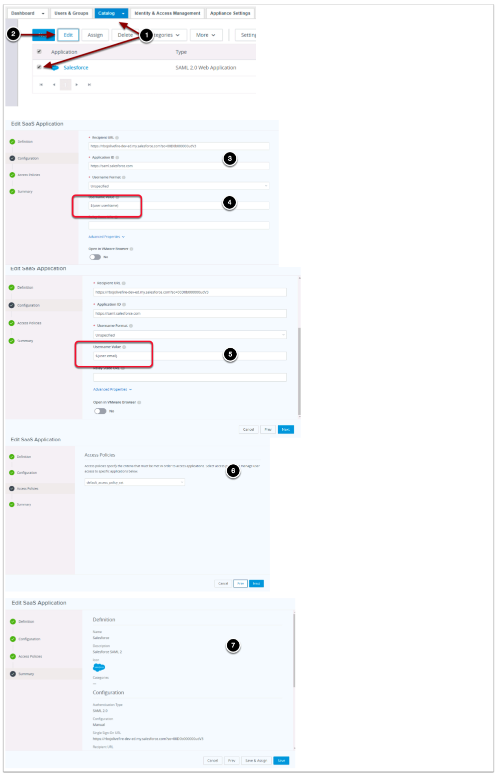


```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://saml.salesforce.com"
validUntil="2029-07-09T14:17:58.224Z" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="signing">
         <ds:KeyInfo>
            <ds:X509Data>

<ds:X509Certificate>[illegible]</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
      <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="https://globalrn01-dev-ed.my.salesforce.com" index="0" isDefault="true"/>
   </md:SPSSODescriptor>
</md:EntityDescriptor>
```

```
Location="https://globalrn01-dev-ed.my.salesforce.cor
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

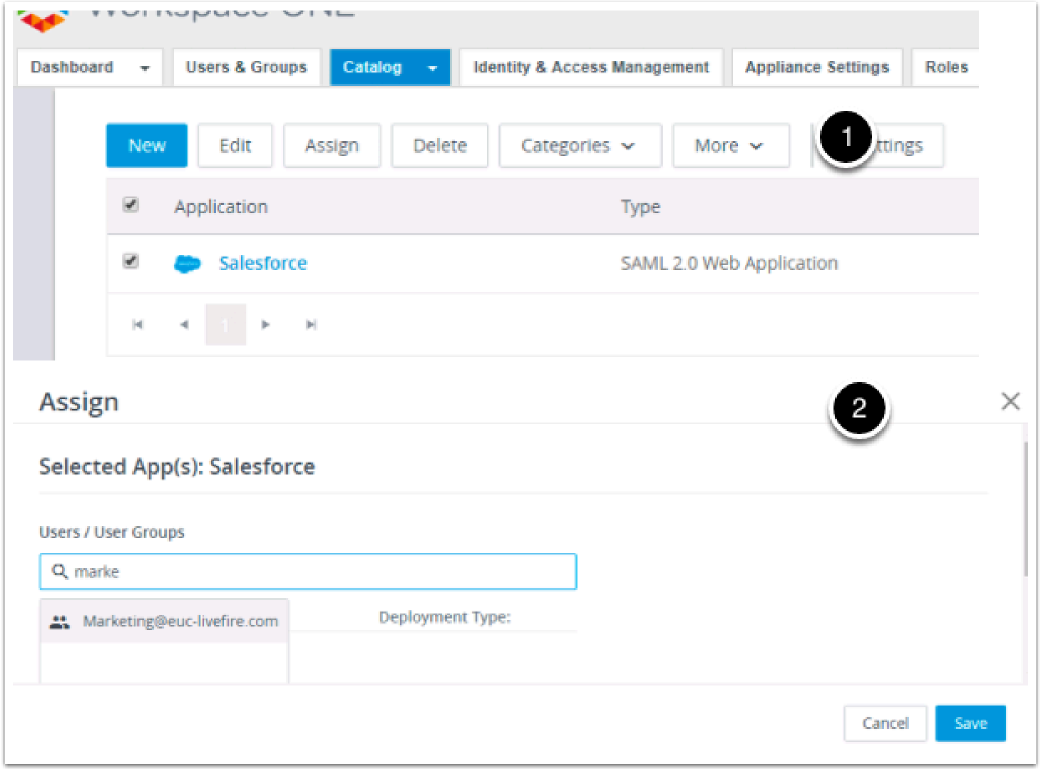
2.8

- On the **Catalog tab**, select **Salesforce** select **Edit**,
  1. Select Configuration, to the right of configuration, **scroll down** to **Username Value** and change **${user.username}** to **${user.email}**.
  2. Select **Next**, on the **Access Policies** page, select **Next**, on the **definition** page, select **Save.**



2.9

1. In the **Catalog** area next to Salesforce, select the **check box** and then select **Assign**
2. In the **Assign** window under **Users / User Groups** box type **marke** and select **Marketing@euc-livefire.com** and select Save



Selected App(s): Salesforce

Users / User Groups

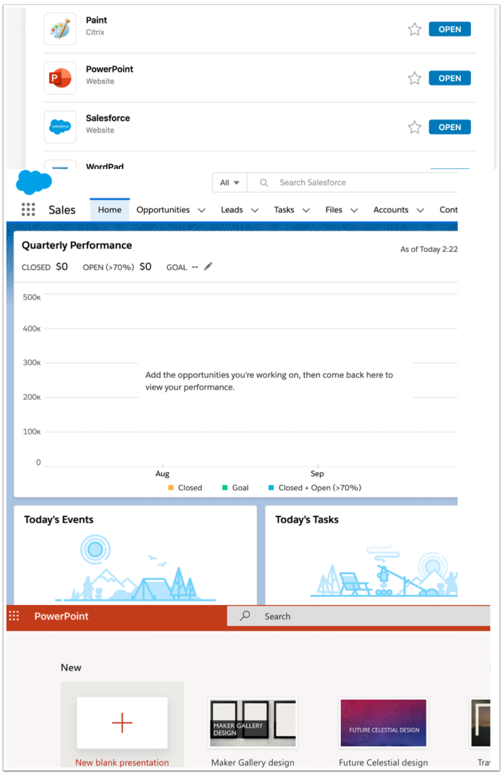
marke

Marketing@euc-livefire.com

Deployment Type:

3.0 Testing your custom account with the Salesforce and office 365 Federation

- Open up an Incognito window an alternate browser and login to your SaaS instance of Workspace ONE Access with your custom user account
  - Select and **open** your Salesforce Application
  - Select and **open** one of your Office Applications. NB! Depending on what Microsoft application you might still get messages stating that Office 365 is being setup. At this point all we are concerned is the federation of office 365



Add the opportunities you're working on, then come back here to view your performance.

(Optional) Android emulator setup

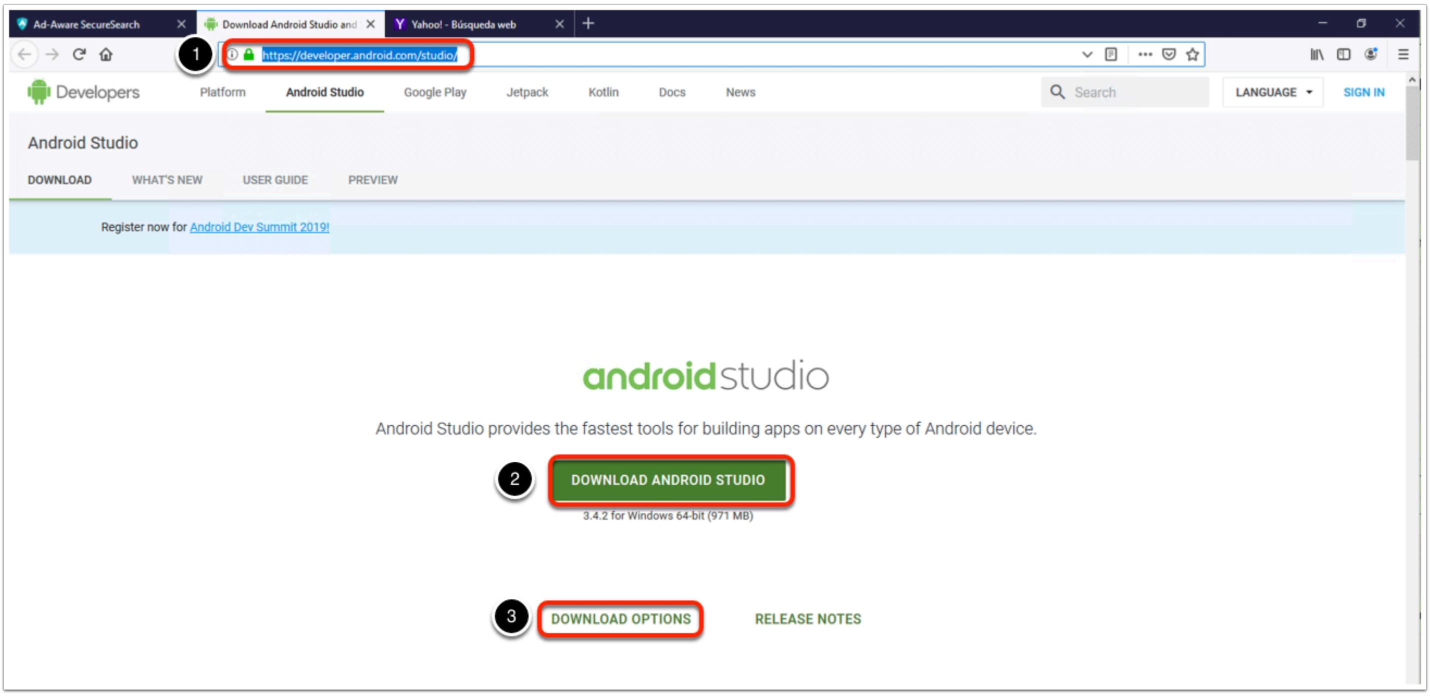
Introduction

If you don’t have an android test device and you want to test the Device enrollment, android single sign on, and other android based labs, theres an emulator you can install in your laptop an follow along with the particular lab manual as you would do on a physical device. What follows is the installation instructions for the installation of such software.

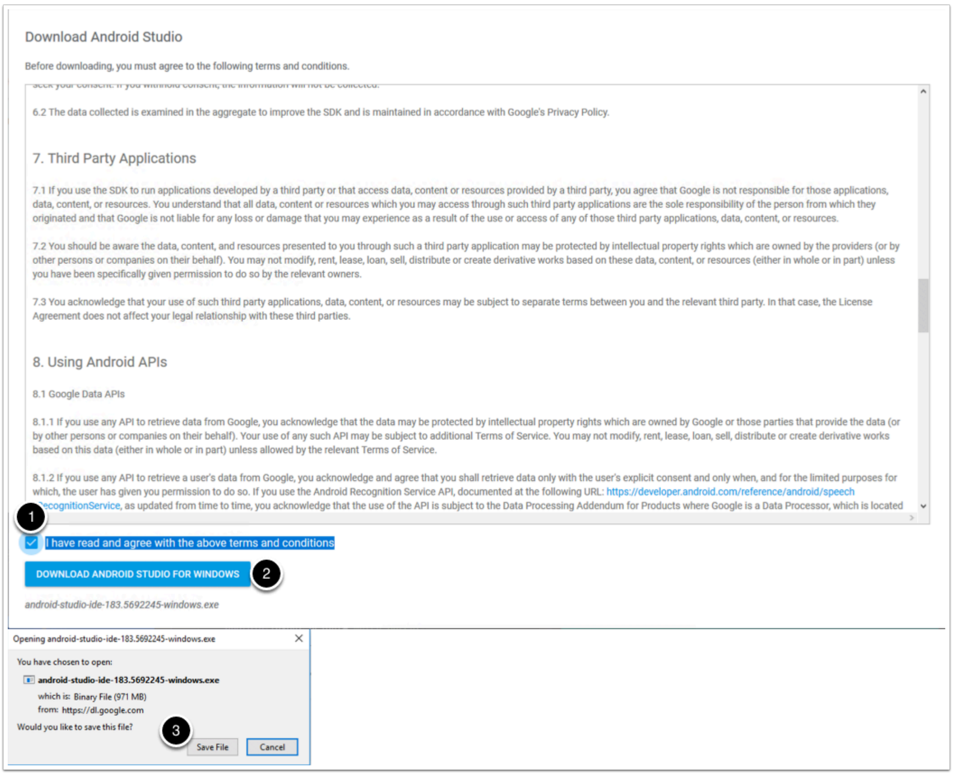
If something goes wrong and you want to start again with a fresh device, instructions are included for redeploying the os image.

downloading the installer

1. Go to **https://developer.android.com/studio/**
2. in the middle of your screen click on **Download Android Studio**
3. if the correct os version is not displaying click on **download options** and download the correct one



1. Check the box next to **I have read and agree with the above terms and conditions**
2. Click on **Download android Studio for your platform**
3. Click on **save file** when prompted



Download Android Studio

Before downloading, you must agree to the following terms and conditions.

seek your consent. If you withhold consent, the information will not be collected.

6.2 The data collected is examined in the aggregate to improve the SDK and is maintained in accordance with Google's Privacy Policy.

7. Third Party Applications

7.1 If you use the SDK to run applications developed by a third party or that access data, content or resources provided by a third party, you agree that Google is not responsible for those applications, data, content, or resources. You understand that all data, content or resources which you may access through such third party applications are the sole responsibility of the person from which they originated and that Google is not liable for any loss or damage that you may experience as a result of the use or access of any of those third party applications, data, content, or resources.

7.2 You should be aware the data, content, and resources presented to you through such a third party application may be protected by intellectual property rights which are owned by the providers (or by other persons or companies on their behalf). You may not modify, rent, lease, loan, sell, distribute or create derivative works based on these data, content, or resources (either in whole or in part) unless you have been specifically given permission to do so by the relevant owners.

7.3 You acknowledge that your use of such third party applications, data, content, or resources may be subject to separate terms between you and the relevant third party. In that case, the License Agreement does not affect your legal relationship with these third parties.

8. Using Android APIs

8.1 Google Data APIs

8.1.1 If you use any API to retrieve data from Google, you acknowledge that the data may be protected by intellectual property rights which are owned by Google or those parties that provide the data (or by other persons or companies on their behalf). Your use of any such API may be subject to additional Terms of Service. You may not modify, rent, lease, loan, sell, distribute or create derivative works based on this data (either in whole or in part) unless allowed by the relevant Terms of Service.

8.1.2 If you use any API to retrieve a user's data from Google, you acknowledge and agree that you shall retrieve data only with the user's explicit consent and only when, and for the limited purposes for which, the user has given you permission to do so. If you use the Android Recognition Service API, documented at the following URL: https://developer.android.com/reference/android/speech RecognitionService, as updated from time to time, you acknowledge that the use of the API is subject to the Data Processing Addendum for Products where Google is a Data Processor, which is located

1

☑ I have read and agree with the above terms and conditions

android-studio-ide-183.5692245-windows.exe

Opening android-studio-ide-183.5692245-windows.exe

You have chosen to open:

android-studio-ide-183.5692245-windows.exe

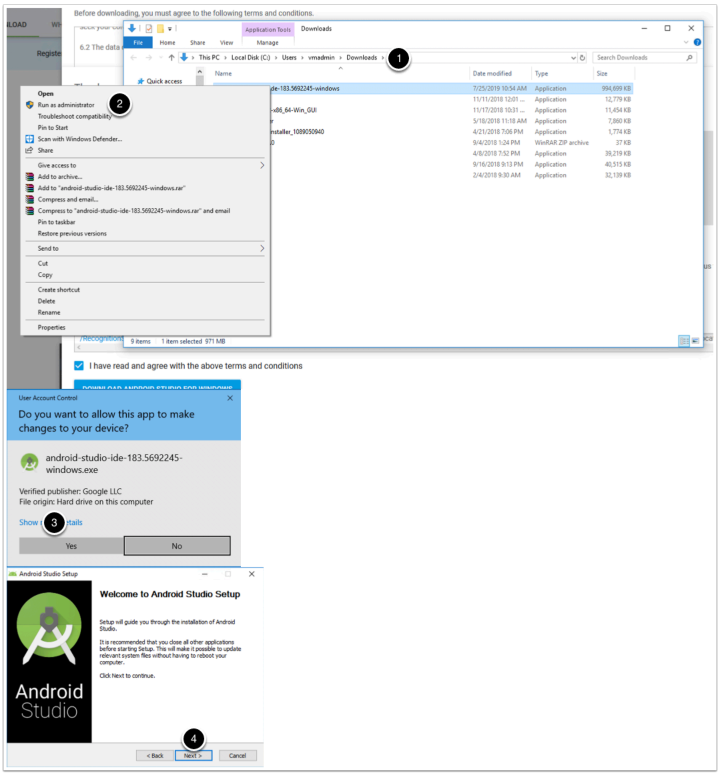
which is: Binary File (971 MB)

from: https://dl.google.com

Would you like to save this file?

Windows installation

1. go to your downloads folder
2. right click on your recently downloaded file and click on **run as and administrator**
3. click on **yes** to allow the installer to make changes to your machine
4. Click next on the welcome to android studio setup window



Before downloading, you must agree to the following terms and conditions.

Name	Date modified	Type	Size
de-183.5692245-windows	7/25/2019 10:54 AM	Application	994,699 KB
	11/11/2018 12:01 ...	Application	12,779 KB
-x86_64-Win_GUI	11/17/2018 10:31 ...	Application	11,454 KB
r	5/18/2018 11:18 AM	Application	7,860 KB
nstaller_1089050940	4/21/2018 7:06 PM	Application	1,774 KB
0	9/4/2018 1:24 PM	WinRAR ZIP archive	37 KB
	4/8/2018 7:52 PM	Application	39,219 KB
	9/16/2018 9:13 PM	Application	40,515 KB
	2/4/2018 9:30 AM	Application	32,139 KB

9 items 1 item selected 971 MB

☑ I have read and agree with the above terms and conditions

User Account Control

Do you want to allow this app to make changes to your device?

android-studio-ide-183.5692245-windows.exe

Verified publisher: Google LLC
File origin: Hard drive on this computer

Show more details

Android Studio Setup

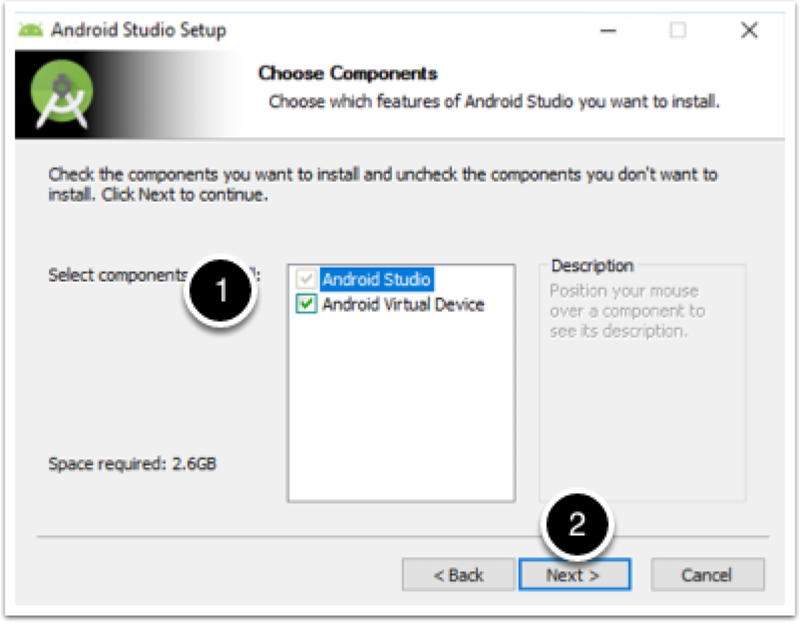
Welcome to Android Studio Setup

Setup will guide you through the installation of Android Studio.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Make sure both **Android studio** and **android virtual device** are selected and click **next**



Android Studio Setup

Choose Components

Choose which features of Android Studio you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

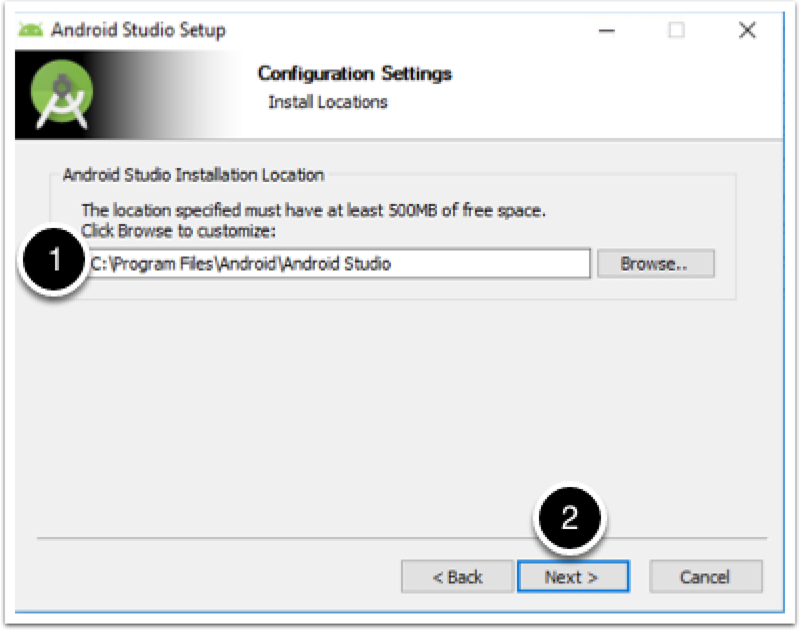
Select components to install:

☑ Android Studio
☑ Android Virtual Device

Description
Position your mouse over a component to see its description.

Space required: 2.6GB

Select your installation location and click **next**



Android Studio Setup

Configuration Settings

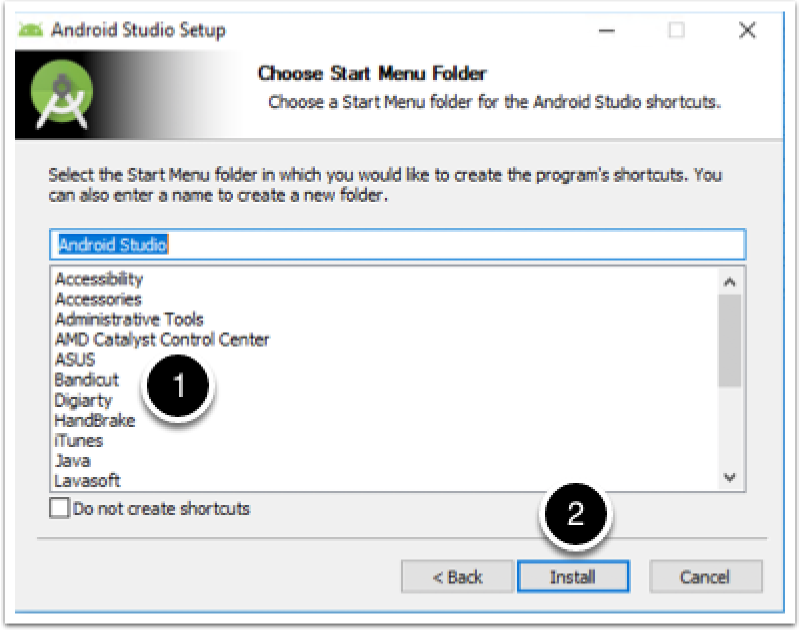
Install Locations

Android Studio Installation Location

The location specified must have at least 500MB of free space.
Click Browse to customize:

C:\Program Files\Android\Android Studio

choose your start menu shortcut configuration and click **install**



Android Studio Setup

Choose Start Menu Folder

Choose a Start Menu folder for the Android Studio shortcuts.

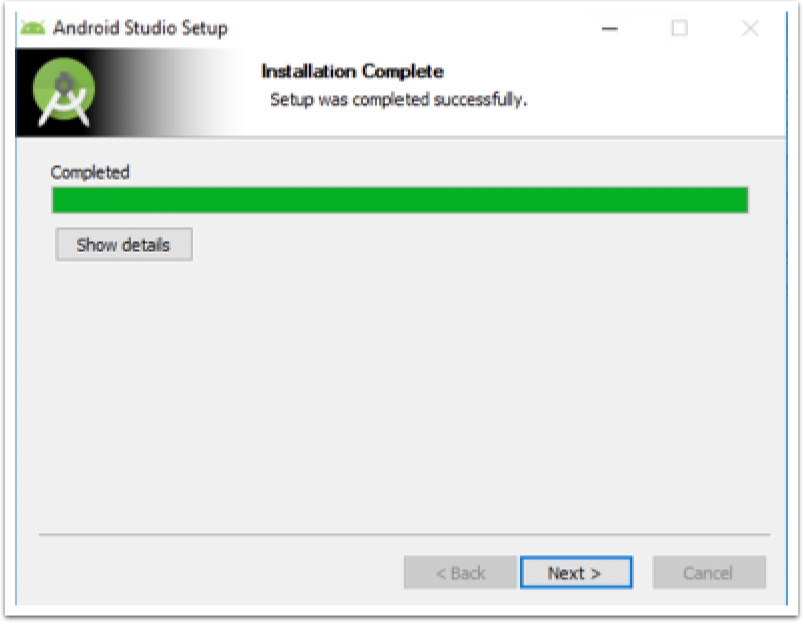
Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Android Studio

Accessibility
Accessories
Administrative Tools
AMD Catalyst Control Center
ASUS
Bandicut
Digiarty
HandBrake
iTunes
Java
Lavasoft

□ Do not create shortcuts

on the installation complete window click **next**



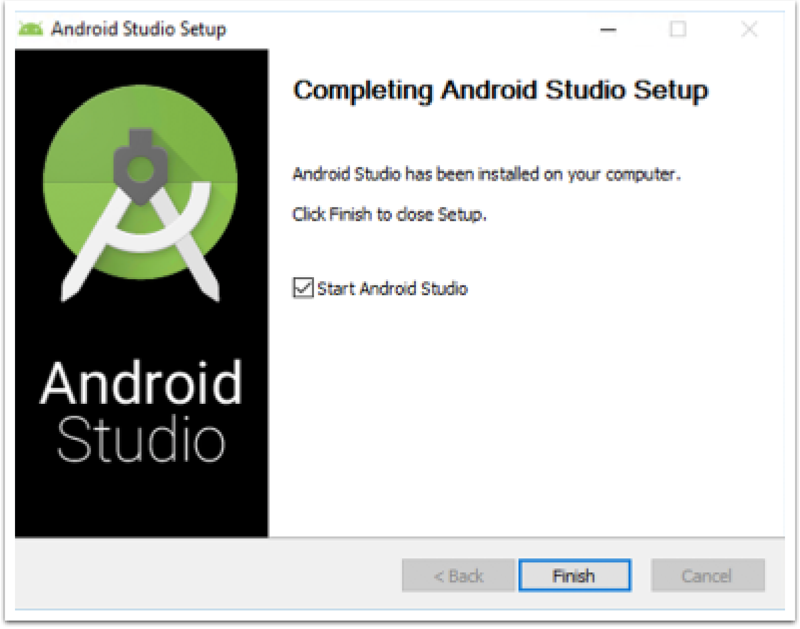
Android Studio Setup

Installation Complete

Setup was completed successfully.

Completed

In the completing Android Studio Setup window check the **Start Android Studio** checkbox and click **finish**



Android Studio Setup

Completing Android Studio Setup

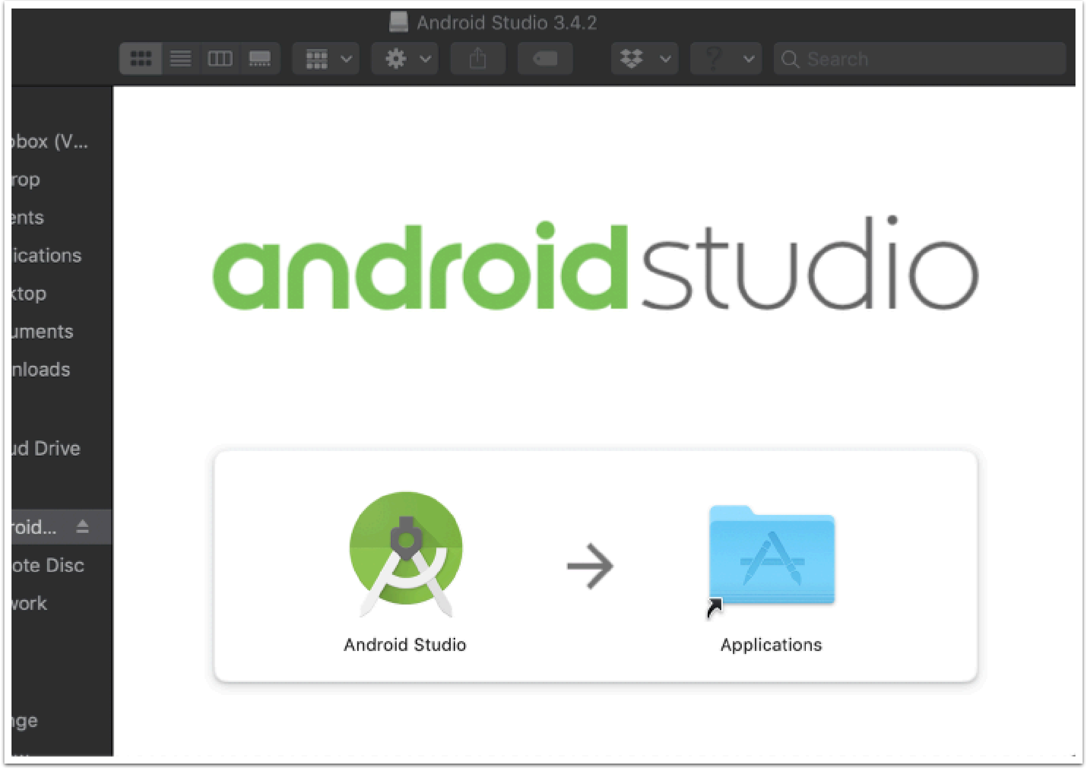
Android Studio has been installed on your computer.

Click Finish to close Setup.

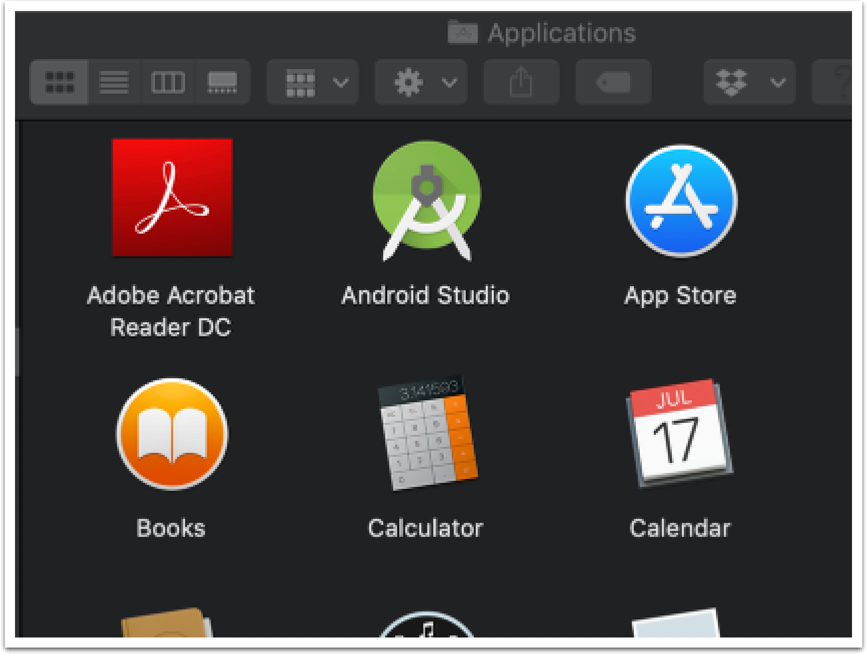
☑ Start Android Studio

Mac os installation

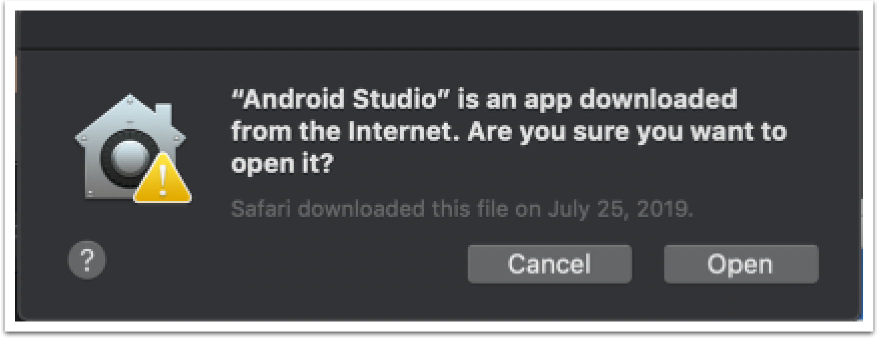
mount and open your downloaded dmg image. Drag the **Android studio** icon into the **Applications** folder.



From your applications folder double click your **Android Studio** icon



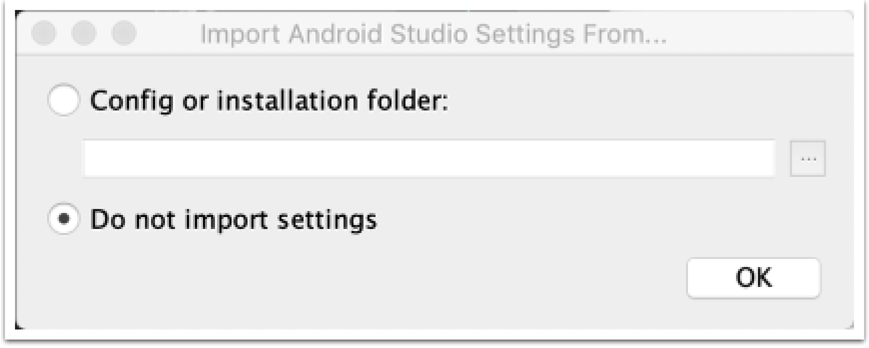
Click on **Open** if you get a security prompt



"Android Studio" is an app downloaded from the Internet. Are you sure you want to open it?

Safari downloaded this file on July 25, 2019.

in the Import android Studio settings From.. window select **Do not import settings** and click **ok**



Import Android Studio Settings From...

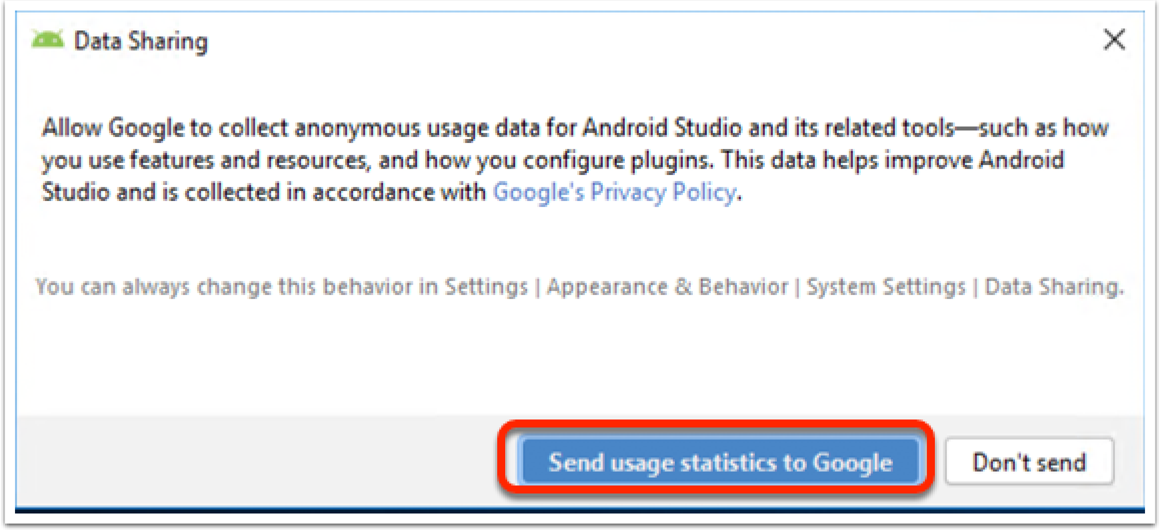
○ Config or installation folder:

● Do not import settings

on the Android Setup Wizard, in the Welcome window click **Next.** From this point on you can follow the initial configuration steps, plese ignore anything regarding the HAXM plugin as this has been already installed for you in the initial installation process.

Initial configuration

in the Data Sharing window click on **Send usage statistics to Google**

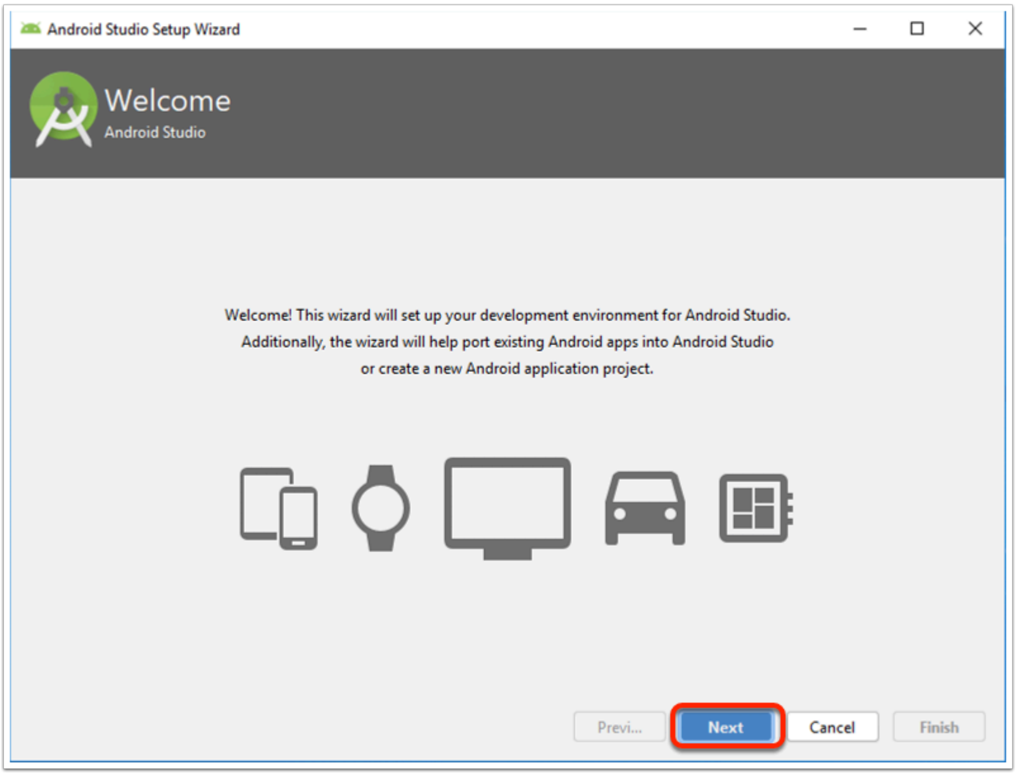


Data Sharing

Allow Google to collect anonymous usage data for Android Studio and its related tools—such as how you use features and resources, and how you configure plugins. This data helps improve Android Studio and is collected in accordance with Google's Privacy Policy.

You can always change this behavior in Settings | Appearance & Behavior | System Settings | Data Sharing.

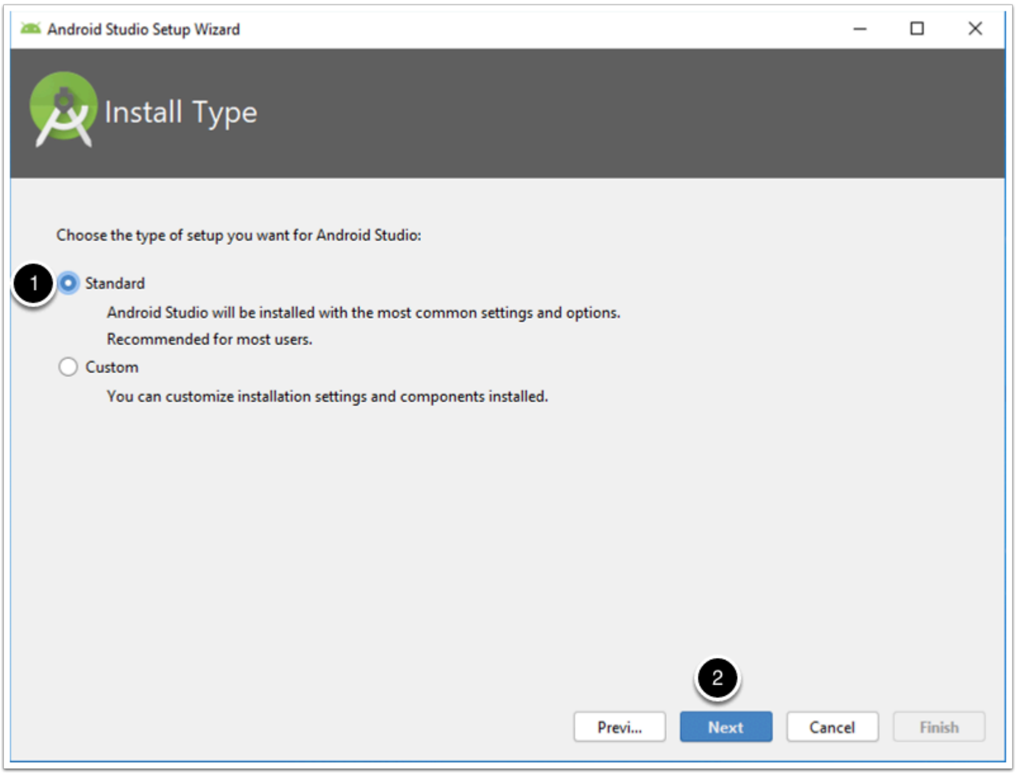
In the android Studio setup wizard, in the Welcome window click **Next**



Welcome! This wizard will set up your development environment for Android Studio.
Additionally, the wizard will help port existing Android apps into Android Studio
or create a new Android application project.

In the Android Studio Setup Wizard in the install type window

1. Make sure **Standard** setup radio button is selected
2. Click **Next**



Choose the type of setup you want for Android Studio:

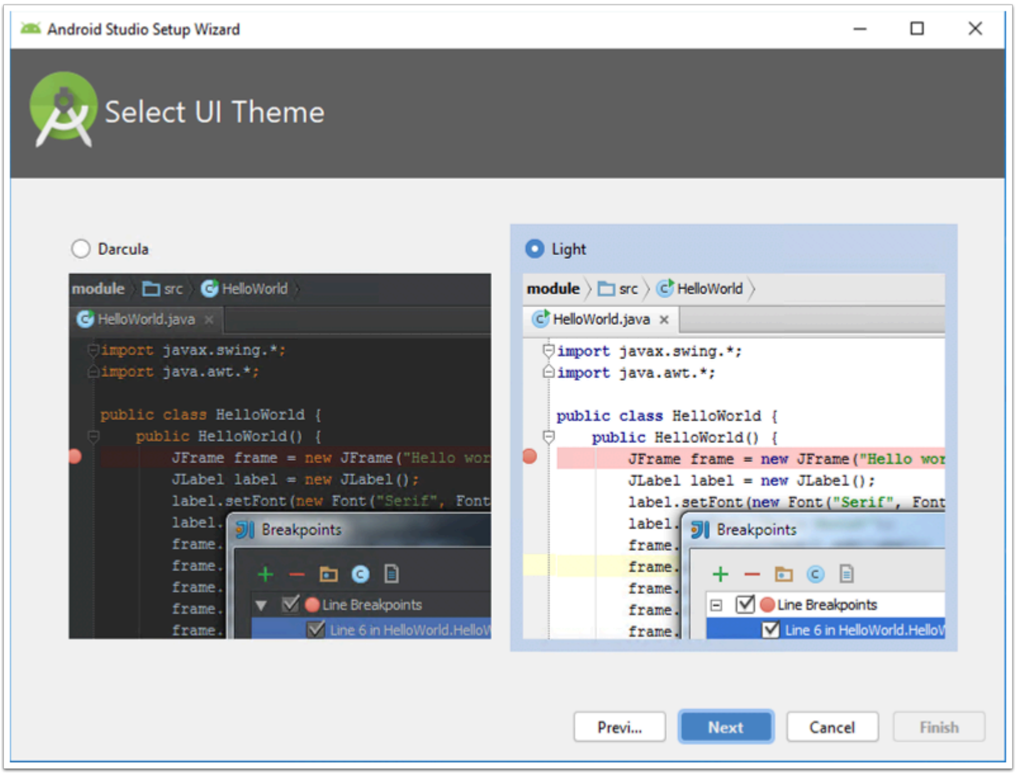
1 ● Standard

Android Studio will be installed with the most common settings and options.
Recommended for most users.

○ Custom

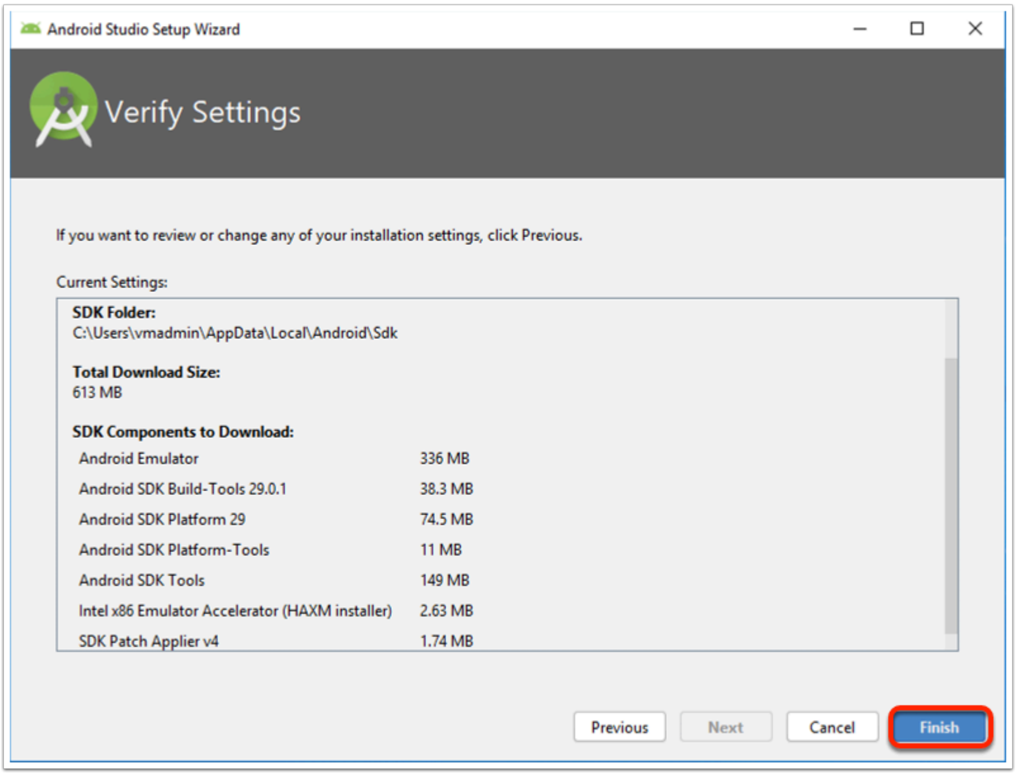
You can customize installation settings and components installed.

Choose your preffered UI theme and click **Next**



```
import javax.swing.*;
import java.awt.*;

public class HelloWorld {
    public HelloWorld() {
        JFrame frame = new JFrame("Hello wor
        JLabel label = new JLabel();
        label.setFont(new Font("Serif", Font
        label.
        frame.
        frame.
        frame.
        frame.
        frame.
```

On the verify Settings window click **Finish**



If you want to review or change any of your installation settings, click Previous.

Current Settings:

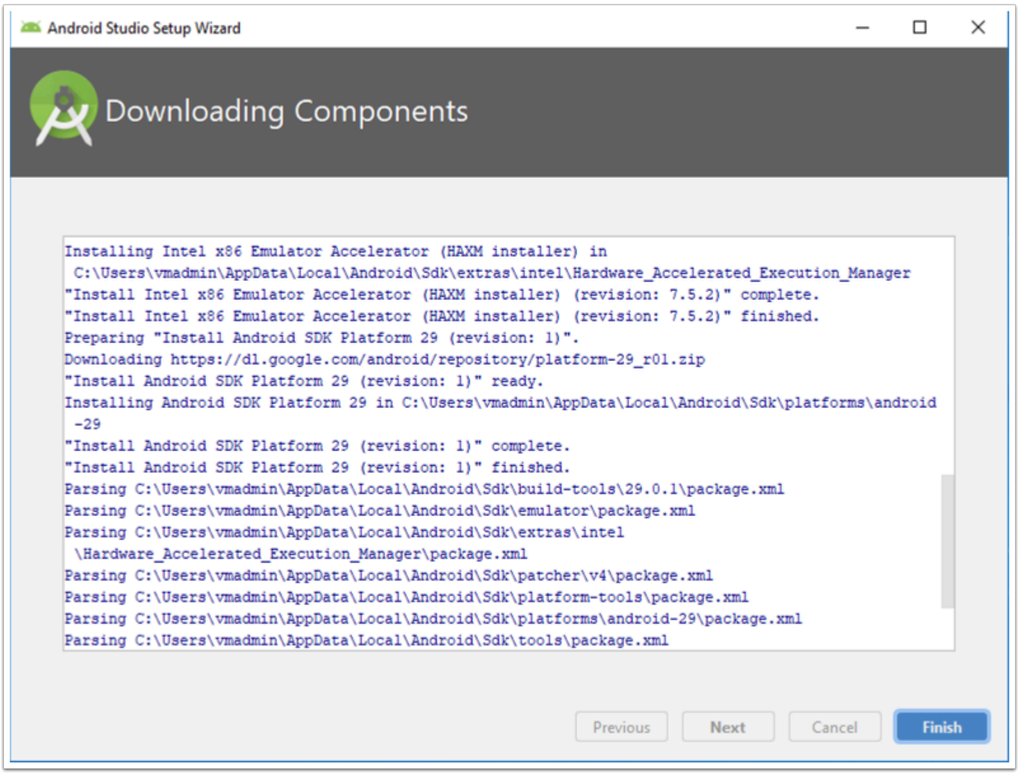
SDK Folder:
C:\Users\vmadmin\AppData\Local\Android\Sdk

Total Download Size:
613 MB

SDK Components to Download:

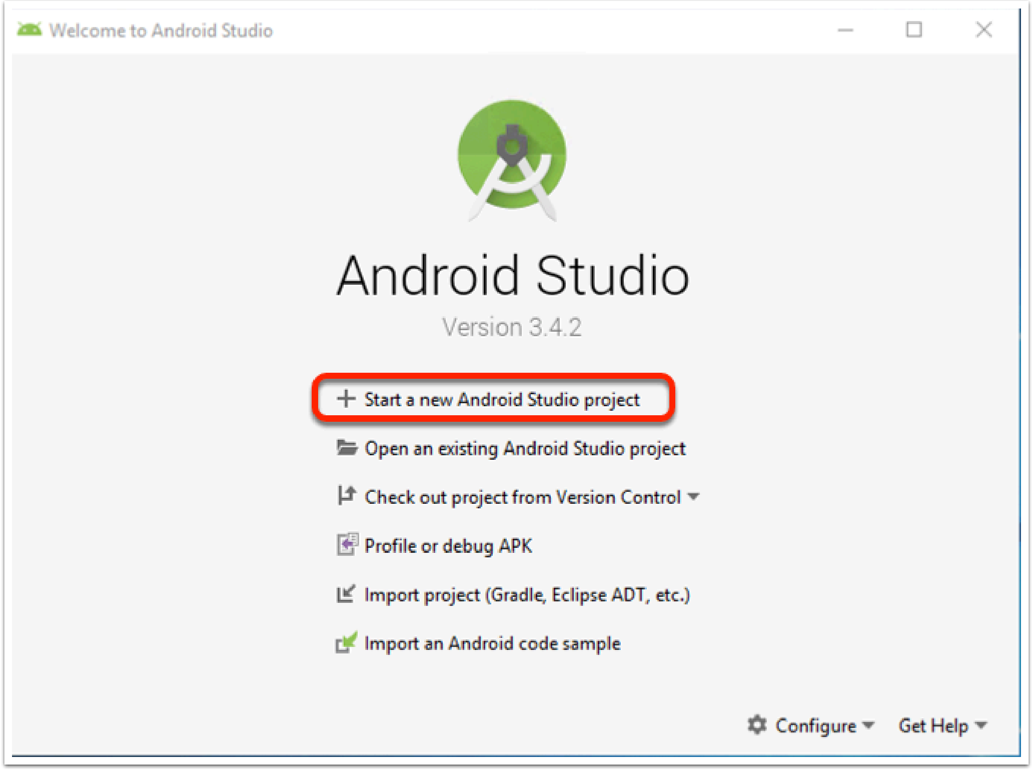
Android Emulator	336 MB
Android SDK Build-Tools 29.0.1	38.3 MB
Android SDK Platform 29	74.5 MB
Android SDK Platform-Tools	11 MB
Android SDK Tools	149 MB
Intel x86 Emulator Accelerator (HAXM installer)	2.63 MB
SDK Patch Applier v4	1.74 MB

In the Downloading Components window click **Finish**

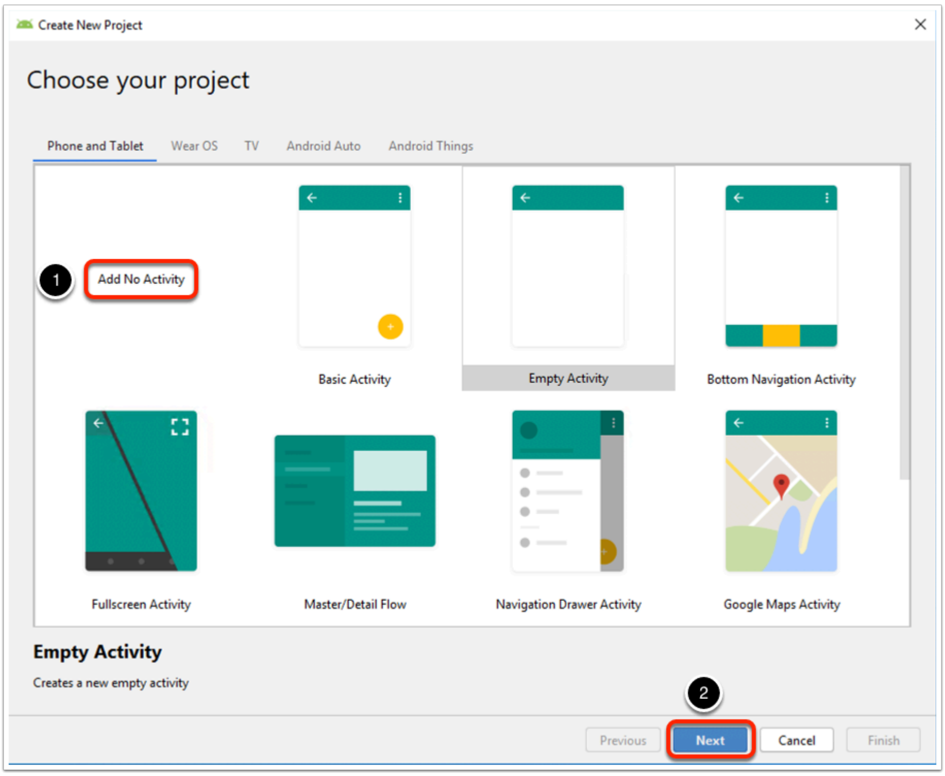


```
Installing Intel x86 Emulator Accelerator (HAXM installer) in
 C:\Users\vmadmin\AppData\Local\Android\Sdk\extras\intel\Hardware_Accelerated_Execution_Manager
"Install Intel x86 Emulator Accelerator (HAXM installer) (revision: 7.5.2)" complete.
"Install Intel x86 Emulator Accelerator (HAXM installer) (revision: 7.5.2)" finished.
Preparing "Install Android SDK Platform 29 (revision: 1)".
Downloading https://dl.google.com/android/repository/platform-29_r01.zip
"Install Android SDK Platform 29 (revision: 1)" ready.
Installing Android SDK Platform 29 in C:\Users\vmadmin\AppData\Local\Android\Sdk\platforms\android
 -29
"Install Android SDK Platform 29 (revision: 1)" complete.
"Install Android SDK Platform 29 (revision: 1)" finished.
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\build-tools\29.0.1\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\emulator\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\extras\intel
 \Hardware_Accelerated_Execution_Manager\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\patcher\v4\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\platform-tools\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\platforms\android-29\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\tools\package.xml
```

In the Welcome to android studio window click on **start a new android project**


Welcome to Android Studio
Android Studio
Version 3.4.2
+ Start a new Android Studio project
Open an existing Android Studio project
Check out project from Version Control
Profile or debug APK
Import project (Gradle, Eclipse ADT, etc.)
Import an Android code sample
Configure
Get Help

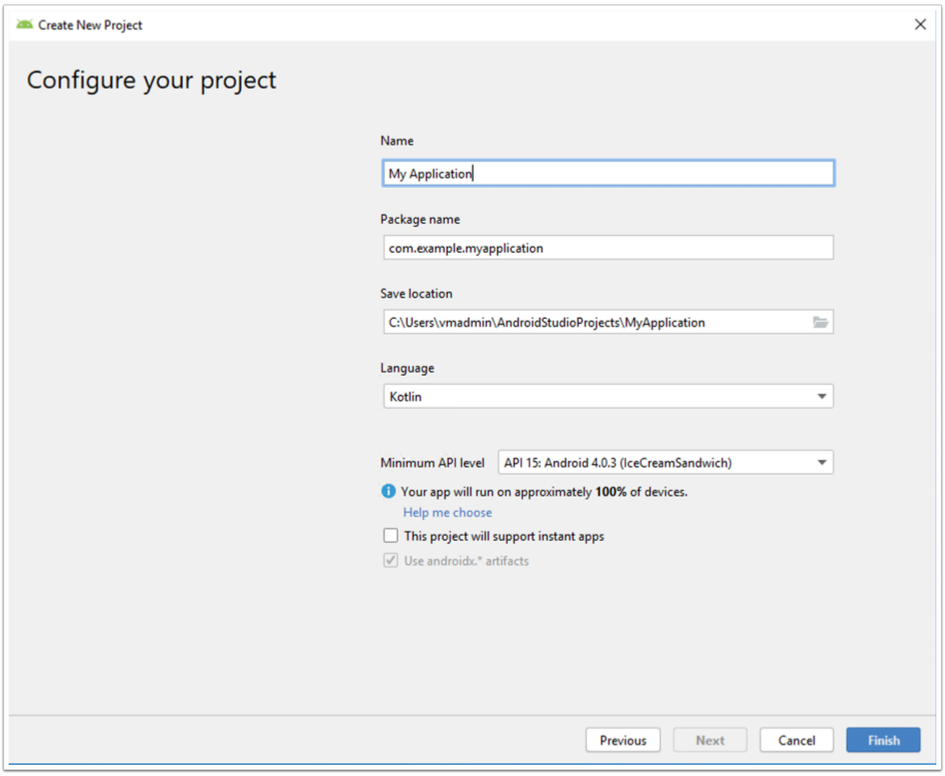
In the choose your project window, choose **add no activity** and click **Next**



Empty Activity

Creates a new empty activity

In the configure your project window leave the default settings and click **Finish**



Name: My Application

Package name: com.example.myapplication

Save location: C:\Users\vmadmin\AndroidStudioProjects\MyApplication

Language: Kotlin

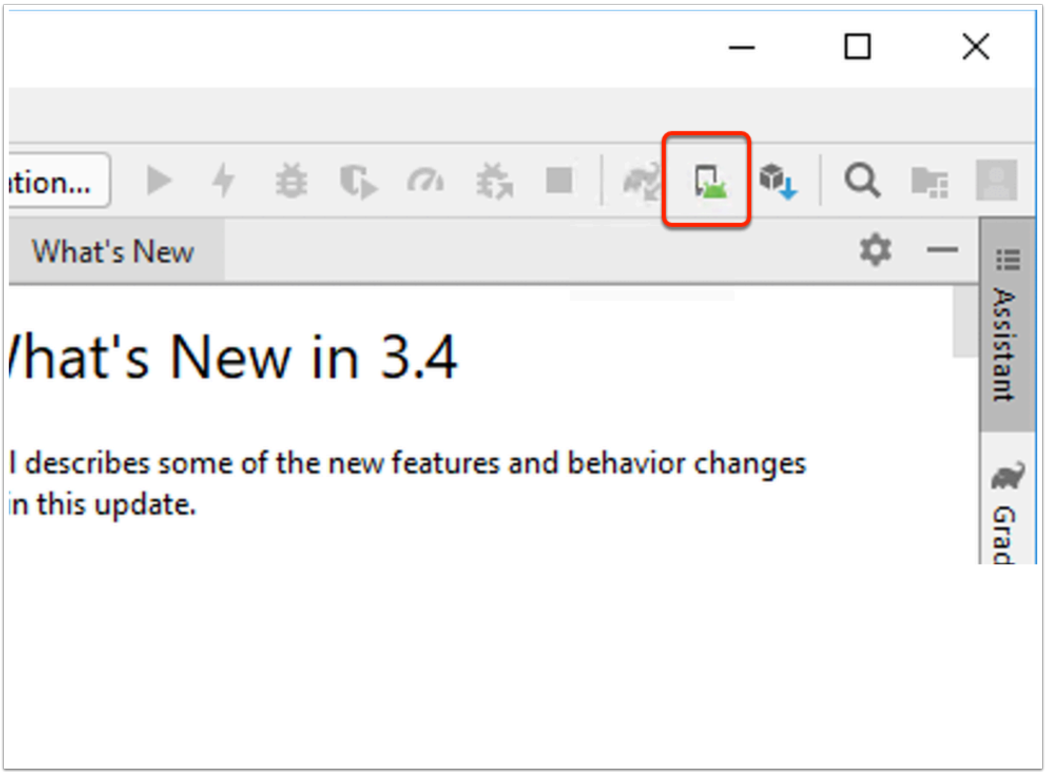
Minimum API level: API 15: Android 4.0.3 (IceCreamSandwich)

Your app will run on approximately **100%** of devices.

☐ This project will support instant apps

☑ Use androidx.* artifacts

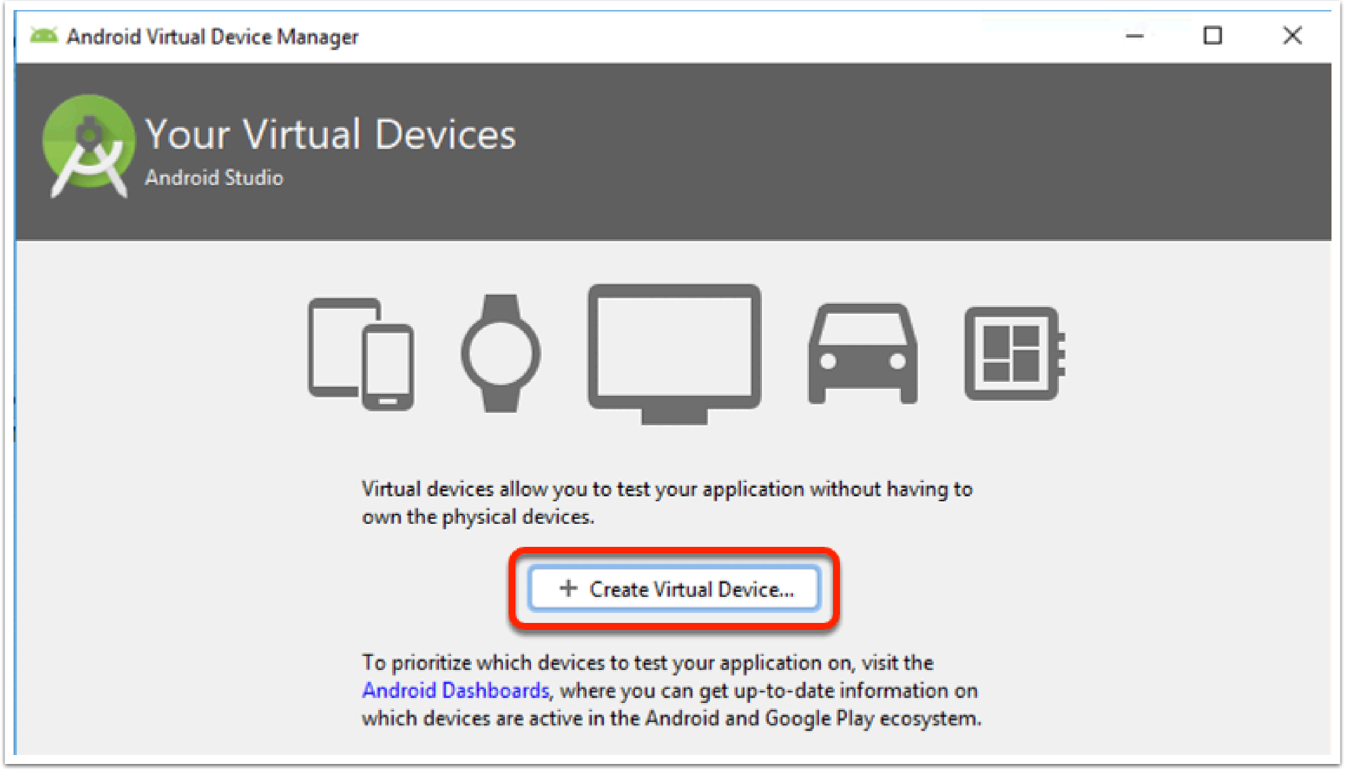
Click on the AVD Manager icon on the toolbar



/hat's New in 3.4

l describes some of the new features and behavior changes in this update.

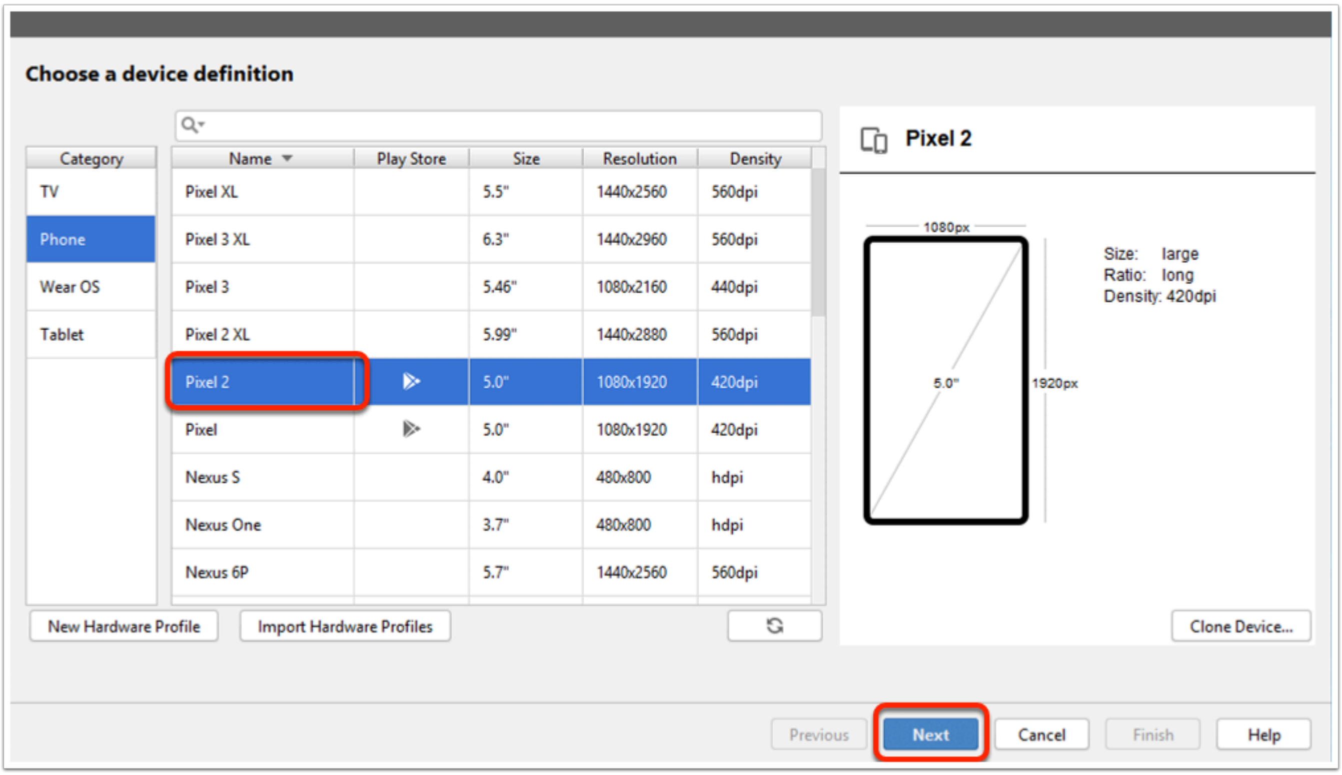
Click on **Create Virtual Device**



Virtual devices allow you to test your application without having to own the physical devices.

To prioritize which devices to test your application on, visit the Android Dashboards, where you can get up-to-date information on which devices are active in the Android and Google Play ecosystem.

Select the **Pixel 2** Image marked with Play Store access and click **Next**



Choose a device definition

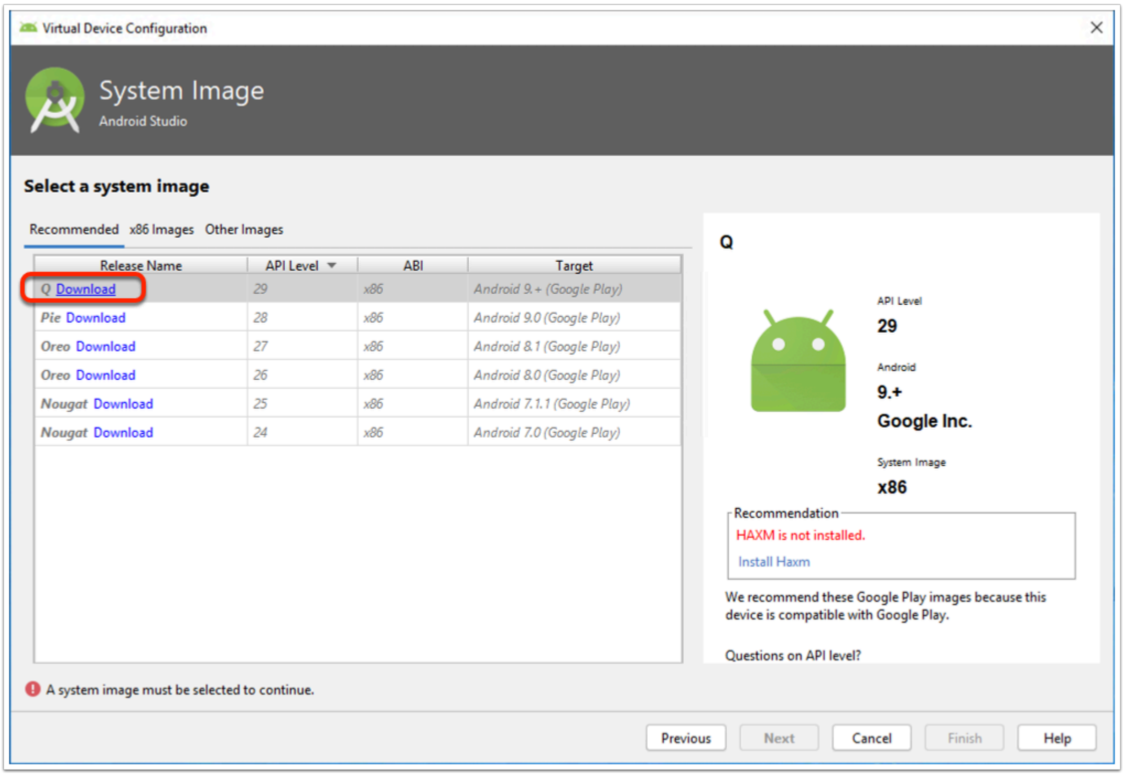
Category
TV
Phone
Wear OS
Tablet

Name	Play Store	Size	Resolution	Density
Pixel XL		5.5"	1440x2560	560dpi
Pixel 3 XL		6.3"	1440x2960	560dpi
Pixel 3		5.46"	1080x2160	440dpi
Pixel 2 XL		5.99"	1440x2880	560dpi
Pixel 2	▶	5.0"	1080x1920	420dpi
Pixel	▶	5.0"	1080x1920	420dpi
Nexus S		4.0"	480x800	hdpi
Nexus One		3.7"	480x800	hdpi
Nexus 6P		5.7"	1440x2560	560dpi

Pixel 2

Size: large
Ratio: long
Density: 420dpi

in the release name column click Download next to **Q**



Virtual Device Configuration

System Image
Android Studio

Select a system image

Release Name	API Level	ABI	Target
Q Download	29	x86	Android 9.+ (Google Play)
Pie Download	28	x86	Android 9.0 (Google Play)
Oreo Download	27	x86	Android 8.1 (Google Play)
Oreo Download	26	x86	Android 8.0 (Google Play)
Nougat Download	25	x86	Android 7.1.1 (Google Play)
Nougat Download	24	x86	Android 7.0 (Google Play)

Q

API Level
29

Android
9.+

Google Inc.

System Image
x86

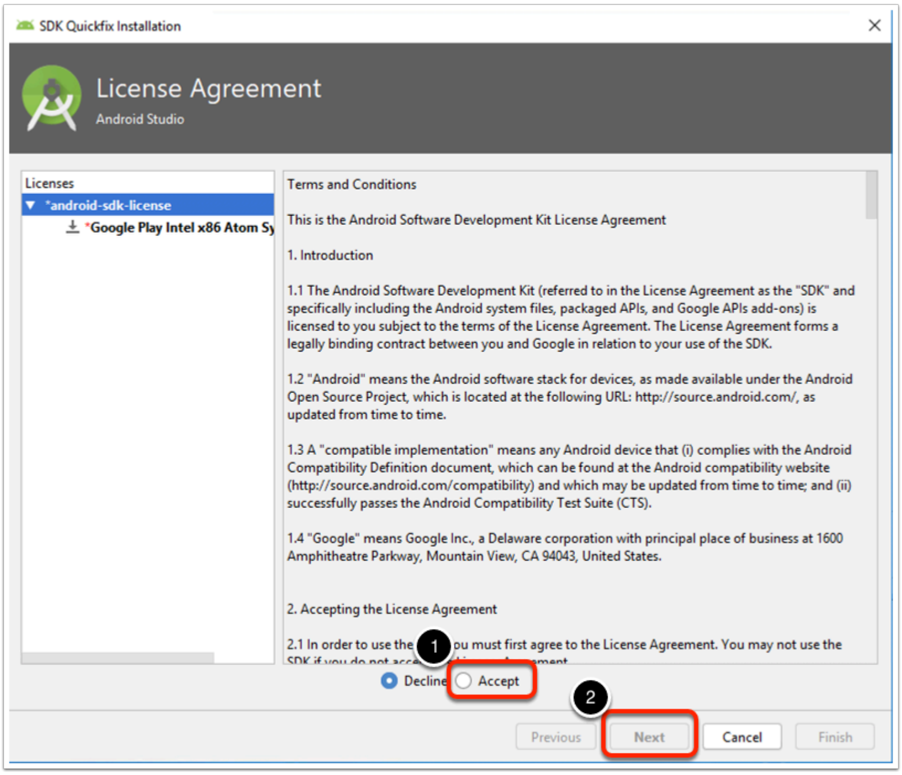
Recommendation
HAXM is not installed.
Install Haxm

We recommend these Google Play images because this device is compatible with Google Play.

Questions on API level?

A system image must be selected to continue.

In the license agreement window select the radio button next to **I agree** and click **Next**



Terms and Conditions

This is the Android Software Development Kit License Agreement

1. Introduction

1.1 The Android Software Development Kit (referred to in the License Agreement as the "SDK" and specifically including the Android system files, packaged APIs, and Google APIs add-ons) is licensed to you subject to the terms of the License Agreement. The License Agreement forms a legally binding contract between you and Google in relation to your use of the SDK.

1.2 "Android" means the Android software stack for devices, as made available under the Android Open Source Project, which is located at the following URL: http://source.android.com/, as updated from time to time.

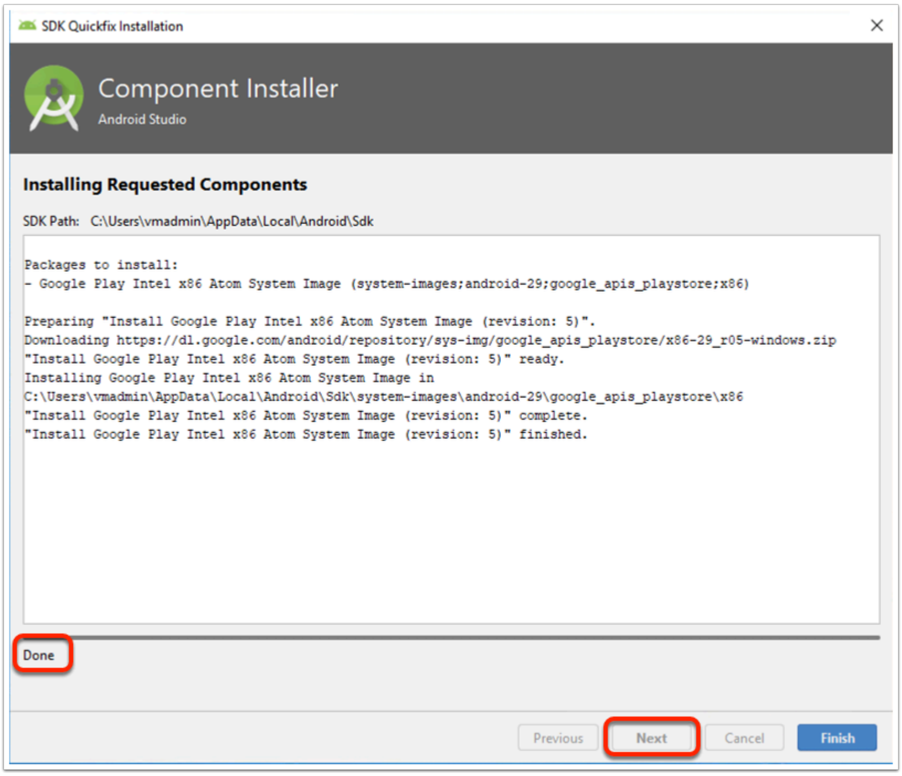
1.3 A "compatible implementation" means any Android device that (i) complies with the Android Compatibility Definition document, which can be found at the Android compatibility website (http://source.android.com/compatibility) and which may be updated from time to time; and (ii) successfully passes the Android Compatibility Test Suite (CTS).

1.4 "Google" means Google Inc., a Delaware corporation with principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

2. Accepting the License Agreement

2.1 In order to use the ou must first agree to the License Agreement. You may not use the SDK if you do not acce

In the Installing Requested Components window Click **Next** when the progress bar shows DONE

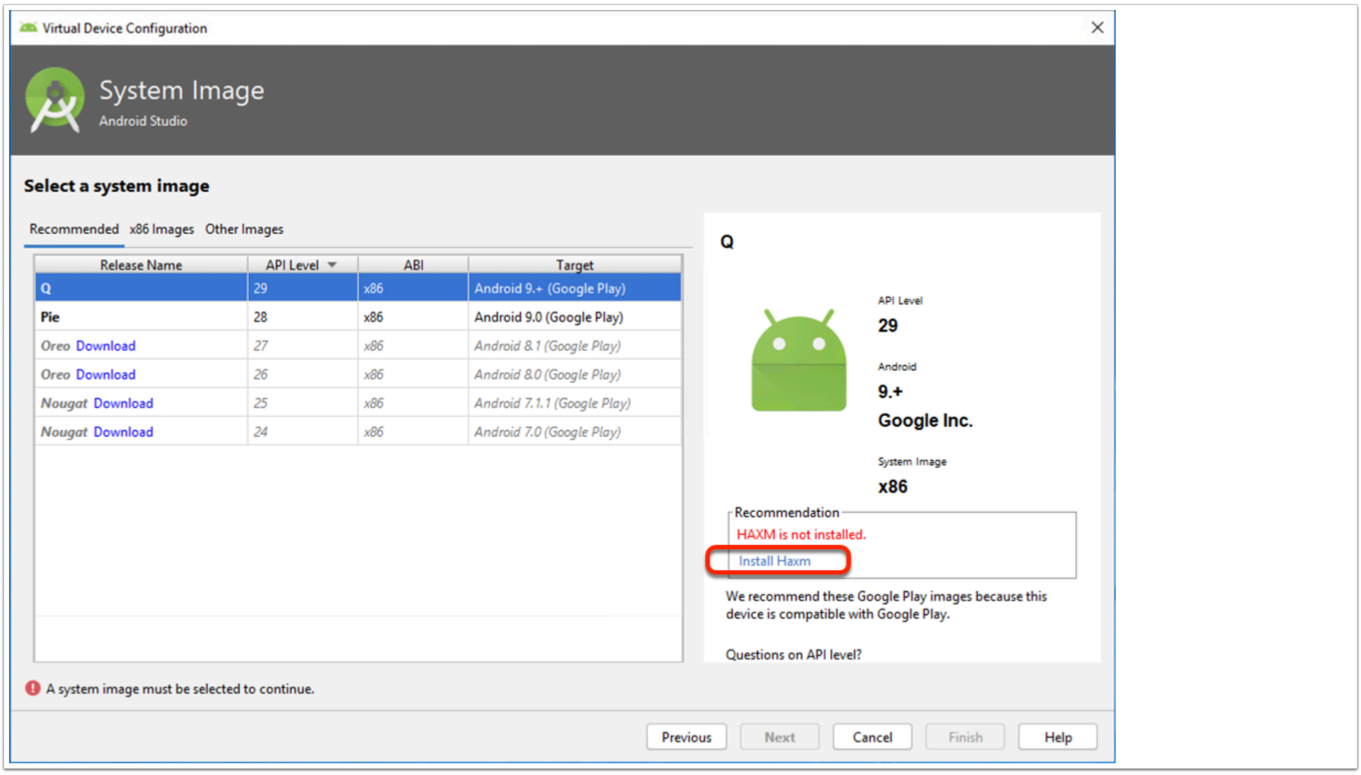


Installing Requested Components

SDK Path: C:\Users\vmadmin\AppData\Local\Android\Sdk

```
Packages to install:
- Google Play Intel x86 Atom System Image (system-images;android-29;google_apis_playstore;x86)

Preparing "Install Google Play Intel x86 Atom System Image (revision: 5)".
Downloading https://dl.google.com/android/repository/sys-img/google_apis_playstore/x86-29_r05-windows.zip
"Install Google Play Intel x86 Atom System Image (revision: 5)" ready.
Installing Google Play Intel x86 Atom System Image in
C:\Users\vmadmin\AppData\Local\Android\Sdk\system-images\android-29\google_apis_playstore\x86
"Install Google Play Intel x86 Atom System Image (revision: 5)" complete.
"Install Google Play Intel x86 Atom System Image (revision: 5)" finished.
```

In the Select a system image window click on **Install Haxm**



Virtual Device Configuration
System Image
Android Studio

Select a system image

Recommended x86 Images Other Images

Release Name	API Level	ABI	Target
Q	29	x86	Android 9.+ (Google Play)
Pie	28	x86	Android 9.0 (Google Play)
Oreo Download	27	x86	Android 8.1 (Google Play)
Oreo Download	26	x86	Android 8.0 (Google Play)
Nougat Download	25	x86	Android 7.1.1 (Google Play)
Nougat Download	24	x86	Android 7.0 (Google Play)

Q

API Level
29

Android
9.+
Google Inc.

System Image
x86

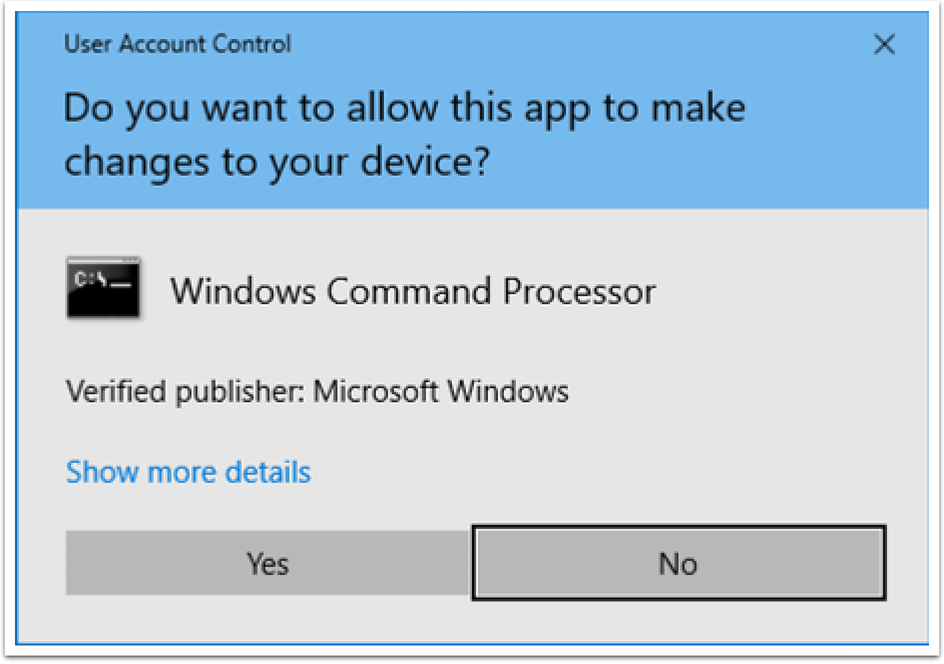
Recommendation
HAXM is not installed.
Install Haxm

We recommend these Google Play images because this device is compatible with Google Play.

Questions on API level?

A system image must be selected to continue.

Click **Yes** to allow windows command processor to make changes to your device

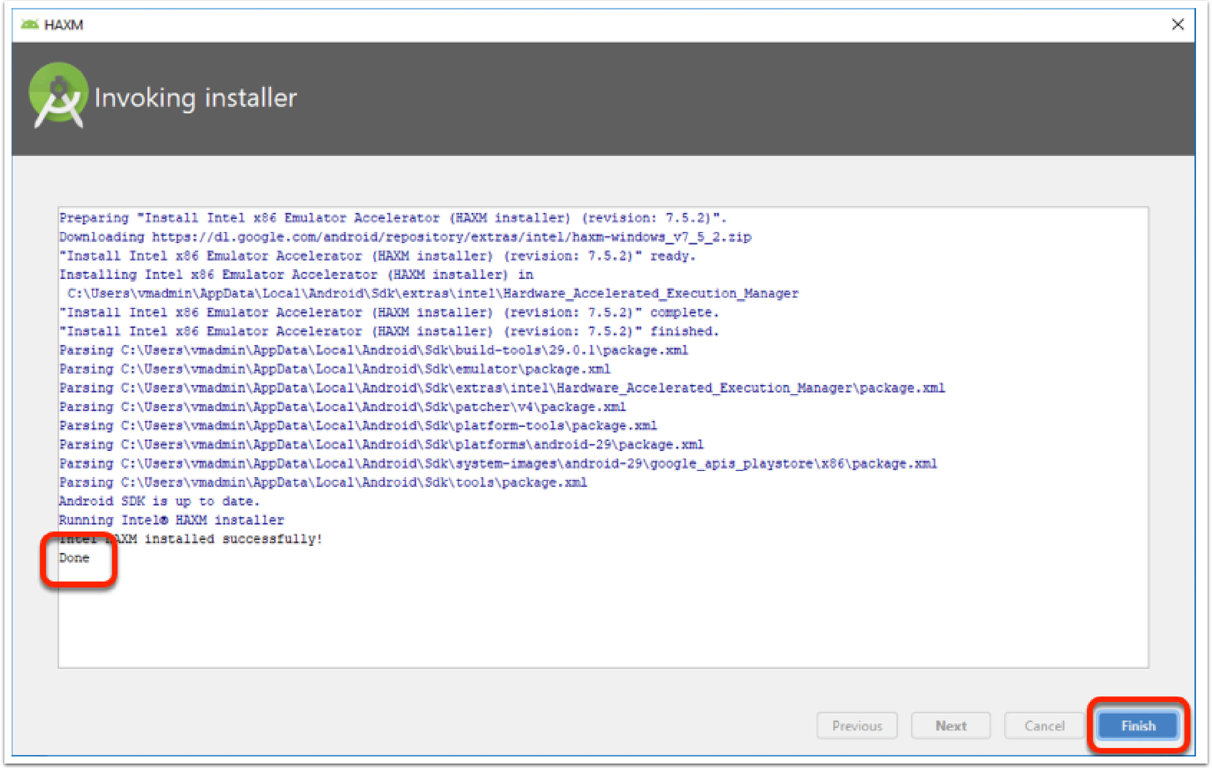


User Account Control

Do you want to allow this app to make changes to your device?

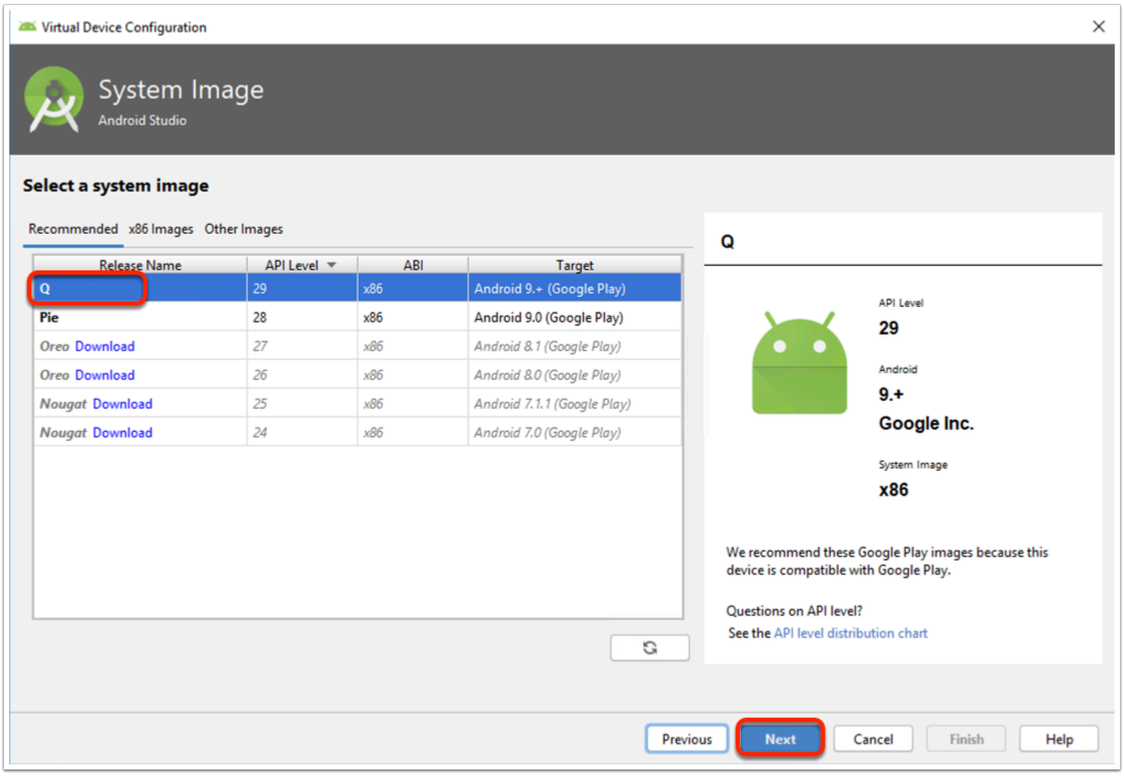
Windows Command Processor

Verified publisher: Microsoft Windows



```
Preparing "Install Intel x86 Emulator Accelerator (HAXM installer) (revision: 7.5.2)".
Downloading https://dl.google.com/android/repository/extras/intel/haxm-windows_v7_5_2.zip
"Install Intel x86 Emulator Accelerator (HAXM installer) (revision: 7.5.2)" ready.
Installing Intel x86 Emulator Accelerator (HAXM installer) in
 C:\Users\vmadmin\AppData\Local\Android\Sdk\extras\intel\Hardware_Accelerated_Execution_Manager
"Install Intel x86 Emulator Accelerator (HAXM installer) (revision: 7.5.2)" complete.
"Install Intel x86 Emulator Accelerator (HAXM installer) (revision: 7.5.2)" finished.
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\build-tools\29.0.1\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\emulator\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\extras\intel\Hardware_Accelerated_Execution_Manager\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\patcher\v4\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\platform-tools\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\platforms\android-29\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\system-images\android-29\google_apis_playstore\x86\package.xml
Parsing C:\Users\vmadmin\AppData\Local\Android\Sdk\tools\package.xml
Android SDK is up to date.
Running Intel® HAXM installer
Intel HAXM installed successfully!
Done
```

Back in the Select a system image window Select **Q** and click **Next**



Select a system image

Release Name	API Level	ABI	Target
Q	29	x86	Android 9.+ (Google Play)
Pie	28	x86	Android 9.0 (Google Play)
Oreo Download	27	x86	Android 8.1 (Google Play)
Oreo Download	26	x86	Android 8.0 (Google Play)
Nougat Download	25	x86	Android 7.1.1 (Google Play)
Nougat Download	24	x86	Android 7.0 (Google Play)

Q

API Level
29

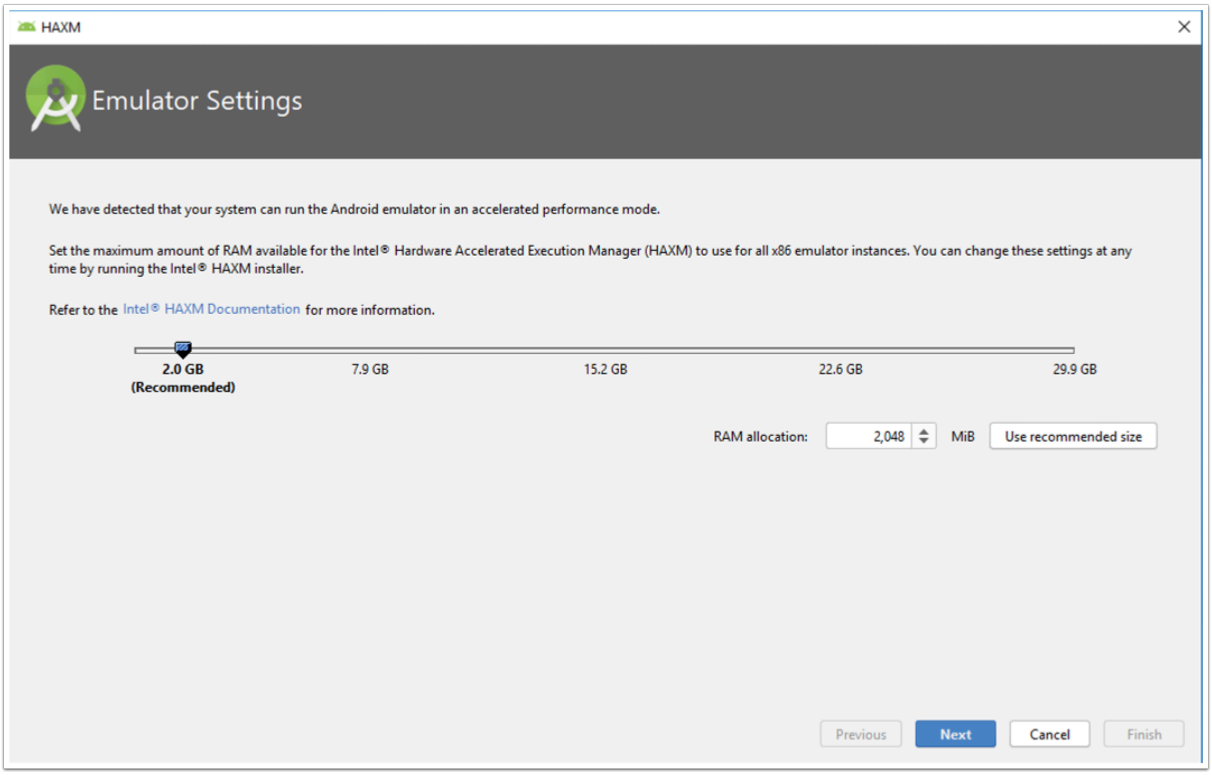
Android
9.+
Google Inc.

System Image
x86

We recommend these Google Play images because this device is compatible with Google Play.

Questions on API level?
See the API level distribution chart

In the emulator settings window, Use the recommended memory settings and click **Next**



HAXM

Emulator Settings

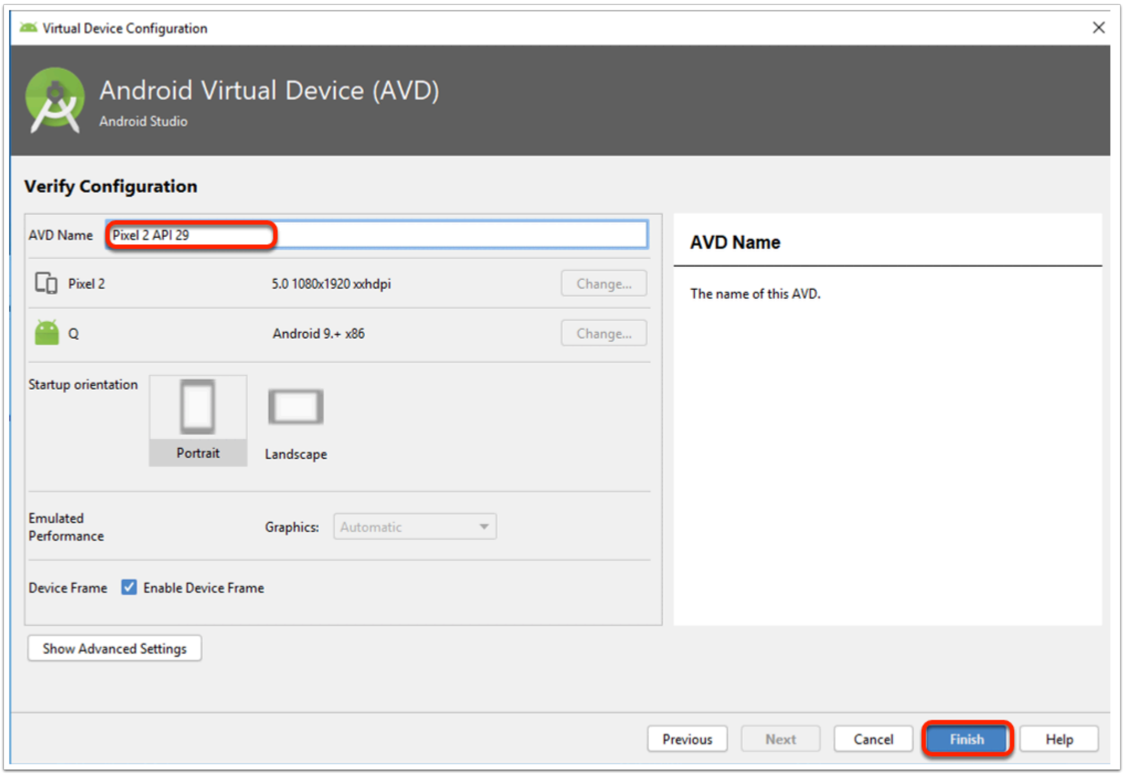
We have detected that your system can run the Android emulator in an accelerated performance mode.

Set the maximum amount of RAM available for the Intel® Hardware Accelerated Execution Manager (HAXM) to use for all x86 emulator instances. You can change these settings at any time by running the Intel® HAXM installer.

Refer to the Intel® HAXM Documentation for more information.

RAM allocation: 2,048 MiB

Give a name to your virtual device and click **Finish**



Virtual Device Configuration

Android Virtual Device (AVD)

Android Studio

Verify Configuration

AVD Name: Pixel 2 API 29

Pixel 2 — 5.0 1080x1920 xxhdpi

Q — Android 9.+ x86

Startup orientation: Portrait

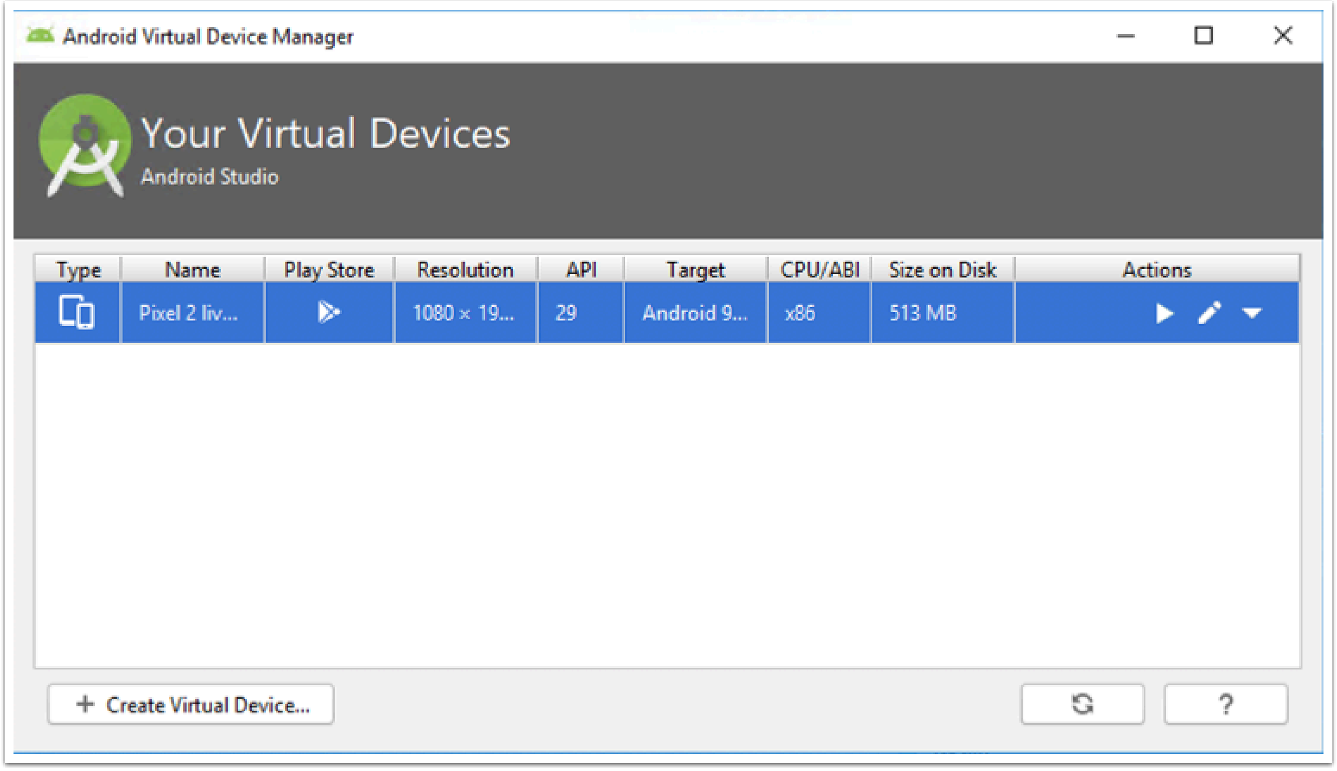
Emulated Performance — Graphics: Automatic

Device Frame: ☑ Enable Device Frame

AVD Name

The name of this AVD.

In your Android virtual device Manager window, in the actions column click on the "**Play**" icon to start the emulator

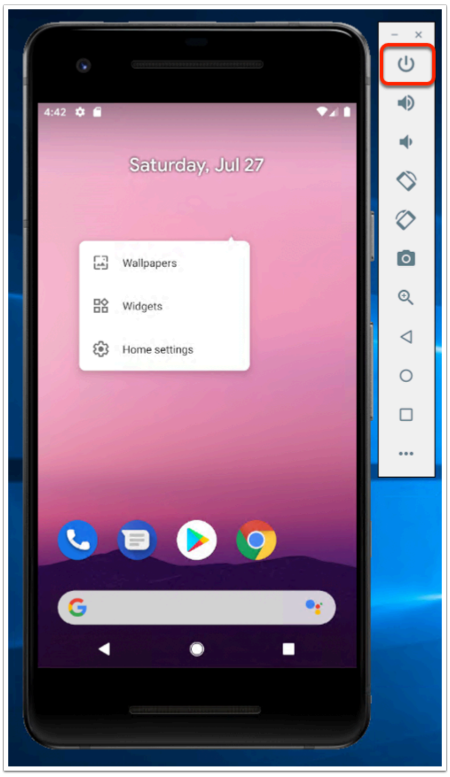

Android Virtual Device Manager

Your Virtual Devices

Android Studio

Type	Name	Play Store	Resolution	API	Target	CPU/ABI	Size on Disk	Actions
	Pixel 2 liv...	▷	1080 × 19...	29	Android 9...	x86	513 MB	▶ ✎ ▾

Your emulator is ready to use, if you need to restart your device you can hold the power icon to see the power options.



Day 2

Citrix Integration with VMware Identity Manager

In this lab you will install and configure the Citrix Integration broker to communicate with the existing on premise Citrix Farm and the VMware Identity Manager SaaS instance

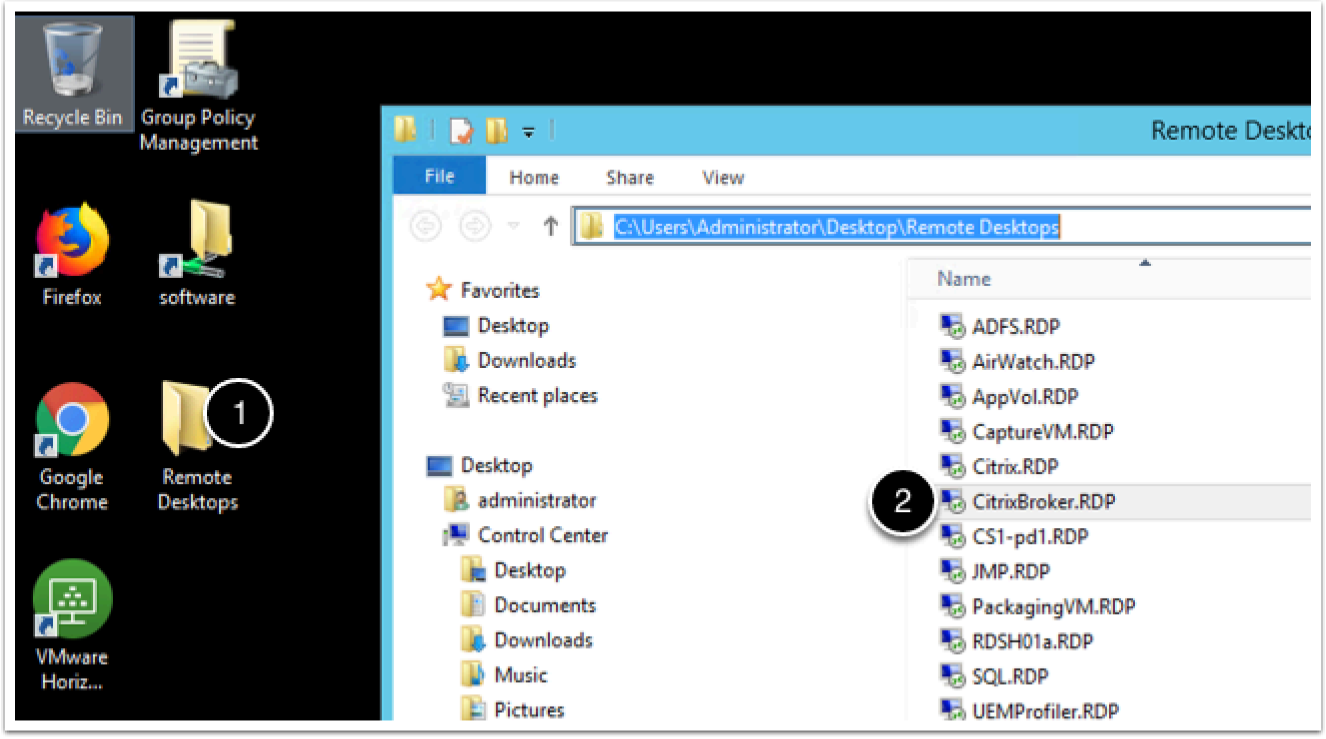
Section 1 - Integration broker installation

Part 1a - Preparing the integration broker virtual machine

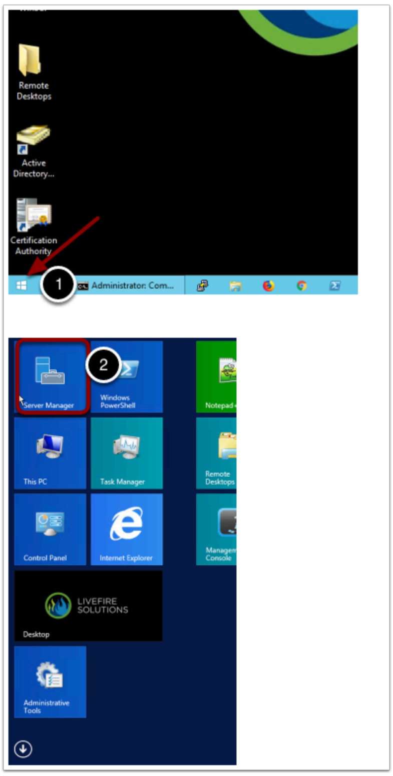
Part 1a has been completed beforehand for your convenience, this material is here for future reference. Please move on to part 1b.

In this part you will install the roles and software requirements for the installation of the Citrix integration broker.

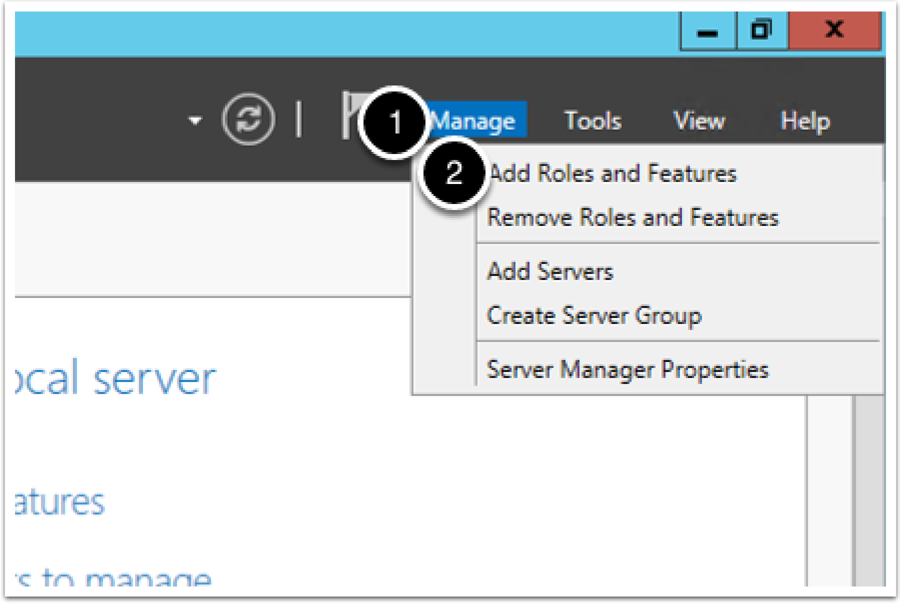
1. Log on to your **Controlcenter** virtual machine.
2. On your desktop, go to the **Remote Desktop** folder
3. Open **citrixbroker.rdp**
4. Log on with **username: euc-livefire\administrator** and **password: VMware1!**



5. In the **Citrix broker** machine go to **Start > Server Manager**



6. In **Server Manager**, select **Manage > Add Roles and Features**

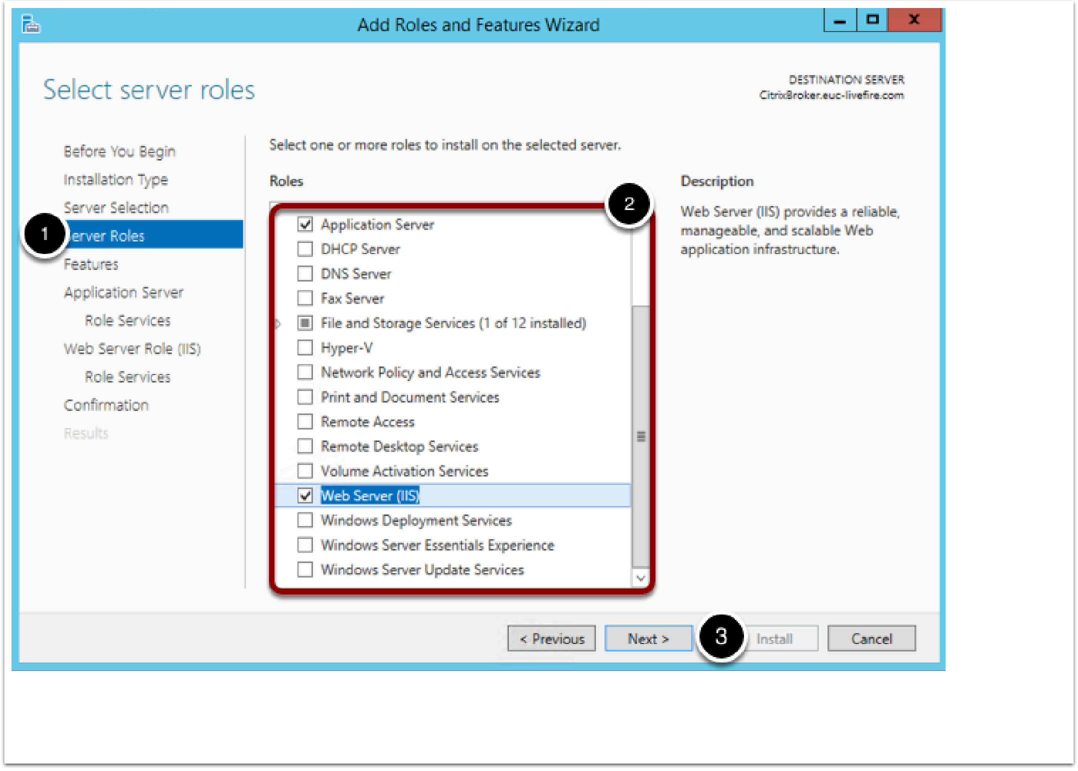


7. Click **Next** until you get to the **Server Roles** screen

8. Select the following roles:

- **Application Server**
- **File and Storage Services** (leave as default if selected)
- **Web Server (IIS)** (accept any aditional required roles)

9. Click **Next**



Select one or more roles to install on the selected server.

Roles

☑ Application Server
☐ DHCP Server
☐ DNS Server
☐ Fax Server
▣ File and Storage Services (1 of 12 installed)
☐ Hyper-V
☐ Network Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☑ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Essentials Experience
☐ Windows Server Update Services

Description

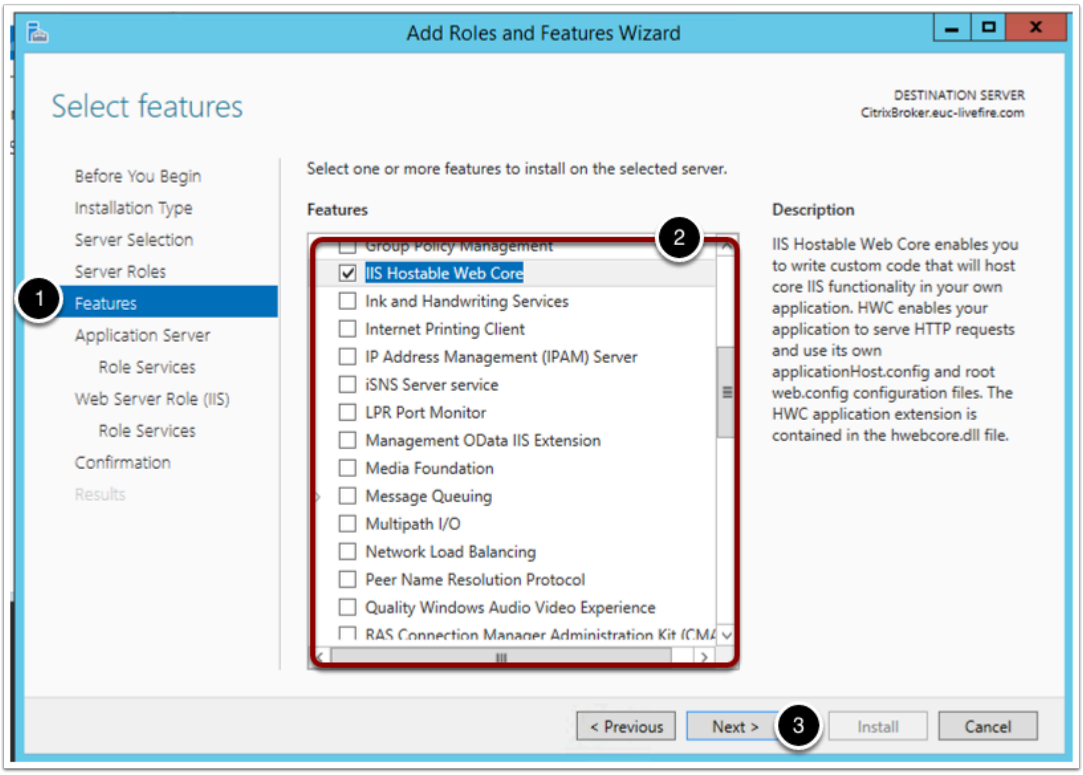
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

10. In the **Features** window, select the following options:

- **.NET Framework 3.5 Features**
  - **.NET Framework 3.5 (includes .NET 2.0 and 3.0)**
  - **HTTP Activation** (accept any required features)

- **IIS Hostable Web Core**
- **Windows Process Activation Service** (leave as default if already selected)
- **WinRM IIS Extension** (accept any required features)

11. Click **Next** until you reach **Application Services Role Services.**



Select features

DESTINATION SERVER
CitrixBroker.euc-livefire.com

Select one or more features to install on the selected server.

Features

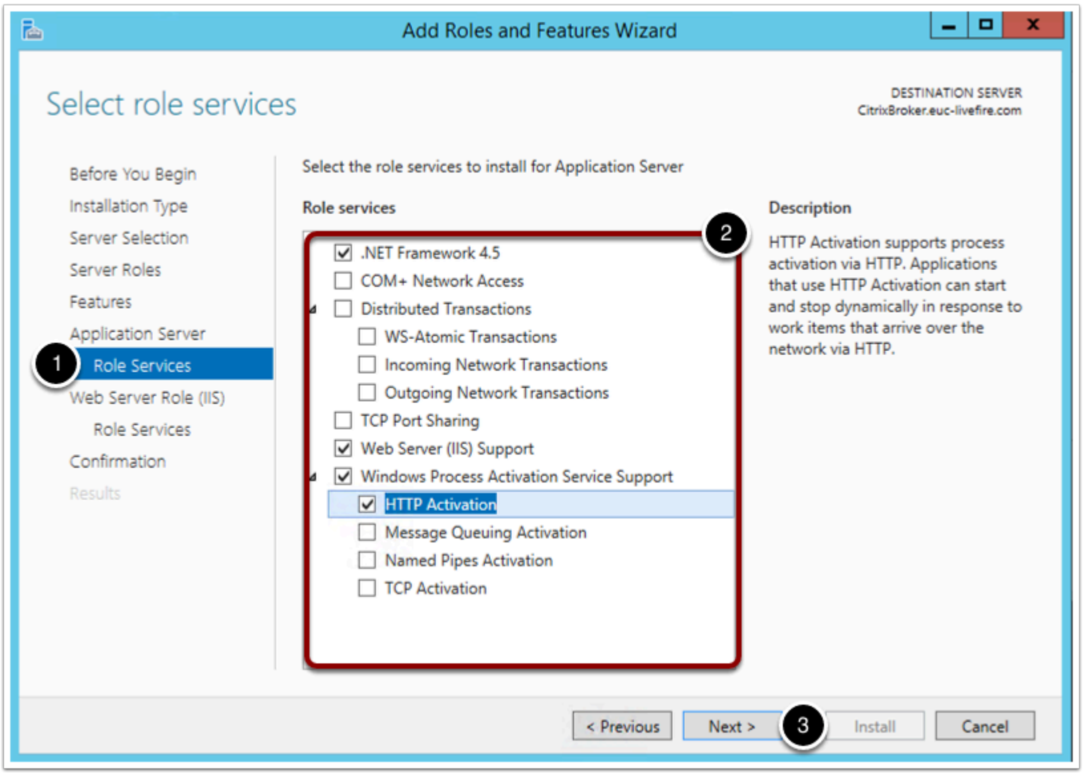
□ Group Policy Management
☑ IIS Hostable Web Core
□ Ink and Handwriting Services
□ Internet Printing Client
□ IP Address Management (IPAM) Server
□ iSNS Server service
□ LPR Port Monitor
□ Management OData IIS Extension
□ Media Foundation
□ Message Queuing
□ Multipath I/O
□ Network Load Balancing
□ Peer Name Resolution Protocol
□ Quality Windows Audio Video Experience
□ RAS Connection Manager Administration Kit (CMA

Description

IIS Hostable Web Core enables you to write custom code that will host core IIS functionality in your own application. HWC enables your application to serve HTTP requests and use its own applicationHost.config and root web.config configuration files. The HWC application extension is contained in the hwebcore.dll file.

12. Select the following role services:

- **.NET Framework 4.5** (do not change if preselected)
- **Web Server (IIS) Support** (accept the installation of any required roles)
- **Windows Process Activation Service Support**
  - **HTTP Activation** (accept the installation of any required roles)



Select the role services to install for Application Server

Role services

- ☑ .NET Framework 4.5
- ☐ COM+ Network Access
- ☐ Distributed Transactions
  - ☐ WS-Atomic Transactions
  - ☐ Incoming Network Transactions
  - ☐ Outgoing Network Transactions
- ☐ TCP Port Sharing
- ☑ Web Server (IIS) Support
- ☑ Windows Process Activation Service Support
  - ☑ HTTP Activation
  - ☐ Message Queuing Activation
  - ☐ Named Pipes Activation
  - ☐ TCP Activation

Description

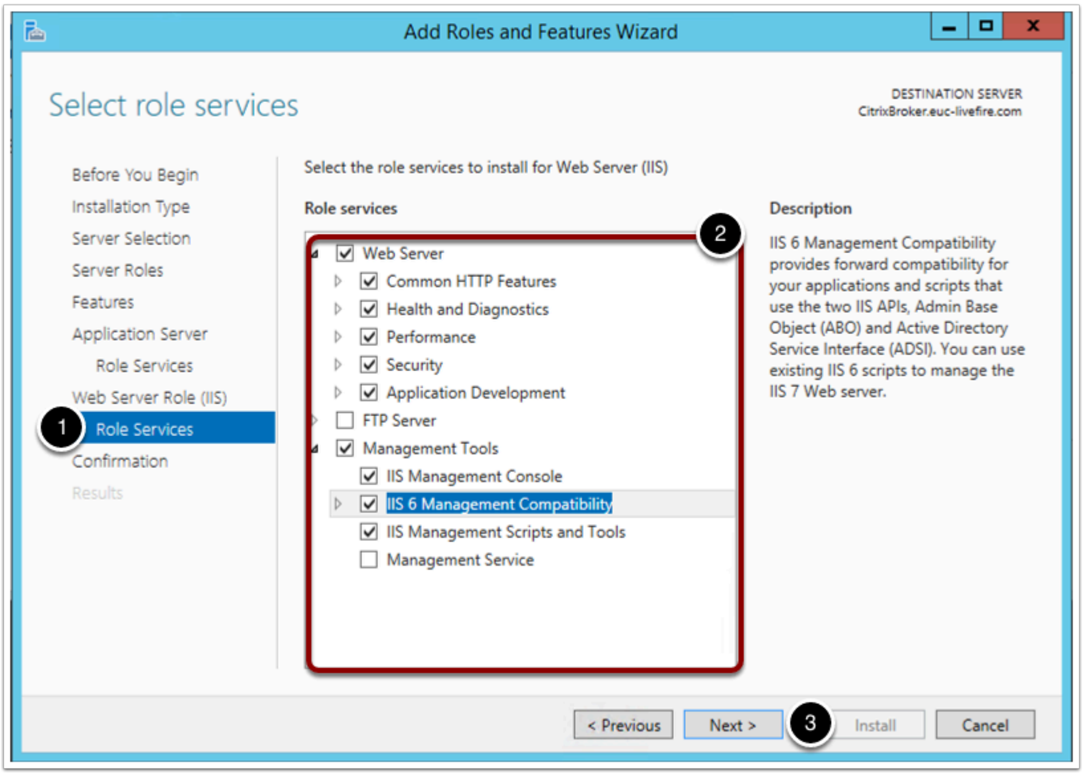
HTTP Activation supports process activation via HTTP. Applications that use HTTP Activation can start and stop dynamically in response to work items that arrive over the network via HTTP.

13. Click **Next** until you reach the **Web Server Role (IIS) Role Services** page.

14. Select the following services:

- **Web Server** (Accept the default selections)
- **Management Tools**
  - **IIS Management Console**
  - **IIS 6 Management Compatibility**

15. Click **Next** then **Install.**



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
CitrixBroker.euc-livefire.com

Select the role services to install for Web Server (IIS)

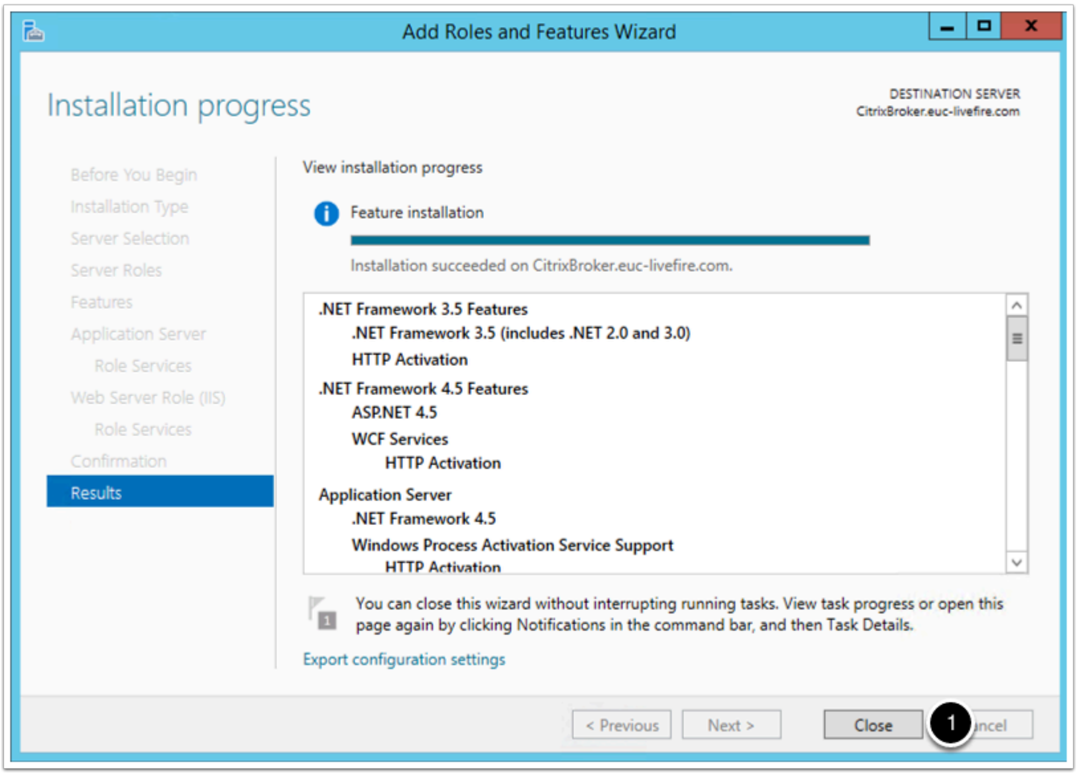
Role services

- ☑ Web Server
  - ☑ Common HTTP Features
  - ☑ Health and Diagnostics
  - ☑ Performance
  - ☑ Security
  - ☑ Application Development
- □ FTP Server
- ☑ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS 6 Management Compatibility
  - ☑ IIS Management Scripts and Tools
  - □ Management Service

Description

IIS 6 Management Compatibility provides forward compatibility for your applications and scripts that use the two IIS APIs, Admin Base Object (ABO) and Active Directory Service Interface (ADSI). You can use existing IIS 6 scripts to manage the IIS 7 Web server.

16. Click **Close** when the installation finishes.



Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
CitrixBroker.euc-livefire.com

View installation progress

Feature installation

Installation succeeded on CitrixBroker.euc-livefire.com.

.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)
    HTTP Activation
.NET Framework 4.5 Features
    ASP.NET 4.5
    WCF Services
        HTTP Activation
Application Server
    .NET Framework 4.5
    Windows Process Activation Service Support
        HTTP Activation

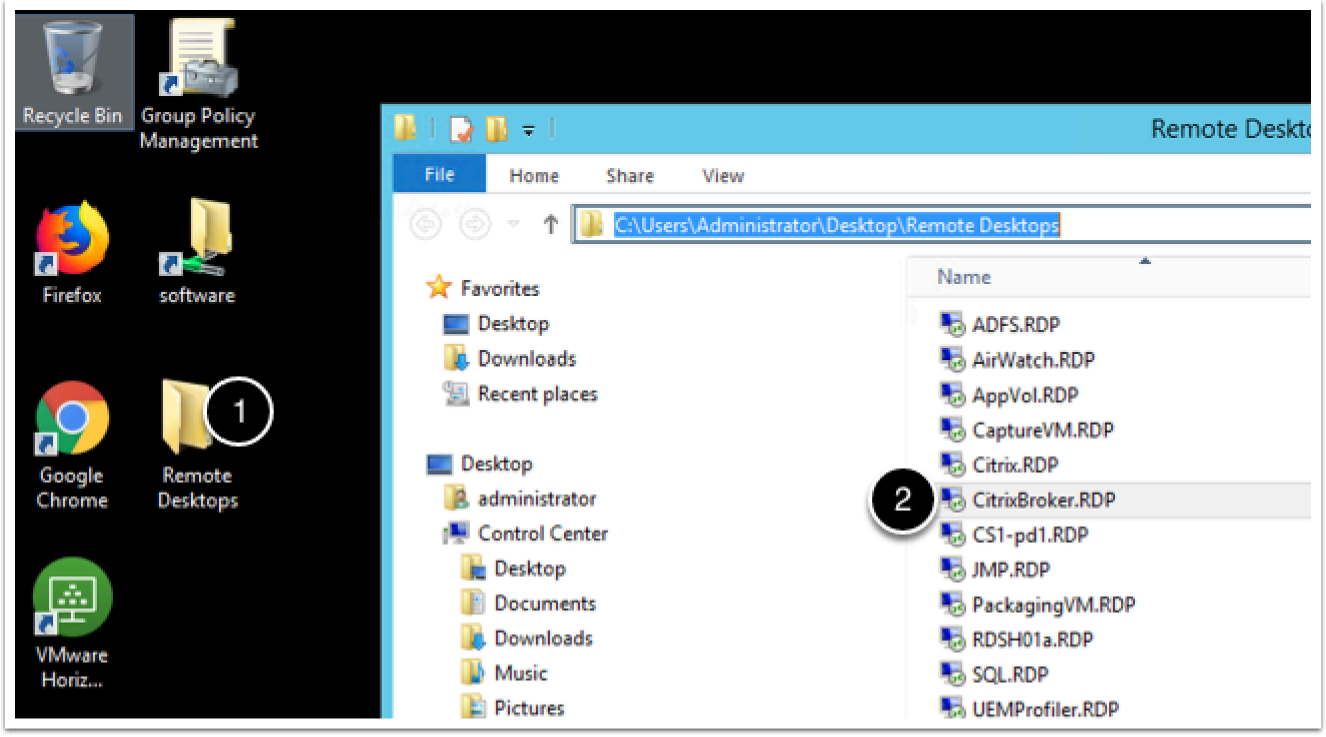
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Part 1b - Integration broker installation

Connect to your citrixbroker virtualmachine

1. Log on to your **Controlcenter** virtual machine.
2. On your desktop, go to the **Remote Desktop** folder
3. Open **citrixbroker.rdp**
4. Log on with **username: euc-livefire\administrator** and **password: VMware1!**

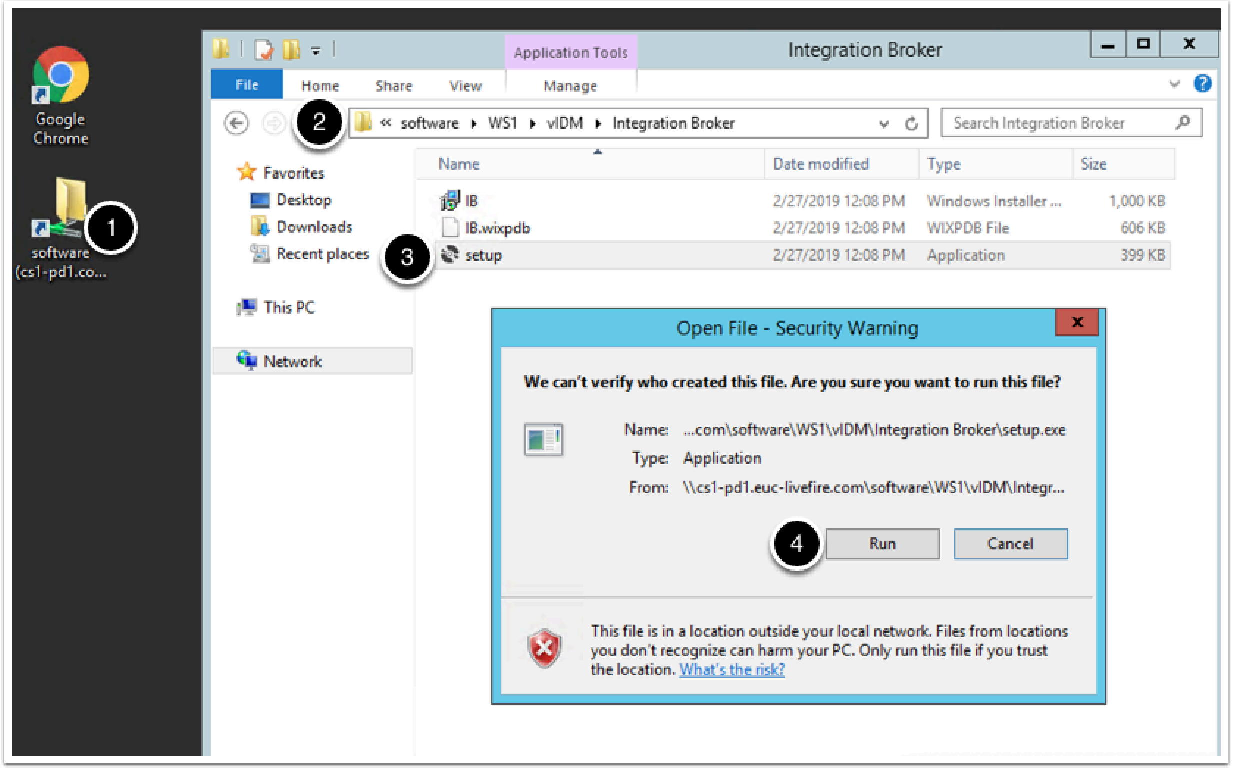


In this part you install the integration broker software

5. from the **Citrixbroker** virtual machine's desktop, go to the **Software** folder shortcut.

6. Navigate to **\software\VIDM\IntegrationBroker-19.03.0-13221855**

7. Run **Setup.exe**, in the **security warning** window click **Run**



Name	Date modified	Type	Size
IB	2/27/2019 12:08 PM	Windows Installer ...	1,000 KB
IB.wixpdb	2/27/2019 12:08 PM	WIXPDB File	606 KB
setup	2/27/2019 12:08 PM	Application	399 KB

Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

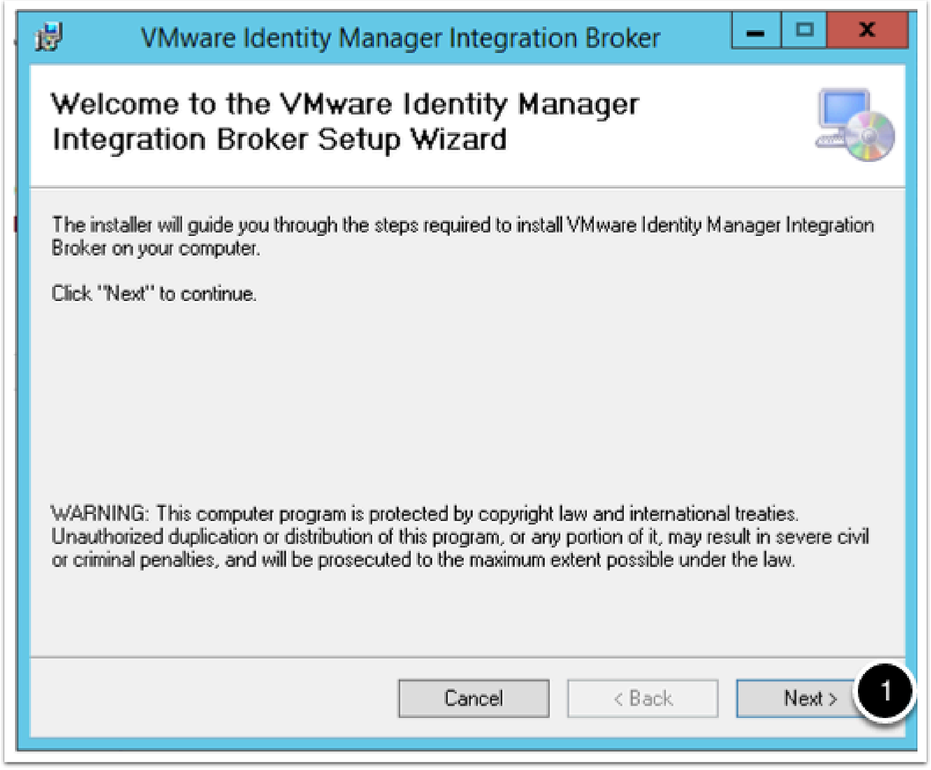
Name: ...com\software\WS1\vIDM\Integration Broker\setup.exe

Type: Application

From: \\cs1-pd1.euc-livefire.com\software\WS1\vIDM\Integr...

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only run this file if you trust the location. What's the risk?

8. Click **Next** on the **Welcome** screen



Welcome to the VMware Identity Manager Integration Broker Setup Wizard

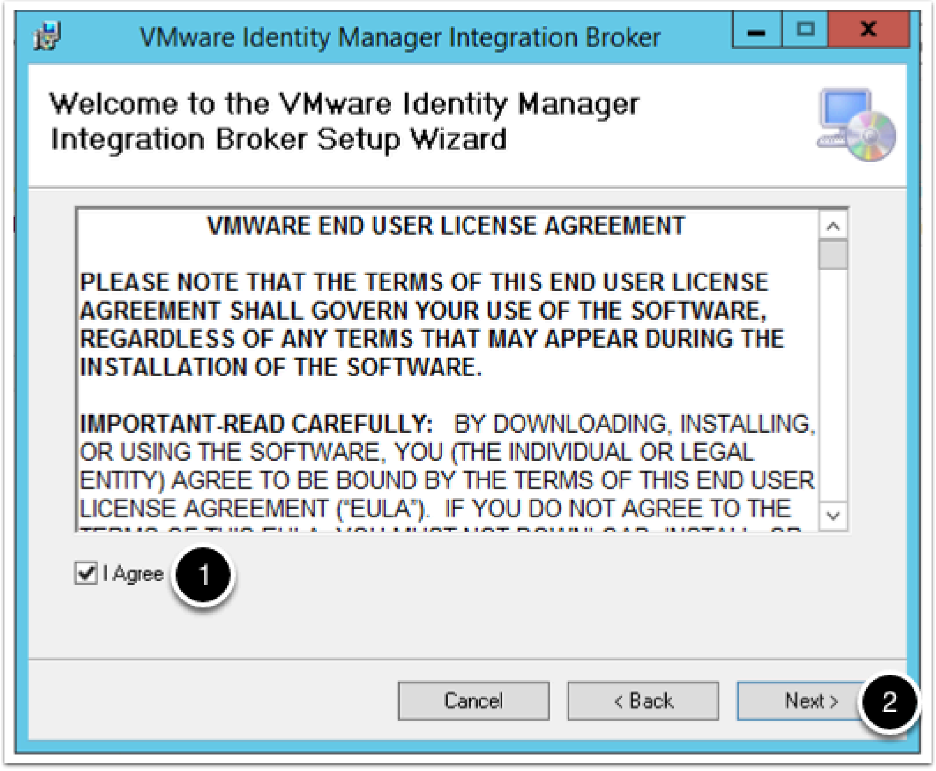
The installer will guide you through the steps required to install VMware Identity Manager Integration Broker on your computer.

Click "Next" to continue.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

9. **Agree** to the **End User License Agreement**

10. Click **Next**



Welcome to the VMware Identity Manager Integration Broker Setup Wizard

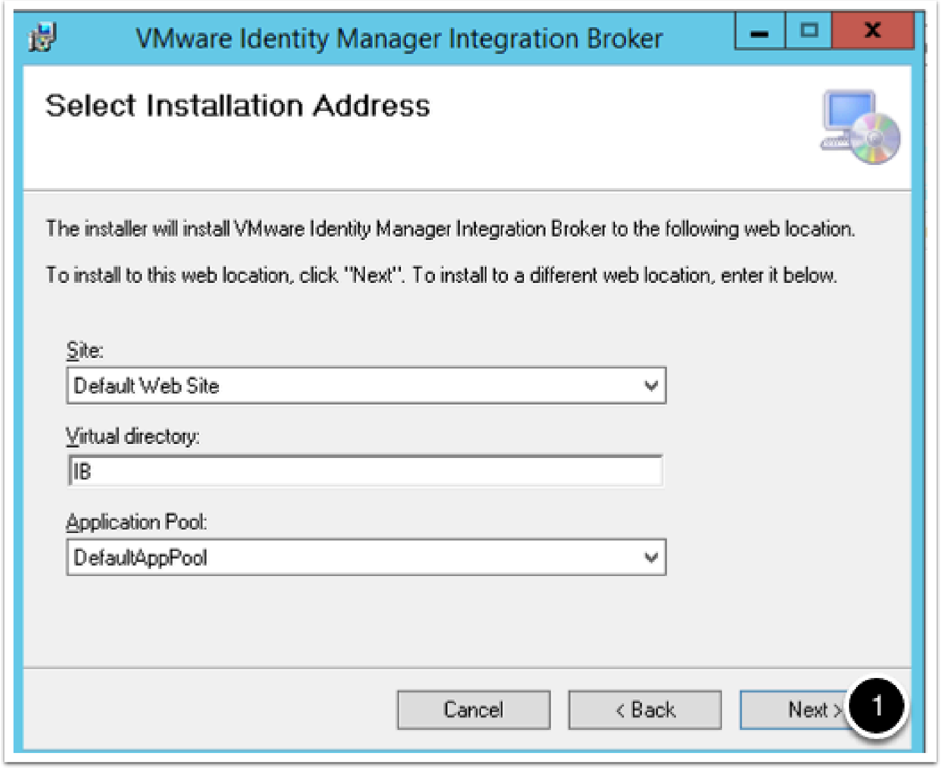
VMWARE END USER LICENSE AGREEMENT

PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE

☑ I Agree

11. Leave the default settings and click **Next**.



Select Installation Address

The installer will install VMware Identity Manager Integration Broker to the following web location.

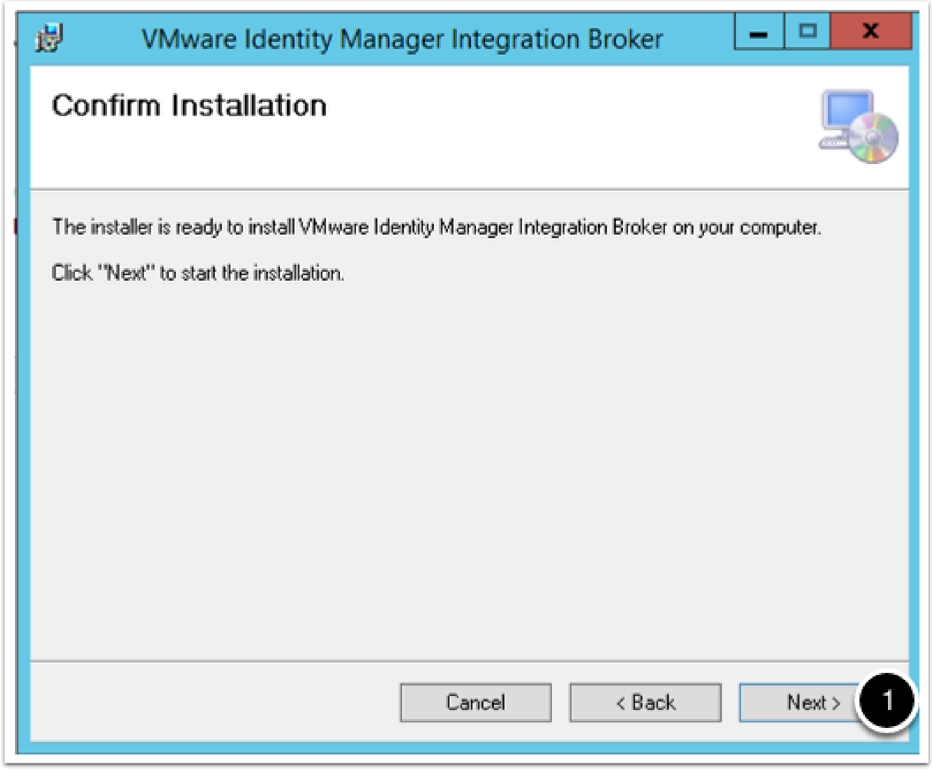
To install to this web location, click "Next". To install to a different web location, enter it below.

Site: Default Web Site

Virtual directory: IB

Application Pool: DefaultAppPool

12. Click **Next** on the **Confirm installation** windows.

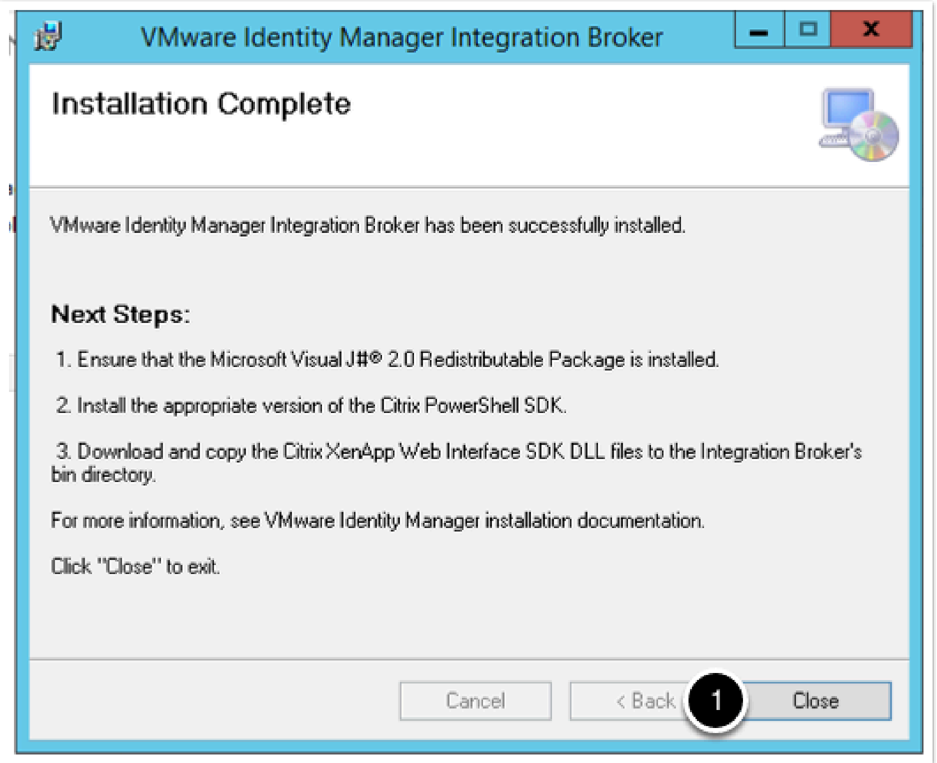

VMware Identity Manager Integration Broker

Confirm Installation

The installer is ready to install VMware Identity Manager Integration Broker on your computer.

Click "Next" to start the installation.

13. Click on **Close** on the **Installation Complete** window.


VMware Identity Manager Integration Broker

Installation Complete

VMware Identity Manager Integration Broker has been successfully installed.

Next Steps:

1. Ensure that the Microsoft Visual J#® 2.0 Redistributable Package is installed.

2. Install the appropriate version of the Citrix PowerShell SDK.

3. Download and copy the Citrix XenApp Web Interface SDK DLL files to the Integration Broker's bin directory.

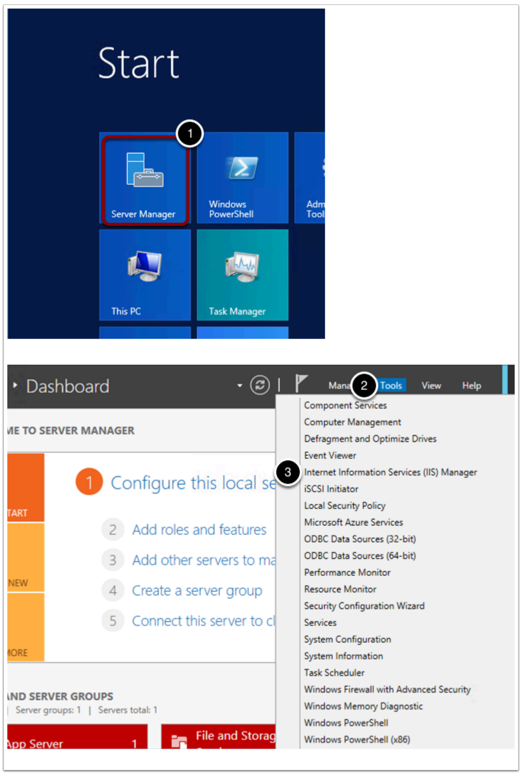
For more information, see VMware Identity Manager installation documentation.

Click "Close" to exit.

Part 1c - IIS Configuration

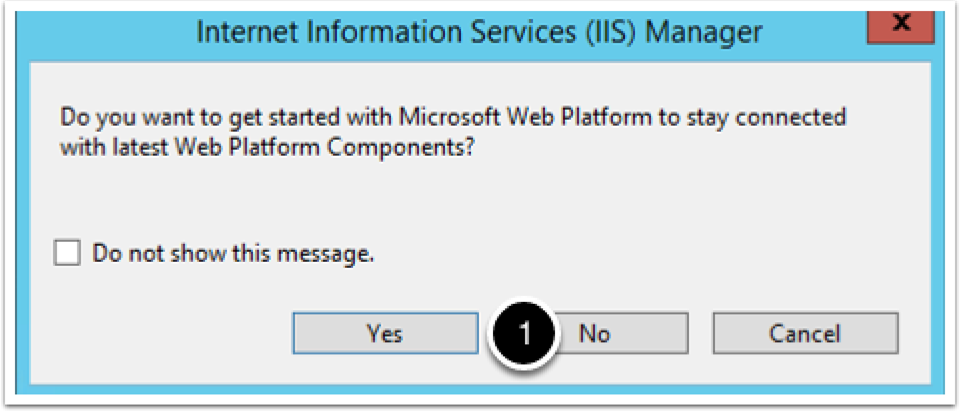
1. Click **Start** > **Server Manager**.

2. In Server Manager, select **Tools** > **Internet Information Services (IIS) Manager**.



3. In the left pane, click **Citrixbroker > Application Pools**.

Click **No** in the **Microsoft Web Platform** pop up message if prompted

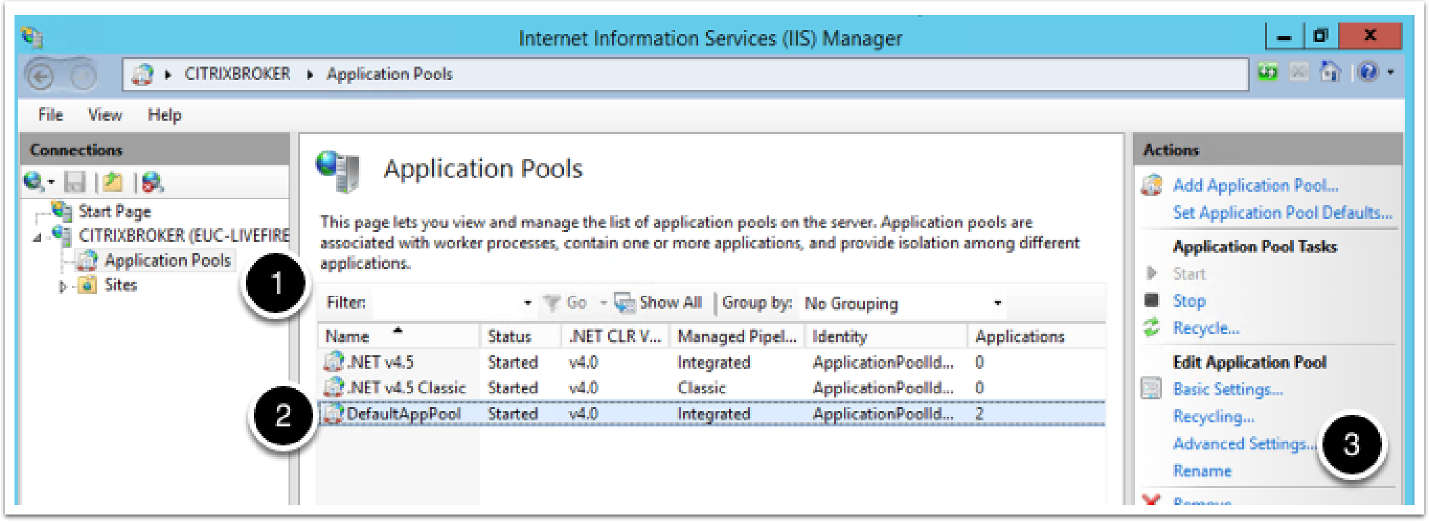


Do you want to get started with Microsoft Web Platform to stay connected with latest Web Platform Components?

□ Do not show this message.

4. Select the **DefaultAppPool**

5. Click **Advanced Settings** in the right pane.



Application Pools

This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

Filter: Go Show All | Group by: No Grouping

Name	Status	.NET CLR V...	Managed Pipel...	Identity	Applications
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	2

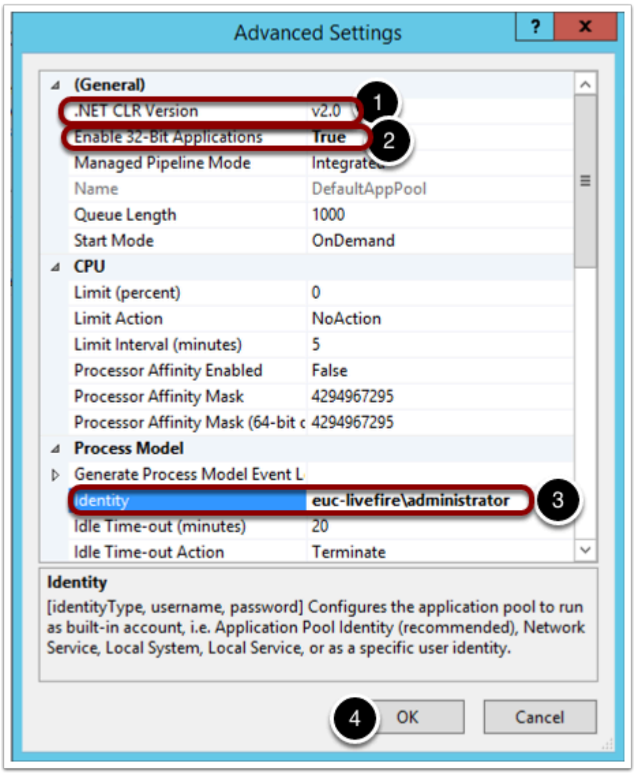
8. Set **.NET CLR Version value** to **2.0**

9. Set value **Enable 32-bit Applications** to True

10. Set **identity** value to euc-livefire\administrator

11. Click **OK**

12. Leave **IIS manager** open for the next step



(General)	
.NET CLR Version	v2.0
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	Integrated
Name	DefaultAppPool
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**euc-livefire\administrator**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

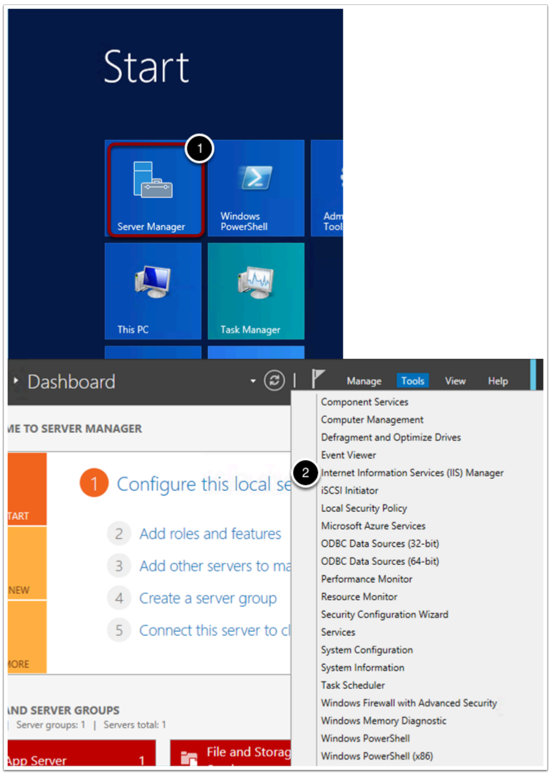
Part 1d - Self signed certificate creation

In this part you create a self signed certificate for the ssl communication with citrix storefront

Open the **IIS manager** if it is not open already

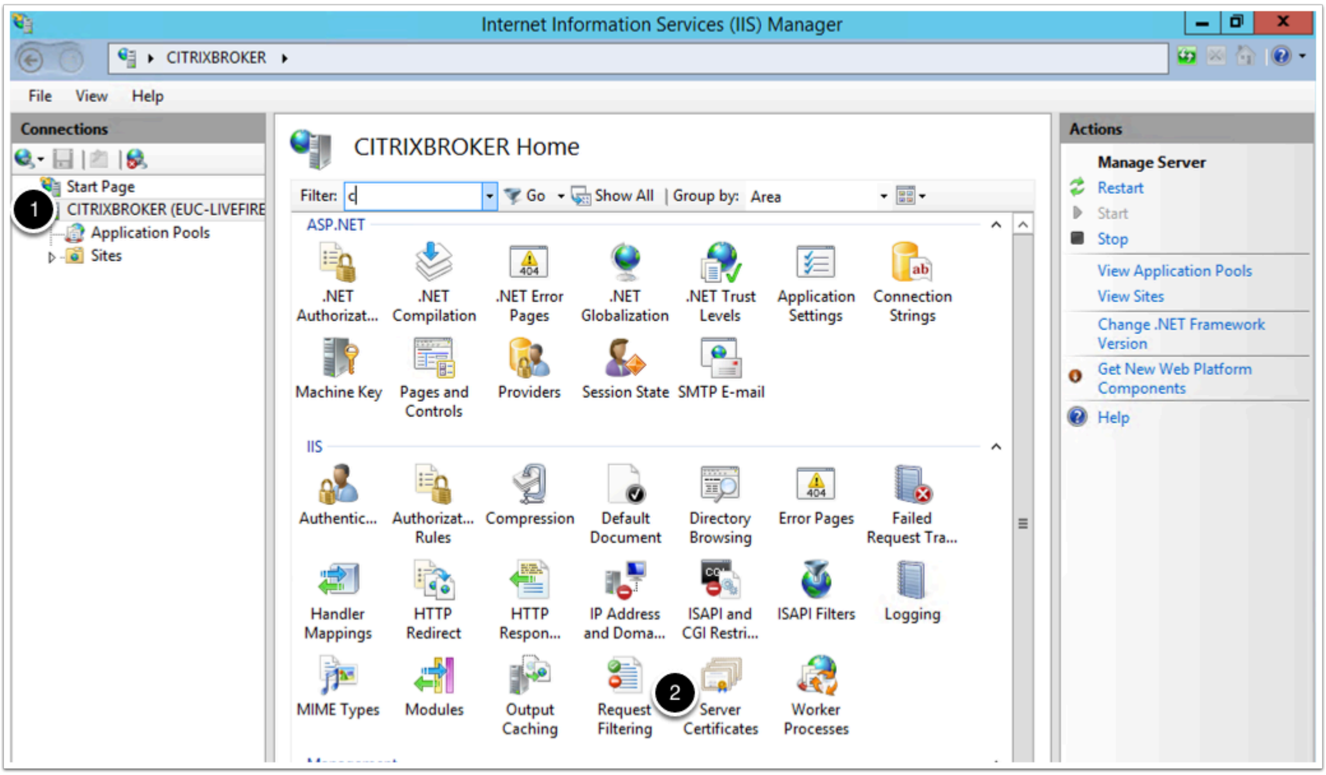
1. Go to **Start** > Server Manager

2. Go to **Tools** > Internet Information Services Manager



3. In your left pane click on the **Citrixbroker** object

4. Navigate to **Server Certificates** in the center pane



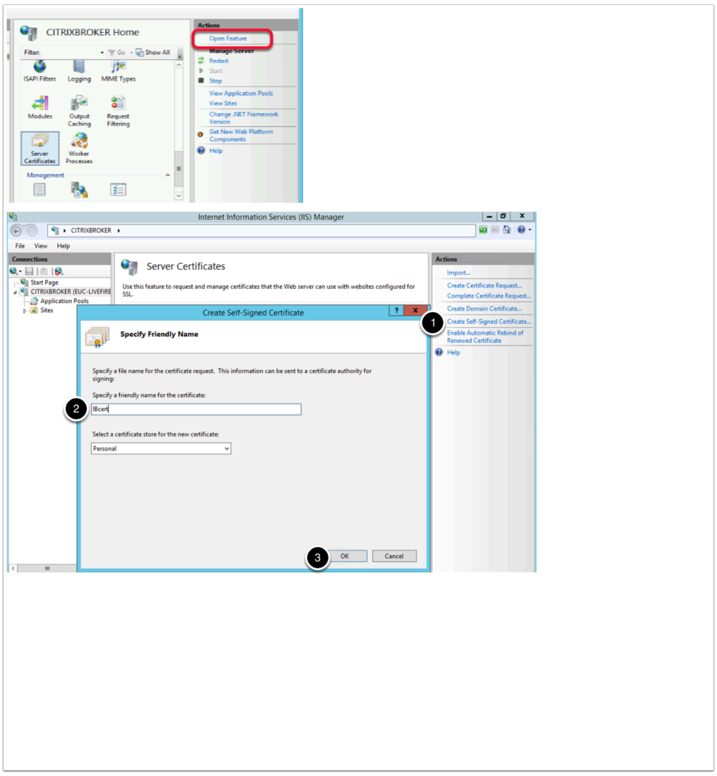
5. On your right pane go to **Actions** > Open Feature

   Under Actions select **Create Self signed certificate**

6. in the **Create Self-Signed Certificate** window, write **IBcert** as a name for the certificate

7. Click **OK**.

8. Leave the **IIS Manager** window open for the next steps


CITRIXBROKER Home
Open Feature
Server Certificates
Internet Information Services (IIS) Manager
Create Self-Signed Certificate
Specify Friendly Name
Specify a friendly name for the certificate:
IBcert
Select a certificate store for the new certificate:
Personal
OK
Cancel
Create Self-Signed Certificate...
1
2
3

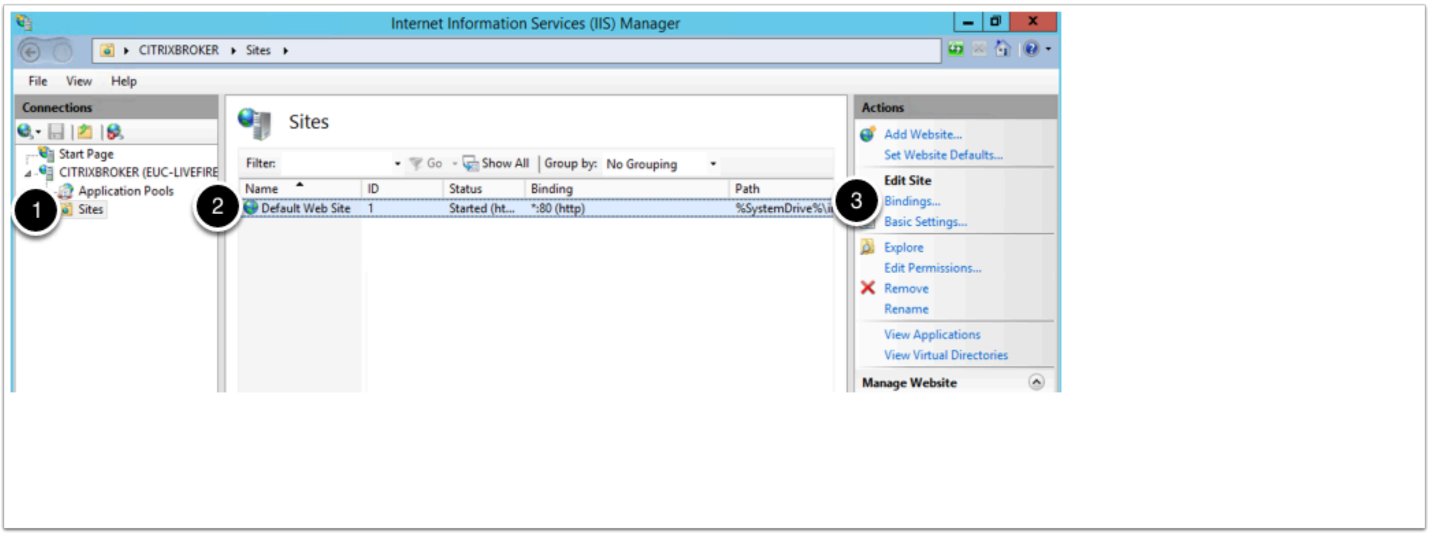
part 1e - Site binding configuration

Open the **IIs Manager** if not opened already

1. On the **IIS Manager** click on **Sites**

2. Click on the **Default Web Site**

3. In the right pane, under **Edit Site** select Bindings



4. On the **Site Bindings** window click on **Add**

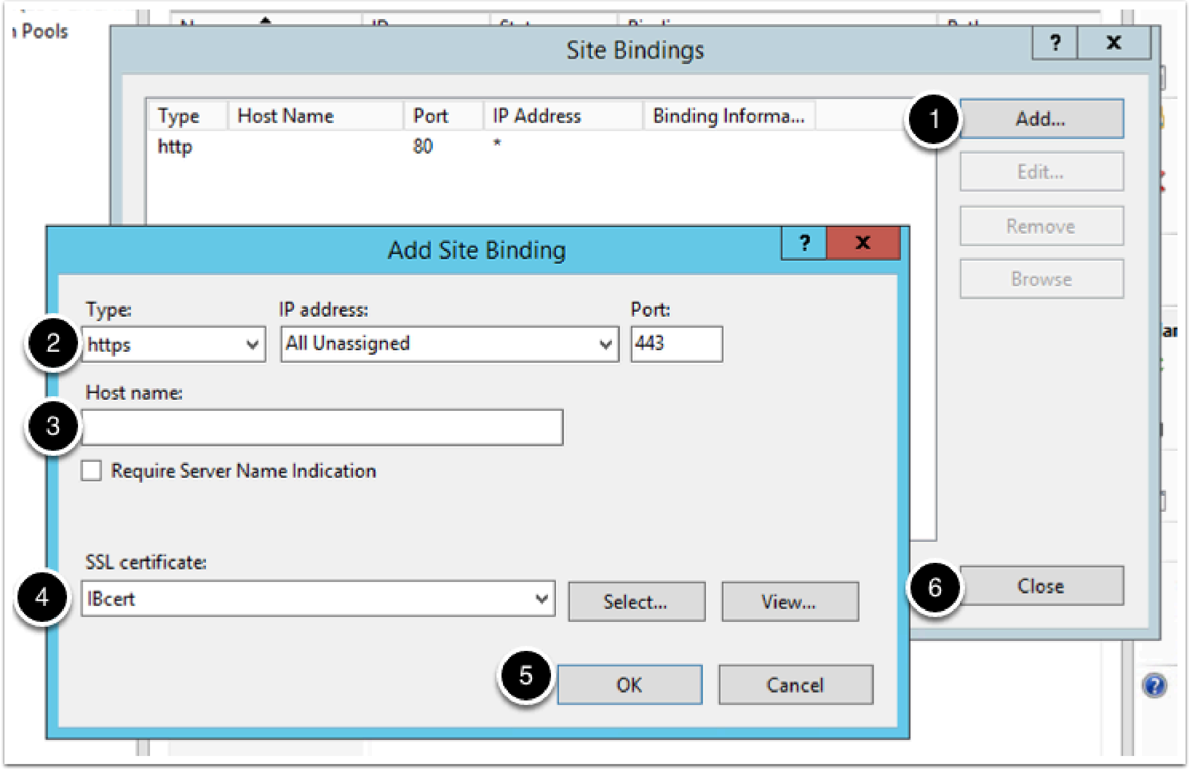
5. On **Type** select **HTTPS**

6. Make sure the **Host Name** field is empty

7. In the **Ssl Certificate** drop down menu choose the **IBcert** certificate you created on previous steps

8. Click **OK** on the **add site binding** window

9. Click **Close** on the **site binding** window



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

Type: https

IP address: All Unassigned

Port: 443

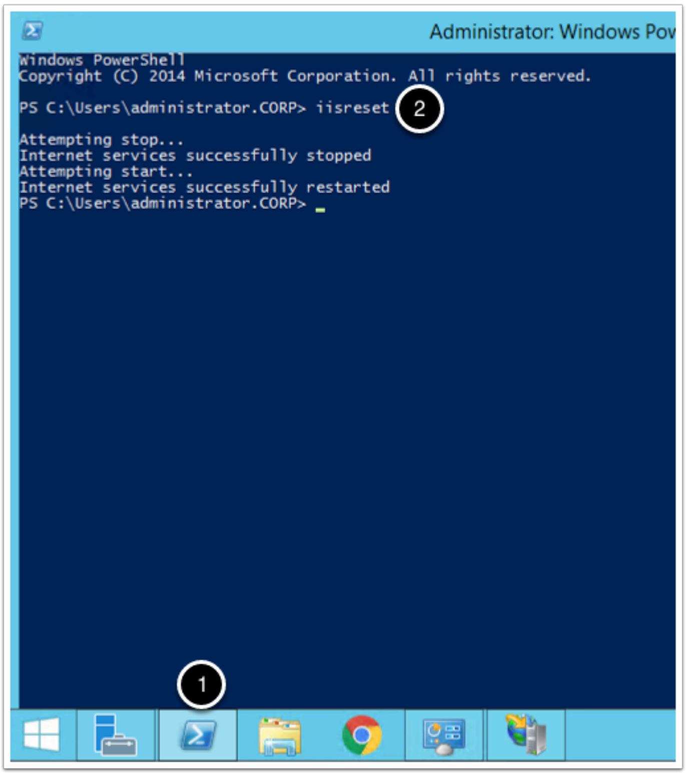
Host name:

☐ Require Server Name Indication

SSL certificate: IBcert

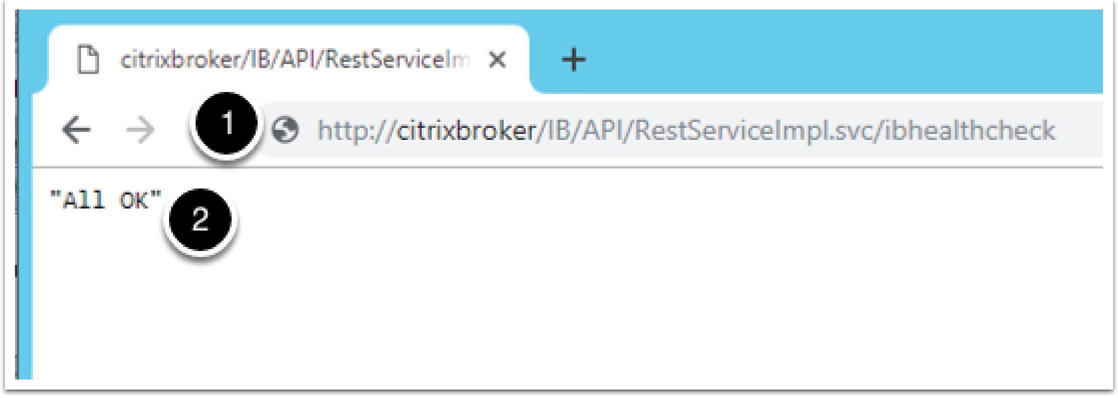
10. Open a **powershell** or **command line** window.

11. Run the **iisreset** command



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.CORP> iisreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
PS C:\Users\administrator.CORP> _
```

12. In your **Controlcenter** VM open a chrome browser and type **http://citrixbroker/IB/API/RestServiceImpl.svc/ibhealthcheck** , you should see an **"ALL OK"** message.


citrixbroker/IB/API/RestServiceIm
1
http://citrixbroker/IB/API/RestServiceImpl.svc/ibhealthcheck
2

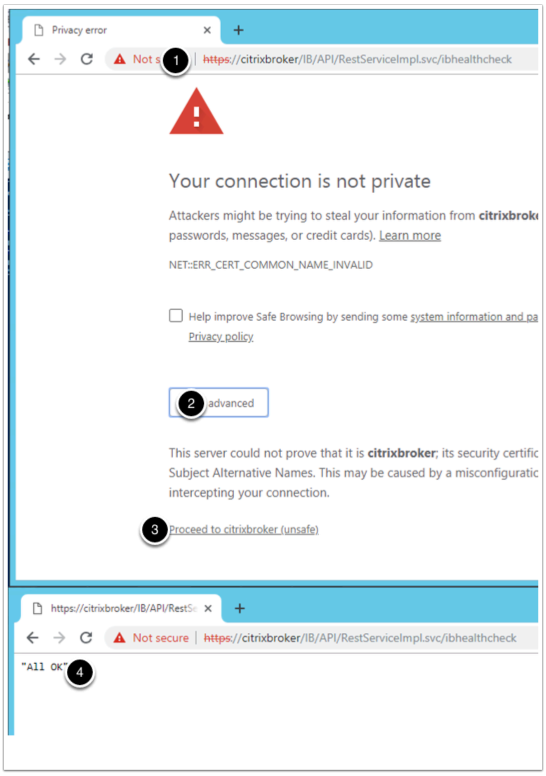
```
"All OK"
```

13. Now type **https://citrixbroker/IB/API/RestServiceImpl.svc/ibhealthcheck**

14. Click on **Advanced**

15. Click on **Proceed To Citrix Broker**

16. You should get an **"ALL OK"** message


Privacy error

Not s | https://citrixbroker/IB/API/RestServiceImpl.svc/ibhealthcheck

Your connection is not private

Attackers might be trying to steal your information from **citrixbrok** passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Help improve Safe Browsing by sending some system information and pa Privacy policy

advanced

This server could not prove that it is **citrixbroker**; its security certific Subject Alternative Names. This may be caused by a misconfiguratic intercepting your connection.

Proceed to citrixbroker (unsafe)

https://citrixbroker/IB/API/RestSe

Not secure | https://citrixbroker/IB/API/RestServiceImpl.svc/ibhealthcheck

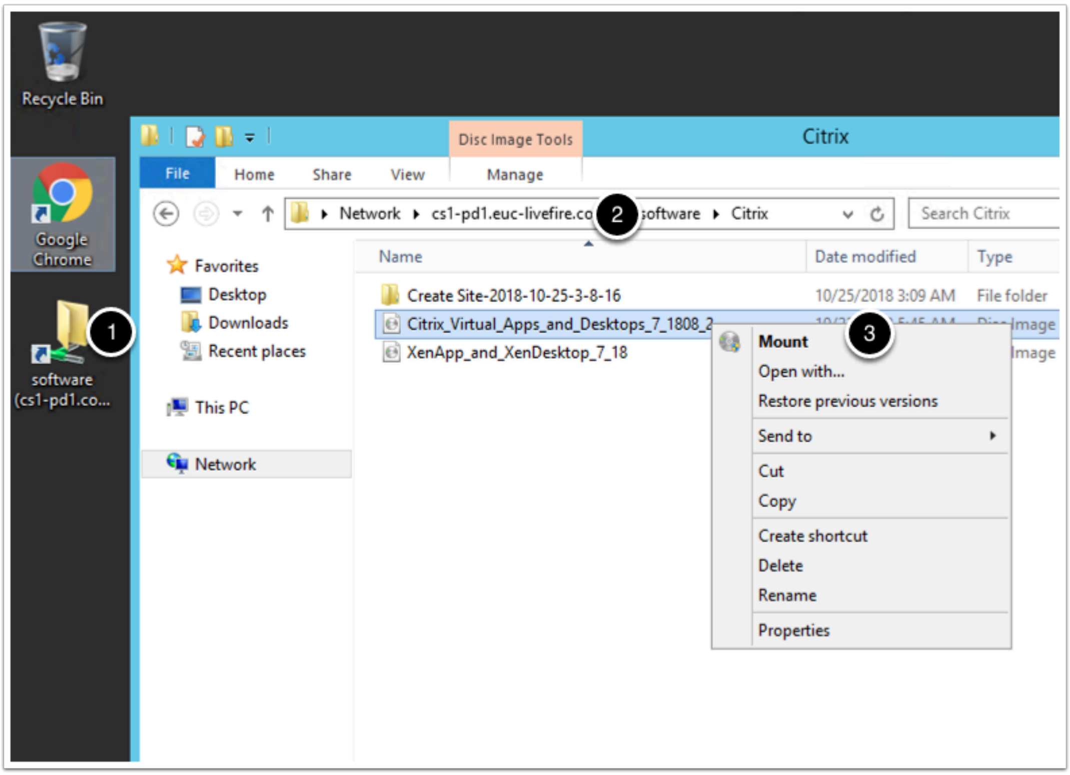
```
"All OK"
```

part 1f - citrix components installation

1. On your **Citrixbroker** machine, open the **Software** folder

2. Navigate to **Software** > Citrix

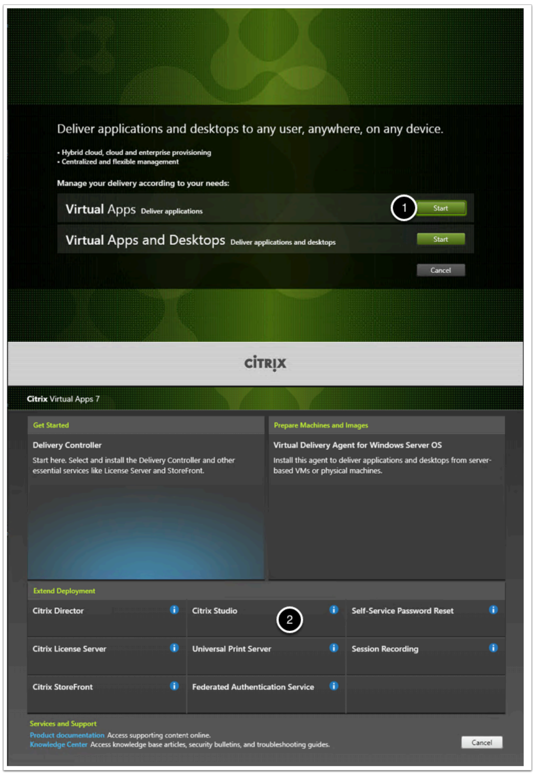
3. Right click and **mount** the **citrix virtual apps and desktops** ISO.



4. In the newly mounted drive navigate to **autoselect**

5. Click on **Start** next to **virtual apps**

6. Click on **Citrix studio**


Deliver applications and desktops to any user, anywhere, on any device.

- Hybrid cloud, cloud and enterprise provisioning
- Centralized and flexible management

Manage your delivery according to your needs:

Virtual Apps Deliver applications

Virtual Apps and Desktops Deliver applications and desktops

Citrix Virtual Apps 7

Get Started

Delivery Controller

Start here. Select and install the Delivery Controller and other essential services like License Server and StoreFront.

Prepare Machines and Images

Virtual Delivery Agent for Windows Server OS

Install this agent to deliver applications and desktops from server-based VMs or physical machines.

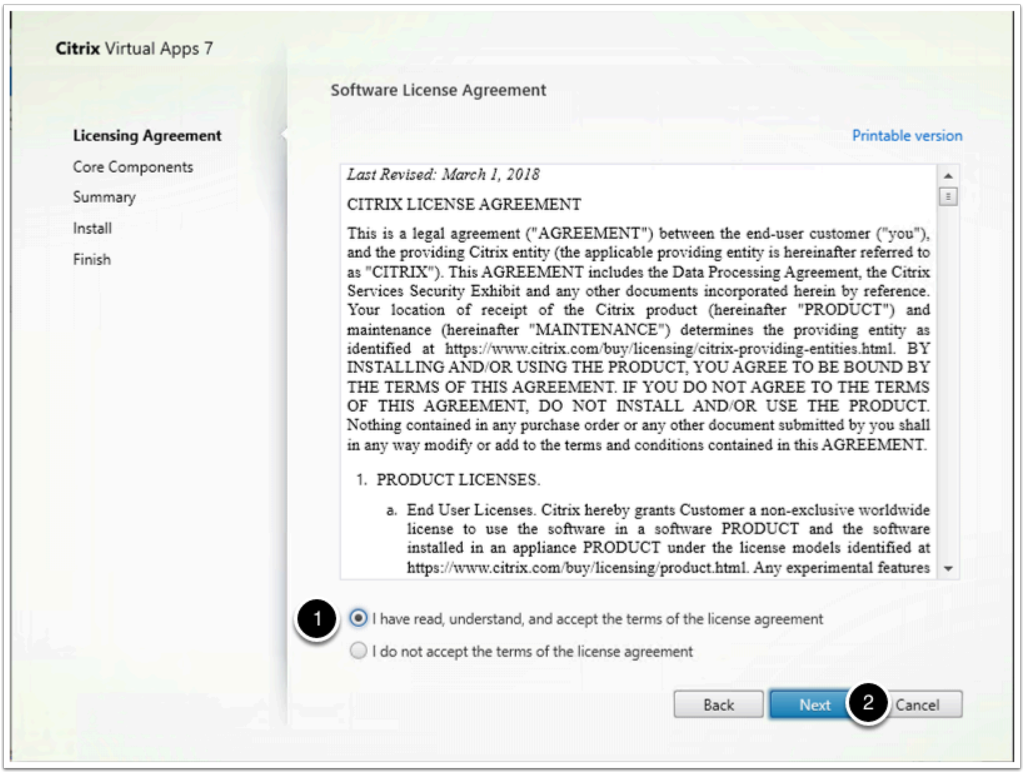
Extend Deployment

Services and Support

Product documentation Access supporting content online.

Knowledge Center Access knowledge base articles, security bulletins, and troubleshooting guides.

7. **Accept** the **software license agreement** and click **NEXT**



Citrix Virtual Apps 7

Software License Agreement

Last Revised: March 1, 2018

CITRIX LICENSE AGREEMENT

This is a legal agreement ("AGREEMENT") between the end-user customer ("you"), and the providing Citrix entity (the applicable providing entity is hereinafter referred to as "CITRIX"). This AGREEMENT includes the Data Processing Agreement, the Citrix Services Security Exhibit and any other documents incorporated herein by reference. Your location of receipt of the Citrix product (hereinafter "PRODUCT") and maintenance (hereinafter "MAINTENANCE") determines the providing entity as identified at https://www.citrix.com/buy/licensing/citrix-providing-entities.html. BY INSTALLING AND/OR USING THE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL AND/OR USE THE PRODUCT. Nothing contained in any purchase order or any other document submitted by you shall in any way modify or add to the terms and conditions contained in this AGREEMENT.

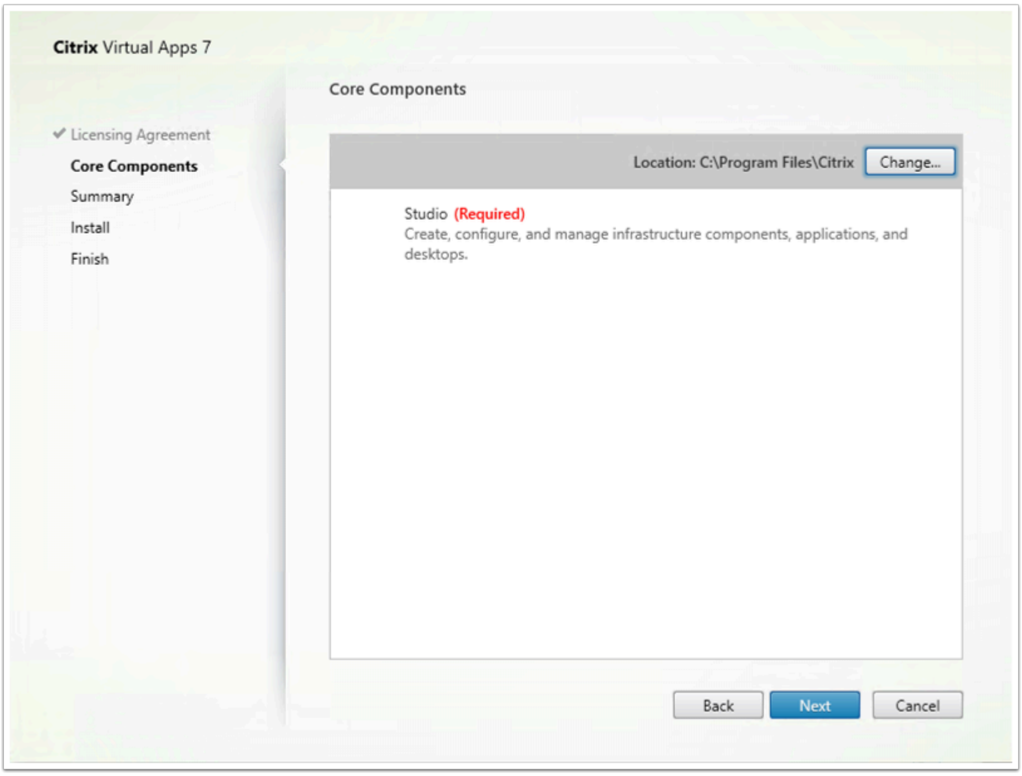
1. PRODUCT LICENSES.

   a. End User Licenses. Citrix hereby grants Customer a non-exclusive worldwide license to use the software in a software PRODUCT and the software installed in an appliance PRODUCT under the license models identified at https://www.citrix.com/buy/licensing/product.html. Any experimental features

1 ● I have read, understand, and accept the terms of the license agreement

○ I do not accept the terms of the license agreement

8. Click **Next** on the **core component** window



Citrix Virtual Apps 7

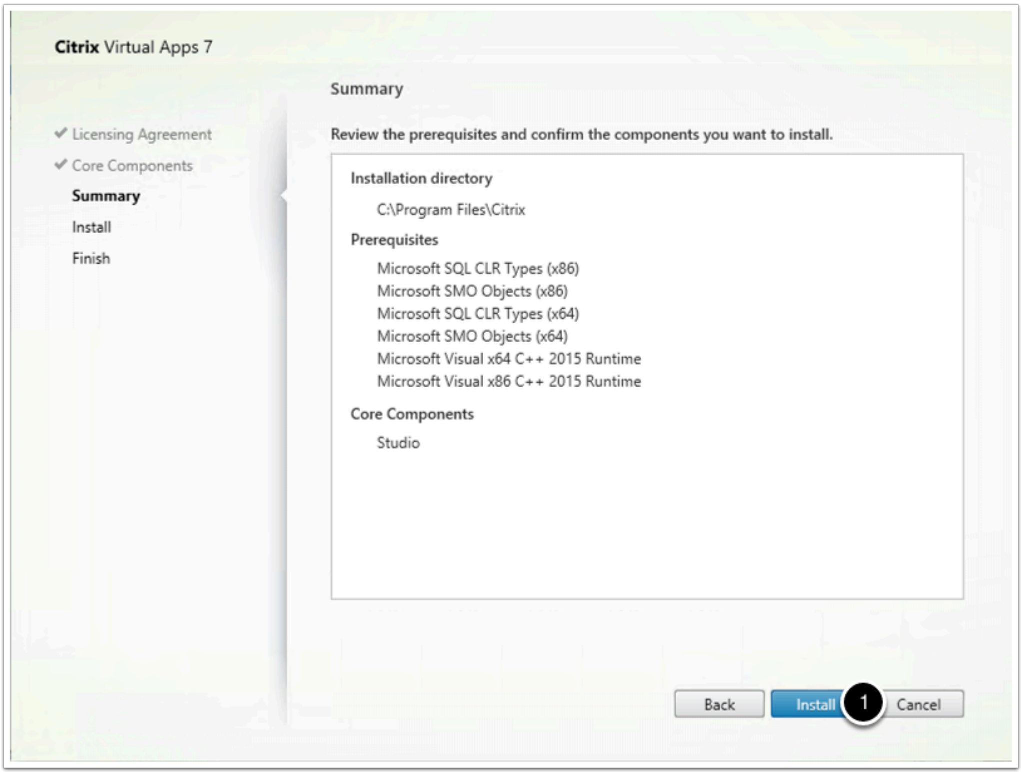
Core Components

Location: C:\Program Files\Citrix

Studio (Required)

Create, configure, and manage infrastructure components, applications, and desktops.

9. Click **install** on the **Summary** window



Citrix Virtual Apps 7

Summary

Review the prerequisites and confirm the components you want to install.

Installation directory

C:\Program Files\Citrix

Prerequisites

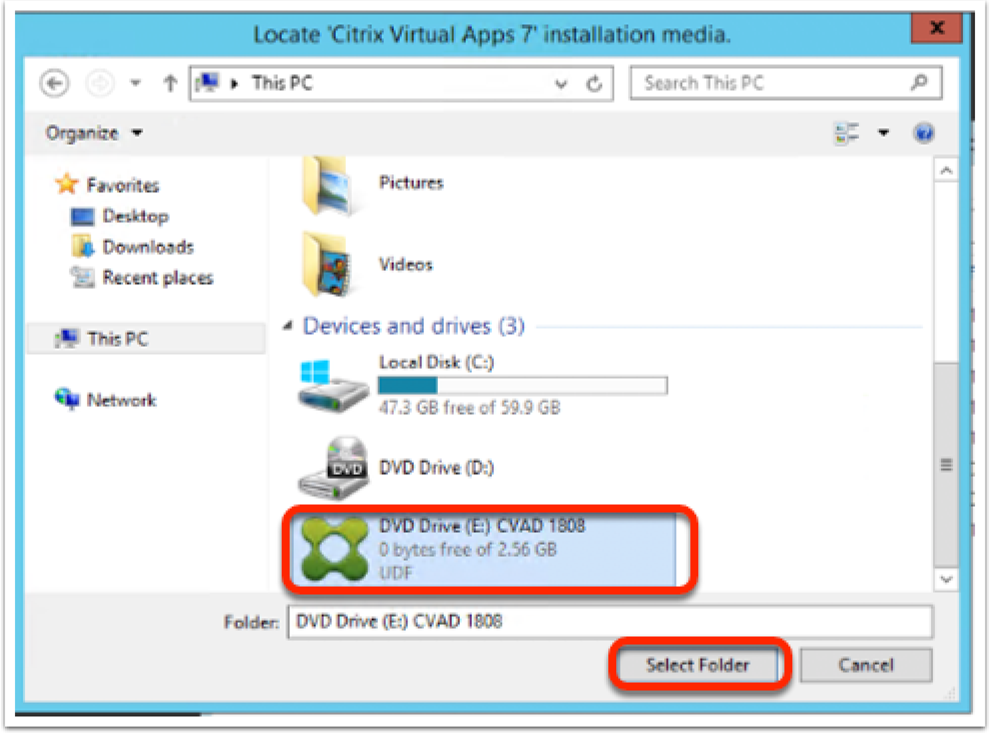
Microsoft SQL CLR Types (x86)
Microsoft SMO Objects (x86)
Microsoft SQL CLR Types (x64)
Microsoft SMO Objects (x64)
Microsoft Visual x64 C++ 2015 Runtime
Microsoft Visual x86 C++ 2015 Runtime

Core Components

Studio

10. if your vm restarts during the installation process, please follow steps 1-3 of part 1f before proceeding.

11. in the "locate Citrix Virtual Apps 7 Installatation Media" window, locate you mounted image and click on "**Select Folder**"

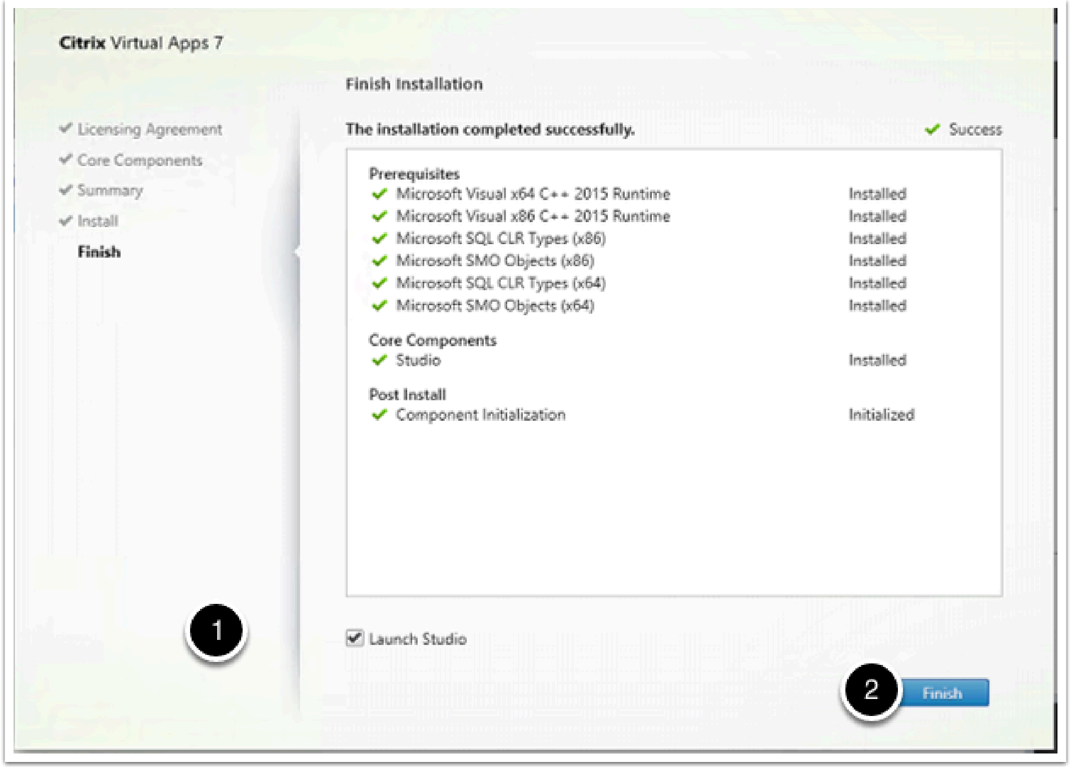


Locate 'Citrix Virtual Apps 7' installation media.

Folder: DVD Drive (E:) CVAD 1808

12. Uncheck "**launch studio**"

13. Click **Finish.** Allow the machine to restart if requested



Citrix Virtual Apps 7

✓ Licensing Agreement
✓ Core Components
✓ Summary
✓ Install
Finish

Finish Installation

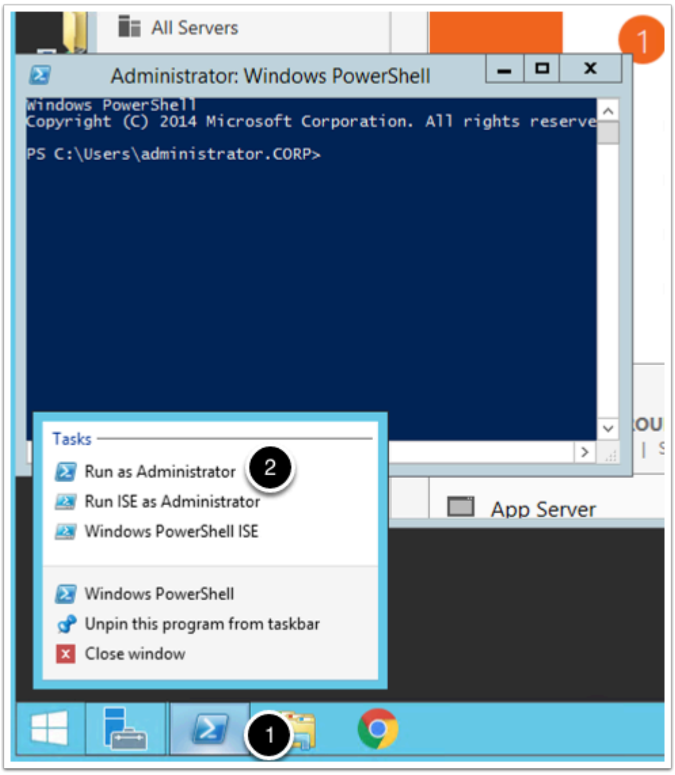
The installation completed successfully. ✓ Success

Prerequisites	
✓ Microsoft Visual x64 C++ 2015 Runtime	Installed
✓ Microsoft Visual x86 C++ 2015 Runtime	Installed
✓ Microsoft SQL CLR Types (x86)	Installed
✓ Microsoft SMO Objects (x86)	Installed
✓ Microsoft SQL CLR Types (x64)	Installed
✓ Microsoft SMO Objects (x64)	Installed
Core Components	
✓ Studio	Installed
Post Install	
✓ Component Initialization	Initialized

☑ Launch Studio

14. On your Citrixbroker vm, on your task bar right click on the **powershell** icon

15. Click run as administrator



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserve

PS C:\Users\administrator.CORP>
```

16. On your powershell windows type **Add-PSSnapin Citrix***

17. Type **Get-BrokerDesktopGroup -AdminAddress Citrix.euc-livefire.com**

you should get an output similar to this:

```
AppDisks                               : {}
AppDnaAnalysisState                    :
AppDnaCompatibility                    :
AutomaticPowerOnForAssigned            : True
AutomaticPowerOnForAssignedDuringPeak : False
ColorDepth                             : TwentyFourBit
ConfigurationSlotUids                  : {}
DeliveryType                           : DesktopsAndApps
Description                            :
DesktopKind                            : Shared
DesktopsAvailable                      : 1
DesktopsDisconnected                   : 0
DesktopsFaulted                        : 0
DesktopsInUse                          : 0
DesktopsNeverRegistered                : 0
DesktopsPreparing                      : 0
DesktopsUnregistered                   : 0
Enabled                                : True
IconUid                                : 1
InMaintenanceMode                      : False
IsRemotePC                             : False
LicenseModel                           :
MachineConfigurationNames              : {}
MachineConfigurationUids               : {}
MetadataMap                            : {}
MinimumFunctionalLevel                 : L7_9
Name                                   : standard delivery group
OffPeakBufferSizePercent               : 10
```

```
OffPeakDisconnectAction              : Nothing
OffPeakDisconnectTimeout             : 0
OffPeakExtendedDisconnectAction      : Nothing
OffPeakExtendedDisconnectTimeout     : 0
OffPeakLogOffAction                  : Nothing
OffPeakLogOffTimeout                 : 0
PeakBufferSizePercent                : 10
PeakDisconnectAction                 : Nothing
PeakDisconnectTimeout                : 0
PeakExtendedDisconnectAction         : Nothing
PeakExtendedDisconnectTimeout        : 0
PeakLogOffAction                     : Nothing
PeakLogOffTimeout                    : 0
ProductCode                          :
ProtocolPriority                     : {}
PublishedName                        : standard delivery group
ReuseMachinesWithoutShutdownInOutage : False
Scopes                               :
SecureIcaRequired                    : False
SessionSupport                       : MultiSession
Sessions                             : 0
SettlementPeriodBeforeAutoShutdown   : 00:00:00
SettlementPeriodBeforeUse            : 00:00:00
ShutdownDesktopsAfterUse             : False
Tags                                 : {}
TenantId                             :
TimeZone                             : Pacific Standard Time
TotalApplicationGroups               : 0
TotalApplications                    : 3
TotalDesktops                        : 1
```

```
TurnOnAddedMachine                : True
UUID                        : 9c5c2e43-85f4-4c20-8ed4-20f323c9544a
Uid                        : 2
ZonePreferences                  : {ApplicationHome, UserHome, UserLocation}
```

18. Type **Get-ConfigSite -AdminAddress Citrix.euc-livefire.com** , you should get an output similar to this:

```
ConfigurationLoggingServiceGroupUid    : 5d466dbe-9f03-49e6-a5d1-4fc4cb5a17bd
ConfigurationServiceGroupUid           : b2456fbb-c9cb-4445-b0ae-dadc70e7a1de
DelegatedAdministrationServiceGroupUid : 4e794a98-a86d-46d9-b0f3-34c20b28bc12
LicenseServerName                  : citrix.euc-livefire.com
LicenseServerPort                 : 27000
LicenseServerUri                 : https://citrix.euc-livefire.com:8083/
LicensingBurnIn                  : 2018.0815
LicensingBurnInDate                  : 8/14/2018 5:00:00 PM
LicensingModel                   : Concurrent
MetadataMap                      : {[CertificateHash,
OU6gnsHLtsTWxKIbQdQ9a5PwnrXwtW6VhKyVbMWfgluHrPwPrJ7AOA5WoKd
                          CLWbfveYPtpCTM+1BCf2ajnNE2Q==],
                          [Citrix_DesktopStudio_License_Is_XD_Apps_Edition, False],
                          [Citrix_StoreFront_Cluster_Id, 195c6821-b6aa-4000-be22-f013375f4aec],
                          [ConfiguredComponents, Admin Config Log Acct Hyp AppLib Prov Broker
Lic
                          Monitor Pvs Sf Trust EnvTest AppV Analytics Orch]...}
PrimaryZoneName                    : Primary
PrimaryZoneUid                   : 66798896-2967-4465-9067-8608775d7a9e
ProductCode                     : MPS
ProductEdition                  : ADV
ProductVersion                   : 7.19
```

```
SiteGuid                    : a5e6adb4-e71c-4397-a34e-a4404e556821

SiteName                     : London
```

19. from yourcontrolcenter vm, in your chrome browser go to **https://citrixbroker/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=citrix&xenappversion=Version7x**

you should get an output similar to this:

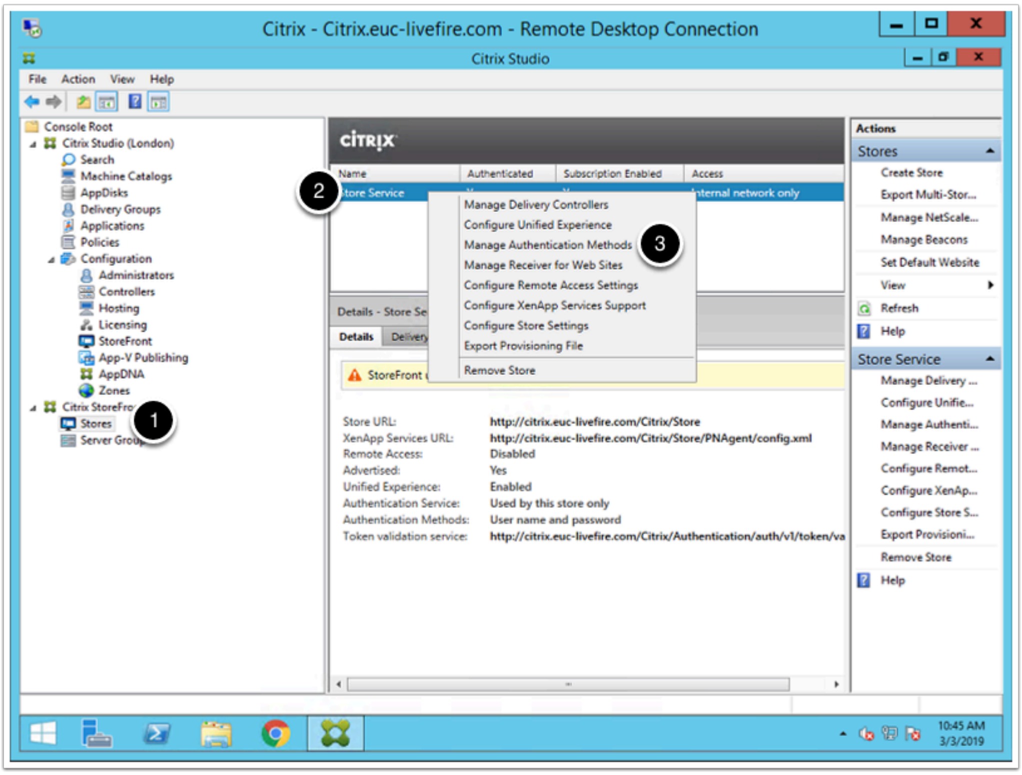
```
"[{\"ConfigurationLoggingServiceGroupUid\":\"5d466dbe-9f03-49e6-a5d1-4fc4cb5a17bd\",\"Configura
c9cb-4445-b0ae-
dadc70e7a1de\",\"DelegatedAdministrationServiceGroupUid\":\"4e794a98-a86d-46d9-b0f3-34c20b28
livefire.com\",\"LicenseServerPort\":\"27000\",\"LicenseServerUri\":\"https:\/\/citrix.euc-
livefire.com:8083\/\",\"LicensingBurnIn\":\"2018.0815\",\"LicensingBurnInDate\":\"8\/14\/2018
5:00:00
PM\",\"LicensingModel\":\"Concurrent\",\"MetadataMap\":\"System.Collections.Generic.Dictionary`2[S
a4404e556821\",\"SiteName\":\"London\"}]"
```

if you get anything starting with "exception name" or. an http error please check your url.

20. On the **ControlCenter** server. Open the **Remote Desktop** folder open **citrix.rdp** and open **citrix studio** from the **Start Menu**

21. In the left pane navigate to **Citrix Storefront** > stores

22. In the main pane, right click on **store service**, and click **manage authentication methods**

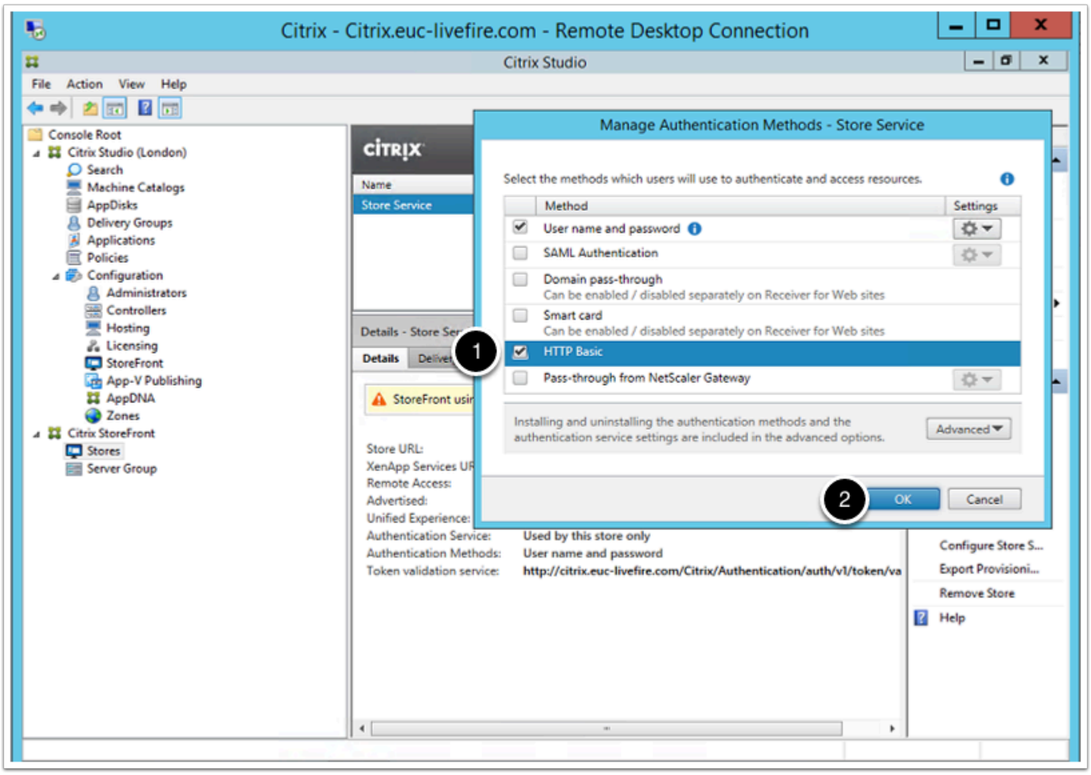


Store URL: http://citrix.euc-livefire.com/Citrix/Store
XenApp Services URL: http://citrix.euc-livefire.com/Citrix/Store/PNAgent/config.xml
Remote Access: Disabled
Advertised: Yes
Unified Experience: Enabled
Authentication Service: Used by this store only
Authentication Methods: User name and password
Token validation service: http://citrix.euc-livefire.com/Citrix/Authentication/auth/v1/token/va

23. Check **HTTP basic**

24. Click **Ok**

25. Close all windows



Manage Authentication Methods - Store Service

Select the methods which users will use to authenticate and access resources.

Method	Settings
☑ User name and password	
☐ SAML Authentication	
☐ Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
☐ Smart card Can be enabled / disabled separately on Receiver for Web sites	
☑ HTTP Basic	
☐ Pass-through from NetScaler Gateway	

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

Advanced

OK Cancel

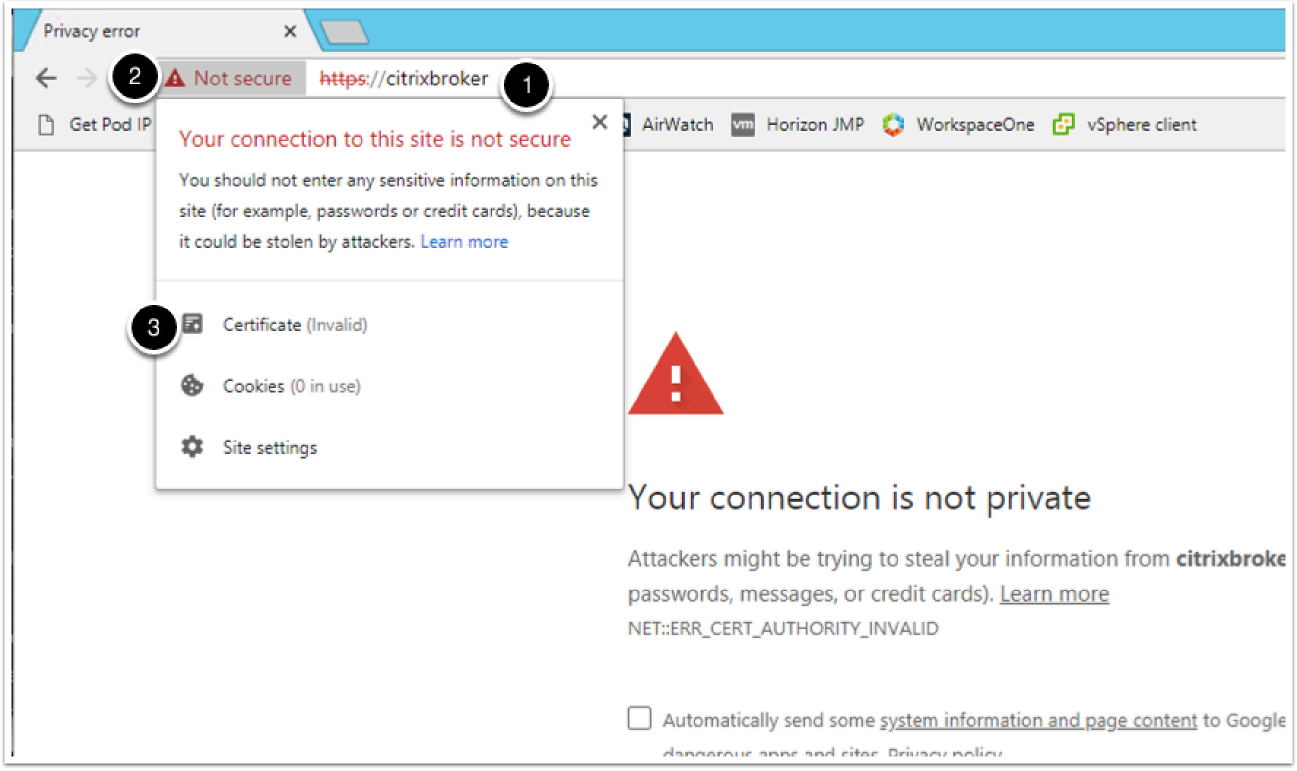
Store URL:
XenApp Services UR
Remote Access:
Advertised:
Unified Experience:
Authentication Service: Used by this store only
Authentication Methods: User name and password
Token validation service: http://citrix.euc-livefire.com/Citrix/Authentication/auth/v1/token/va

part 1g - certificate export

1. From your **Controlcenter** vm open the chrome browser and type **https://citrixbroker** on the address bar

2. Right click on "**not secure**"

3. Click on **Certificate**



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Your connection is not private

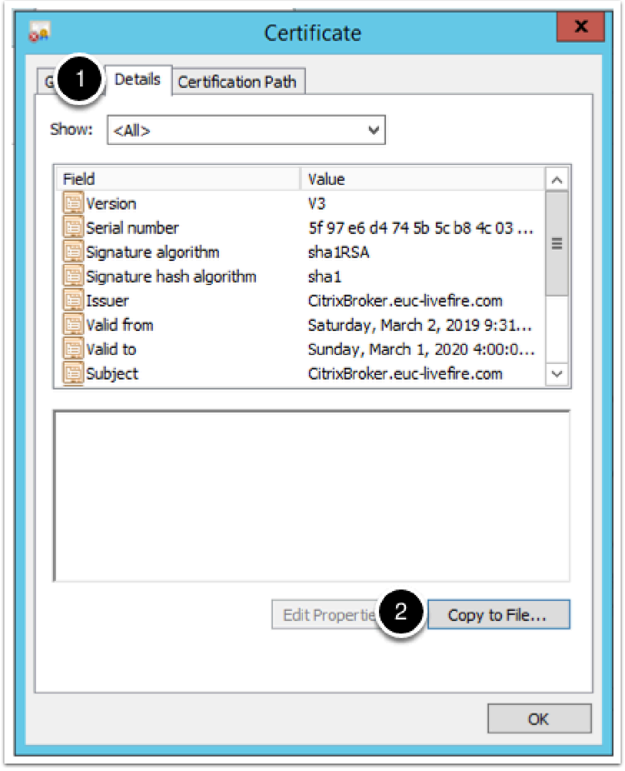
Attackers might be trying to steal your information from **citrixbroke** passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google

4. On the certificate window, go to the **details tab**

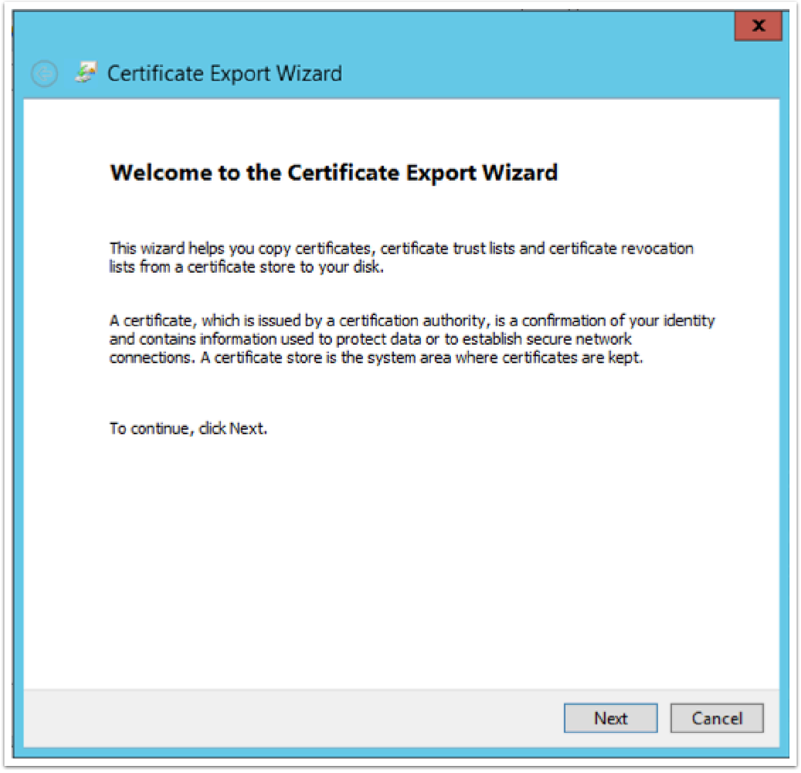
5. Click **copy to file**



Show: <All>

Field	Value
Version	V3
Serial number	5f 97 e6 d4 74 5b 5c b8 4c 03 ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	CitrixBroker.euc-livefire.com
Valid from	Saturday, March 2, 2019 9:31...
Valid to	Sunday, March 1, 2020 4:00:0...
Subject	CitrixBroker.euc-livefire.com

6. In the **Certificate Export Wizard** window, click **Next**



Welcome to the Certificate Export Wizard

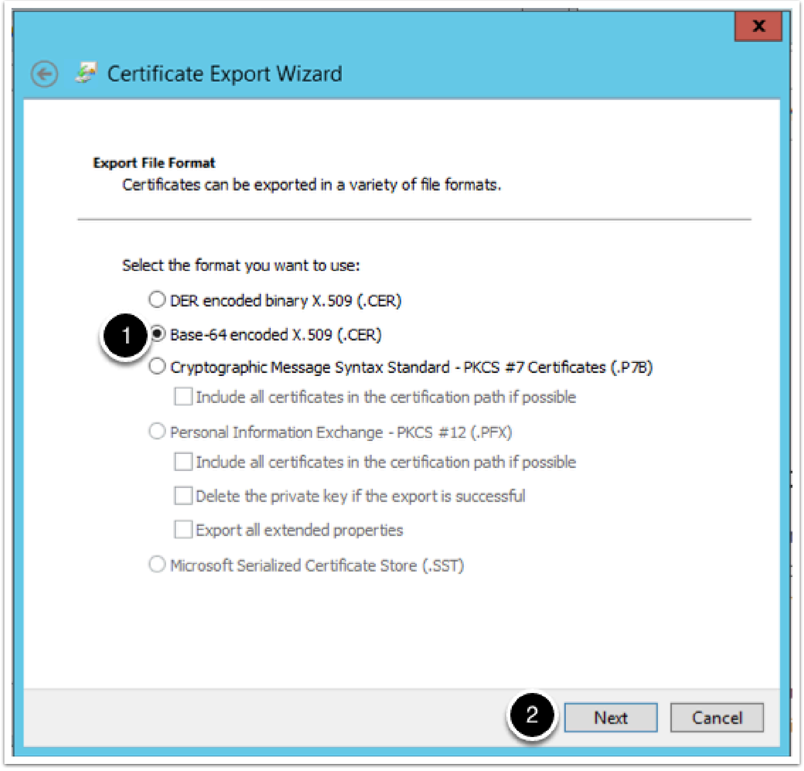
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Click on **Base-64 enconded x.509 (.CER)**

8. Click **Next**



Certificate Export Wizard

Export File Format

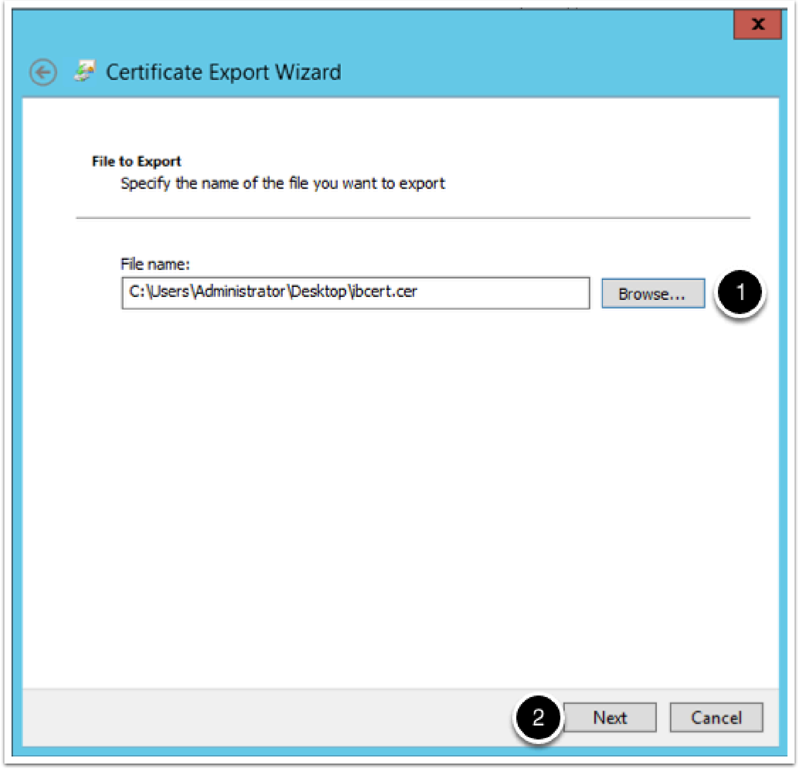
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ● Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
- ○ Microsoft Serialized Certificate Store (.SST)

9. Click on **Browse** and point to your desktop, and save the certificate with the name **ibcert**.

10. Click **Next**



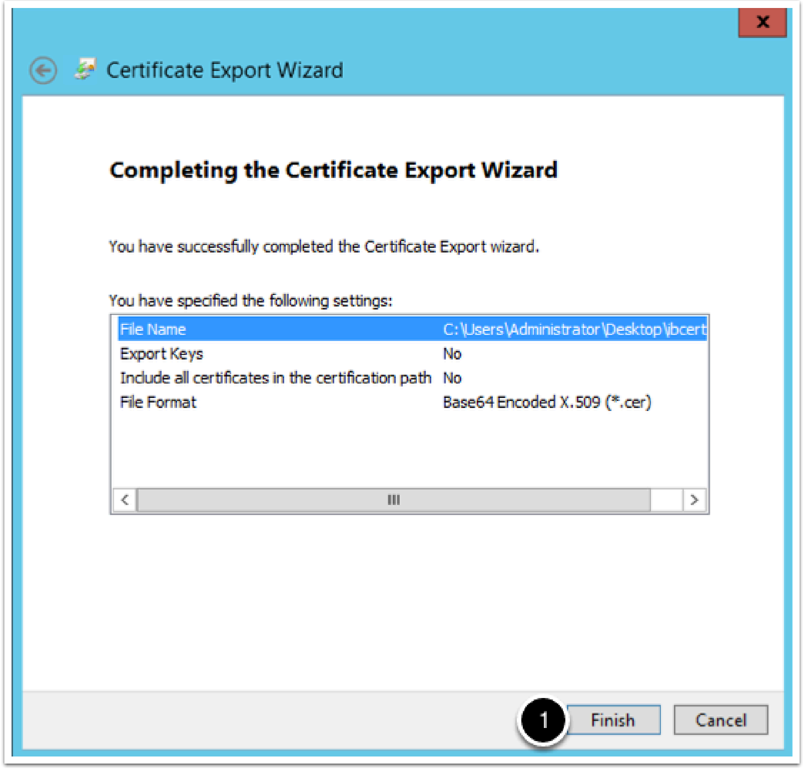
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\Users\Administrator\Desktop\ibcert.cer

11. click **Finish**



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Desktop\ibcert
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

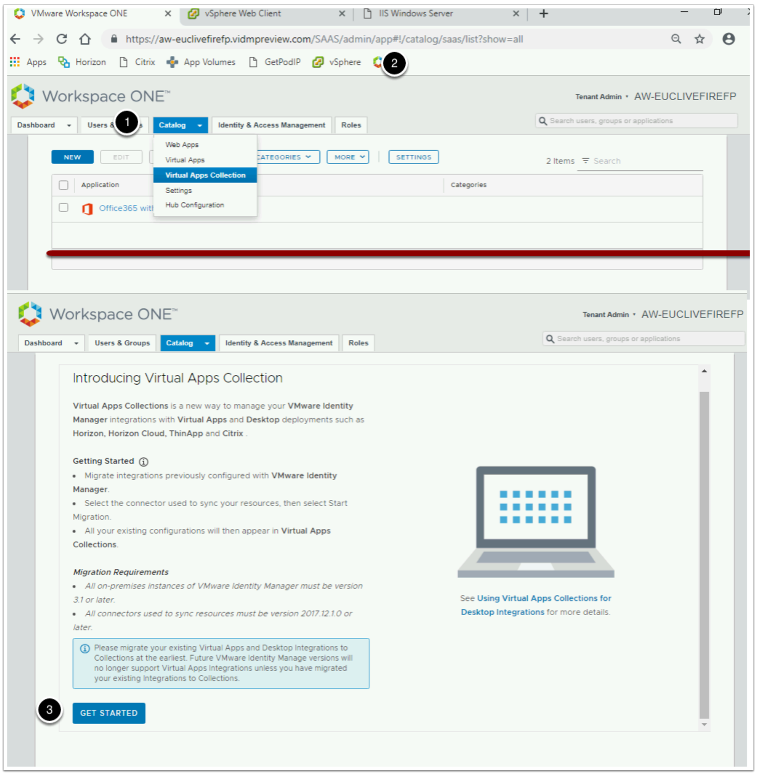
Section 2 - VMware Identity Manager Configuration

Part 1 - Configuring virtual app collection

1. Go to your **identity manager tenant url**, and login with your administrator user.

2. in the **administration console** navigate to **Catalog** > Virtual Apps Collection

3. Select **GET STARTED** if prompted



Introducing Virtual Apps Collection

Virtual Apps Collections is a new way to manage your **VMware Identity Manager** integrations with **Virtual Apps** and **Desktop** deployments such as **Horizon, Horizon Cloud, ThinApp** and **Citrix** .

Getting Started

- Migrate integrations previously configured with **VMware Identity Manager**.
- Select the connector used to sync your resources, then select Start Migration.
- All your existing configurations will then appear in **Virtual Apps Collections**.

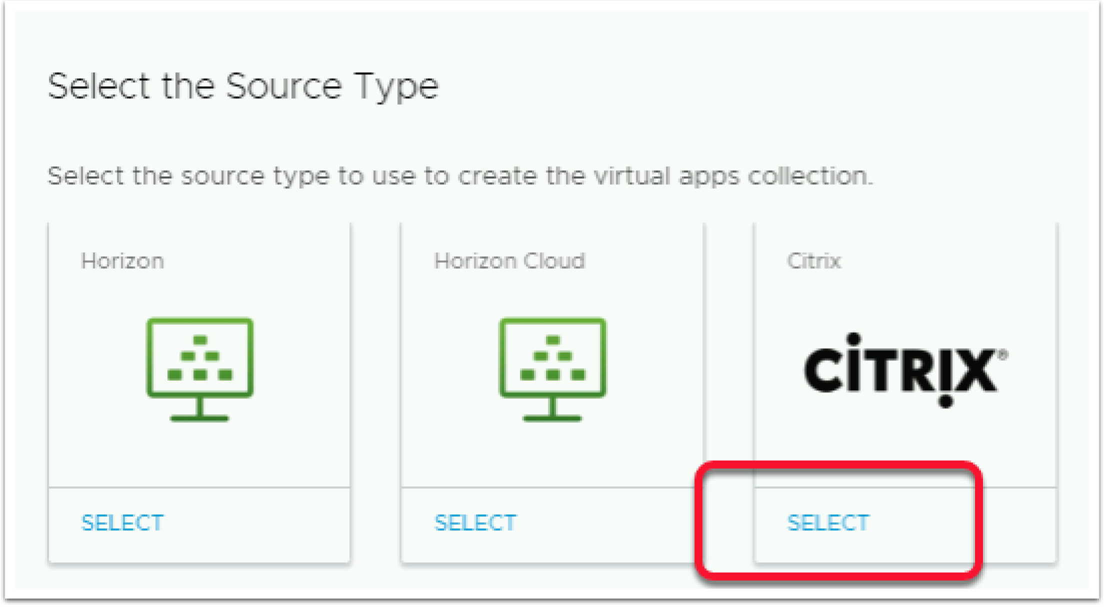
Migration Requirements

- *All on-premises instances of VMware Identity Manager must be version 3.1 or later.*
- *All connectors used to sync resources must be version 2017.12.1.0 or later.*

Please migrate your existing Virtual Apps and Desktop Integrations to Collections at the earliest. Future VMware Identity Manage versions will no longer support Virtual Apps Integrations unless you have migrated your existing Integrations to Collections.

See **Using Virtual Apps Collections for Desktop Integrations** for more details.

4. On the **Select the Source Type** page in the **Citrix Box** select the **SELECT** hyperlink



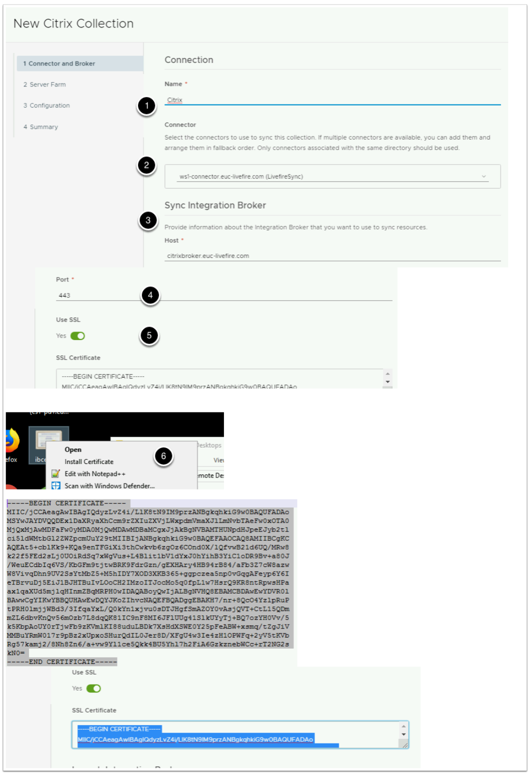
Select the Source Type

Select the source type to use to create the virtual apps collection.

5. In the New **Citrix Collection** window, in **Section 1 Connector and Broker**

1. Next to **Name** type **Citrix**
2. Under **Connector** accept the default connector that being **ws1-Connector.euc-livefire.com (LivefireSync)**
3. In the **Sync Intergration Broker** section, under **Host** type **citrixbroker.euc-livefire.com**
4. Under **Port** type **443**

5. Under **Use SSL** change the radio button from **No** to **Yes**
6. Go back to your desktop and **open** the **ibcert** file saved in Part 1G with Notepad++ . **Copy** the contents of the **ibcert** file.
   - Under SSL Certificate **paste** the contents into the box



New Citrix Collection

Connection

Name * Citrix

Connector

Select the connectors to use to sync this collection. If multiple connectors are available, you can add them and arrange them in fallback order. Only connectors associated with the same directory should be used.

ws1-connector.euc-livefire.com (LivefireSync)

Sync Integration Broker

Provide information about the Integration Broker that you want to use to sync resources.

Host * citrixbroker.euc-livefire.com

Port * 443

Use SSL Yes

SSL Certificate

```
-----BEGIN CERTIFICATE-----
MIIC/jCCAeagAwIBAgIQdyzLvZ4i/LlK8tN9IM9przANBgkqhkiG9w0BAQUFADAo
MSYwJAYDVQQDEx1DaXRyaXhCcm9rZXIuZXVjLWxpdmVmaXJlLmNvbTAeFw0xOTA0
MjQxMjAwMDFaFw0yMDA0MjQwMDAwMDBaMCgxJjAkBgNVBAMTHUNpdHJpeEJyb2tl
ci5ldWMtbGl2ZWZpcmUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAt5+cblKk9+KQa9enTFGiXi3thCwkvb6zgOz6COnd0X/lQfvwB21d6UQ/MRw8
k22f5FEd2sLj0UOiRdSq7xWgVus+L4Blit1bV1dYxJ0hYihB3YiC1oDR9Bv+a80J
/WeuECdbIq6VS/KbGFm9tjtwBRK9FdrGzn/gEXHAry4HB94rB84/aFb3Z7cW8azw
W8VivqDhn9UV2SsYtMbZ5+M5hIDY7XOD3XKB365+ggpczea5np0vGqgAFeyp6Y6I
eTBrvuDj5EiJ1BJHTBuIvLOoCH2IMzoITJocMo5q0fpL1w7HsrQ9KR8ntRpwsHPa
ax1qaXUd5mjlqHInmZBqMRPH0wIDAQABoyQwIjALBgNVHQ8EBAMCBDAwEwYDVR0l
BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEBAKH7/nr+8Qc04YzlpRuP
tPRH0lmjjWBd3/3IfqaYxL/Q0kYn1xjvu0sDTJHgfSmAZOY0vAsjQVT+CtL15QDm
mZL6dbvKnQv56mOzb7L8dqQK81IC9nF8MI6JFlUUg41SlkUYyTj+BQ7ozYH0Vv/5
k5KbpAoUY0rTjwFb9zKVmlKI88uduLBDk7XsHdXSWE0Y25pFeABW+xsmq/tZgJiV
MMBuYRmW017r9pBz2xUpxoSHurQdIL0Jer8D/XFgU4w3Ie4zH1OPWFq+2yV5tKVb
Rg57kamj2/8Nh8Zn6/a+vw9Yl1ce5Qkk4BU5Yhl7h2FiA6GzkznebWCc+rT2NG2s
kN0=
-----END CERTIFICATE-----
```

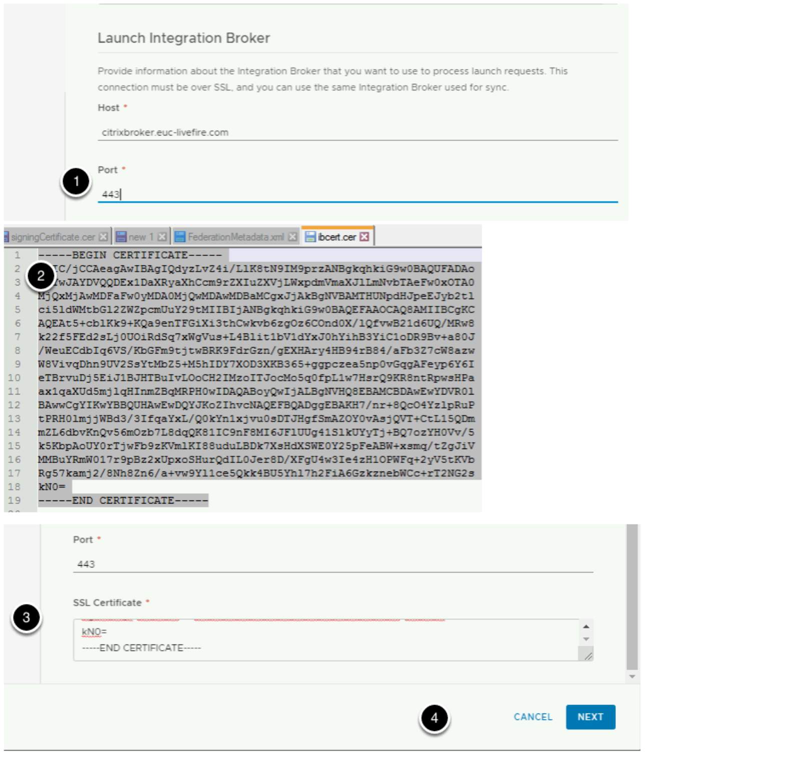
Use SSL Yes

SSL Certificate

-----BEGIN CERTIFICATE-----
MIIC/jCCAeagAwIBAgIQdyzLvZ4i/LlK8tN9IM9przANBgkqhkiG9w0BAQUFADAo

6. In **Section 1 Connector and Broker,** under Launch integration broker

1. Under **Host** type **citrixbroker.euc-livefire.com**
2. Under Port type **443**
3. Copy the contents of the **ibcert** file and Paste the **ssl certificate field**
4. In the **New Citrix Collection** window select **Next**



Provide information about the Integration Broker that you want to use to process launch requests. This connection must be over SSL, and you can use the same Integration Broker used for sync.

Host *

citrixbroker.euc-livefire.com

1 Port *

443

```
-----BEGIN CERTIFICATE-----
IC/jCCAeagAwIBAgIQdyzLvZ4i/L1K8tN9IM9przANBgkqhkiG9w0BAQUFADAo
/wJAYDVQQDEx1DaXRyaXhCcm9rZXIuZXVjLWxpdmVmaXJlLmNvbTAeFw0xOTA0
MjQxMjAwMDFaFw0yMDA0MjQwMDAwMDBaMCgxJjAkBgNVBAMTHUNpdHJpeEJyb2tl
ci5ldWMtbGl2ZWZpcmUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAt5+cblKk9+KQa9enTFGiXi3thCwkvb6zgOz6COnd0X/lQfvwB21d6UQ/MRw8
k22f5FEd2sLj0UOiRdSq7xWgVus+L4Blit1bV1dYxJ0hYihB3YiC1oDR9Bv+a80J
/WeuECdbIq6VS/KbGFm9tjtwBRK9FdrGzn/gEXHAry4HB94rB84/aFb3Z7cW8azw
W8VivqDhn9UV2SsYtMbZ5+M5hIDY7XOD3XKB365+ggpczea5np0vGqgAFeyp6Y6I
eTBrvuDj5EiJ1BJHTBuIvLOoCH2IMzoITJocMo5q0fpL1w7HsrQ9KR8ntRpwsHPa
ax1qaXUd5mjlqHInmZBqMRPH0wIDAQABoyQwIjALBgNVHQ8EBAMCBDAwEwYDVR0l
BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEBAKH7/nr+8QcO4YzlpRuP
tPRH0lmjjWBd3/3IfqaYxL/Q0kYn1xjvu0sDTJHgfSmAZOY0vAsjQVT+CtL15QDm
mZL6dbvKnQv56mOzb7L8dqQK81IC9nF8MI6JFlUUg41SlkUYyTj+BQ7ozYH0Vv/5
k5KbpAoUY0rTjwFb9zKVmlKI88uduLBDk7XsHdXSWE0Y25pFeABW+xsmq/tZgJiV
MMBuYRmW017r9pBz2xUpxoSHurQdIL0Jer8D/XFgU4w3Ie4zH1OPWFq+2yV5tKVb
Rg57kamj2/8Nh8Zn6/a+vw9Yl1ce5Qkk4BU5Yhl7h2FiA6GzkznebWCc+rT2NG2s
kN0=
-----END CERTIFICATE-----
```

Port *

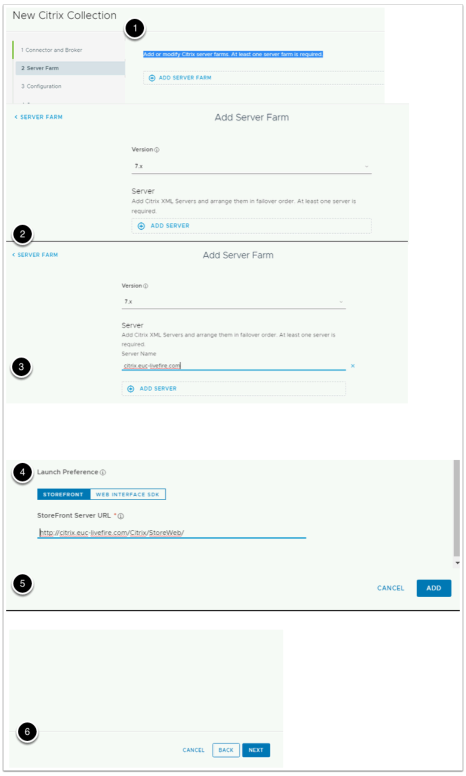
443

3 SSL Certificate *

kN0=
-----END CERTIFICATE-----

7. In the New **Citrix Collection** window, in **Section 2 Server Farm**

1. Under **Add or modify Citrix server farms. At least one server farm is required.** select the **+ ADD SERVER FARM**
2. On the **Add Server Farm** window select **+ADD SERVER**
3. Under Server Name type **citrix.euc-livefire.com**
4. Under the **Launch Preference,**
   - Verify **STOREFRONT** is selected
   - Under **StoreFront Server URL** type **http://citrix.euc-livefire.com/Citrix/StoreWeb/**
5. Select **ADD**
6. In the New **Citrix Collection** window select **NEXT**



New Citrix Collection

Add or modify Citrix server farms. At least one server farm is required.

Add Server Farm

Version: 7.x

Server
Add Citrix XML Servers and arrange them in failover order. At least one server is required.

Add Server Farm

Version: 7.x

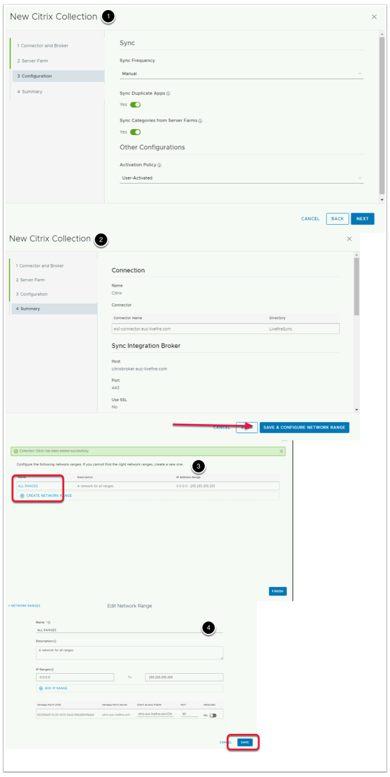
Server
Add Citrix XML Servers and arrange them in failover order. At least one server is required.
Server Name: citrix.euc-livefire.com

Launch Preference: STOREFRONT

StoreFront Server URL *: http://citrix.euc-livefire.com/Citrix/StoreWeb/

7. In the New **Citrix Collection** window

1. **in Section 3. Configuration** Accept the the default values and select **NEXT**
2. **Section 4. Summary**
   - Select **SAVE & CONFIGURE NETWORK RANGE**
3. On the **Network Ranges** window select **ALL RANGES**
4. Observe the defaults, in this lab there is no requirement to make changes, Select **CANCEL.**
5. You will land back at the **Virtual Apps Collection** Page



New Citrix Collection

Sync

Sync Frequency: Manual

Sync Duplicate Apps: Yes

Sync Categories from Server Farms: Yes

Other Configurations

Activation Policy: User-Activated

Connection

Name: Citrix

Connector

Connector Name	Directory
ws1-connector.euc-livefire.com	LivefireSync

Sync Integration Broker

Host: citrixbroker.euc-livefire.com

Port: 443

Use SSL: No

Collection 'Citrix' has been added successfully.

Configure the following network ranges. If you cannot find the right network ranges, create a new one.

Name	Description	IP Address Range
ALL RANGES	A network for all ranges	0.0.0.0 - 255.255.255.255

Edit Network Range

Name: ALL RANGES

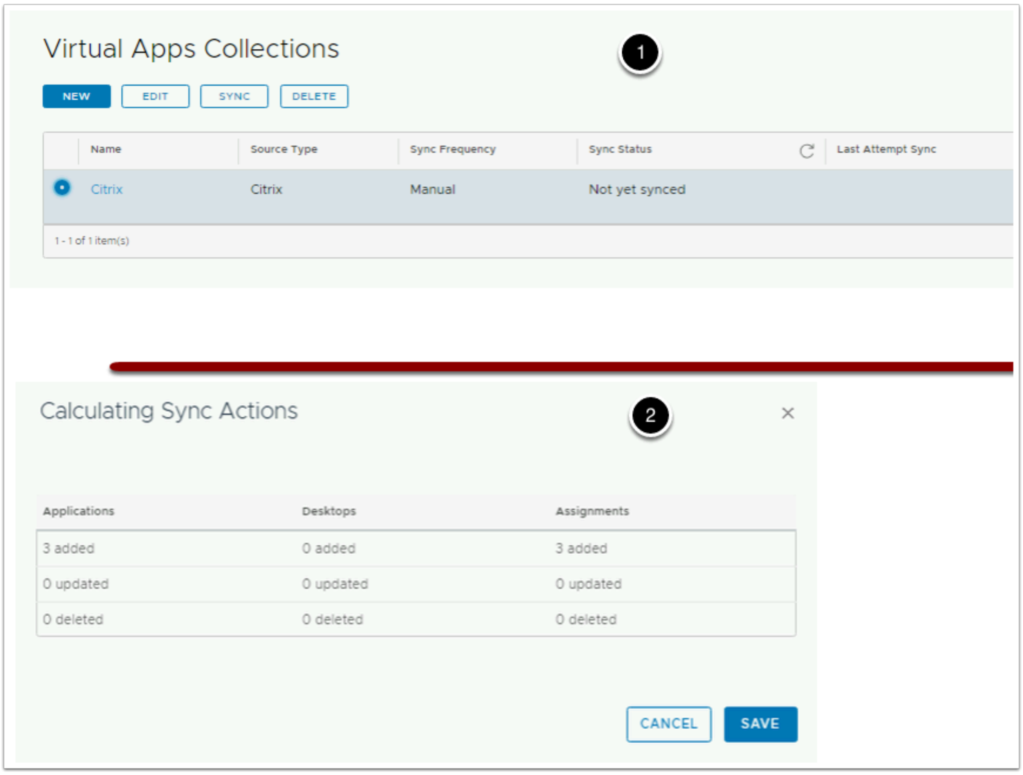
Description: A network for all ranges

IP Ranges: 0.0.0.0 To 255.255.255.255

XenApp Farm UUID	XenApp Farm Server	Client Access FQDN	Port	NetScaler
853356e9-5c30-4210-9ad2-69e2854f6ae6	citrix.euc-livefire.com	citrix.euc-livefire.com/Citr	80	No

8.

- In the **Virtuals APPs Collections** window
  1. Select the radio button next to Citrix, Select the **SYNC** button
  2. On the **Calculating Sync Actions** page select SAVE



Virtual Apps Collections

	Name	Source Type	Sync Frequency	Sync Status	Last Attempt Sync
●	Citrix	Citrix	Manual	Not yet synced	

1 - 1 of 1 item(s)

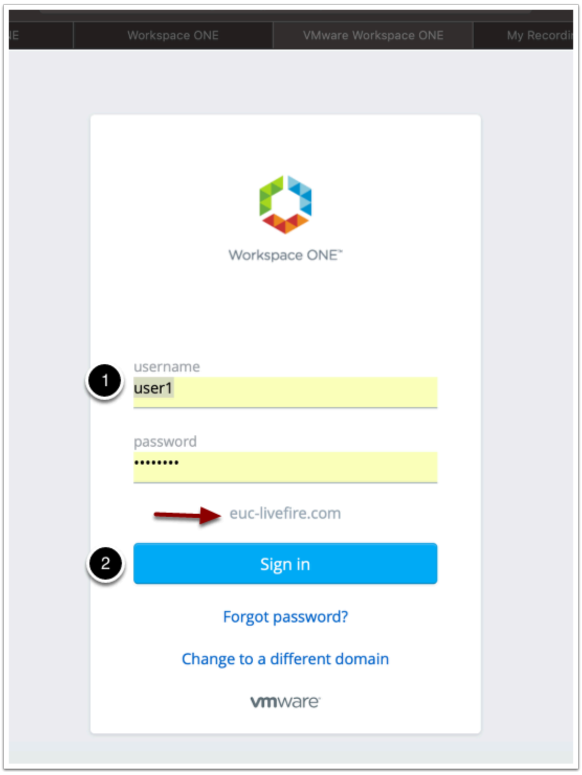
Calculating Sync Actions

Applications	Desktops	Assignments
3 added	0 added	3 added
0 updated	0 updated	0 updated
0 deleted	0 deleted	0 deleted

Part 2 - Verification

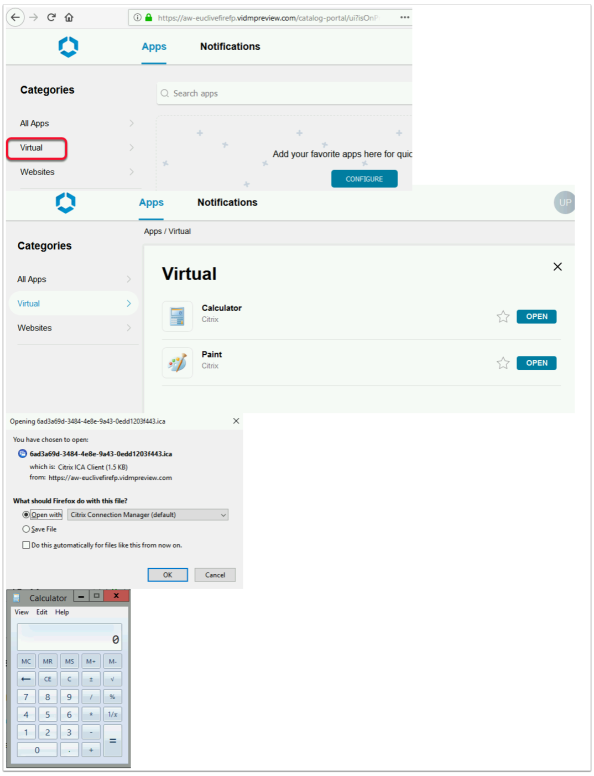
1. From your **ControlCenter** machine's **chrome** browser open your custom **Vmware identity Manager** SaaS tenant url

2. Log in with your **user1** credential, in the **euc-livefire.com** authentication domain with the password VMware1!



3.

1. In the **Web based Hub interface** under Categories select **Virtual**
2. Under the **Virtual Category** next Calculator select **OPEN**
3. If you are in Mozilla Firefox you will be prompted with **What Should Firefox do with this file? Accept the default** and select **OK**
4. You can now observe the integration of **Citrix** into **VMware Identity Manager.**



Opening 6ad3a69d-3484-4e8e-9a43-0edd1203f443.ica

You have chosen to open:

6ad3a69d-3484-4e8e-9a43-0edd1203f443.ica

which is: Citrix ICA Client (1.5 KB)

from: https://aw-euclivefirefp.vidmpreview.com

What should Firefox do with this file?

● Open with Citrix Connection Manager (default)

○ Save File

□ Do this automatically for files like this from now on.

OK Cancel

OKTA Integration with Workspace ONE Access

Scenario and Objectives of this Lab Module

We will come into to many existing environments and they will already have existing Federations in place. We will see what is required when the customer has **OKTA** Federated with existing Applications.

OKTA sees **Workspace ONE Access** as their go to market solution for cross-platform SSO solutions and have officially deprecated the MDM component in favour of using Workspace ONE

In this scenario **OKTA** could be the first point of call and we would use **Workspace ONE Access** to authenticate and provide SSO access to mobile devices and **Workspace ONE UEM** to manage compliance

Please note we will complete the testing of this lab in the latter part of this course once we have **Mobile SSO for Android** and **Mobile SSO for IOS** for **Workspace ONE Access**.

This lab is comprised of 5 parts

Part 1. Configuring an **OKTA** individual developer account.

Part 2. Federating **OKTA** with **Workspace ONE Access.**

Part 3. Federating **BambooHR** with **OKTA.**

Part 4. Configuring **Workspace ONE Access** to be an **OKTA** application source.

Note! After we have setup Single Sign On for Android and IOS. We will then Configure Conditional Access policies in Workspace One UEM, then we will test the integrations for SSO through **OKTA, VMware Identity Manger** and **Workspace ONE UEM.**

Just a reminder that when creating custom Accounts. Be sure to write down the exact details related to this account. One suggestion might be to standardize on passwords and keep the password as simple as possible, to ensure success of these labs. In the future if you have concerns related to accessing these accounts feel free to reset the passwords.

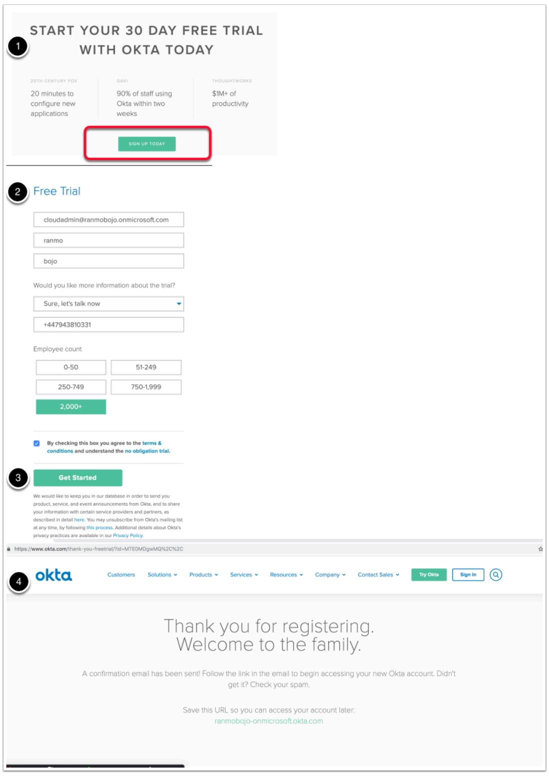
Failure to follow these guidelines could result in being locked out of your tenant and you would then have to take for responsibility for regaining access leading to a loss of time.

Part 1. Setting up an OKTA Overview free trial

1. Setting up an OKTA Overview free trial (PART 1)

- In this section we will register a 30 day free trial with OKTA account that we will use for this lab. It can be used beyond the scope of this lab as well and does not expire.

1. Open your **Chrome Browser** on the Control Center and browse to **https://www.okta.com/free-trial/#** On the **START YOUR 30 DAY FREE TRIAL WITH OKTA TODAY** page select **SIGN UP TODAY**
2. Fill in the **Free Trial** Form
   1. Using either a ***work e-mail address*** or your ***custom office365 CloudAdmin email account eg. cloudadmin@ranmobojo.onmicrosoft.com.*** Fill in your **first** and ***last name***
      - ***Do not use a EUC-Livefire.com email address.***
   2. In the drop down ***Would you like more information about the trial?*** select Yes....
   3. In the phone area type a valid phone number
   4. Under Employee count select a one the numbered check boxes
3. Select **Get Started**
4. Notice you have a **Thank You for registering. Welcome to the family.** NB! NOTE the url and save your unique URL to notepad e.g. ranmobojo-onmicrosoft.okta.com



START YOUR 30 DAY FREE TRIAL WITH OKTA TODAY

20TH CENTURY FOX: 20 minutes to configure new applications

GAVI: 90% of staff using Okta within two weeks

THOUGHTWORKS: $1M+ of productivity

Free Trial

cloudadmin@ranmobojo.onmicrosoft.com

ranmo

bojo

Would you like more information about the trial?

Sure, let's talk now

+447943810331

Employee count

0-50 | 51-249 | 250-749 | 750-1,999 | 2,000+

☑ By checking this box you agree to the terms & conditions and understand the no obligation trial.

We would like to keep you in our database in order to send you product, service, and event announcements from Okta, and to share your information with certain service providers and partners, as described in detail here. You may unsubscribe from Okta's mailing list at any time, by following this process. Additional details about Okta's privacy practices are available in our Privacy Policy.

https://www.okta.com/thank-you-freetrial/?id=MTE0MDgwMQ%2C%2C

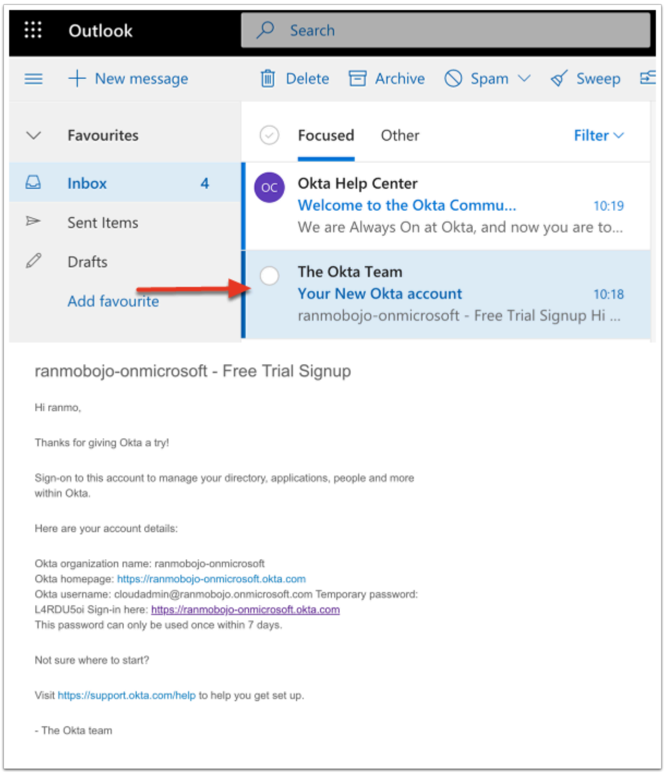
Thank you for registering.
Welcome to the family.

A confirmation email has been sent! Follow the link in the email to begin accessing your new Okta account. Didn't get it? Check your spam.

Save this URL so you can access your account later:
ranmobojo-onmicrosoft.okta.com

2. Setting up an OKTA Overview free trial (PART 1)

- Go to **Office 365** . Log-in to office.com with your ***Cloud Admin account*** and check your office 365 email. **Open** your email from the ***The Okta Team***
- Click on the **sign in here** URL



OC Okta Help Center
Welcome to the Okta Commu... 10:19
We are Always On at Okta, and now you are to...

The Okta Team
Your New Okta account 10:18
ranmobojo-onmicrosoft - Free Trial Signup Hi ...

ranmobojo-onmicrosoft - Free Trial Signup

Hi ranmo,

Thanks for giving Okta a try!

Sign-on to this account to manage your directory, applications, people and more within Okta.

Here are your account details:

Okta organization name: ranmobojo-onmicrosoft
Okta homepage: https://ranmobojo-onmicrosoft.okta.com
Okta username: cloudadmin@ranmobojo.onmicrosoft.com Temporary password:
L4RDU5oi Sign-in here: https://ranmobojo-onmicrosoft.okta.com
This password can only be used once within 7 days.

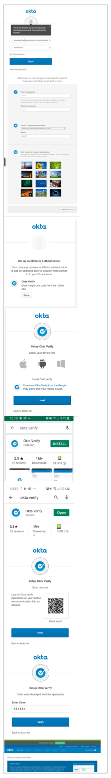
Not sure where to start?

Visit https://support.okta.com/help to help you get set up.

- The Okta team

3. Setting up an OKTA Overview free trial (PART 1)

- . In the **Login console** use your Okta username the **temporary password**. Select **Sign In.** On the **Welcome** window ,
  1. **Enter** and **Confirm** your **new password,**
  2. Choose a **forgot password question** and **Answer**
  3. Click a picture to choose a **security image**
  4. Select **Create My Account**
  5. On the **Set up multifactor Authentication** page select **Setup**
  6. On the **Setup Okta Verify** page. Complete the following
     1. Choose your device type. (either windows, Android or IOS) In this setup we will demonstrate Android .
     2. **Download and install** the Okta Verify Application. When done open the Okta Verify application on your Device.
     3. Select **Next**
  7. On the **Scan Barcode,** page using your device ***Scan your Barcode*** and select **Next**
  8. On the **Enter Code** page, enter your device Code and select **Verify**
  9. On the **Getting Started with Okta** window notice you now have a 30 day trial of OKTA. Browse around to familiarize with the Console.



Welcome to ranmobojo-onmicrosoft, ranmo!
Create your ranmobojo-onmicrosoft account

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

Enter single-use code from the mobile app.

Download Okta Verify from the Google Play Store onto your mobile device.

Launch Okta Verify application on your mobile device and select Add an account.

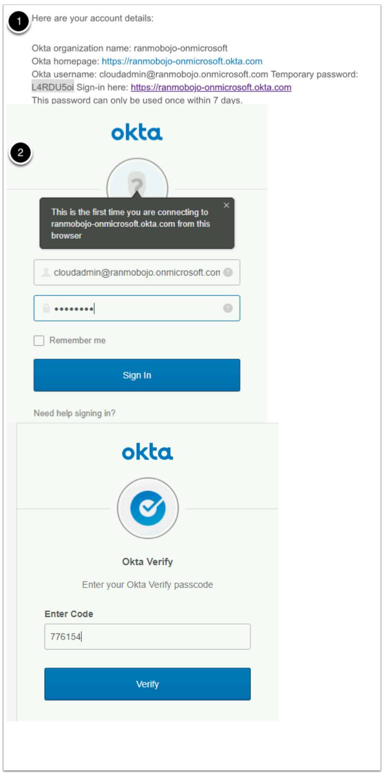
Enter code displayed from the application

4. Setting up an OKTA Overview free trial (PART 1)

- To complete our setup we will setup Directory sync with your EUC-Livefire Active Directory Domain you and your OKTA environment.

  Log into your **"on-prem" lab** environment as **euc-livefire.com\administrator** with the password **VMware1!**

  1. On the **ControlCenter2** server open your **chrome browser** and copy **OKTA url** on the ControlCenter server. e.g. https://ranmobojo-onmicrosoft.okta.com/
  2. Sign in with your **OKTA admin console** with your OKTA ***username*** and ***password*** select **Sign In**
  3. Use your Okta Verify Code to sign in



1 Here are your account details:

Okta organization name: ranmobojo-onmicrosoft
Okta homepage: https://ranmobojo-onmicrosoft.okta.com
Okta username: cloudadmin@ranmobojo.onmicrosoft.com Temporary password: L4RDU5oi Sign-in here: https://ranmobojo-onmicrosoft.okta.com
This password can only be used once within 7 days.

2

This is the first time you are connecting to ranmobojo-onmicrosoft.okta.com from this browser

cloudadmin@ranmobojo.onmicrosoft.con

••••••••

□ Remember me

Okta Verify

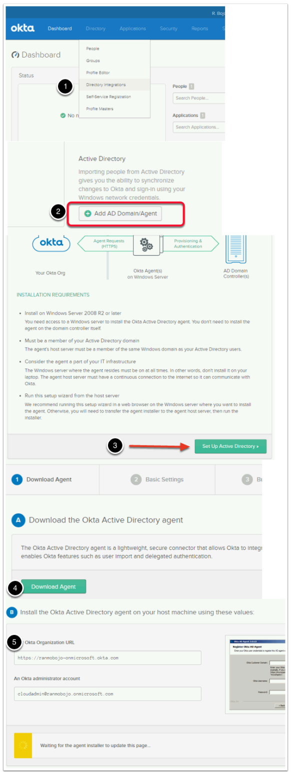
Enter your Okta Verify passcode

Enter Code: 776154

5. Setting up an OKTA Overview free trial (PART 1)

Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. In the Okta Admin console select **Directory** > **Directory Integrations**
2. In the **Directory Integrations** interface, bottom right-hand corner, select **Add AD Domain/ Agent**
3. Select **Set Up Active Directory** in the bottom right-hand corner
4. Select **Download Agent,**
5. Note the ***installation information*** on your admin Console, you will use this information when installing the agent.



Active Directory

Importing people from Active Directory gives you the ability to synchronize changes to Okta and sign-in using your Windows network credentials.

INSTALLATION REQUIREMENTS

- Install on Windows Server 2008 R2 or later
  You need access to a Windows server to install the Okta Active Directory agent. You don't need to install the agent on the domain controller itself.
- Must be a member of your Active Directory domain
  The agent's host server must be a member of the same Windows domain as your Active Directory users.
- Consider the agent a part of your IT infrastructure
  The Windows server where the agent resides must be on at all times. In other words, don't install it on your laptop. The agent host server must have a continuous connection to the internet so it can communicate with Okta.
- Run this setup wizard from the host server
  We recommend running this setup wizard in a web browser on the Windows server where you want to install the agent. Otherwise, you will need to transfer the agent installer to the agent host server, then run the installer.

A Download the Okta Active Directory agent

The Okta Active Directory agent is a lightweight, secure connector that allows Okta to integr enables Okta features such as user import and delegated authentication.

B Install the Okta Active Directory agent on your host machine using these values:

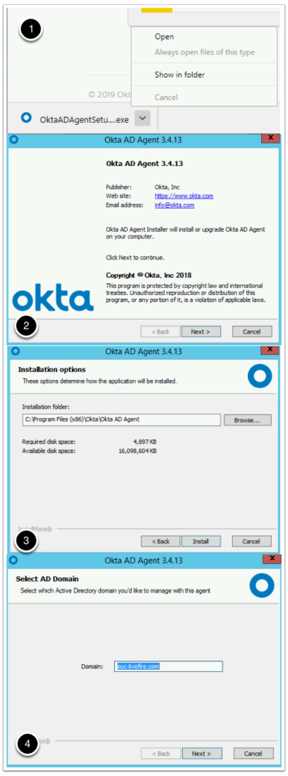
Okta Organization URL
https://ranmobojo-onmicrosoft.okta.com

An Okta administrator account
cloudadmin@ranmobojo.onmicrosoft.com

Waiting for the agent installer to update this page...

6. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. in your control center VM Select the downloaded **OktaADAgentSetup.exe** and select **Open** select **Run**
2. On the downloaded Okta AD Agent, select **Next**
3. On the **Installation options** window select **Install**
4. In the **Select AD Domain** window *accept your **default Domain*** and select **Next**



Okta AD Agent 3.4.13

Okta AD Agent 3.4.13

Publisher: Okta, Inc
Web site: https://www.okta.com
Email address: info@okta.com

Okta AD Agent Installer will install or upgrade Okta AD Agent on your computer.

Click Next to continue.

Copyright © Okta, Inc 2018

This program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, is a violation of applicable laws.

Okta AD Agent 3.4.13

Installation options

These options determine how the application will be installed.

Installation folder: C:\Program Files (x86)\Okta\Okta AD Agent

Required disk space: 4,897 KB
Available disk space: 16,098,604 KB

Okta AD Agent 3.4.13

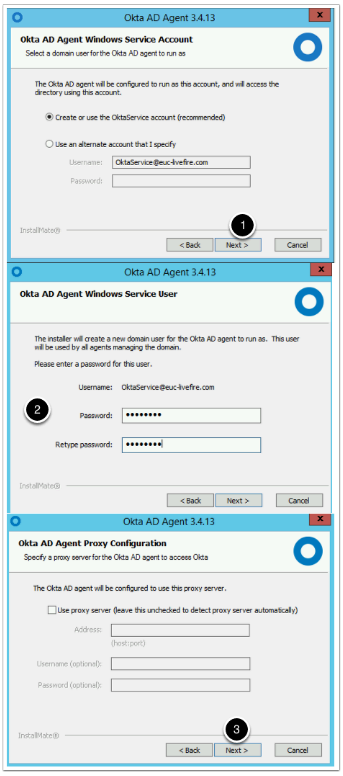
Select AD Domain

Select which Active Directory domain you'd like to manage with this agent

Domain: euc-livefire.com

7. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. On the **Okta AD Agent Windows Service Account** window ***accept the default,*** select **Next**
2. On the **Okta AD Agent Windows Service User**, type and **confirm** the **password, VMware1!** select **Next**
3. On the **Okta AD Agent Proxy Configuration** window, select **Next**



Okta AD Agent 3.4.13

Okta AD Agent Windows Service Account

Select a domain user for the Okta AD agent to run as

The Okta AD agent will be configured to run as this account, and will access the directory using this account.

● Create or use the OktaService account (recommended)

○ Use an alternate account that I specify

Username: OktaService@euc-livefire.com

Password:

Okta AD Agent 3.4.13

Okta AD Agent Windows Service User

The installer will create a new domain user for the Okta AD agent to run as. This user will be used by all agents managing the domain.

Please enter a password for this user.

Username: OktaService@euc-livefire.com

Password: ••••••••

Retype password: ••••••••

Okta AD Agent 3.4.13

Okta AD Agent Proxy Configuration

Specify a proxy server for the Okta AD agent to access Okta

The Okta AD agent will be configured to use this proxy server.

□ Use proxy server (leave this unchecked to detect proxy server automatically)

Address:

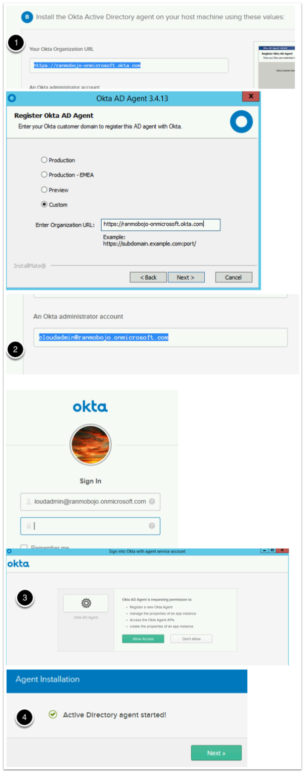
(host:port)

Username (optional):

Password (optional):

8. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. On the **Register Okta AD Agent** window, select the Custom radio button, next to Enter Organizational URL: in the **Enter Organizagtion URL:** box type ***your Organization URL*** Select **Next**
2. In the **Sign in** page under **Username**, type the ***OKTA Administrator account*** and ***password*** and select **Sign In**
3. Select **Allow Access**
4. On the Agent Installation window select **Next**



Install the Okta Active Directory agent on your host machine using these values:

1 Your Okta Organization URL: https://ranmobojo-onmicrosoft.okta.com

Okta AD Agent 3.4.13

Register Okta AD Agent

Enter your Okta customer domain to register this AD agent with Okta.

○ Production
○ Production - EMEA
○ Preview
● Custom

Enter Organization URL: https://ranmobojo-onmicrosoft.okta.com

Example:
https://subdomain.example.com:port/

2 An Okta administrator account: cloudadmin@ranmobojo.onmicrosoft.com

Sign In: loudadmin@ranmobojo.onmicrosoft.com

3 Sign into Okta with agent service account

Okta AD Agent is requesting permission to:

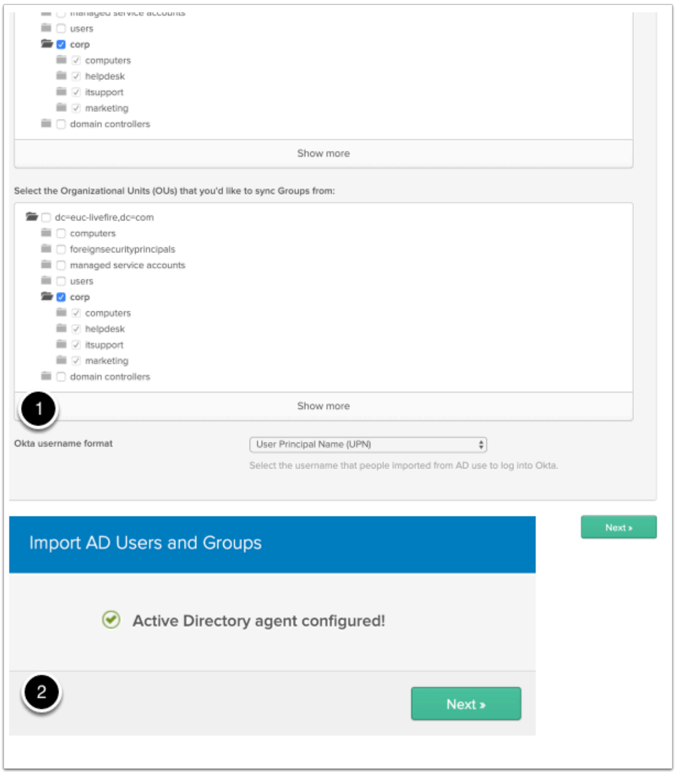
- Register a new Okta Agent
- manage the properties of an app instance
- Access the Okta Agent APIs
- create the properties of an app instance

4 Agent Installation

Active Directory agent started!

9. Setting up Directory sync with our Active Domain and this OKTA environment continued..

1. In the **Set Up Active Directory** window , In the **Connect an Organizational Units (OU) to Okta i**nterface ensure that only **corp ou** is selected in the **users** and **groups** interface. Select **Next**
2. In the **Import Ad Users and Groups** window select **Next**



managed service accounts
□ users
☑ corp
✓ computers
✓ helpdesk
✓ itsupport
✓ marketing
□ domain controllers

Select the Organizational Units (OUs) that you'd like to sync Groups from:

□ dc=euc-livefire,dc=com
□ computers
□ foreignsecurityprincipals
□ managed service accounts
□ users
☑ corp
✓ computers
✓ helpdesk
✓ itsupport
✓ marketing
□ domain controllers

Okta username format: User Principal Name (UPN)

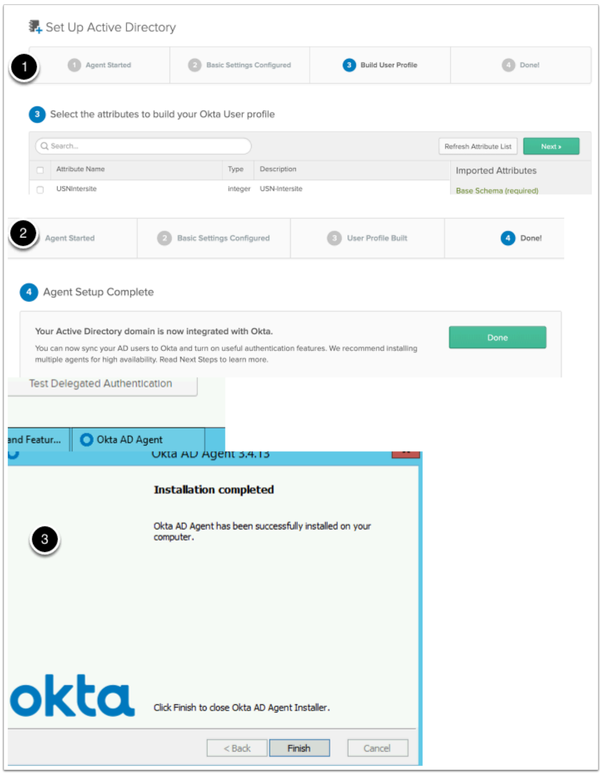
Select the username that people imported from AD use to log into Okta.

Import AD Users and Groups

Active Directory agent configured!

10. Setting up Directory sync with our Active Domain and this OKTA environment continued....

1. On the **Select the attributes to build your Okta User profile** page select **Next**
2. On the **Agent Setup Complete** page select **Done**
3. Select the **Okta AD Agent** on your Taskbar and select **Finish**



Set Up Active Directory

3 Select the attributes to build your Okta User profile

	Attribute Name	Type	Description
□	USNIntersite	integer	USN-Intersite

Imported Attributes

Base Schema (required)

4 Agent Setup Complete

Your Active Directory domain is now integrated with Okta.

You can now sync your AD users to Okta and turn on useful authentication features. We recommend installing multiple agents for high availability. Read Next Steps to learn more.

Okta AD Agent 3.4.13

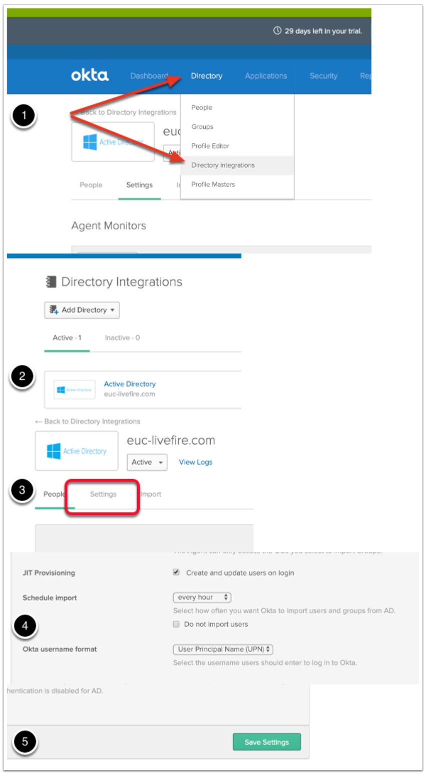
Installation completed

Okta AD Agent has been successfully installed on your computer.

Click Finish to close Okta AD Agent Installer.

11. Setting up Directory sync with our Active Domain and this OKTA environment continued....

1. In the **Okta admin** console select **Directory** > **Directory Integrations**
2. Below the **Active** tab select **Active Directory**
3. In the **Active Directory** area next to **People** select **Settings**
4. In the **IMPORT AND ACCOUNT SETTINGS** console scroll down and select the following:-
    1. Select the **check box** in line with **JIT Provisioning** called ***Create and update users on login***
    2. Next to **Schedule import** change the **dropdown** from **never** to **every hour**
5. Scroll down to the bottom and select **Save Settings**



JIT Provisioning ☑ Create and update users on login

Schedule import: every hour

Select how often you want Okta to import users and groups from AD.

□ Do not import users

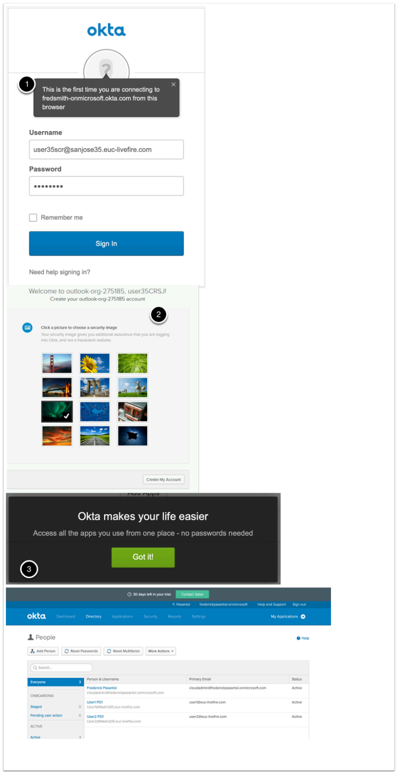
Okta username format: User Principal Name (UPN)

Select the username users should enter to log in to Okta.

hentication is disabled for AD.

12. We will validate our provisioning of user provision now in OKTA

1. Open up an **Incognito window** in your browser and launch your **OKTA login URL.** Login with **your custom user account** user eg **user35SCR@sanjose35.euc-livefire.com** with password **VMware1!** select **Sign In**
2. On the **Welcome to your OKTA page**, click a ***picture to choose a security image*** , select **Create My Account**
3. Close the **OKTA IS THE IDENTITY STANDARD** page by selecting **Got it** on the bottom right hand corner.
4. If you go back to your **OKTA admin Console**, select **Directory** > **People**, you will now notice your provisioned users



This is the first time you are connecting to fredsmith-onmicrosoft.okta.com from this browser

Username: user35scr@sanjose35.euc-livefire.com

Password: ••••••••

□ Remember me

Welcome to outlook-org-275185, user35CRSJ!
Create your outlook-org-275185 account

Click a picture to choose a security image
Your security image gives you additional assurance that you are logging into Okta, and not a fraudulent website.

Okta makes your life easier
Access all the apps you use from one place - no passwords needed

30 days left in your trial.

F. Pasantol · frederickpasantol-onmicrosoft · Help and Support · Sign out

Person & Username	Primary Email	Status
Frederick Pasantol cloudadmin@frederickpasantol.onmicrosoft.com	cloudadmin@frederickpasantol.onmicrosoft.com	Active
User1 PD1 User1@Madrid35.euc-livefire.com	user1@euc-livefire.com	Active
User2 PD1 User2@Madrid35.euc-livefire.com	user2@euc-livefire.com	Active

Part 2. OKTA and Workspace ONE Access Federation Configuration

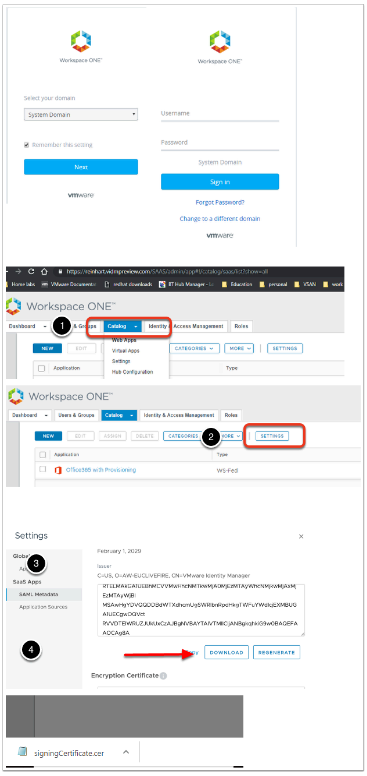
Summary

We have accomplished a few things in Part 1 . You have seen how well **Just In Tme (JIT)** provisioning works with external applications and OKTA. OKTA supports a much broader ecosystem of applications than Workspace ONE Access. This part of the lab would represent what an organisation might already have in place or it might represent what we might have put in place first before using Workspace ONE Access. A very important concept to realize is if we are going to federate 3rd party solutions we have to have a basic understanding of the workings / capabilities of the solution we want to federate with to offer the best solution to the customer.
Okta themselves realize that VMware have a very powerful Single-Sign On (SSO) solution using Workspace ONE. We will now federate with Workspace ONE Access.

In this section we will retrieve information required by Okta to setup an Identity Provider . In this scenario Workspace ONE Access will be the Identity Provider.

1. Login to the **Workspace ONE Administration Console** on the **System Domain** with ***Admin*** privileges to your New SaaS Workspace ONE Access Tenant.
    1. Select the **Catalog** -> **Web Apps** tab
    2. To the right select the **Settings** button from the sub-menu
    3. In the resulting dialog navigate to **SaaS Apps** -> **SAML Metadata**

4. Download the **Signing Certificate**. Note the location of the downloaded file ***signingCertificate.cer***



February 1, 2029

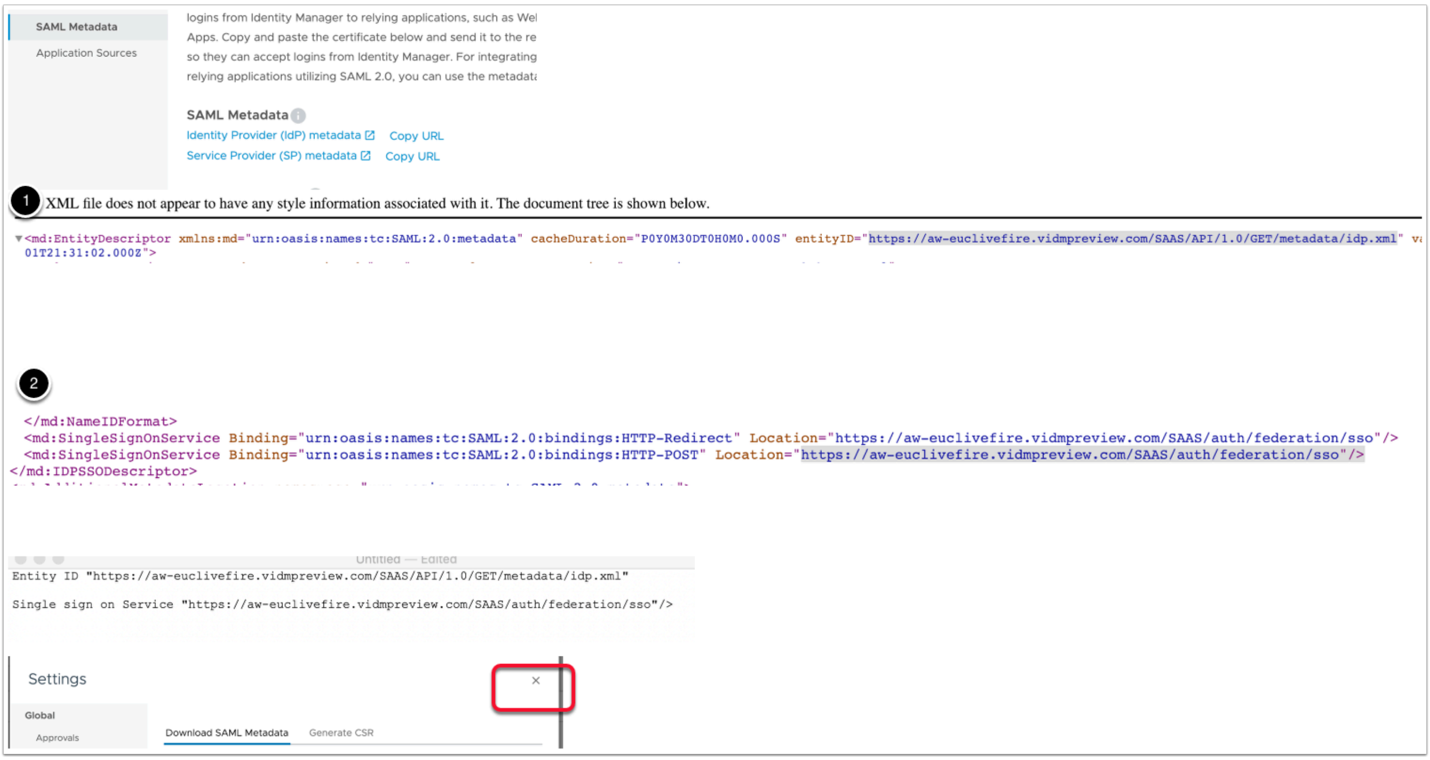
Issuer

C=US, O=AW-EUCLIVEFIRE, CN=VMware Identity Manager

```
RTELMAkGA1UEBhMCVVMwHhcNMTkwMjA0MjEzMTAyWhcNMjkwMjAxMj
EzMTAyWjBI
MSAwHgYDVQQDDBdWTXdhcmUgSWRlbnRpdHkgTWFuYWdlcjEXMBUG
A1UECgwOQVct
RVVDTEIWRUZJUkUxCzAJBgNVBAYTAlVTMIICIjANBgkqhkiG9w0BAQEFA
AOCAg8A
```

2. Part 2. OKTA and Workspace ONE Access Federation Configuration

- In the right pane under **SAML Metadata**, click on **Identity Provider (Idp) Metadata** link and record and save the following 2 configurations using **Notepad**
  1. *Next to* **entityID** copy ***your version*** of the following url from the address bar **:** **e.g. https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml**
  2. Search for **urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST** and next to **Location** copy **your version** of the following: **"**https://aw-livefirerplaston.vidmpreview.com/SAAS/auth/federation/sso"
  3. *Select **X** in the right hand corner of the pane to close the window*



logins from Identity Manager to relying applications, such as Wel
Apps. Copy and paste the certificate below and send it to the re
so they can accept logins from Identity Manager. For integrating
relying applications utilizing SAML 2.0, you can use the metadat‹

SAML Metadata

Identity Provider (IdP) metadata Copy URL

Service Provider (SP) metadata Copy URL

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://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml" va
 01T21:31:02.000Z">
```

```
  </md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
</md:IDPSSODescriptor>
```

Untitled — Edited

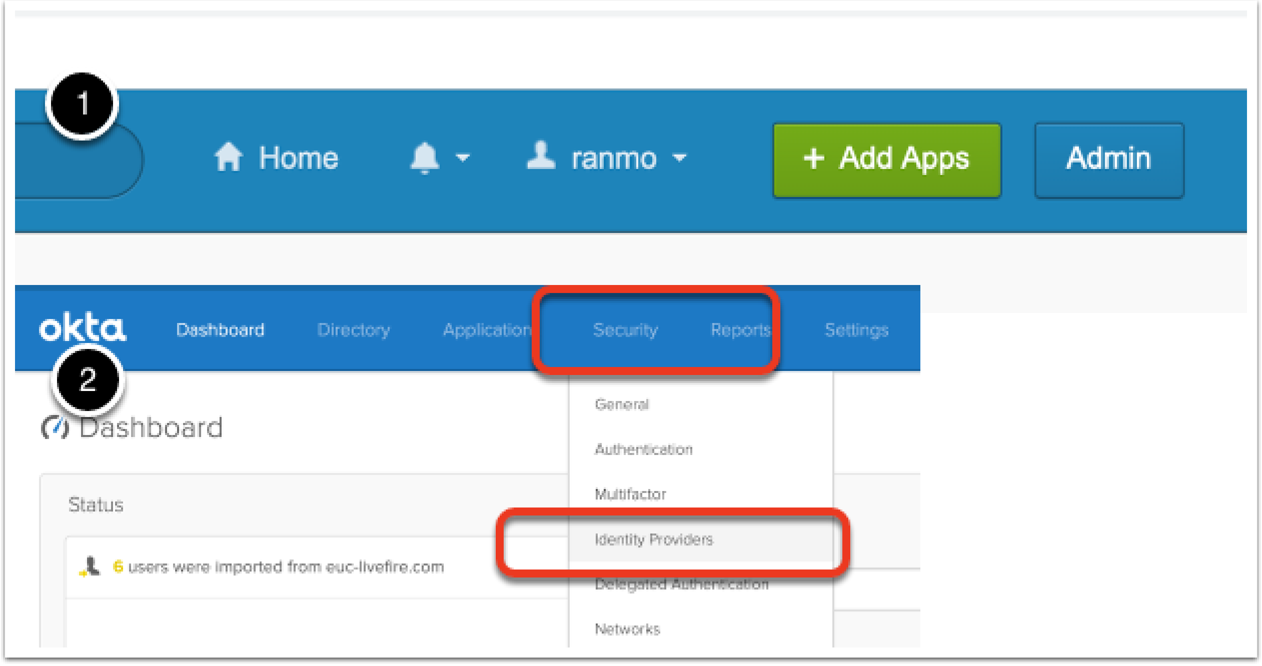
```
Entity ID "https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml"

Single sign on Service "https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso"/>
```

3. *Part 2. OKTA and Workspace ONE Access Federation Configuration*

- In this section we will create the Identity Provider (IdP) record in the **Okta admin UI** with system
  Administrator login.

In the OKTA admin Console (on your Chrome browser)

1. If required, In the top right hand corner. Select the **Admin** button
2. Navigate to **Security** -> Identity Providers

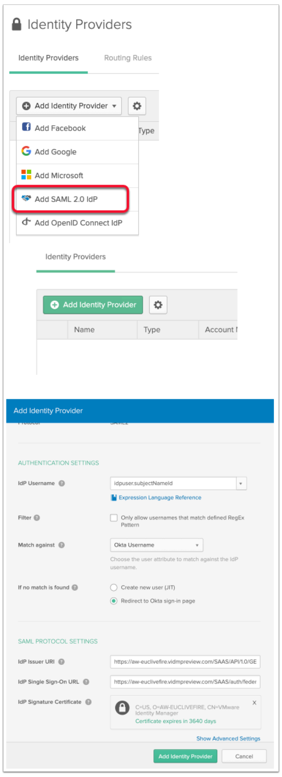


4. *Part 2. OKTA and Workspace ONE Access Federation Configuration*

- **In the OKTA admin Console continued...**
  1. Select **Add Identity Provider** button window, select **Add SAML 2.0 Idp** :
  2. Under **GENERAL SETTINGS** next to **Name**: type ***WorkspaceONE***
  3. Under **AUTHENTICATION SETTINGS**
     1. **Idp UserName :** idpuser.subjectNameid
     2. **Filter:** ***Unchecked***
     3. **Match Against:** ***Okta Username***
     4. **If no match is found:** ***Redirect to Okta sign-in page*** radio button

  4. Under **SAML PROTOCOL SETTINGS**
     1. **IdP Issuer URI: e.g. https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GET/metadata/idp.xml**
        Entity ID value value from the Workspace ONE Access IdP metadata file saved to Notepad
     2. **IdP Single Sign-On URL:** e.g. **https://aw-euclivefire.vidmpreview.com/SAAS/auth/federation/sso**
        (*Single Sign on Service value from IdP metadata file from the Workspace ONE Access Idp metadata file)*
     3. **IdP Signature Certificate. Browse** , select **All files** next to filename and **select the Signing Certificate** from your SAAS Workspace ONE Access Tenant. *If your cer files is greyed out, make sure you are using **Chrome** as your browser.*

  5. Select **Add Identity Provider**



AUTHENTICATION SETTINGS

IdP Username: idpuser.subjectNameId

Expression Language Reference

Filter: □ Only allow usernames that match defined RegEx Pattern

Match against: Okta Username

Choose the user attribute to match against the IdP username.

If no match is found: ○ Create new user (JIT) ● Redirect to Okta sign-in page

SAML PROTOCOL SETTINGS

IdP Issuer URI: https://aw-euclivefire.vidmpreview.com/SAAS/API/1.0/GE

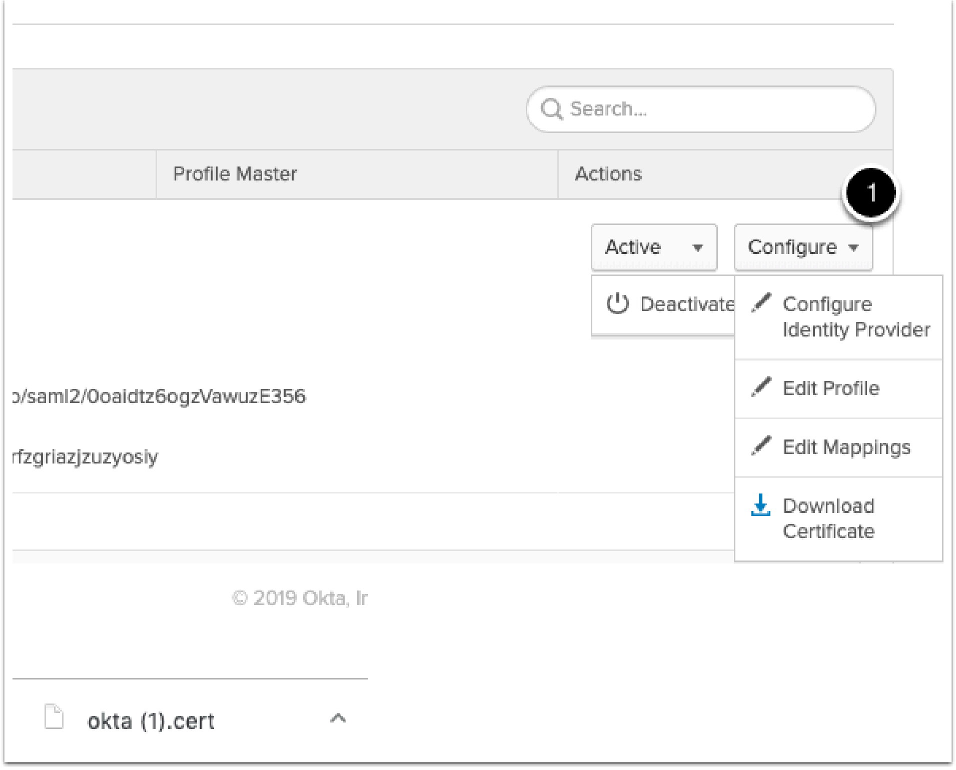
IdP Single Sign-On URL: https://aw-euclivefire.vidmpreview.com/SAAS/auth/feder

IdP Signature Certificate: C=US, O=AW-EUCLIVEFIRE, CN=VMware Identity Manager

Certificate expires in 3640 days

5. *Part 2. OKTA and Workspace ONE Access Federation Configuration*

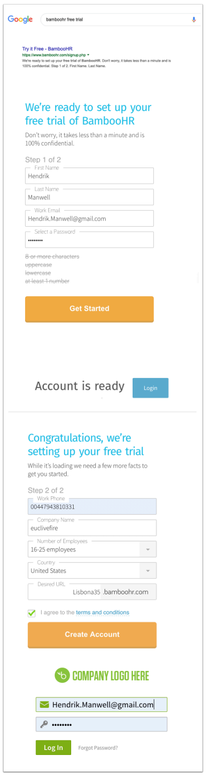
- **In the OKTA admin Console continued...**
  - In the **Identity Providers** interface, to the right, select the **drop down arrow** next to **Configure** and select **Download Certificate**



Part 3: Federating BambooHR with OKTA

1. Federation of BambooHR with OKTA (Part 3)

- In this section we setup a Federation with BambooHR web application. You are entitled to a 7 day trial of the BambooHR SaaS software.
  1. We will start off by going to a **browser** and In google type **BambooHR free trial.**
  2. Where it says **Try it Free** select
  3. In the **Were Ready to you up page** aenter the following credentials
     - **First Name** *(same First Name you registered with OKTA)*
     - **Last Name** *(same Last Name you registered with OKTA)*
     - **Work email address,** (same email address you registered with OKTA)
     - **Select a Password** (VMware1!)
  4. Select Get Started
  5. On the **Congratulations page** type your
     - work phone number, your phone number
     - **company Name,** eg. Euclivefire
     - **custom domain name** eg. Madrid34.bamboohr.com
  6. Select **Create Account**
  7. On the **Account is ready page** select **Login**
  8. On the login page , login with your email and password



bamboohr free trial

Try it Free - BambooHR
https://www.bamboohr.com/signup.php
We're ready to set up your free trial of BambooHR. Don't worry, it takes less than a minute and is 100% confidential. Step 1 of 2. First Name. Last Name.

We're ready to set up your free trial of BambooHR

Don't worry, it takes less than a minute and is 100% confidential.

Step 1 of 2

First Name: Hendrik

Last Name: Manwell

Work Email: Hendrik.Manwell@gmail.com

Select a Password: ••••••••

~~8 or more characters~~
~~uppercase~~
~~lowercase~~
~~at least 1 number~~

Account is ready

Congratulations, we're setting up your free trial

While it's loading we need a few more facts to get you started.

Step 2 of 2

Work Phone: 00447943810331

Company Name: euclivefire

Number of Employees: 16-25 employees

Country: United States

Desired URL: Lisbona35 .bamboohr.com

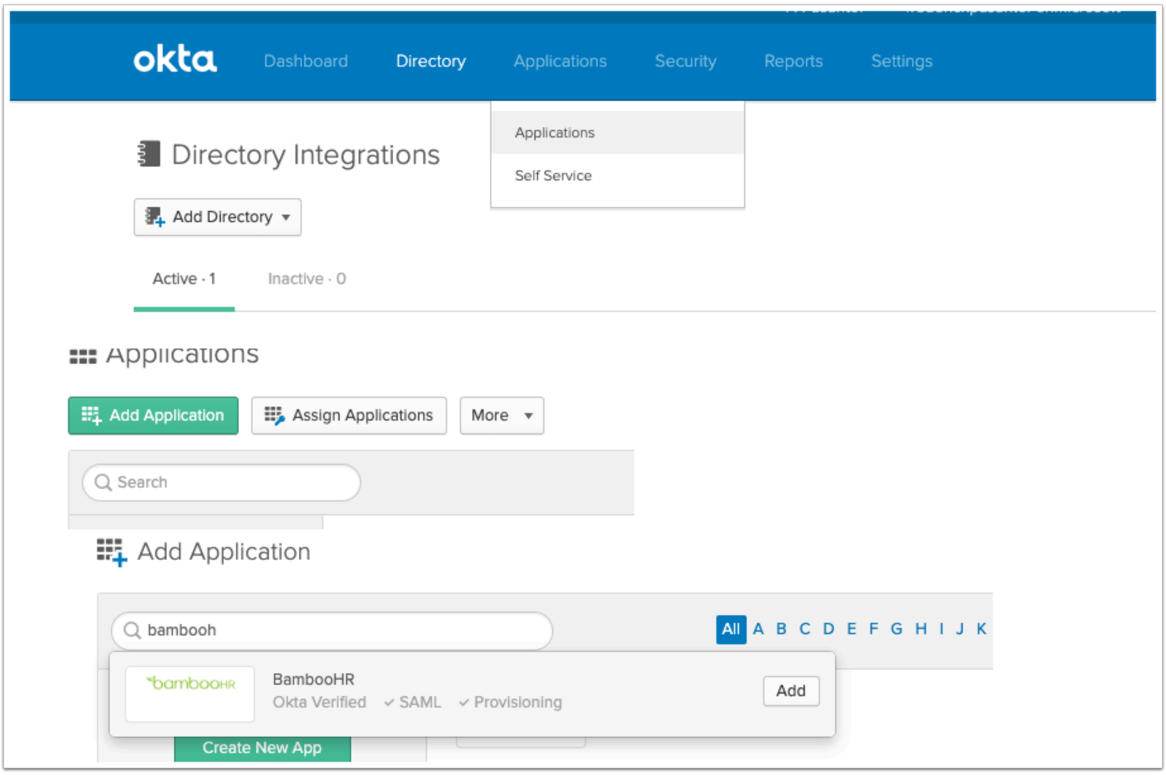
☑ I agree to the terms and conditions

Hendrik.Manwell@gmail.com

••••••••

2. Federation BambooHR with OKTA (Part 3)

- Switch to your OKTA admin console to complete the next step of the configuration
  1. In the **Okta Admin Console** select **Applications** > Applications
  2. Under **Applications** select **Add Application**
  3. In the **Search** type **BambooHR** and select **Add**

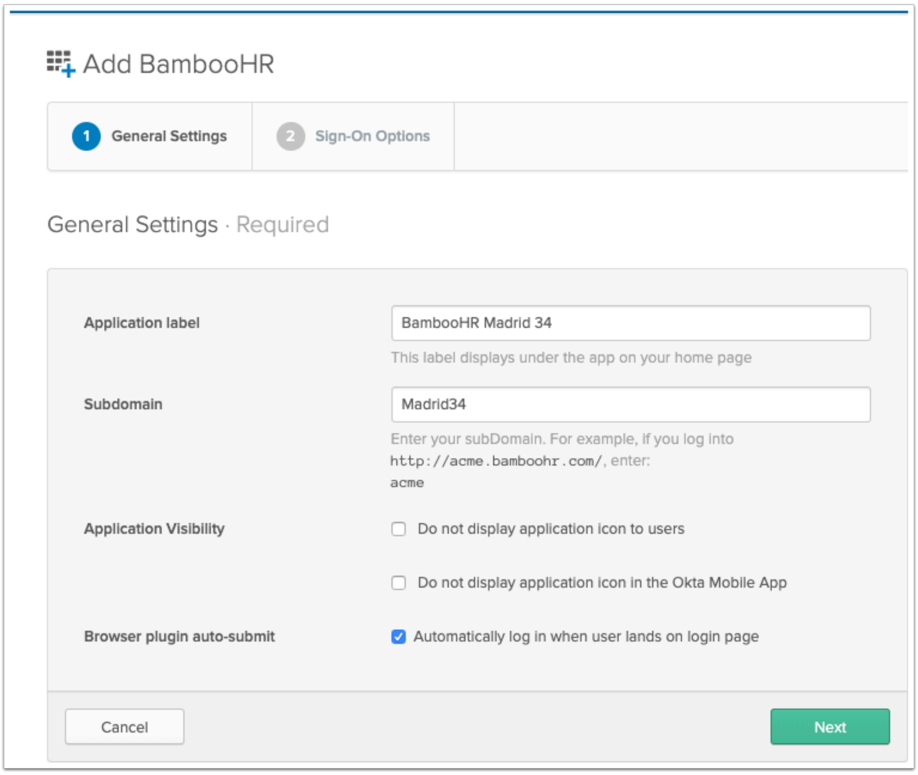


bamboohr

BambooHR
Okta Verified ✓ SAML ✓ Provisioning

3. Federation BambooHR with OKTA (Part 3)

- In the **Add BambooHR** interface under **General Settings** type the following
  1. Next to **Application Label**, type **BambooHR(customdomain) BambooHR Madrid 34**
  2. Next **Subdomain** type your **custom domain e.g Madrid34** select **Next**



General Settings · Required

Application label: BambooHR Madrid 34

This label displays under the app on your home page

Subdomain: Madrid34

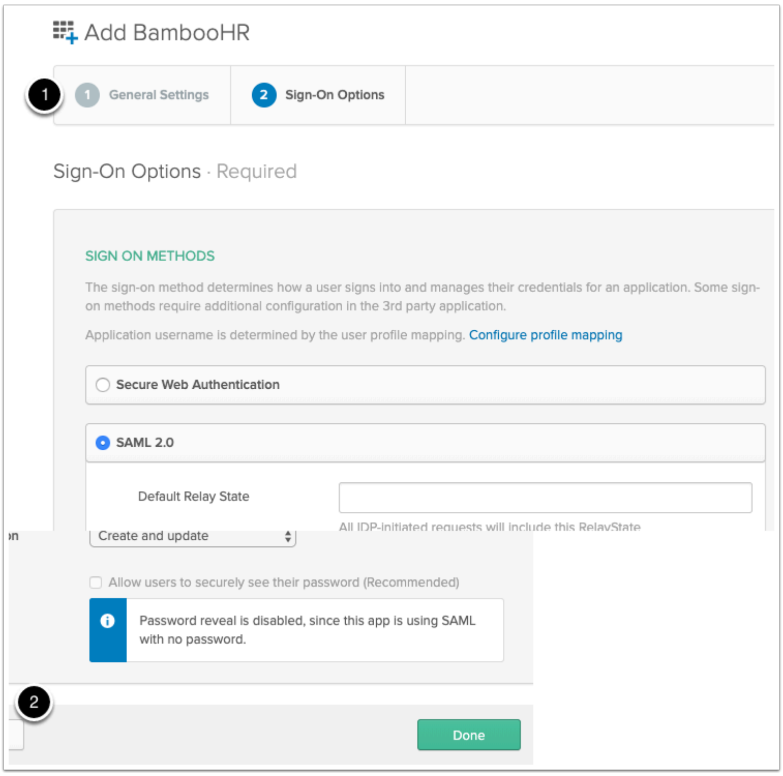
Enter your subDomain. For example, if you log into `http://acme.bamboohr.com/`, enter: `acme`

Application Visibility
□ Do not display application icon to users
□ Do not display application icon in the Okta Mobile App

Browser plugin auto-submit
☑ Automatically log in when user lands on login page

4. Federation BambooHR with OKTA (Part 3)

- In the **OKTA Add BambooHR** interface under **Sign-On Options** select the following
  1. Next to **SAML 2.0** select the **radio button**
  2. At the bottom of the window select **Done**



Add BambooHR

1 General Settings | 2 Sign-On Options

Sign-On Options · Required

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ Secure Web Authentication

● SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

Create and update

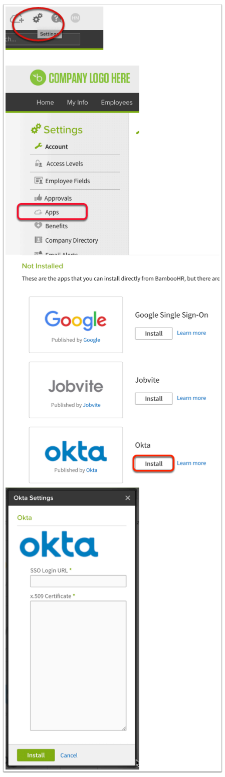
□ Allow users to securely see their password (Recommended)

Password reveal is disabled, since this app is using SAML with no password.

Done

5. Federation BambooHR with OKTA (Part 3)

- Switch back to your custom **BambooHR** Saas AP
  1. In top right-hand select **Settings,** this is a wheel-cog icon
  2. In the left-hand pane select **Apps**
  3. Under **Apps** select **Single Sign-On**
  4. In the **Single Sign-On** window select **OKTA**
  5. Scroll down and select **Install**

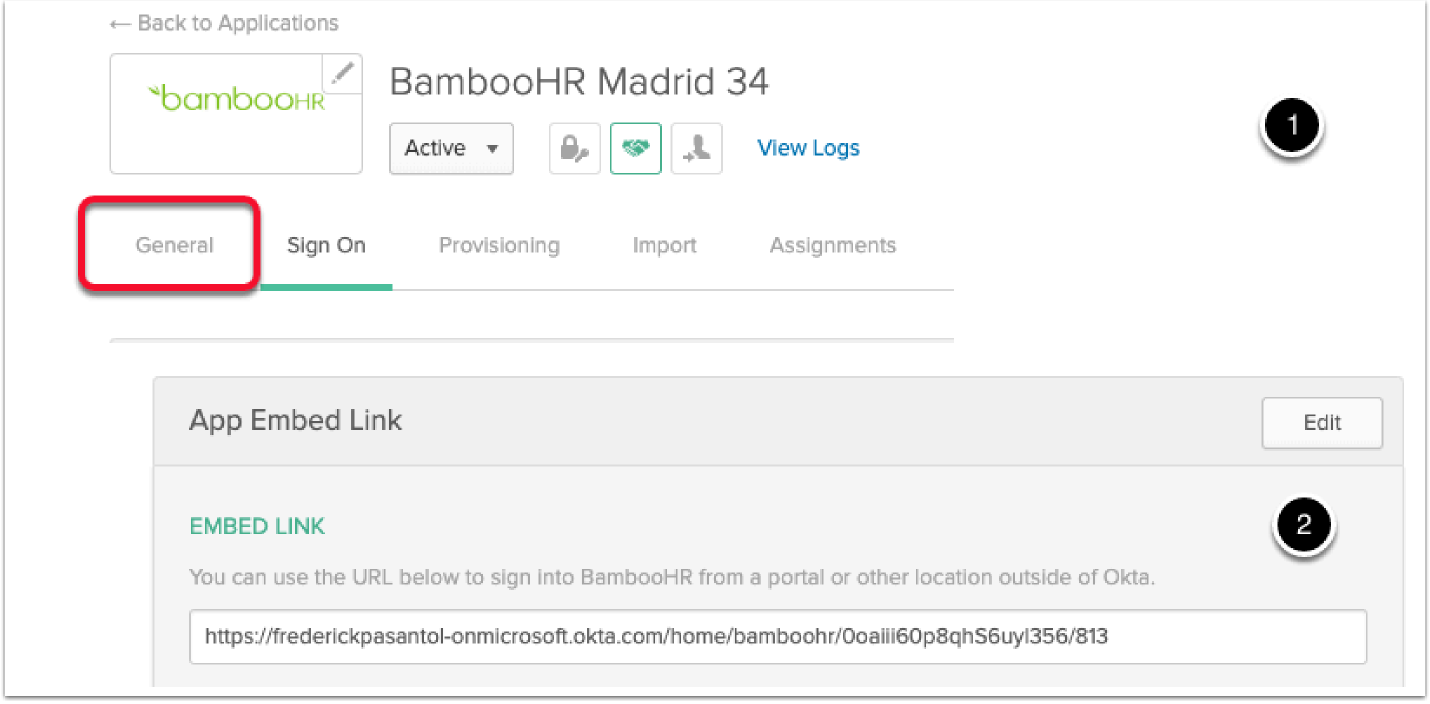


These are the apps that you can install directly from BambooHR, but there are

6. Federation BambooHR with OKTA (Part 3)

- Switch back to your **Okta Console**

1. In the **Applications** interface next to **Sign On** select **General**
2. Scroll down to **App Embed Link** and under **EMBED LINK** copy **the entire URL** and save in **Notepad**

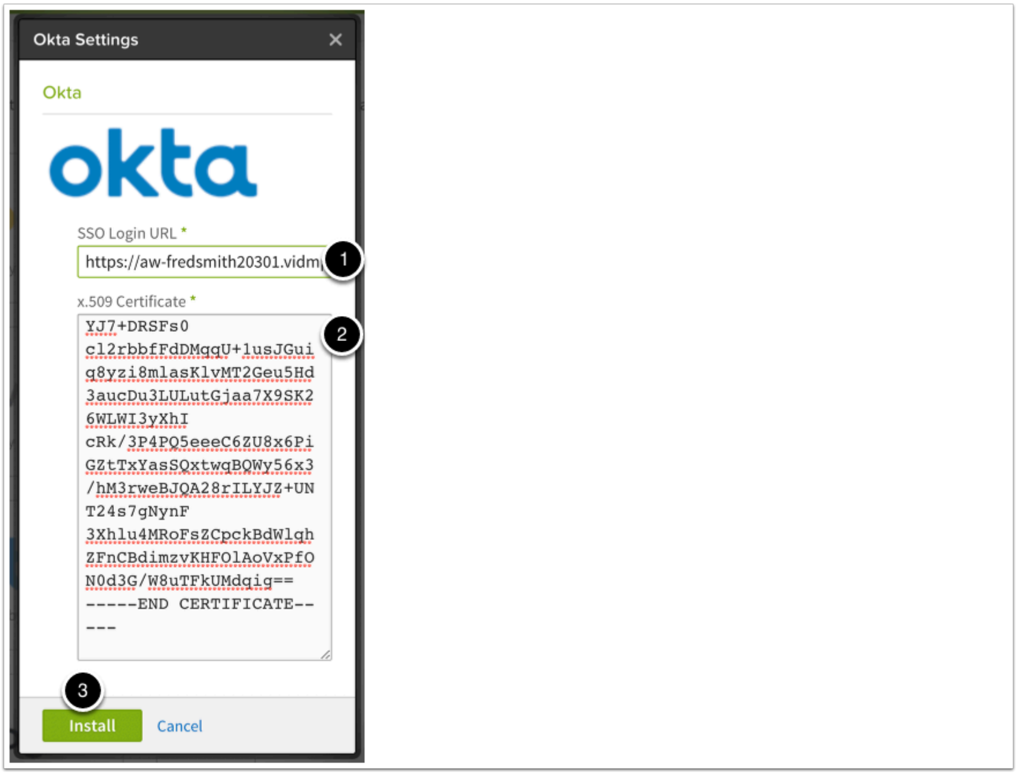


You can use the URL below to sign into BambooHR from a portal or other location outside of Okta.

https://frederickpasantol-onmicrosoft.okta.com/home/bamboohr/0oaiii60p8qhS6uyl356/813

7. Federation BambooHR with OKTA (Part 3)

- Switch back to your **BambooHR Admin Console**
  1. From your Notepad file copy the **SSO Login URL** and under **SSO Login URL** paste the copied link from OKTA
  2. Next open the **Okta.cert** file with a text editor and **copy** the entire certificate, this includes **---begin certificate xxx --- END CERTIFICATE---** and paste into the **x.509 Certificate box**
  3. Scroll to the botton of the page and select **Install**



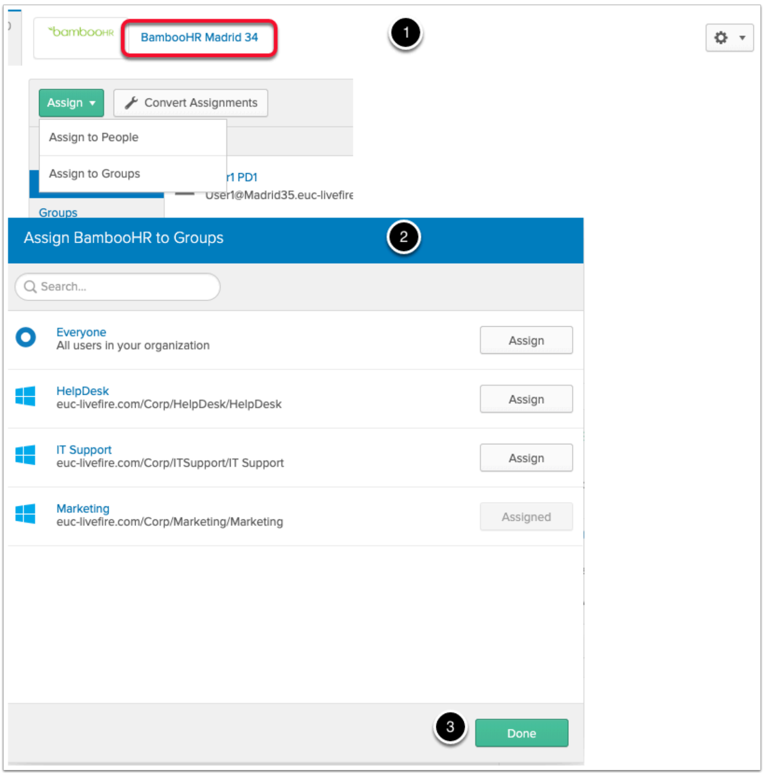
SSO Login URL *
https://aw-fredsmith20301.vidm

x.509 Certificate *

```
YJ7+DRSFs0
cl2rbbfFdDMqqU+lusJGui
q8yzi8mlasKlvMT2Geu5Hd
3aucDu3LULutGjaa7X9SK2
6WLWI3yXhI
cRk/3P4PQ5eeeC6ZU8x6Pi
GZtTxYasSQxtwqBQWy56x3
/hM3rweBJQA28rILYJZ+UN
T24s7gNynF
3Xhlu4MRoFsZCpckBdWlqh
ZFnCBdimzvKHFOlAoVxPfO
N0d3G/W8uTFkUMdqig==
-----END CERTIFICATE--
---
```

8. Federation BambooHR with OKTA (Part 3)

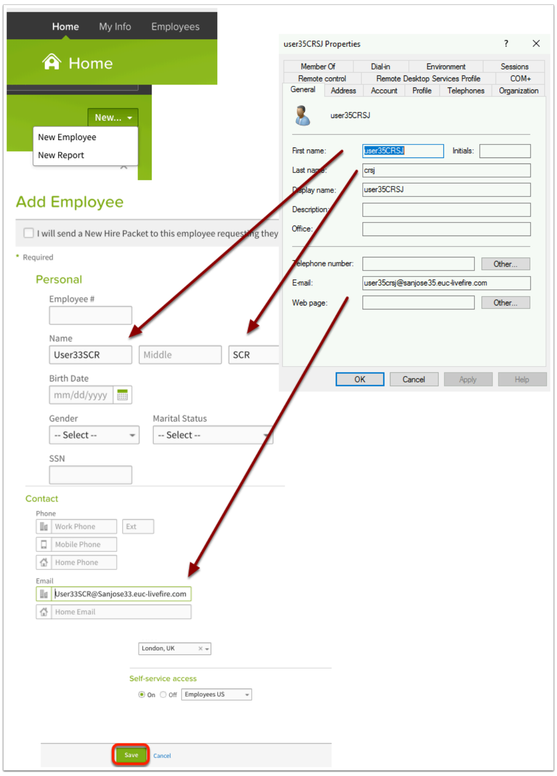
- Switch back to your **OKTA Admin Console**
  1. Go back to **Applications** > **Applications** and select your **BambooHR application**
  2. Select **Assign** > **Assign to Groups**
  3. In the **Assign BambooHR to Groups** next to **Marketing** select **Assign** and select **Done**
  4. Select **Assign** > **assign to people**
  5. Assign to your administrator user.


BambooHR Madrid 34
1
Assign
Convert Assignments
Assign to People
Assign to Groups
r1 PD1
User1@Madrid35.euc-livefire
Groups
Assign BambooHR to Groups
2
Search...
Everyone
All users in your organization
Assign
HelpDesk
euc-livefire.com/Corp/HelpDesk/HelpDesk
Assign
IT Support
euc-livefire.com/Corp/ITSupport/IT Support
Assign
Marketing
euc-livefire.com/Corp/Marketing/Marketing
Assigned
3
Done

9. Federation BambooHR with OKTA (Part 3)

- Switch back to your **BAMBOOHR Admin Console**
  1. In the Bamboo HR application select the **Home tab**
  2. To right of the page select the **drop down arrow** next **New...** and select **New Employee**
  3. In the **Add Employee** interface , use the following information, type next to:
     1. **Name**: **Unique User from AD** (the one you created in the SFDC lab)
     2. **Last**: Last name of the unique User
     3. **Email address**: **XXXXX@euc-livefire.com** (unique username + @euc-livefire.com)
     4. **Self Service Access:** ON

  4. When done select **Save.**



user35CRSJ Properties

Member Of | Dial-in | Environment | Sessions | Remote control | Remote Desktop Services Profile | COM+ | General | Address | Account | Profile | Telephones | Organization

user35CRSJ

First name: user35CRSJ
Initials:
Last name: crsj
Display name: user35CRSJ
Description:
Office:
Telephone number:
E-mail: user35crsj@sanjose35.euc-livefire.com
Web page:

Add Employee

□ I will send a New Hire Packet to this employee requesting they

* Required

Personal

Employee #

Name: User33SCR | Middle | SCR

Birth Date: mm/dd/yyyy

Gender: -- Select --
Marital Status: -- Select --

SSN

Contact

Phone: Work Phone | Ext | Mobile Phone | Home Phone

Email: User33SCR@Sanjose33.euc-livefire.com | Home Email

London, UK

Self-service access

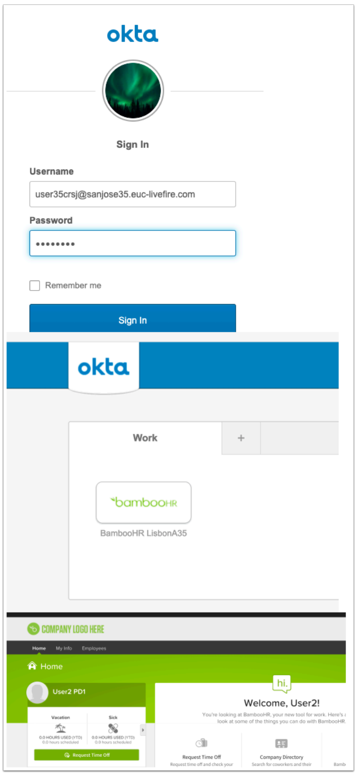
● On ○ Off Employees US

10. Federation BambooHR with OKTA (Part 3)

- We will now validate the single sign-on process with OKTA and BambooHR

1. Open an **Incognito session** of your browser and copy **your custom login url** for OKTA in the address bar. Login with XXXXuniqueuser**@customsuffix.euc-livefire.com** (example user35buk@auckland35.euc-livefire.com) and password **VMware1!** select Sign In
    - If this is the first time you login you will be prompted to choose a custom icon and you will have to close default pop ups

2. Under the **Work** tab you should see your **BambooHR entitlement.** Select your **BambooHR** entitlement.
3. You should see the single sign on between **OKTA** and **BambooHR.**



Username: user35crsj@sanjose35.euc-livefire.com

Password: ••••••••

Welcome, User2!

You're looking at BambooHR, your new tool for work. Here's a look at some of the things you can do with BambooHR.

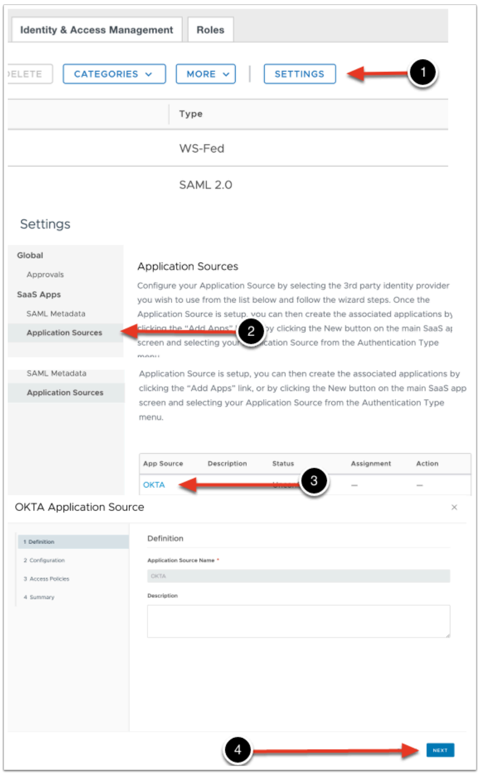
Request time off and check your

Search for coworkers and their

Part 4. Configuring An OKTA Application Source in Workspace ONE Access.

1. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Ensure you are logged into your Workspace ONE Access Session
  1. Under **Catalog > Web Apps** to the right select **SETTINGS**
  2. In the Inventory pane under **SaasApps** select **Application Sources**
  3. In the **Application Sources** section under **App Source** select **OKTA**
  4. On the **OKTA Application Source** window select **NEXT**



Application Sources

Configure your Application Source by selecting the 3rd party identity provider you wish to use from the list below and follow the wizard steps. Once the Application Source is setup, you can then create the associated applications by clicking the "Add Apps" by clicking the New button on the main SaaS ap screen and selecting your cation Source from the Authentication Type menu.

Application Source is setup, you can then create the associated applications by clicking the "Add Apps" link, or by clicking the New button on the main SaaS app screen and selecting your Application Source from the Authentication Type menu.

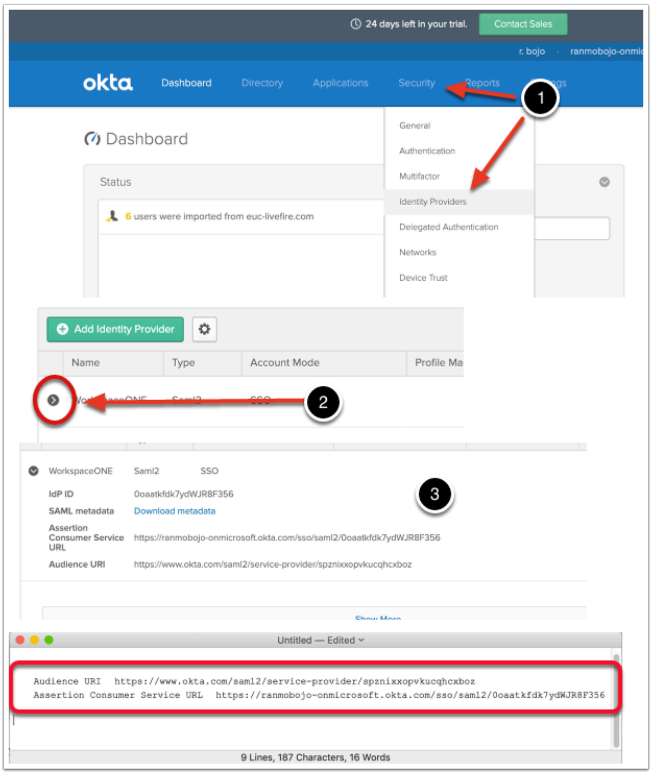
Application Source Name * OKTA

Description

2. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Switch back to your **OTKA admin Console**
  - Select **Security** > **Identity Providers**

1. Expand your ***arrow >*** next to your existing ***WorkspaceONE*** configuration to face down.
2. Notice under WorkspaceONE you have 4 rows of information.
   - Save your **Assertion Consumer Service URL** and your **Audience URI** to Notepad

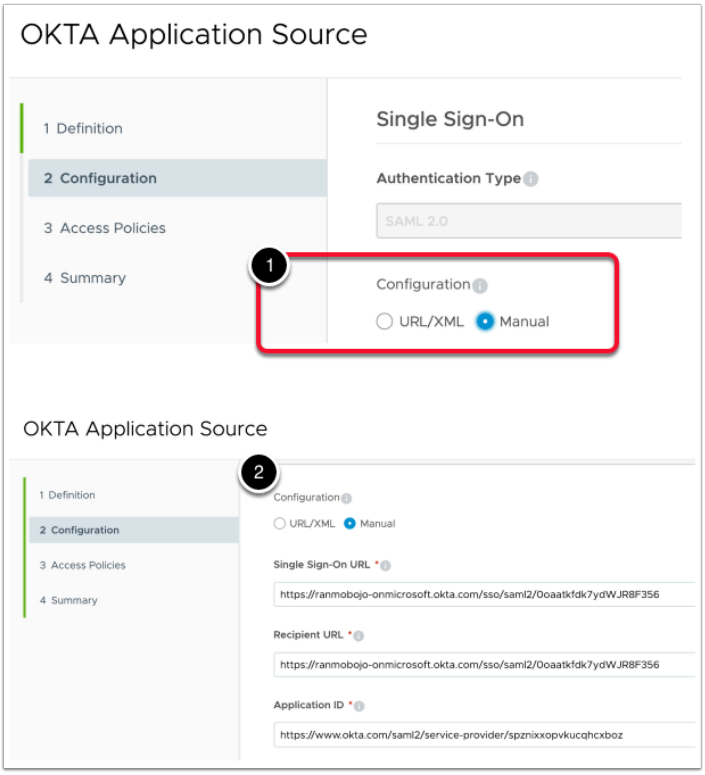


WorkspaceONE	Saml2	SSO
IdP ID	0oaatkfdk7ydWJR8F356	
SAML metadata	Download metadata	
Assertion Consumer Service URL	https://ranmobojo-onmicrosoft.okta.com/sso/saml2/0oaatkfdk7ydWJR8F356	
Audience URI	https://www.okta.com/saml2/service-provider/spznixxopvkucqhcxboz	

```
Audience URI  https://www.okta.com/saml2/service-provider/spznixxopvkucqhcxboz
Assertion Consumer Service URL  https://ranmobojo-onmicrosoft.okta.com/sso/saml2/0oaatkfdk7ydWJR8F356
```

3. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- Switch back to your **Workspace ONE admin console**
  1. In the **OKTA Application Source** under **Configuration** change the **radio button** to **Manual**
  2. In section **2. Configuration** of the **OKTA Application Source** page add the following:-
     1. In the ***Single Sign-On URL*** section **copy and paste** your ***Assertion Consumer URL***
     2. In the **Recipient URL** section **copy and paste** your ***Assertion Consumer URL***
     3. Next to **Application ID: copy and paste** your ***Audience URI***



Single Sign-On

Authentication Type: SAML 2.0

Configuration: ○ URL/XML ● Manual

OKTA Application Source

Configuration: ○ URL/XML ● Manual

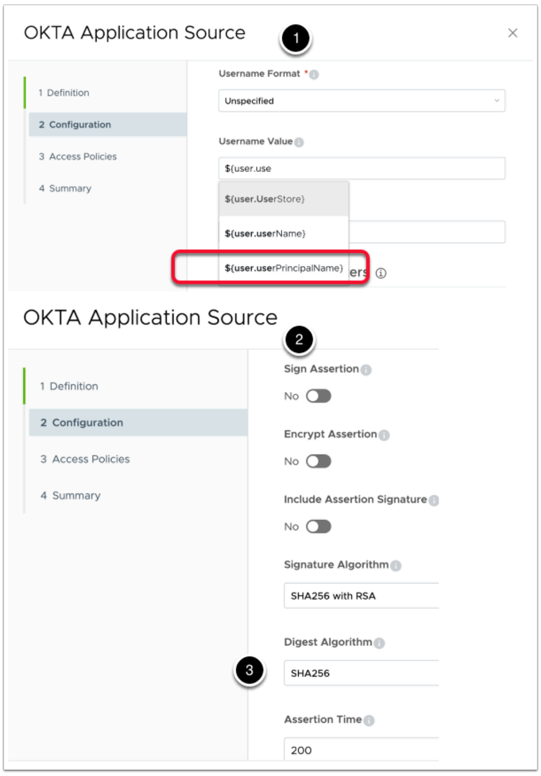
Single Sign-On URL *: https://ranmobojo-onmicrosoft.okta.com/sso/saml2/0oaatkfdk7ydWJR8F356

Recipient URL *: https://ranmobojo-onmicrosoft.okta.com/sso/saml2/0oaatkfdk7ydWJR8F356

Application ID *: https://www.okta.com/saml2/service-provider/spznixxopvkucqhcxboz

4. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the **OKTA Application Source** wizard
  1. Under **Configuration** Scroll down, next to:
     1. **Username Format:** Unspecified, (default)
     2. Under the **Username Value:** **${user.userPrincipalName}**
  2. **Scroll down** until **Advanced Properties**, and **expand** configure the following Next to:
     1. **Sign Response**: Yes (default)
     2. **Sign Assertion**: No (default)
     3. **Encrypted Assertion:** No (default)
     4. **Include Assertion Signature:** No (default)
     5. **Signature Algorithm:** SHA256 with RSA (default)
     6. **Digest Algorithm**: **SHA256**
     7. **Assertion Time**: 200 (default)



OKTA Application Source

1 Definition
2 Configuration
3 Access Policies
4 Summary

Username Format *: Unspecified

Username Value: ${user.use

${user.UserStore}
${user.userName}
${user.userPrincipalName}

OKTA Application Source

1 Definition
2 Configuration
3 Access Policies
4 Summary

Sign Assertion: No

Encrypt Assertion: No

Include Assertion Signature: No

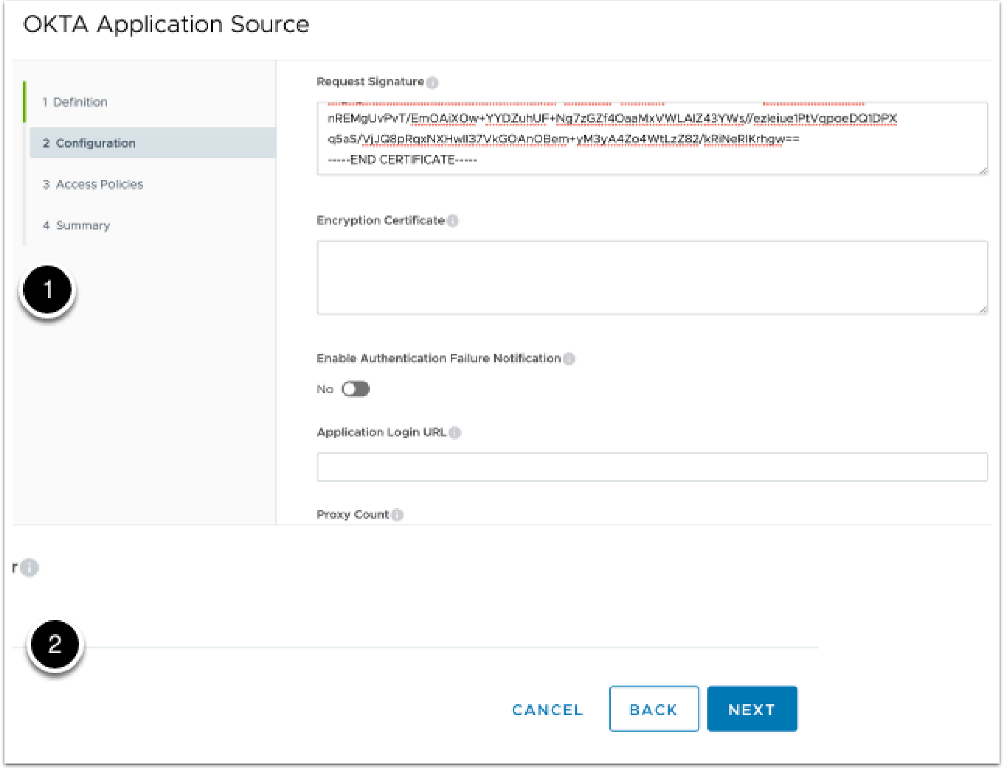
Signature Algorithm: SHA256 with RSA

Digest Algorithm: SHA256

Assertion Time: 200

5. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the **OKTA Application Source** under **Configuration** continue scrolling down
  1. Under **Request Signature:** **open** the contents of the ***Okta.cert*** file previously downloaded from Okta. **Copy** and **paste** the contents including the **"-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"**
  2. Select **Next**



OKTA Application Source

Request Signature

```
nREMgUvPvT/EmOAiXOw+YYDZuhUF+Ng7zGZf4OaaMxVWLAIZ43YWs//ezleiue1PtVqpoeDQ1DPX
q5aS/VjJQ8pRqxNXHwlI37VkGOAnOBem+yM3yA4Zo4WtLzZ82/kRiNeRIKrhgw==
-----END CERTIFICATE-----
```

Encryption Certificate

Enable Authentication Failure Notification

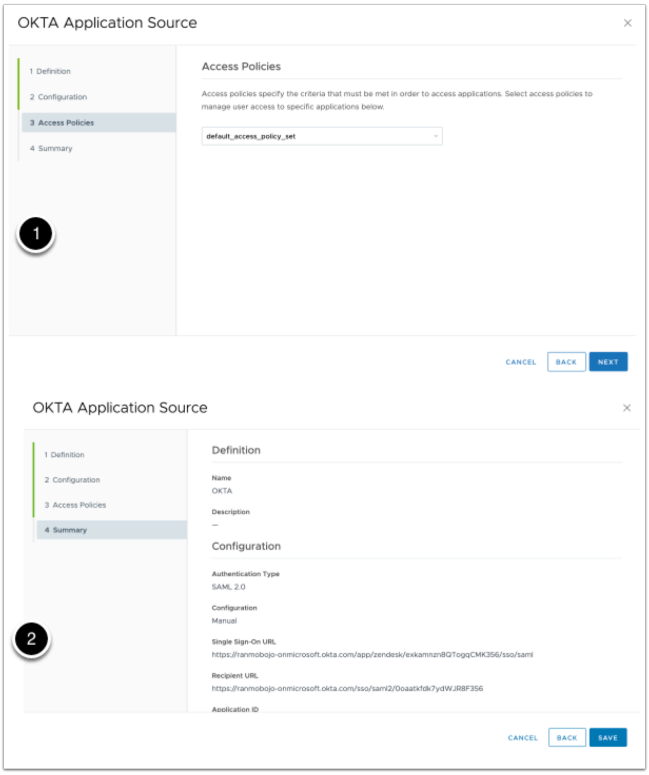
No

Application Login URL

Proxy Count

6. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- **OKTA Application Source** under **Configuration** continued
  1. On the **Access policies** page select **NEXT**
  2. On the **Summary** page select **SAVE**



OKTA Application Source

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

OKTA Application Source

Definition

Name
OKTA

Description
—

Configuration

Authentication Type
SAML 2.0

Configuration
Manual

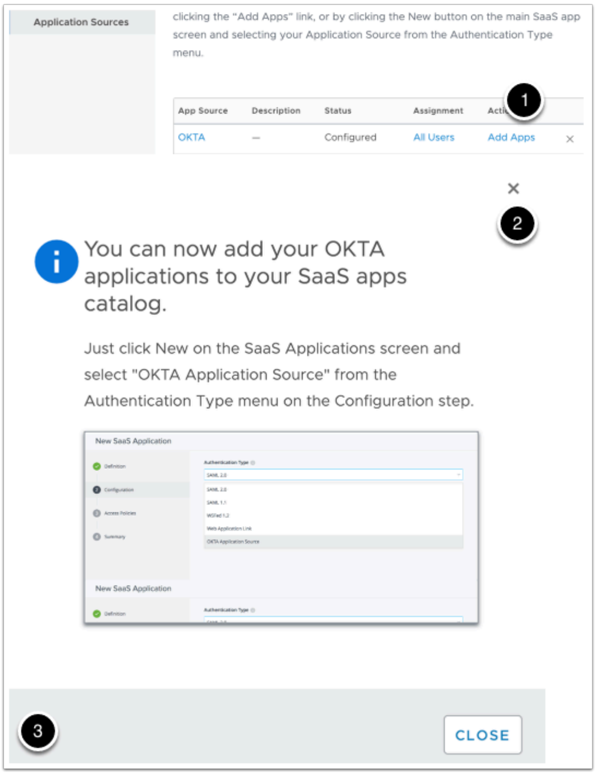
Single Sign-On URL
https://ranmobojo-onmicrosoft.okta.com/app/zendesk/exkamnzn8QTogqCMK356/sso/saml

Recipient URL
https://ranmobojo-onmicrosoft.okta.com/sso/saml2/0oaatkfdk7ydWJR8F356

Application ID

7. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- **OKTA Application Source** under **Configuration** continued
  1. Under **Settings** notice that your **OKTA Source** is now configured. Under **Action** select **Add Apps**
  2. Read the message: When done, select **Close** and select **X** to close the **Settings** page.



Application Sources

clicking the "Add Apps" link, or by clicking the New button on the main SaaS app screen and selecting your Application Source from the Authentication Type menu.

App Source	Description	Status	Assignment	Acti…	
OKTA	—	Configured	All Users	Add Apps	×

You can now add your OKTA applications to your SaaS apps catalog.

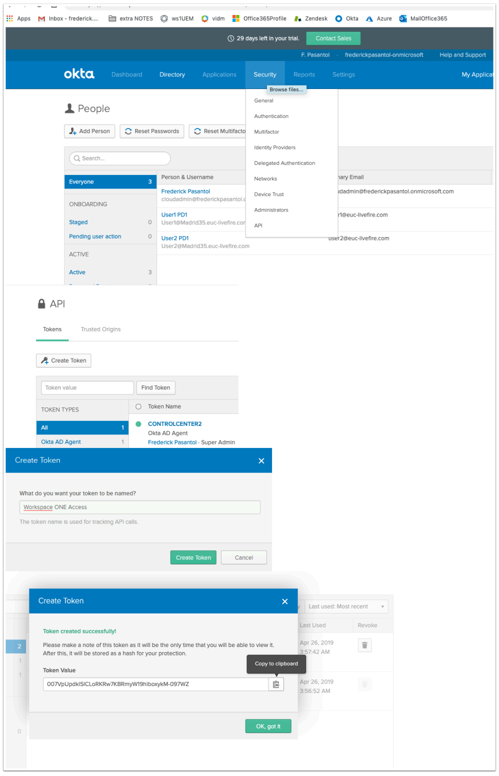
Just click New on the SaaS Applications screen and select "OKTA Application Source" from the Authentication Type menu on the Configuration step.

New SaaS Application

Authentication Type: SAML 2.0

8. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- We will now configure the automatic sync of OKTA applications into the **User Catalog**
  1. Go back to your **OKTA admin Console** and select **Security** > **API**
     - **Very IMPORTANT! We are now going to create a TOKEN, we will only get ONE CHANCE to save this Token. Open a copy of Notepad or Word to document this**
  2. In the **API** console under **Tokens** select **Create Token**
  3. In the **Create Token** window under **What do you want your token to be named?** type **Workspace ONE Access** and select **Create Token**
  4. On the **Create Token** window under **Token Value** select the **Copy to Clipboard** option and **save** and **paste** to Notepad . Then select **OK, got it.**



29 days left in your trial.

Person & Username	...ary Email
Frederick Pasantol cloudadmin@frederickpasantol.c...	...udadmin@frederickpasantol.onmicrosoft.com
User1 PD1 User1@Madrid35.euc-livefire.com	...r1@euc-livefire.com
User2 PD1 User2@Madrid35.euc-livefire.com	user2@euc-livefire.com

CONTROLCENTER2
Okta AD Agent
Frederick Pasantol · Super Admin

Create Token

What do you want your token to be named?

Workspace ONE Access

The token name is used for tracking API calls.

Create Token

Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

Token Value

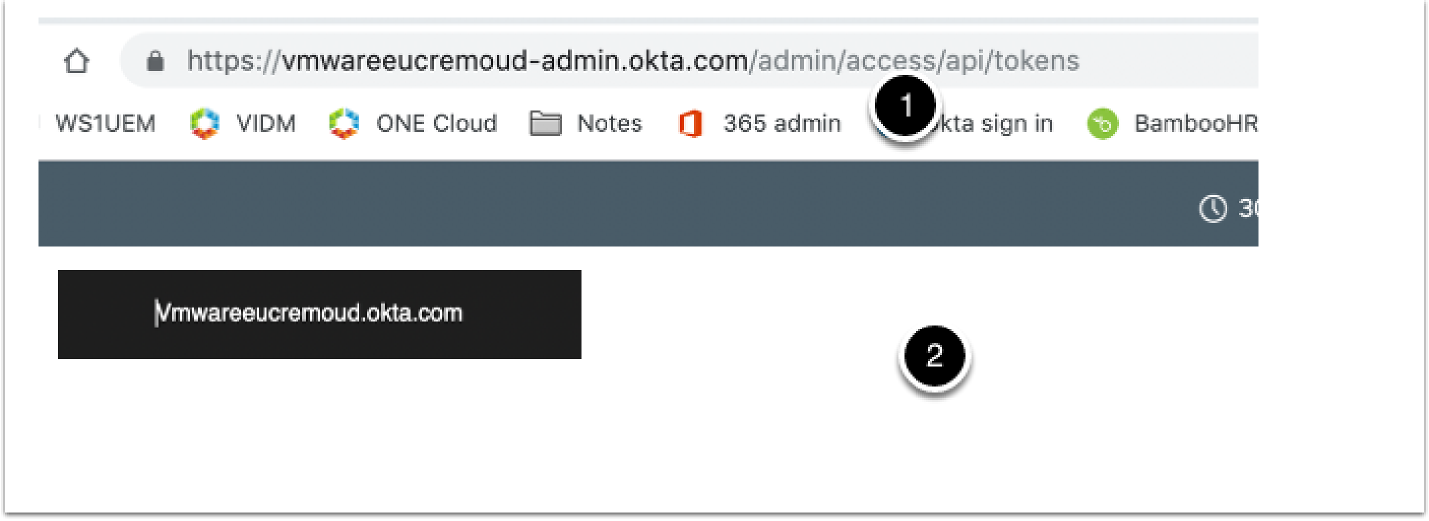
007VpUpdkISICLoRKRw7KBRmyW19hiboxykM-097WZ

Apr 26, 2019 3:57:42 AM

Apr 26, 2019 3:56:52 AM

1. 9. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the Okta Console configure the following:
  1. Copy your **OKTA ADMIN URL** and save to **NOTEPAD**
  2. In **Notepad** **REMOVE** anything after **.com** and the **-admin** part of the hostname portion from the URL, then **copy the URL**

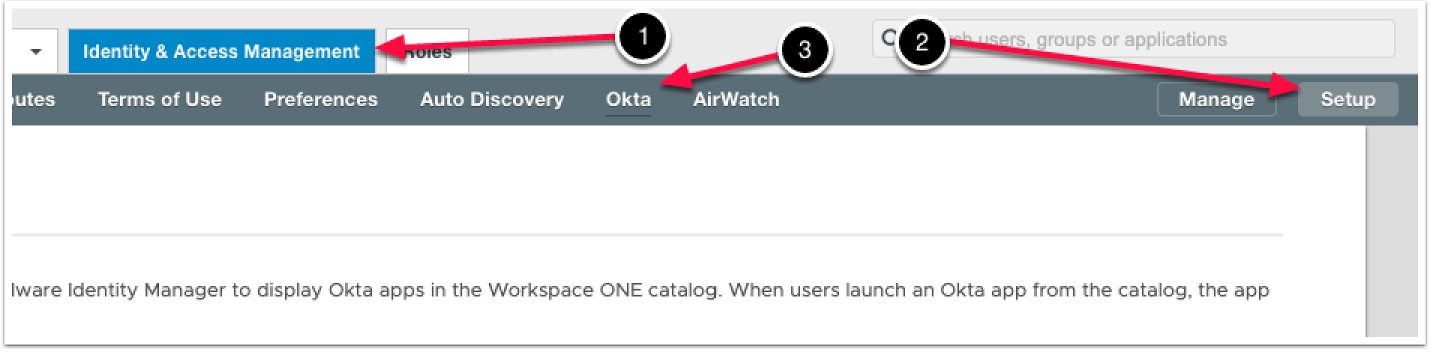


https://vmwareeucremoud-admin.okta.com/admin/access/api/tokens

Vmwareeucremoud.okta.com

10. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

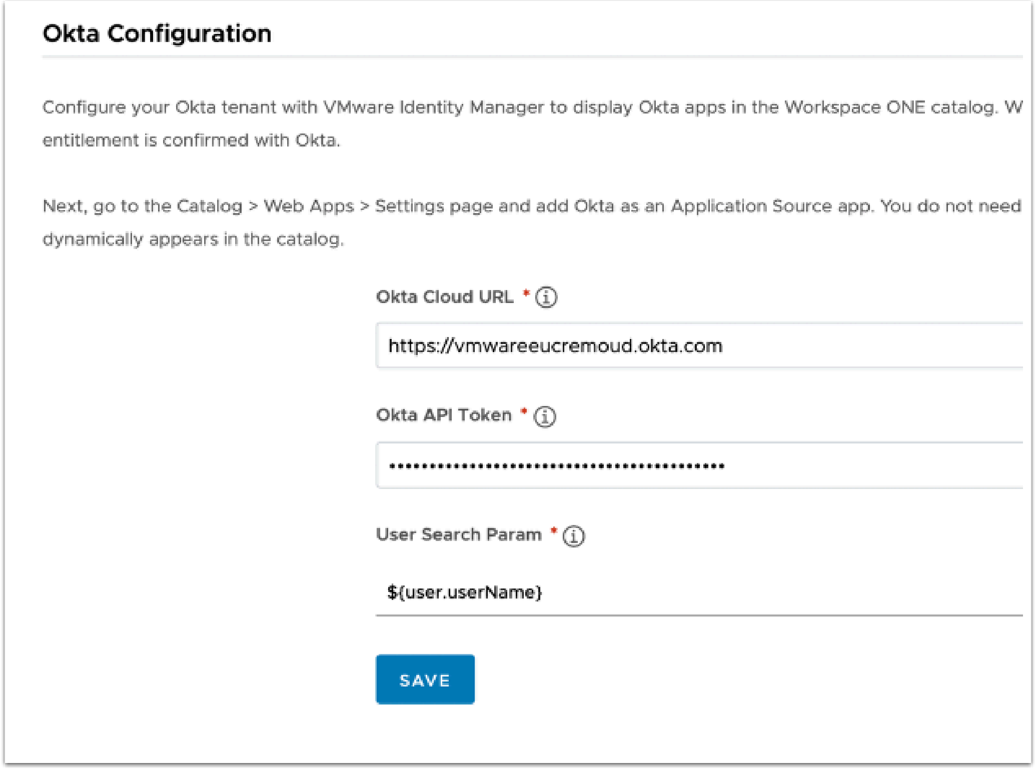
- Switch back to your Workspace ONE Access Console
  - Select the **Identity & Access Management** tab and select **Setup**
  - Select **Okta**



lware Identity Manager to display Okta apps in the Workspace ONE catalog. When users launch an Okta app from the catalog, the app

11. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- In the Workspace ONE Access Console under **Setup** > **Okta**
  1. Under **Okta Cloud URL** paste your **edited OKTA URL** from Notepad
  2. Under **Okta API** token paste your **OKTA access token** from Notepad
  3. Under **Search Param** select **$(user.userName)** in the dropdown
  4. Select **SAVE**



Okta Configuration

Configure your Okta tenant with VMware Identity Manager to display Okta apps in the Workspace ONE catalog. W entitlement is confirmed with Okta.

Next, go to the Catalog > Web Apps > Settings page and add Okta as an Application Source app. You do not need dynamically appears in the catalog.

Okta Cloud URL * ⓘ
https://vmwareeucremoud.okta.com

Okta API Token * ⓘ
••

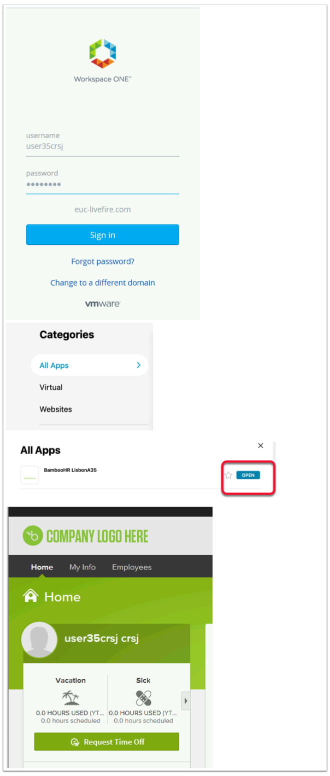
User Search Param * ⓘ
${user.userName}

SAVE

12. Configuring an OKTA application Source in Workspace ONE Access (Part 4)

- We will now validate the Single Sign On process from Workspace ONE Access to OKTA to BambooHR
  1. Open a new browser or Incognito session. Make sure all cookies are deleted from previous sessions.
  2. Use your **Workspace ONE Access Url** and login as your **unique user** from the **euc-livefire.com** domain with the password **VMware1!**
  3. Under **Categories** select **All Apps**

4. Under **All Apps** next to **BambooHR** select **OPEN**, you should now be redirected and signed into ***BambooHR***



username: user35crsj

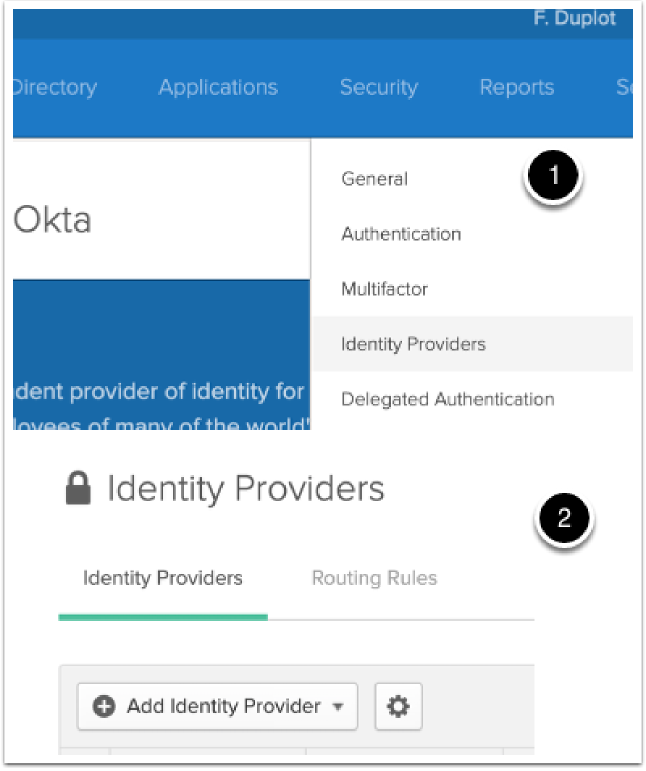
password: ••••••••

euc-livefire.com

Part 5. Configuring An OKTA Routing rules for Workspace ONE Access.

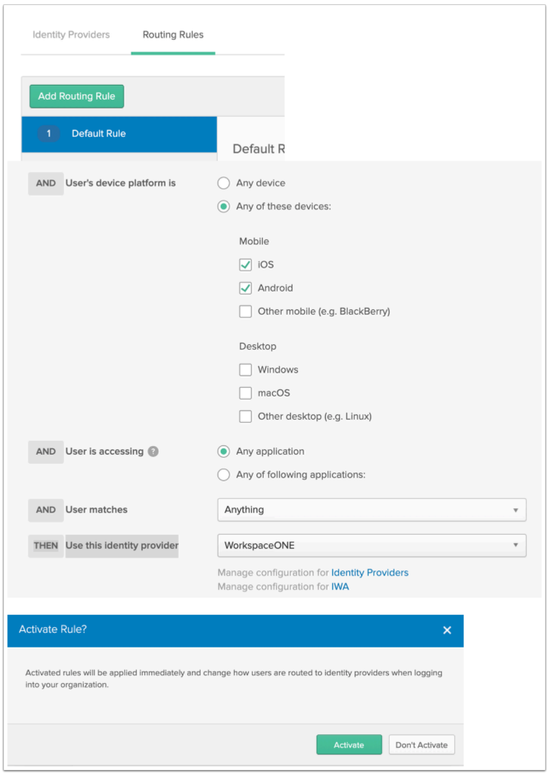
5.1

- Ensure you logged into your trial OKTA Admin console with your Custom admin account
  1. Select **Security** > **Identity Providers**
  2. Next to **Identity Providers** select **Routing Rules**



5.2

- In the Routing Rules section
  1. Select **Add Routing Rule**
  2. In the Add Rule Box select and add the following:
     - **Rule Name: Workspace ONE**
     - **AND User's device platform is :**
       - **Any of these devices: radio button**
         - **Mobile: IOS** and **Android checkboxes**
     - **THEN Use this identity provider :WorkspaceONE**
  3. Select **Create Rule**
  4. On the **Activate Rule?** Window select **Activate**
- When we complete the Mobile SSO IOS and Android labs we can test BambooHR authentication using Workspace ONE Access



AND User's device platform is
○ Any device
● Any of these devices:

Mobile
☑ iOS
☑ Android
□ Other mobile (e.g. BlackBerry)

Desktop
□ Windows
□ macOS
□ Other desktop (e.g. Linux)

AND User is accessing
● Any application
○ Any of following applications:

AND User matches: Anything

THEN Use this identity provider: WorkspaceONE

Manage configuration for Identity Providers
Manage configuration for IWA

Activate Rule?

Activated rules will be applied immediately and change how users are routed to identity providers when logging into your organization.

ADFS as Application Source in ACCESS (Service Now)

Part 1: Creating a ServiceNow Developer Instance

This lab will address the scenario in which customers have an on-premise ADFS server. Customer that have federated their application with ADFS can now leverage the authentication methods of WorkspaceONE Access. This requires a simple setup of Claims Provider Trust with WorkspaceONE Access.

In this lab we will use **ServiceNow** as the Relying Party Trust and WorkspaceONE Access as the Claims Provider Trust.

The order of the LAB

Part 1: Setup a ServiceNow Developer Instance

Part 2: Add ServiceNow as RelyingParty to ADFS

Part 3: Adding Access As Claims Provider in ADFS

Part 4: Adding ADFS As Application Source to WorkspaceOne Access

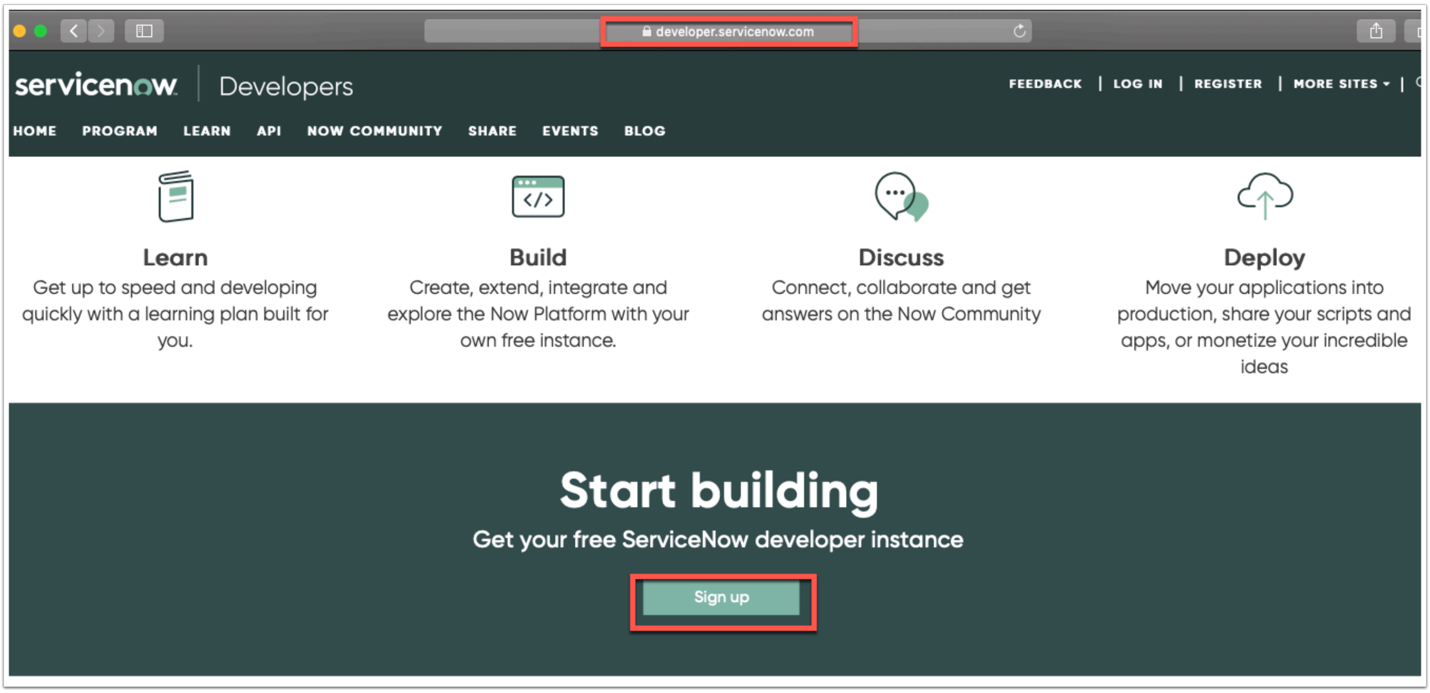
Sign up for a ServiceNow Tenant

1. Open a **browser** on your physical or virtual machine and navigate to https://developer.servicenow.com

2. Click on **Sign up** and enter your details for the Developer Account. Make sure you use your **cloudadmin** account for e-mail. This is the one you created on Day1 of the labs. (example: **cloudadmin@sfmustermann.onmicrosoft.com**) Password can be **VMware1!.** Click **Sign Up** at the bottom of the page once all fields have been entered.

NOTE: We highly recommend documenting all of the **URLs** in this lab as well as the **credentials** in a separate note taking application.

3. Check your e-mail on the **login.microsoft.com** and click the **Verify Email** button in the **Welcome Email** that has come from Service Now. The link will take you to a page click **Sign In** on that page that says **Thank You!**


developer.servicenow.com
servicenow | Developers
FEEDBACK | LOG IN | REGISTER | MORE SITES ▾ |
HOME PROGRAM LEARN API NOW COMMUNITY SHARE EVENTS BLOG
Sign up

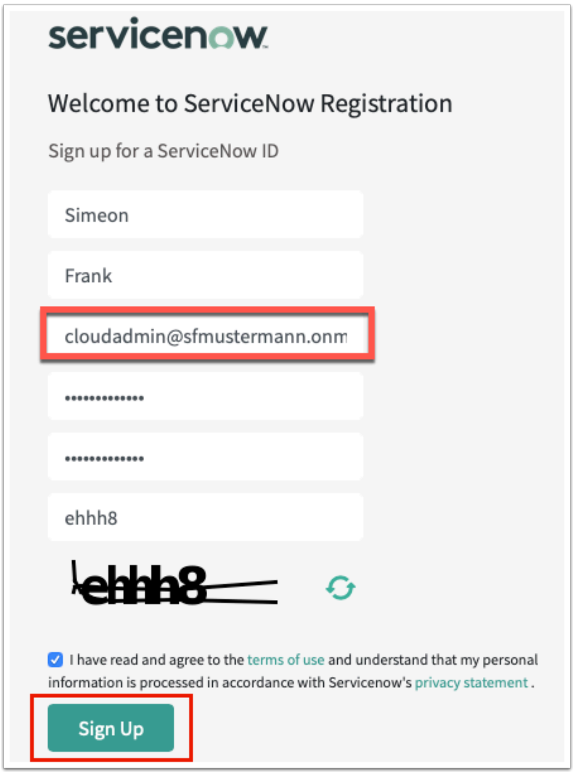
Learn
Get up to speed and developing quickly with a learning plan built for you.

Build
Create, extend, integrate and explore the Now Platform with your own free instance.

Discuss
Connect, collaborate and get answers on the Now Community

Deploy
Move your applications into production, share your scripts and apps, or monetize your incredible ideas

Start building
Get your free ServiceNow developer instance



Welcome to ServiceNow Registration

Sign up for a ServiceNow ID

Simeon

Frank

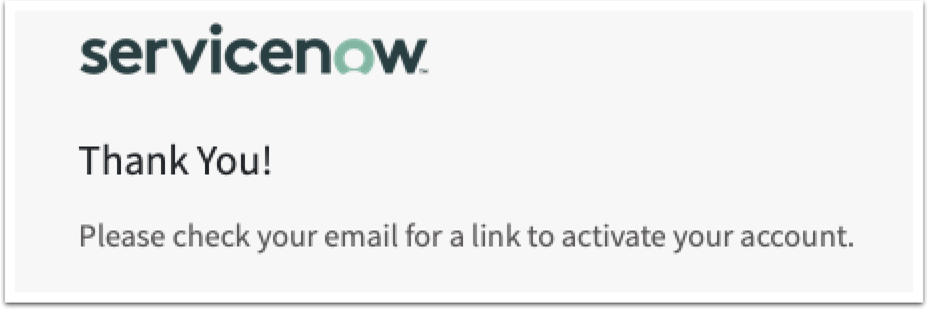
cloudadmin@sfmustermann.onm

•••••••••••••

•••••••••••••

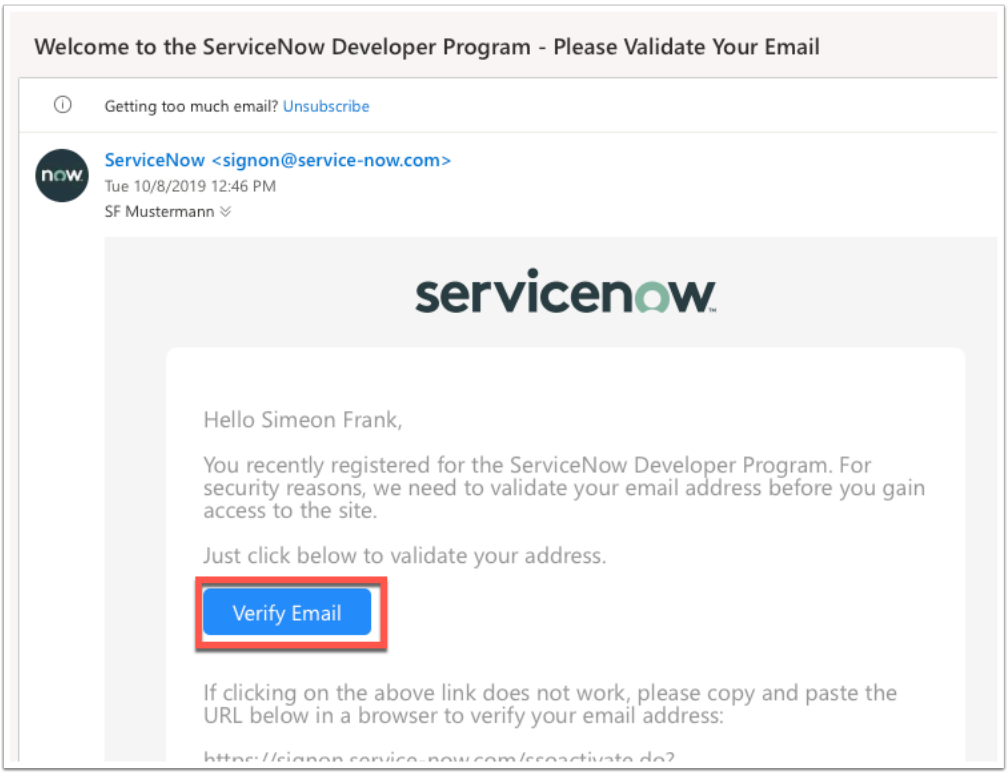
ehhh8

☑ I have read and agree to the terms of use and understand that my personal information is processed in accordance with Servicenow's privacy statement .



Thank You!

Please check your email for a link to activate your account.



Welcome to the ServiceNow Developer Program - Please Validate Your Email

Getting too much email? Unsubscribe

ServiceNow <signon@service-now.com>
Tue 10/8/2019 12:46 PM
SF Mustermann

Hello Simeon Frank,

You recently registered for the ServiceNow Developer Program. For security reasons, we need to validate your email address before you gain access to the site.

Just click below to validate your address.

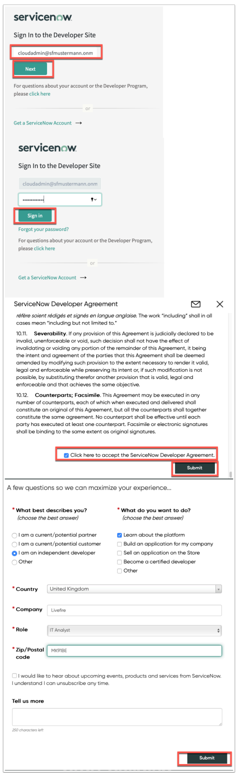
If clicking on the above link does not work, please copy and paste the URL below in a browser to verify your email address:

https://signon.service-now.com/ssoactivate.do?

4. Now that you have created an account. Let's sign in to the Developer Site. If you don't already see a **Sign In** Page click on **https://signon.service-now.com**

5. Type in your cloudadmin **e-mail address** and **password** to sign in. You must agree to the Developer Agreement. Scroll all the way to the bottom and check the **tick box** and click **Submit**.

6. Fill in the requested information on the use of the platform and click **Submit**.



Sign In to the Developer Site

cloudadmin@sfmustermann.onm

For questions about your account or the Developer Program, please click here

or

Get a ServiceNow Account →

Sign In to the Developer Site

cloudadmin@sfmustermann.onm

Forgot your password?

For questions about your account or the Developer Program, please click here

or

Get a ServiceNow Account →

ServiceNow Developer Agreement

réfère soient rédigés et signés en langue anglaise. The work "including" shall in all cases mean "including but not limited to."

10.11. **Severability**. If any provision of this Agreement is judicially declared to be invalid, unenforceable or void, such decision shall not have the effect of invalidating or voiding any portion of the remainder of this Agreement, it being the intent and agreement of the parties that this Agreement shall be deemed amended by modifying such provision to the extent necessary to render it valid, legal and enforceable while preserving its intent or, if such modification is not possible, by substituting therefor another provision that is valid, legal and enforceable and that achieves the same objective.

10.12. **Counterparts; Facsimile**. This Agreement may be executed in any number of counterparts, each of which when executed and delivered shall constitute an original of this Agreement, but all the counterparts shall together constitute the same agreement. No counterpart shall be effective until each party has executed at least one counterpart. Facsimile or electronic signatures shall be binding to the same extent as original signatures.

☑ Click here to accept the ServiceNow Developer Agreement.

A few questions so we can maximize your experience...

* **What best describes you?** *(choose the best answer)*

○ I am a current/potential partner
○ I am a current/potential customer
● I am an independent developer
○ Other

* **What do you want to do?** *(choose the best answer)*

☑ Learn about the platform
□ Build an application for my company
□ Sell an application on the Store
□ Become a certified developer
□ Other

* **Country**	United Kingdom
* **Company**	Livefire
* **Role**	IT Analyst
* **Zip/Postal code**	MK91BE

□ I would like to hear about upcoming events, products and services from ServiceNow. I understand I can unsubscribe any time.

Tell us more

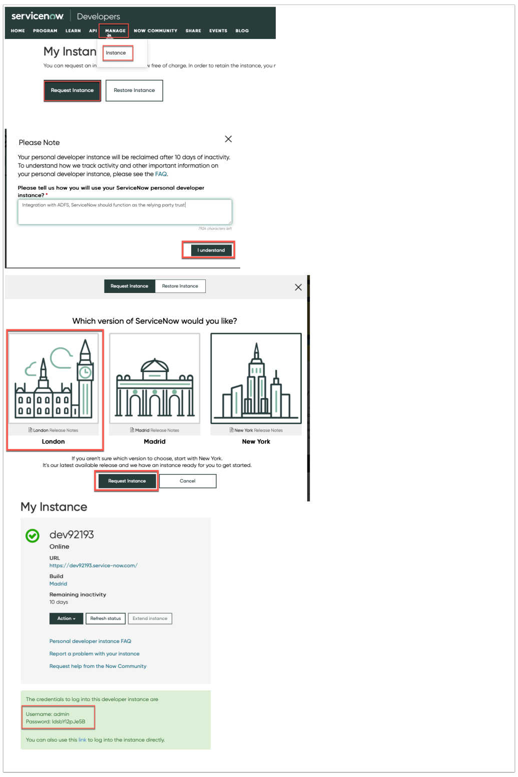
250 characters left

7. On the **Service Now Developers** home Page click on the **Manage** Tab and click **Instance** and click on **Request Instance**

8. You will now be requested to give a reason for this request. Simply put what you are hoping to test. "**Integration with ADFS, ServiceNow should function as the relying part trust.**" - Click **I understand**

9. Finally choose the Service now release you would like to user and click **Request Instance.** (New York is the newest and vendor recommended version)

Very Important: Make sure you note your admin user and password on the next page after the instance has been created.



My Instan

You can request an in v free of charge. In order to retain the instance, you r

Please Note

Your personal developer instance will be reclaimed after 10 days of inactivity. To understand how we track activity and other important information on your personal developer instance, please see the FAQ.

Please tell us how you will use your ServiceNow personal developer instance? *

Integration with ADFS, ServiceNow should function as the relying party trust

7924 characters left

Which version of ServiceNow would you like?

If you aren't sure which version to choose, start with New York.
It's our latest available release and we have an instance ready for you to get started.

My Instance

dev92193
Online

URL
https://dev92193.service-now.com/

Build
Madrid

Remaining inactivity
10 days

Action ▾
Refresh status
Extend instance
Personal developer instance FAQ
Report a problem with your instance
Request help from the Now Community

The credentials to log into this developer instance are

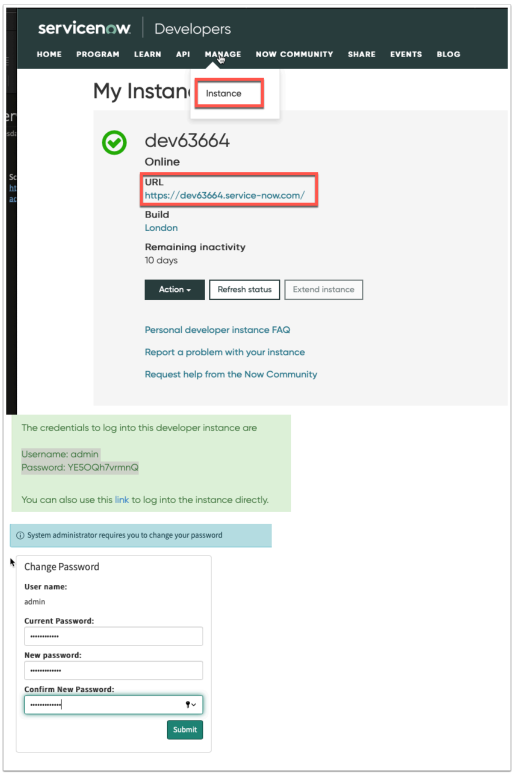
Username: admin
Password: IdsbYI2pJe5B

You can also use this link to log into the instance directly.

10. You will now see your instances if you click on the **Manage** > Instances tab on the top menu. Note your Unique URL that should start with devXXX.service-now.com

11. Click on your unique **Dev Instance** and **sign in** with the admin credentials given to you on the page above. You will be asked to set a new password.

This completes the creation of your Instance in ServiceNow.



My Instan

dev63664

Online

URL
https://dev63664.service-now.com/

Build
London

Remaining inactivity
10 days

Personal developer instance FAQ

Report a problem with your instance

Request help from the Now Community

The credentials to log into this developer instance are

Username: admin
Password: YE5OQh7vrmnQ

You can also use this link to log into the instance directly.

System administrator requires you to change your password

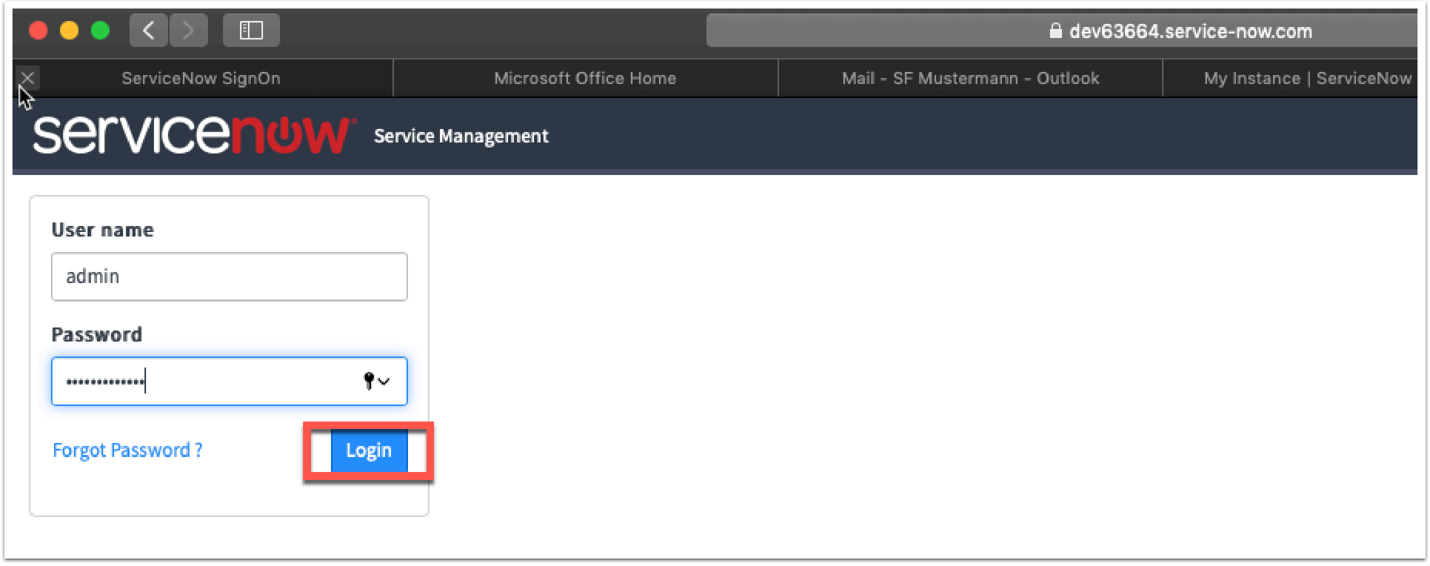
Change Password

User name:
admin

Current Password:
••••••••••••

New password:
•••••••••••••

Confirm New Password:
••••••••••••



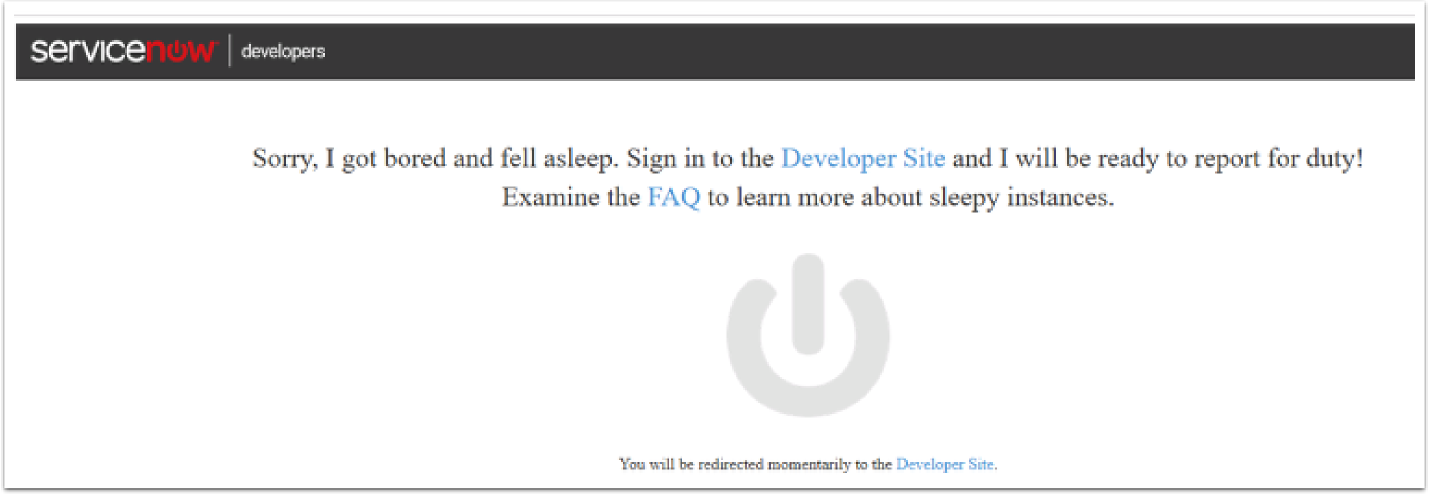
User name
admin

Password
•••••••••••••

JUST FOR NOTE - NO ACTION REQUIRED

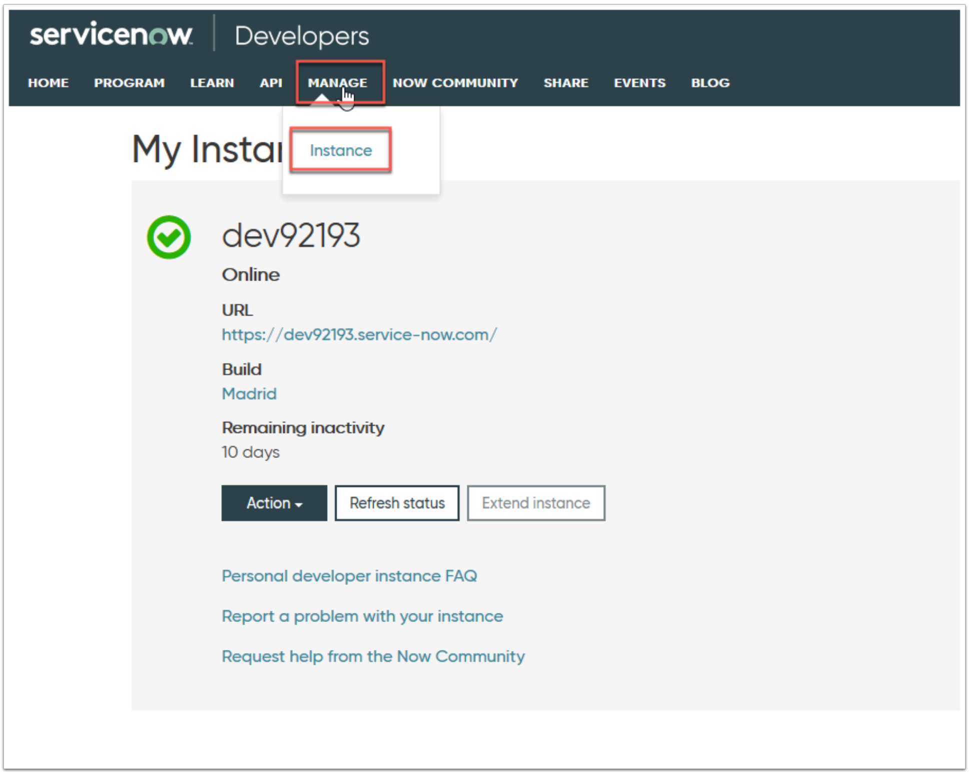
The Developer instance **after 12 hours** will go dormant and it will be required to wake it up. If you see this happen log into the developer Site developer.servicenow.com

Once you have logged into the Developer portal you will have to click on **Manage** and **Instances** to then wake the environment.



Sorry, I got bored and fell asleep. Sign in to the Developer Site and I will be ready to report for duty!
Examine the FAQ to learn more about sleepy instances.

You will be redirected momentarily to the Developer Site.



dev92193

Online

URL
https://dev92193.service-now.com/

Build
Madrid

Remaining inactivity
10 days

Personal developer instance FAQ

Report a problem with your instance

Request help from the Now Community

Setup User in ServiceNow

Now that we have a unique instance of **ServiceNow**, it's time to add your unique user from AD into ServiceNow.

1. In your unique instance of **ServiceNow** on the home page click on the **Filter navigator** in the top left corner.

2. Type **users** and from the navigation bar

3. Under **System Security** > **Users and Groups** select **Users**

4. At the top of the page click **New** in the Users management Interface

5. Fill in the Fields for your **unique user** and click **Submit** at the top right hand corner of the page.

For example

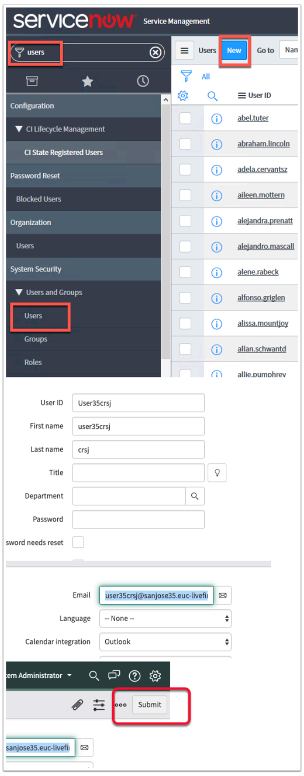
UserID: **user35SCR**

First name: **User35SCR**

Last name: **SCR**

Email: **user35SCR@sanjose35.euc-livefire.com**

Note: Make sure the e-mail attribute you add here matches the e-mail from AD as this will be the SAML attribute we leverage



User ID: User35crsj

First name: user35crsj

Last name: crsj

Title:

Department:

Password:

sword needs reset: □

Email: user35crsj@sanjose35.euc-livefi

Language: -- None --

Calendar integration: Outlook

sanjose35.euc-livefi

Setting up Identity Provider setting in ServiceNow

We will now configure the SAML settings on the your ServiceNow Instance.

1. In the top left hand **Filter navigator** area type in **plugins** and click on **Plugins** below.

2. On the **Plugins** page to the right of **FILTERS** type "**integration**" into the **search** field.

3. Scroll down until you find **Integration - Multiple Provider Single Sign-on Installer**

NOTE: Make sure it is exactly matches "Integration - Multi Provider Single Sign-on Installer"

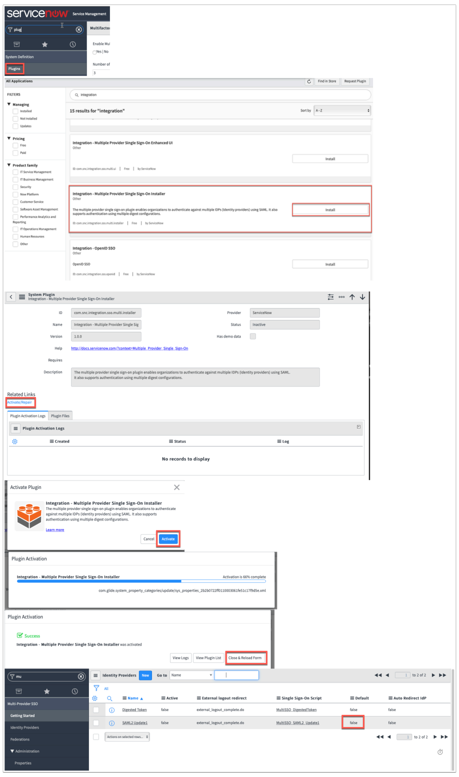
4. Once you found the Plugin has opened click **Install**

5. On the **Activate Plugin** window. Confirm the activation on the pop-up by clicking **Activate**

6. After a few moments the Plugin will have installed and you can click on **Close & Reload Form**

7. If you now type "**Multi**" in to the top Left hand **Filter navigator** area. You will see the option for **Multiple Provider SSO**

8. Under **Multi-Provider SSO** select Identity Providers



15 results for "integration"

Integration - Multiple Provider Single Sign-On Enhanced UI
Other
ID: com.snc.integration.sso.multi.ui | Free | by ServiceNow

Integration - Multiple Provider Single Sign-On Installer
Other
The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML. It also supports authentication using multiple digest configurations.
ID: com.snc.integration.sso.multi.installer | Free | by ServiceNow

Integration - OpenID SSO
Other
OpenID SSO
ID: com.snc.integration.sso.openid | Free | by ServiceNow

System Plugin
Integration - Multiple Provider Single Sign-On Installer

ID: com.snc.integration.sso.multi.installer
Provider: ServiceNow
Name: Integration - Multiple Provider Single Sig
Status: Inactive
Version: 1.0.0
Has demo data: □
Help: http://docs.servicenow.com/?context=Multiple_Provider_Single_Sign-On
Requires:
Description: The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML. It also supports authentication using multiple digest configurations.

No records to display

Activate Plugin
Integration - Multiple Provider Single Sign-On Installer
The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML. It also supports authentication using multiple digest configurations.

Plugin Activation
Integration - Multiple Provider Single Sign-On Installer   Activation is 66% complete
com.glide.system_property_categories/update/sys_properties_2b2b0722ff0110003061fe51c17f9d5e.xml

Plugin Activation
Success
Integration - Multiple Provider Single Sign-On Installer was activated

Name	Active	External logout redirect	Single Sign-On Script	Default	Auto Redirect IdP
Digested Token	false	external_logout_complete.do	MultiSSO_DigestedToken	false	false
SAML2 Update1	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false

9. Navigate to the ControlCenter2 Virtual Machine inside the lab environment and on the desktop click on **Remote Desktop folder** and double click.the **ADFS.rdp**

10 . On the ADFS virtual machine open **Firefox** and navigate to your unique **devXXX.service-now.com** instance. Authenticate as **admin**

11. In the **Filter navigator** area type "**Multi".** Below **Multi-Provider SSO** select **Identity Providers**

12. In the top area. Click on **New** next to the **Identity Providers**

13. Under **Digest** select **SAML**

14. When the **Import Identity Metadata** window launches. Click **Cancel** at will be manually configuring the parameters

15. Fill in the following details on the Form

- **Name: ADFS**
- **Identity Provider URL: http://adfs.euc-livefire.com/adfs/services/trust**
- **Identity Provider's AuthnRequest: https://adfs.euc-livefire.com/adfs/ls**
- **Identity Provider's SingleLogoutRequest:** BLANK
- **ServiceNow Homepage: https://devXXX.service-now.com/navpage.do** (replace XXX with your unique tenant)

- **EntityID/ Issuer :** https://devXXX.service-now.com (replace XXX with your unique tenant)
- **Audience URI:** https://devXXX.service-now.com (replace XXX with your unique tenant)

NOTE: You will not be able to set the Identity Provider to **Active** or **Default** yet as the Connection has not been tested.

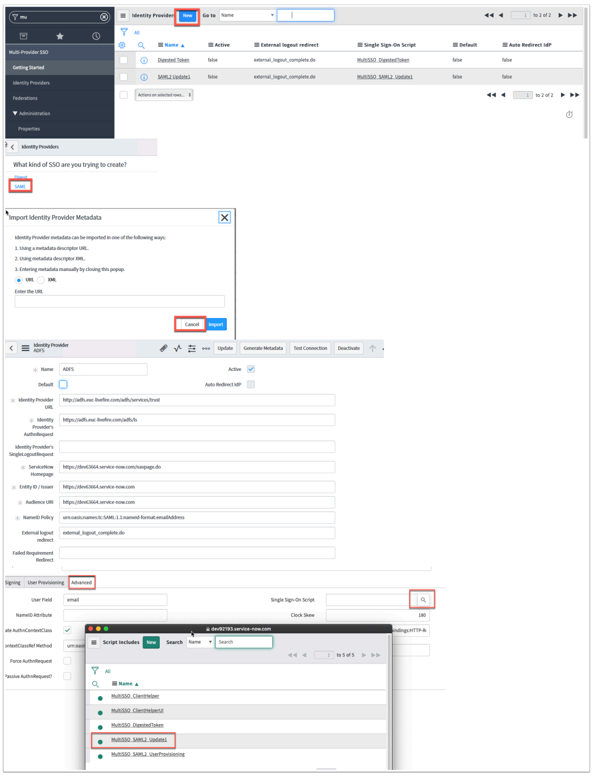
This will be done at a later stage. Leave the rest of the values Default

16. Scroll down and you will see 3 Tabs starting with **Encryption and Signing** and ending with **Advanced.** Select **Advanced** tab

17 . Next to **Single Sign-On Script** click the **Magnifying Loop icon** and in the **new Script includes** window click **MultiSSO_SAML2_Update1**

NOTE: If your Datacenter is the New York Datacenter you might have to use the **MultiSSOv2_SAML2_internal** Single Sign On Script. This will be apparent when you get to the section **Test & Enable Authentication** and you have to **TEST Connection**

18. Click **Submit** at the bottom of the page.



Name	Active	External logout redirect	Single Sign-On Script	Default	Auto Redirect IdP
Digested Token	false	external_logout_complete.do	MultiSSO_DigestedToken	false	false
SAML2 Update1	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false

What kind of SSO are you trying to create?

Digest
SAML

Import Identity Provider Metadata

Identity Provider metadata can be imported in one of the following ways:
1. Using a metadata descriptor URL.
2. Using metadata descriptor XML.
3. Entering metadata manually by closing this popup.

● URL ○ XML

Enter the URL

Name: ADFS
Active: ☑
Default: □
Auto Redirect IdP: □
Identity Provider URL: http://adfs.euc-livefire.com/adfs/services/trust
Identity Provider's AuthnRequest: https://adfs.euc-livefire.com/adfs/ls
Identity Provider's SingleLogoutRequest:
ServiceNow Homepage: https://dev63664.service-now.com/navpage.do
Entity ID / Issuer: https://dev63664.service-now.com
Audience URI: https://dev63664.service-now.com
NameID Policy: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
External logout redirect: external_logout_complete.do
Failed Requirement Redirect:

User Field: email
Single Sign-On Script:
NameID Attribute:
Clock Skew: 180
ate AuthnContextClass: ☑
ontextClassRef Method: urn:oasi
Force AuthnRequest: □
Passive AuthnRequest?: □

MultiSSO_ClientHelper
MultiSSO_ClientHelperUI
MultiSSO_DigestedToken
MultiSSO_SAML2_Update1
MultiSSO_SAML2_UserProvisioning

19. In the middle pane, select the **ADFS** Identity Provider

20. Scroll down to the bottom of the page until you find the heading **Related Links** . Next to **X.509 Certificates** Click **New**.

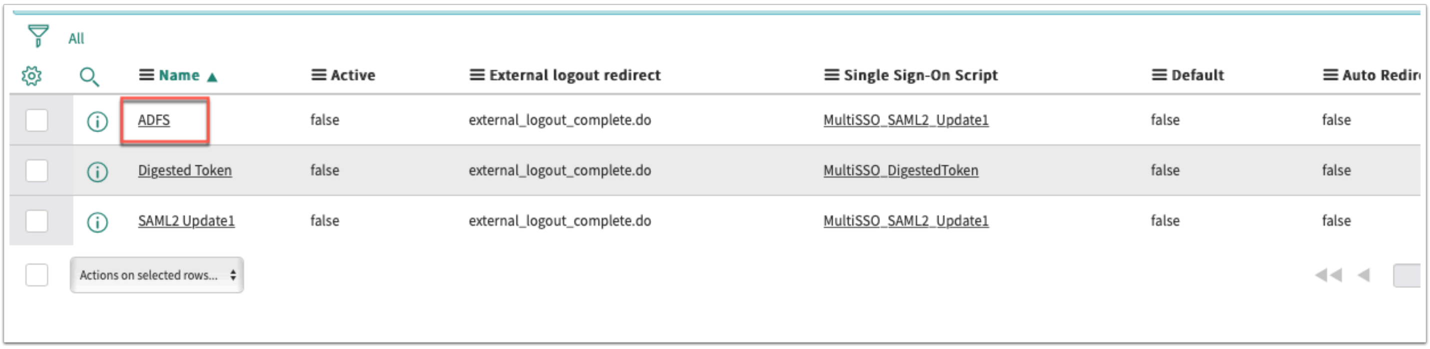
21. In the **X509 New Record** window add the following:

- **Name: ADFS Signing**
- **Copy** the text below and paste in the **PEM Certificate** box at the bottom of the page. Alternatively you can also copy the contents of the certificate located on the desktop called ADFS signing cert.cer

```
-----BEGIN CERTIFICATE-----
MIIC3DCCAcSgAwIBAgIQFbvkYdFx4qVCLeNRwo1NWTANBgkqhkiG9w0BAQsFADAq
MSgwJgYDVQQDEx9BREZTIFNpZ25pbmcgLSBldWMtbGl2ZWZpcmUuY29tMB4XDTE5
MDcwMzA5MDAzNFoXDTIwMDcwMjA5MDAzNFowKjEoMCYGA1UEAxMfQURGUyBTaWdu
aW5nIC0gZXVjLWxpdmVmaXJlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAJ4I7Uzkyui6X4br8LrrVfaRgS+Z9izZZnXDgxczONL+mQ1aKks+e116
mHMEaWNuzVjaK3NqsHzPycBIGPNmSM96qdrWcC+zoz8CmmjnDbWUwlU5LywYs1QN
YZvugi0DtIsnR/c6dDodAc7C44o6gUy1emwTxOHF1zx19xnCWsxGmR4q3liakWwk
n4oaUwSPG3ZBwVbSnji/AZrEDiFu+nz+rkAMAmQ/YnYpwRWhR0ru/sbqjFzkvBb8
lhPdz4HJWe43Vi65Ms+9a4FW4uIqUq3jRQxqtlzfkJdlEaa2hf/k5dgkfakaAuw+
GCJyzfayIAX+i9P/TwirwTImgHqbrv0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
Apa4igdrsvXPD3RcNgcjbYjLUu8dAKkoSIfVLjKJ7GzWEqhr5uIpgNhqgIQpK+yT
rDlMG7kgewWoRhNqpccduRcceRwYXQZzWmlVxOFoCVDIGIMxmat5P2WnYQc/r8IF
QjgGhXv4KyGGSLAs5jAbbInRAN+ViyN/rlji/8jAQr8Cf9o2WE/ZHP1bheGFTIam
/0nOdjDSo+/3rCvx9NPuTn7B99peXeg8sUvKyH8Oj3kgglqODfY0dlhirvuMtgKM
2FdnFdT00h//1XT90A2LVWgdSeYFRWM6KMYYvvfE2DtZByHzQy3f4k3kae6TBrDe
T6FSNfmpB7pYssoeOVoM6Q==
-----END CERTIFICATE-----
```

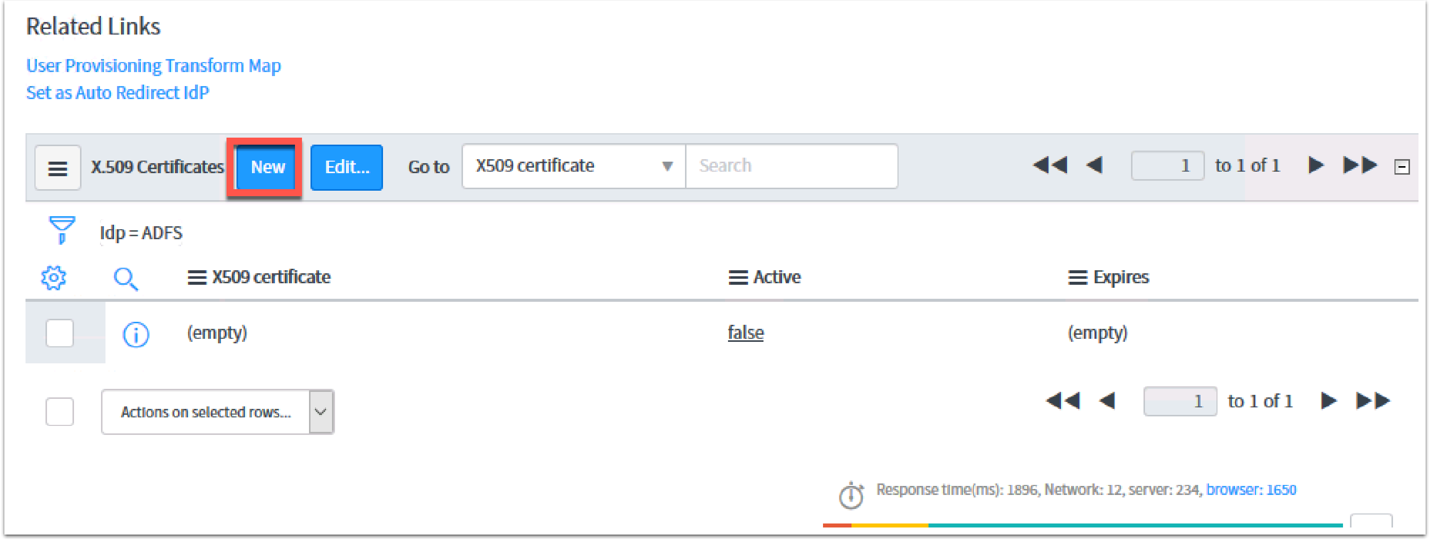
22 . Click **Submit** at the bottom of the page. Once you click back into the certificate you should see the Issuer and Subject fields filled in.

23. At the top of the page click **Update** to reflect the changes made



All

		Name ▲	Active	External logout redirect	Single Sign-On Script	Default	Auto Redir
□	ⓘ	ADFS	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false
□	ⓘ	Digested Token	false	external_logout_complete.do	MultiSSO_DigestedToken	false	false
□	ⓘ	SAML2 Update1	false	external_logout_complete.do	MultiSSO_SAML2_Update1	false	false



Related Links

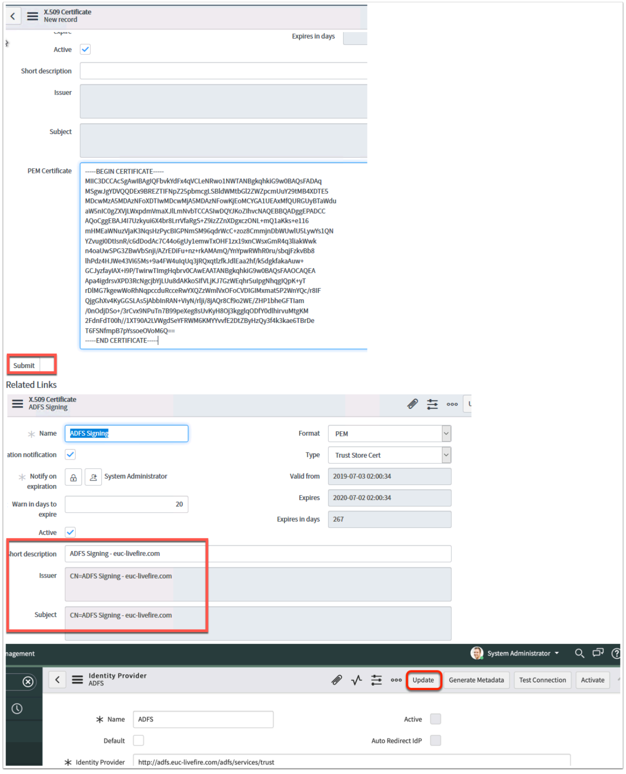
User Provisioning Transform Map
Set as Auto Redirect IdP

X.509 Certificates
New
Edit...
Go to
X509 certificate
Search
1
to 1 of 1

Idp = ADFS

		X509 certificate	Active	Expires
□	ⓘ	(empty)	false	(empty)

Actions on selected rows...
1
to 1 of 1
Response time(ms): 1896, Network: 12, server: 234, browser: 1650



Expires in days

Active ☑

Short description

Issuer

Subject

PEM Certificate

```
-----BEGIN CERTIFICATE-----
MIIC3DCCAcSgAwIBAgIQFbvkYdFx4qVCLeNRwo1NWTANBgkqhkiG9w0BAQsFADAq
MSgwJgYDVQQDEx9BREZTIFNpZ25pbmcgLSBldWMtbGl2ZWZpcmUuY29tMB4XDTE5
MDcwMzA5MDAzNFoXDTIwMDcwMjA5MDAzNFowKjEoMCYGA1UEAxMfQURGUyBTaWdu
aW5nIC0gZXVjLWxpdmVmaXJlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAJ4I7Uzkyui6X4br8LrrVfaRgS+Z9izZZnXDgxczONL+mQ1aKks+e116
mHMEaWNuzVjaK3NqsHzPycBIGPNmSM96qdrWcC+zoz8CmmjnDbWUwlU5LywYs1QN
YZvugi0DtIsnR/c6dDodAc7C44o6gUy1emwTxOHF1zx19xnCWsxGmR4q3liakWwk
n4oaUwSPG3ZBwVbSnji/AZrEDiFu+nz+rkAMAmQ/YnYpwRWhR0ru/sbqjFzkvBb8
lhPdz4HJWe43Vi65Ms+9a4FW4uIqUq3jRQxqtlzfkJdlEaa2hf/k5dgkfakaAuw+
GCJyzfayIAX+i9P/TwirwTImgHqbrv0CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
Apa4igdrsvXPD3RcNgcjbYjLUu8dAKkoSIfVLjKJ7GzWEqhr5uIpgNhqgIQpK+yT
rDlMG7kgewWoRhNqpccduRcceRwYXQZzWmlVxOFoCVDIGIMxmat5P2WnYQc/r8IF
QjgGhXv4KyGGSLAs5jAbbInRAN+ViyN/rlji/8jAQr8Cf9o2WE/ZHP1bheGFTIam
/0nOdjDSo+/3rCvx9NPuTn7B99peXeg8sUvKyH8Oj3kgglqODfY0dlhirvuMtgKM
2FdnFdT00h//1XT90A2LVWgdSeYFRWM6KMYYvvfE2DtZByHzQy3f4k3kae6TBrDe
T6FSNfmpB7pYssoeOVoM6Q==
-----END CERTIFICATE-----
```

Name: ADFS Signing

ation notification ☑

Notify on expiration: System Administrator

Warn in days to expire: 20

Active ☑

Format: PEM

Type: Trust Store Cert

Valid from: 2019-07-03 02:00:34

Expires: 2020-07-02 02:00:34

Expires in days: 267

hort description: ADFS Signing - euc-livefire.com

Issuer: CN=ADFS Signing - euc-livefire.com

Subject: CN=ADFS Signing - euc-livefire.com

Name: ADFS

Default □

Active □

Auto Redirect IdP □

Identity Provider: http://adfs.euc-livefire.com/adfs/services/trust

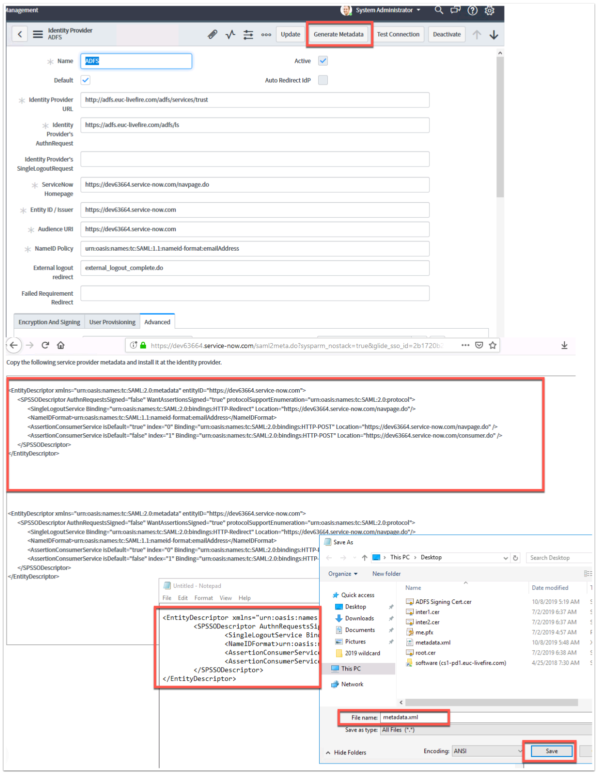
Let's now Generate the Metada to later import into ADFS.

24. In the middle pane select the **ADFS** Identity Provider. that you have just created.

25, At the top of the **Identity Provider ADFS** page next to **Update** click **Generate Metadata**

26. This will open a new tab in your browser and give you a the metadata as text format. **Copy** the text into Notepad and **Save** as **Metadata.xml** to the desktop of the **ADFS virtual machine**.

This will allow us to later import the metadata.xml into ADFS.



Name: ADFS
Active ☑
Default ☑
Auto Redirect IdP ☐
Identity Provider URL: http://adfs.euc-livefire.com/adfs/services/trust
Identity Provider's AuthnRequest: https://adfs.euc-livefire.com/adfs/ls
Identity Provider's SingleLogoutRequest:
ServiceNow Homepage: https://dev63664.service-now.com/navpage.do
Entity ID / Issuer: https://dev63664.service-now.com
Audience URI: https://dev63664.service-now.com
NameID Policy: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
External logout redirect: external_logout_complete.do
Failed Requirement Redirect:

https://dev63664.service-now.com/saml2meta.do?sysparm_nostack=true&glide_sso_id=2b1720b2

Copy the following service provider metadata and install it at the identity provider.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://dev63664.service-now.com">
    <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://dev63664.service-now.com/navpage.do"/>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
        <AssertionConsumerService isDefault="true" index="0" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev63664.service-now.com/navpage.do" />
        <AssertionConsumerService isDefault="false" index="1" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://dev63664.service-now.com/consumer.do" />
    </SPSSODescriptor>
</EntityDescriptor>
```

Name	Date modified
ADFS Signing Cert.cer	10/8/2019 5:19 AM
inter1.cer	7/2/2019 6:37 AM
inter2.cer	7/2/2019 6:37 AM
me.pfx	7/2/2019 4:57 AM
metadata.xml	10/8/2019 5:48 AM
root.cer	7/2/2019 6:38 AM
software (cs1-pd1.euc-livefire.com)	4/25/2018 7:30 AM

File name: metadata.xml
Save as type: All Files (*.*)
Encoding: ANSI

Part 2 : Adding A Rely Party Trust

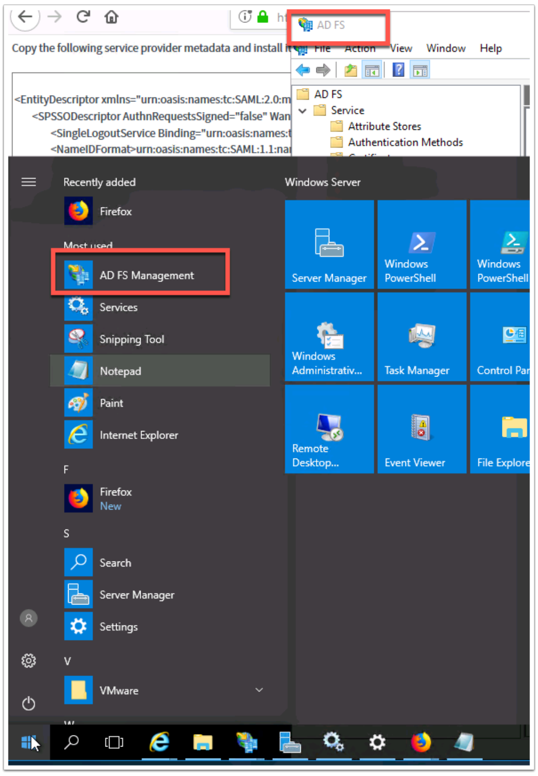
1. On the ADFS virtual machine open the **ADFS Management** interface from the **Start Menu**.

2. In the AD FS Manager navigate to **Relying Party Trusts** and right- click and select **Add Relying Party Trust** in the right hand **Actions** panel.

3. Select **Claims Aware** **radio button** and select **Start**

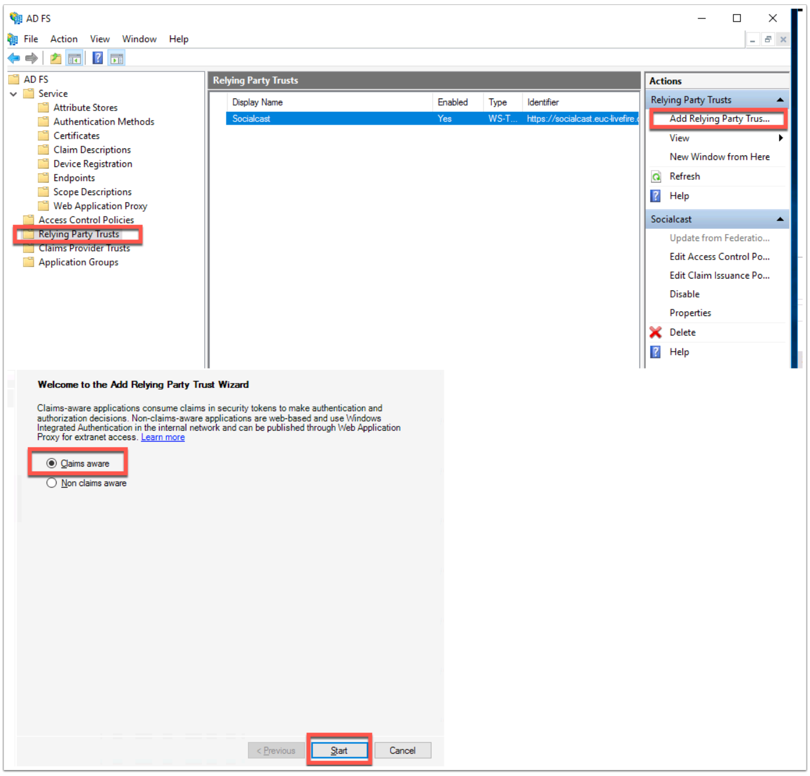
4. On the next screen select **Import data about the relying party from a file** and click **Browse** ... and select the **metadata.xml** file from the desktop.

Click **Next** to confirm



Copy the following service provider metadata and install it

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:m
    <SPSSODescriptor AuthnRequestsSigned="false" Wan
        <SingleLogoutService Binding="urn:oasis:names:t
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nar
```



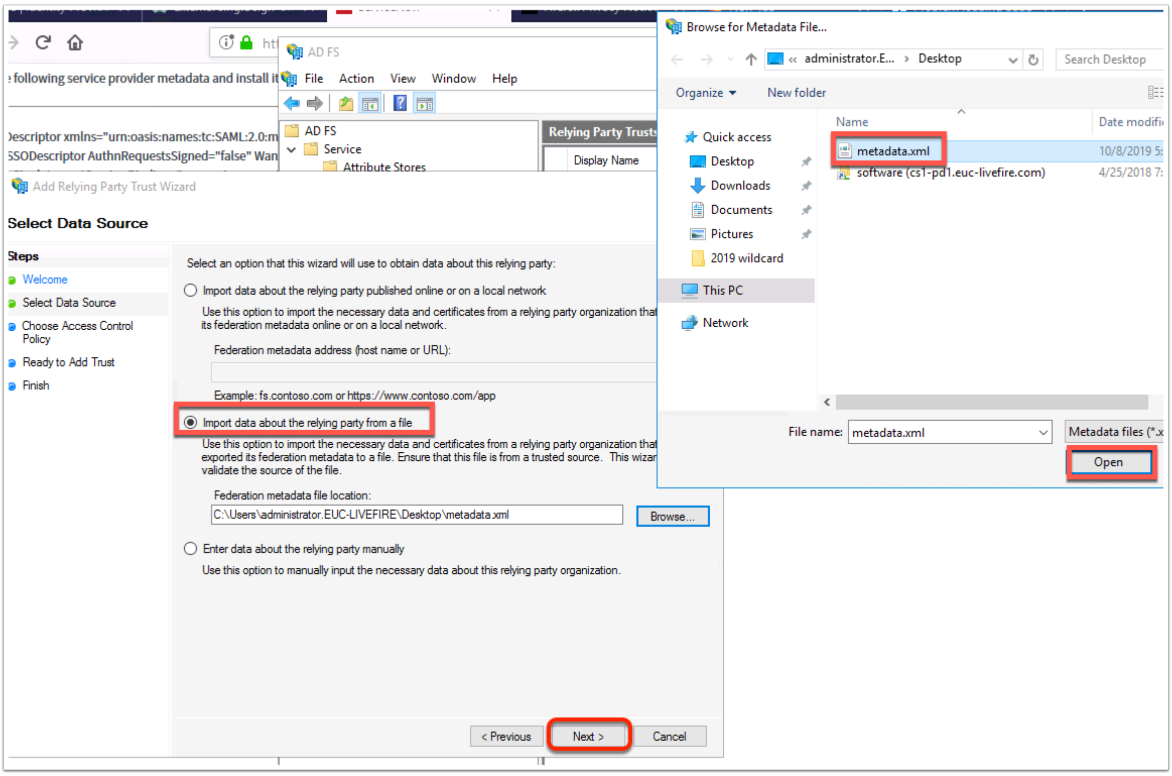
Display Name	Enabled	Type	Identifier
Socialcast	Yes	WS-T...	https://socialcast.euc-livefire.

Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware



Add Relying Party Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

● Import data about the relying party from a file

Federation metadata file location: C:\Users\administrator.EUC-LIVEFIRE\Desktop\metadata.xml

○ Enter data about the relying party manually

Browse for Metadata File... File name: metadata.xml

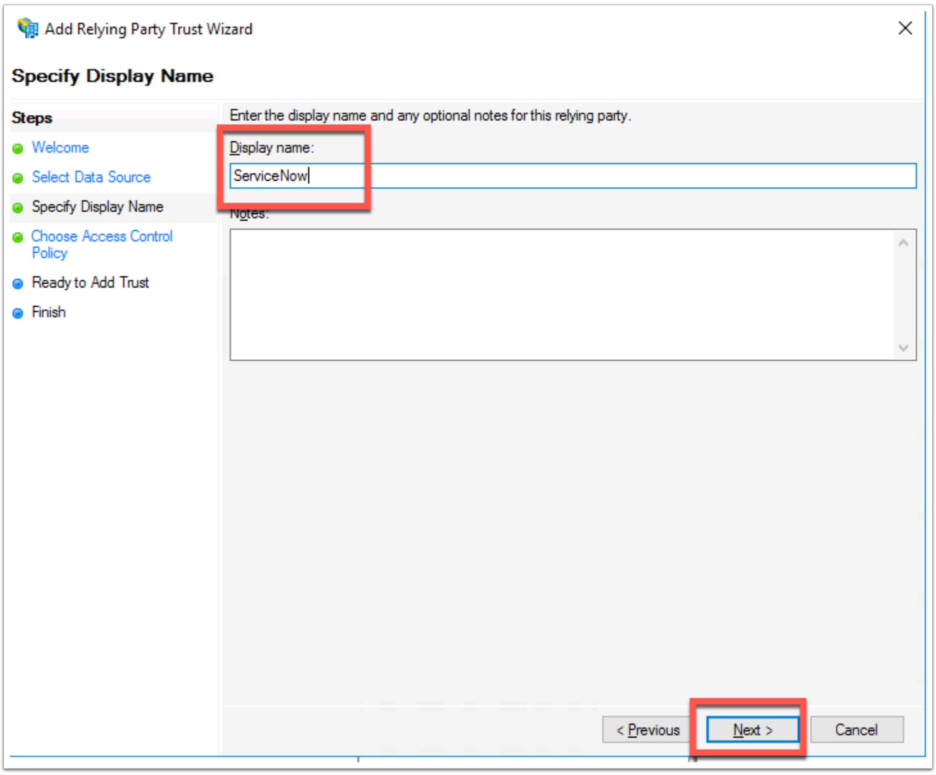
5. Next to **Display name** type : **ServiceNow** and select **Next**

6. Leave the permissions as default to **permit everyone** and select **Next**

7. On the **Ready to Add Trust** page, leave as default and select **Next**

Note: The Metadata we have imported has set the values of the identifiers and endpoints for this connections.

8.On the next page select **Close**.

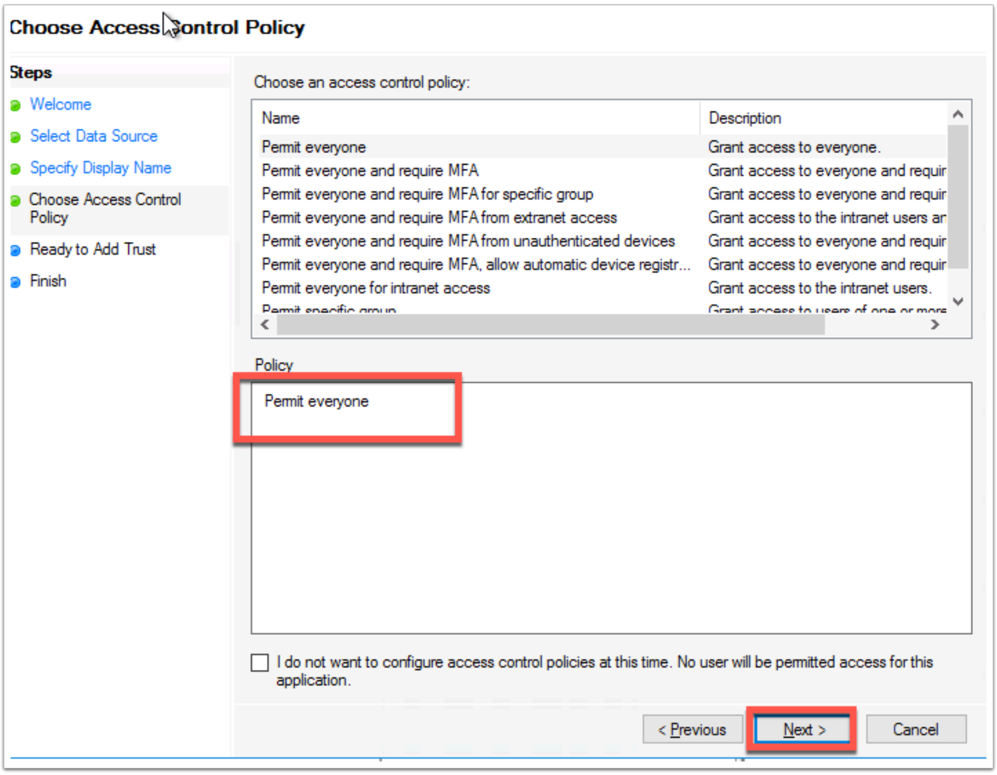


Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: ServiceNow

Notes:



Choose Access Control Policy

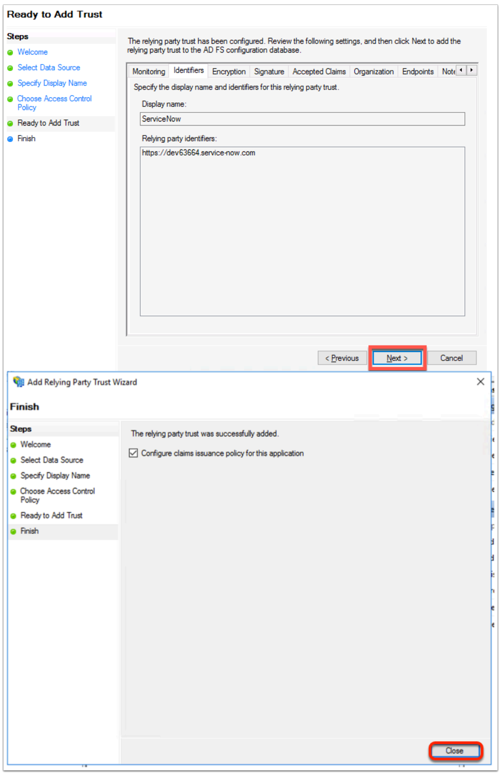
Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

Policy

Permit everyone

□ I do not want to configure access control policies at this time. No user will be permitted access for this application.



The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the display name and identifiers for this relying party trust.

Display name: ServiceNow

Relying party identifiers: https://dev63664.service-now.com

The relying party trust was successfully added.

☑ Configure claims issuance policy for this application

9. **Double click** back into the **ServiceNow** Relying Party Trust we have just set up.

10. This will open the **Properties** of that Relying Party, navigate to the **Advanced** Tab and select **SHA-1** for the Secure Hash algorithm.

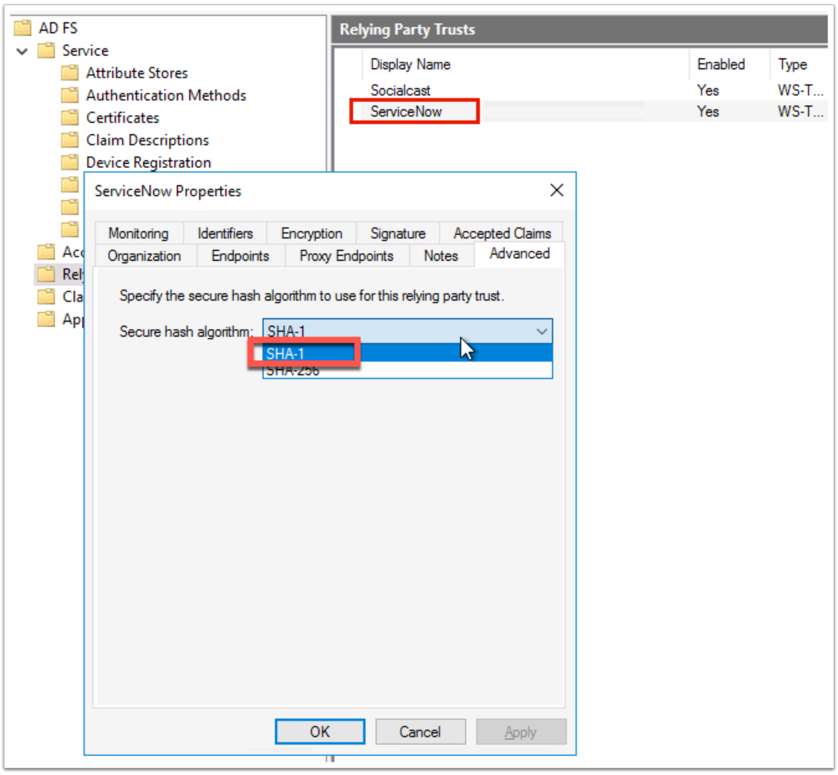
11. Navigate to the **Endpoints** tab in the Properties and click **Add SAML...**

12. Change endpoint type from **SAML Assertion Consumer** to **SAML Logout**

13. Under Binding ensure **Post** is selected

14. In the **Trusted URL:** area **copy** and **paste** the following : https://adfs.euc-livefire.com/adfs/ls/?wa=wsignout1.0

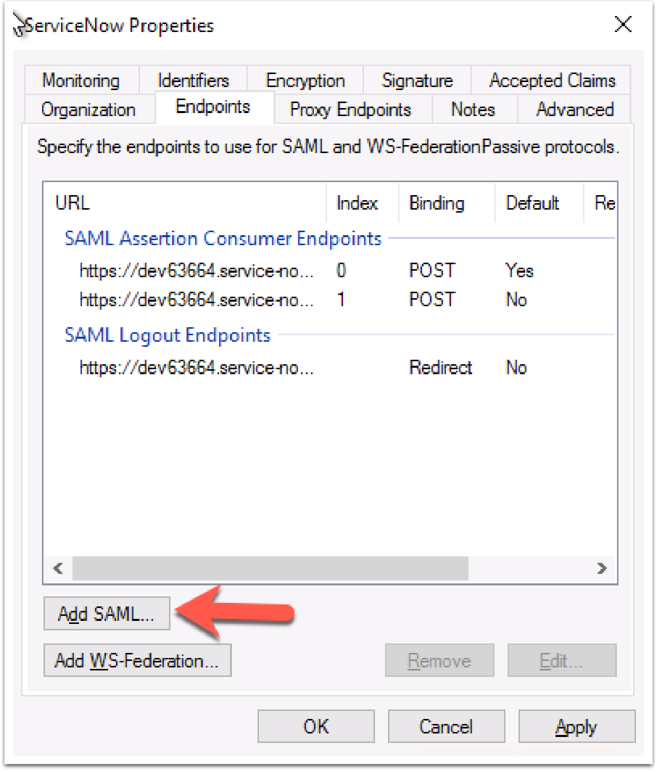
15. Select **OK** and **OK** again to confirm changes



Display Name	Enabled	Type
Socialcast	Yes	WS-T...
ServiceNow	Yes	WS-T...

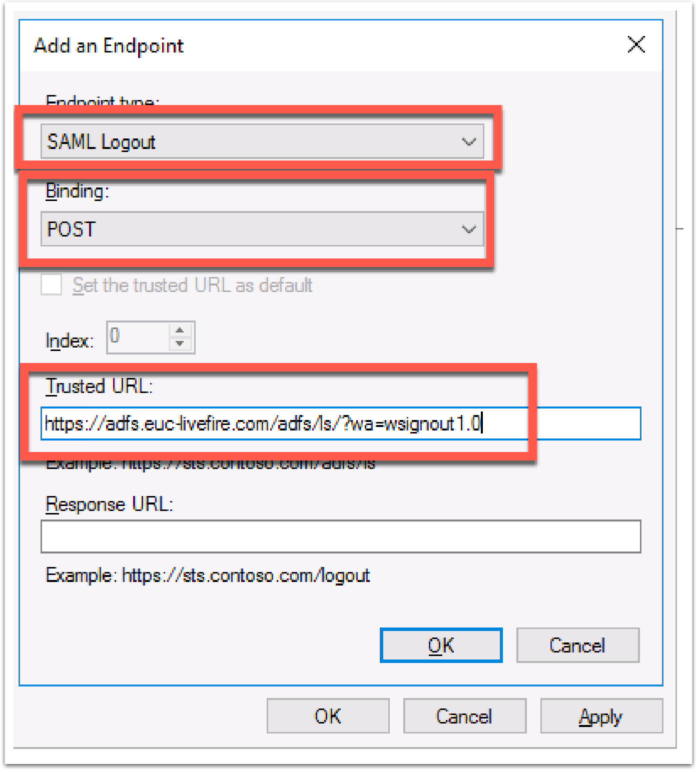
Specify the secure hash algorithm to use for this relying party trust.

Secure hash algorithm: SHA-1



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://dev63664.service-no...	0	POST	Yes	
https://dev63664.service-no...	1	POST	No	
SAML Logout Endpoints				
https://dev63664.service-no...		Redirect	No	



Endpoint type: SAML Logout

Binding: POST

☐ Set the trusted URL as default

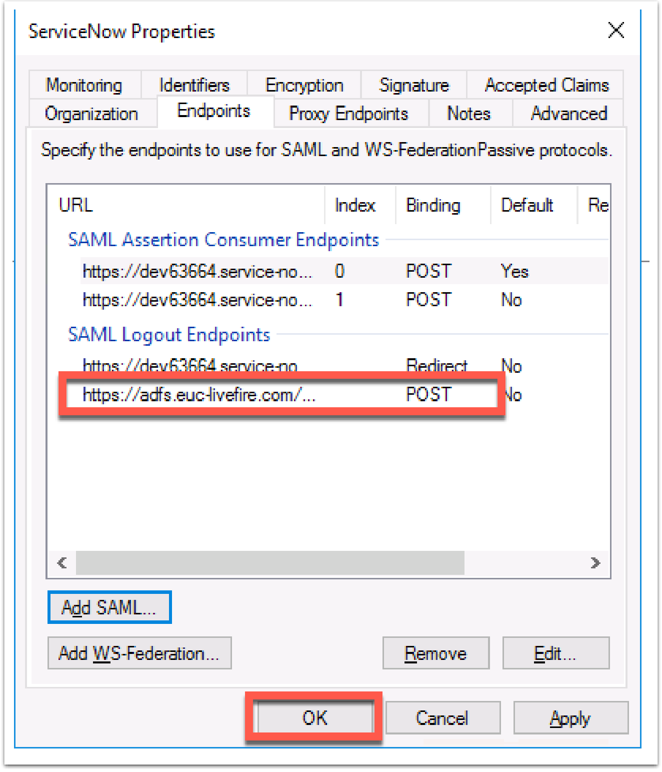
Index: 0

Trusted URL: https://adfs.euc-livefire.com/adfs/ls/?wa=wsignout1.0

Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout



Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Re
SAML Assertion Consumer Endpoints				
https://dev63664.service-no...	0	POST	Yes	
https://dev63664.service-no...	1	POST	No	
SAML Logout Endpoints				
https://dev63664.service-no...		Redirect	No	
https://adfs.euc-livefire.com/...		POST	No	

16. In **Relying Party Trusts** right click **ServiceNow** and click **Edit Claim Issuance Policy**

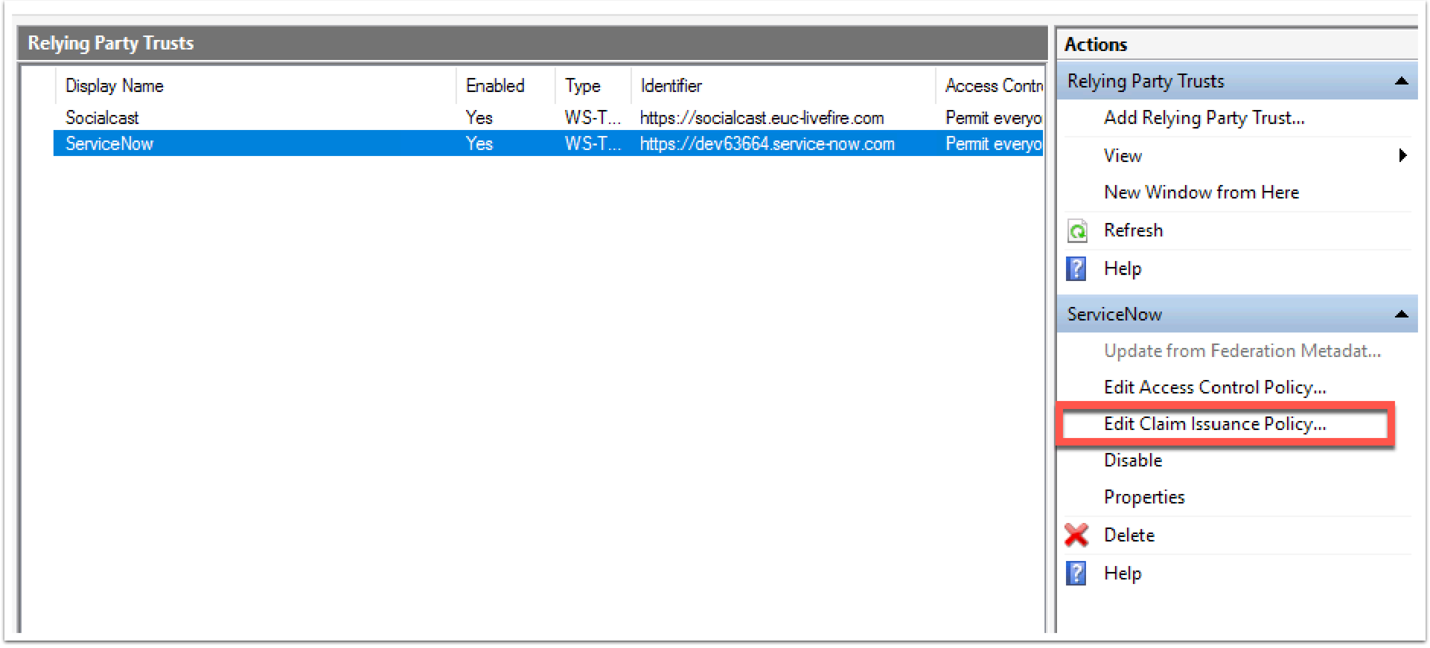
17. Now Click **Add Rule ...** and ensure **Send LDAP attributes as Claims** (default) is selected, select **Next**

18. In the **Claim rule name:** area type **Get Attribute**

19 . In the **dropdown** under **Attribute store.** select **Active Directory**

20. Using the **dropdown** select **E-Mail-Addresses** as the **LDAP Attribute** and **E-mail Address** as the **Outgoing Claim Type**

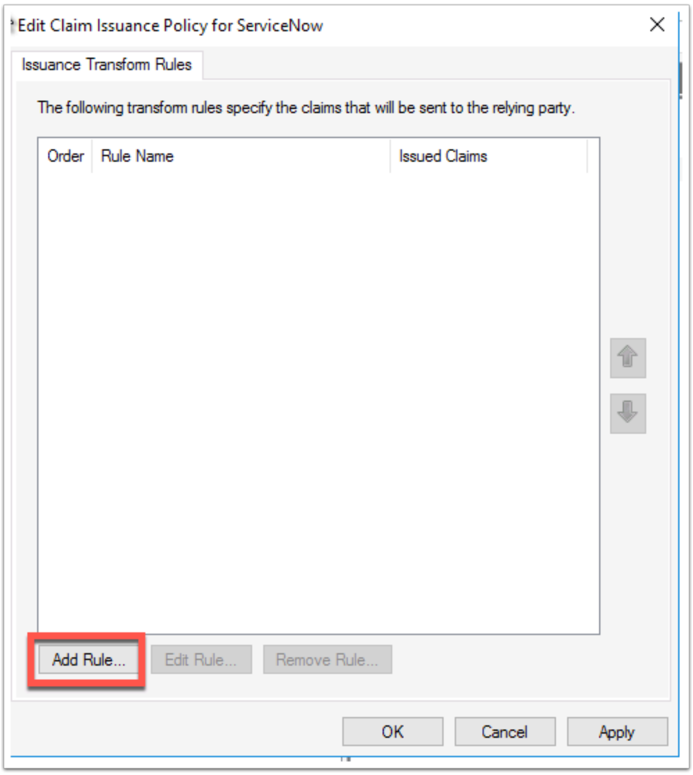
21. Click **Finish** At the bottom of the page to confirm. (Dont Close the window)



Relying Party Trusts

Display Name	Enabled	Type	Identifier	Access Contr
Socialcast	Yes	WS-T...	https://socialcast.euc-livefire.com	Permit everyo
ServiceNow	Yes	WS-T...	https://dev63664.service-now.com	Permit everyo

Actions
Relying Party Trusts
Add Relying Party Trust...
View
New Window from Here
Refresh
Help
ServiceNow
Update from Federation Metadat...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help

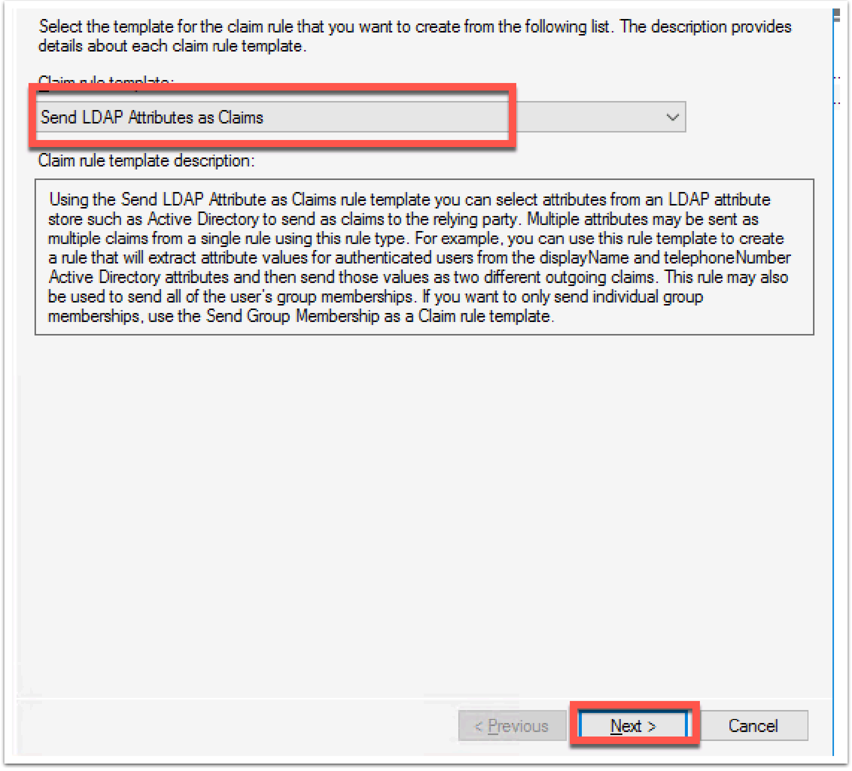


Edit Claim Issuance Policy for ServiceNow

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

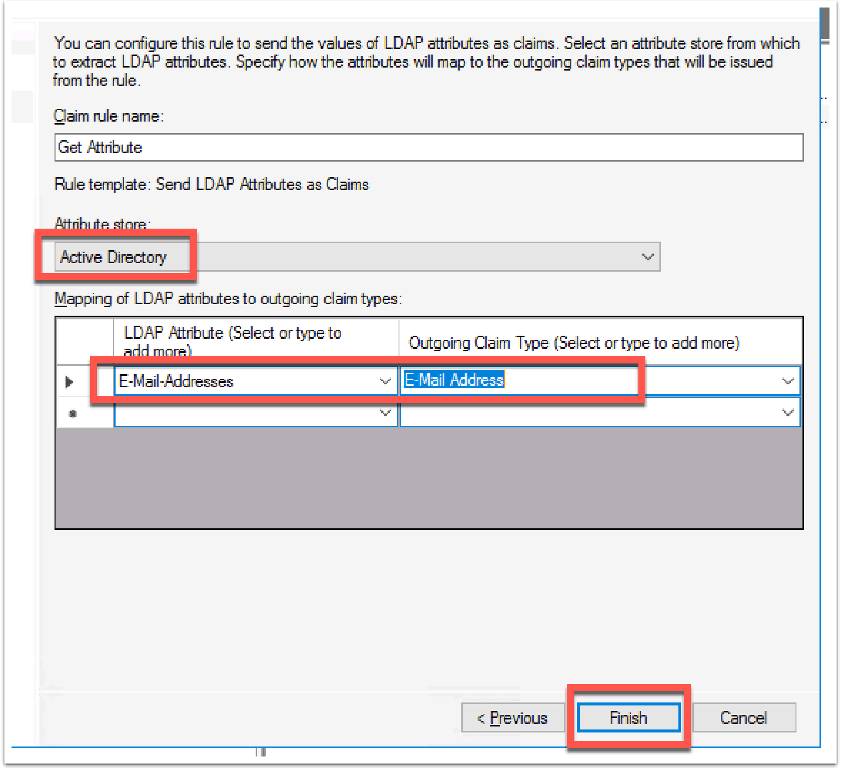

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.


You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Get Attribute

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	E-Mail Address
*		

22. On the **Edit Claim Issuance Policy for ServiceNow** select **Add Rule...**

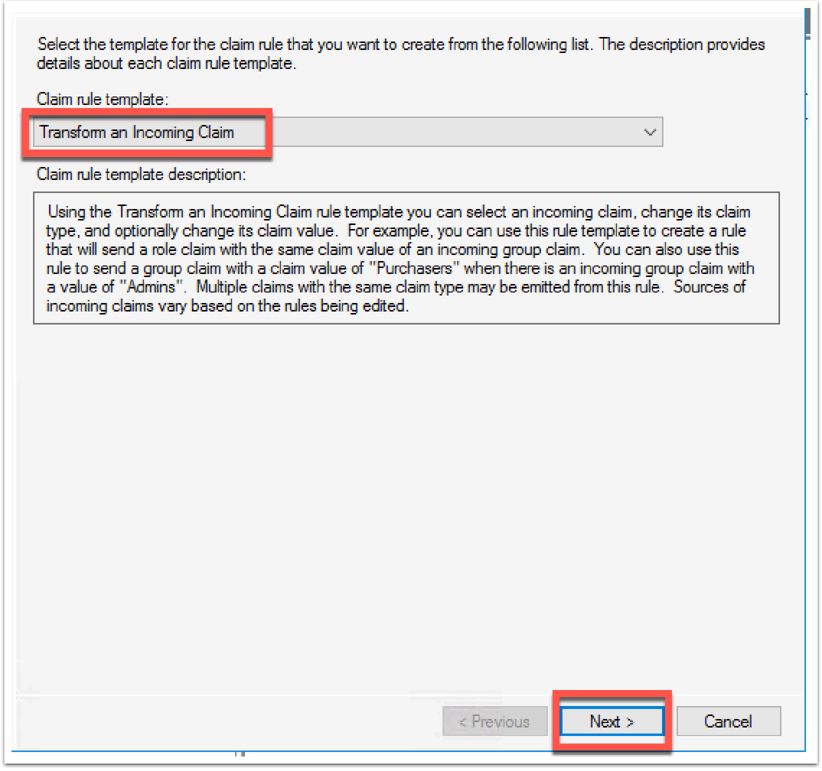
23. This time select **Transform an Incoming Claim** as the template click **Next**

24. Give the Rule the name: **Email to NameID**

- Select **E-mail Address** from **Incoming claim type dropdown**

- Select **Name ID** from **Outgoing claim type**
- Select **Email** from **Outgoing name ID format**

25. Click **Finish** at the bottom of the page to confirm the changes and **OK** to close **Claim Issuance Policy** page.

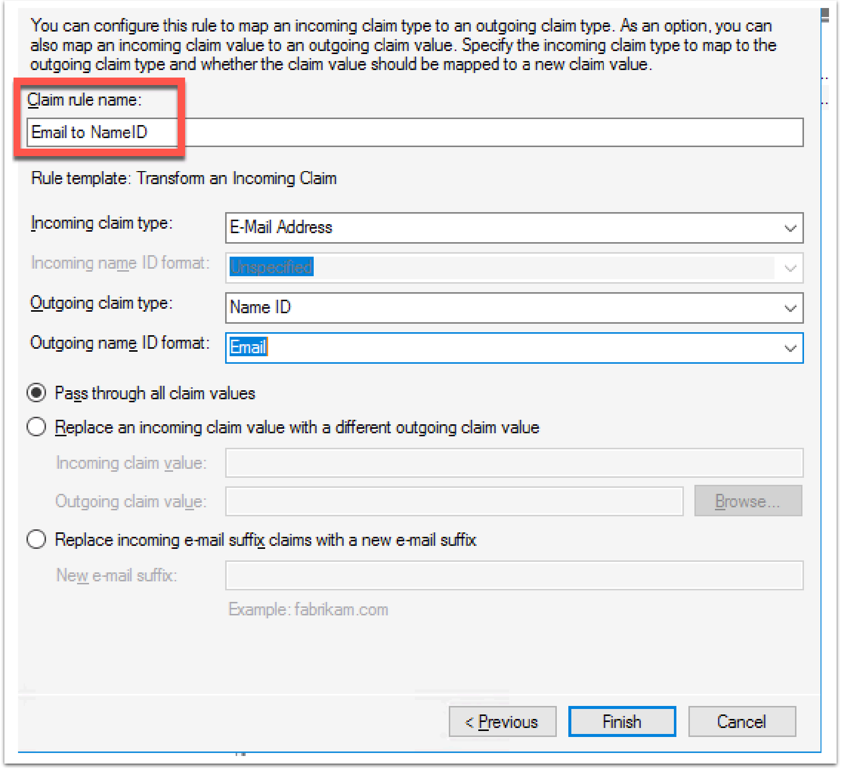


Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.



You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Email to NameID

Rule template: Transform an Incoming Claim

Incoming claim type: E-Mail Address

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Part 3: Test & Enable Authentication for SAML

Let's test now the Federation between ServiceNow and ADFS before we bring WorkspaceONE Access into the picture.

1. Click back into the Firefox browser to your **unique Instance** of ServiceNow. Make sure you are logged in as Admin.

2. In the **ADFS** Identity Provider settings that we setup previously next to **Generate Metadata,** click **Test Connection**

3. Notice a new FireFox window opens where you will see the **Authentication Page for ADFS requesting** authentication.

Enter your **custom account UPN** and the **Password** of your unique user that you added to ServiceNow. Click **Sign in**

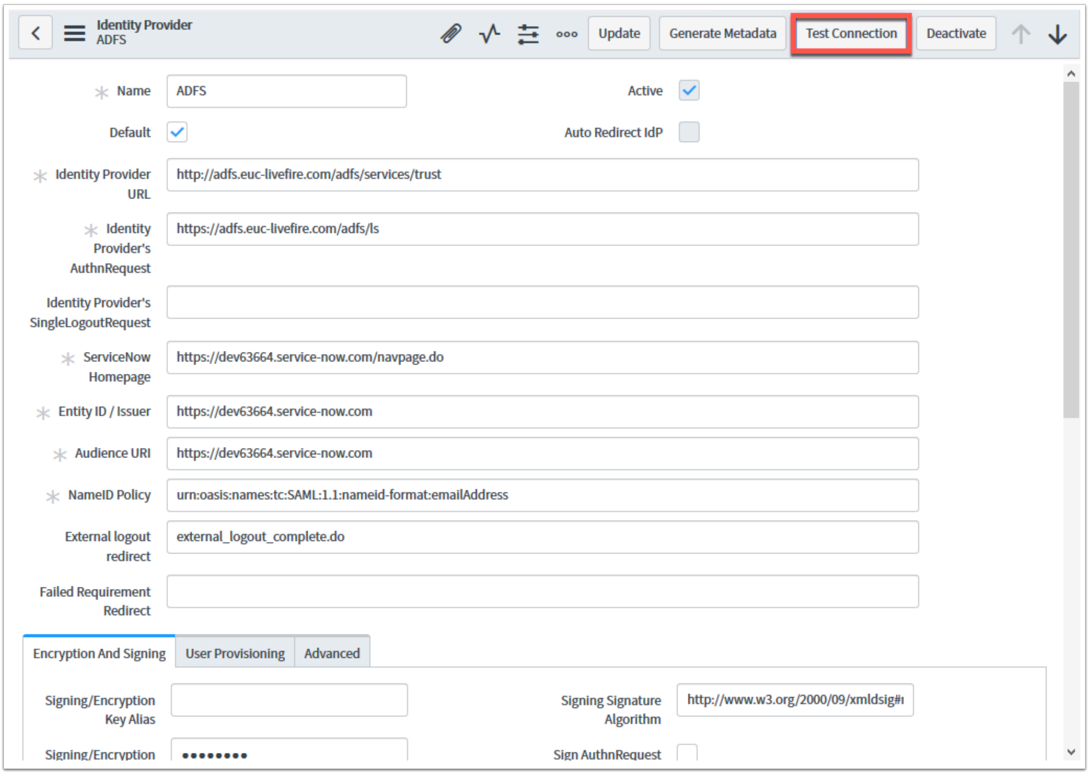
4. It will now run a test on the SAML login parameter. You should have all green tickboxes except for SSO Logout Test.

SSO Logout **Will FAIL** as it cannot do this test. Ignore this for now.

5. At the bottom of the Page select **Activate**

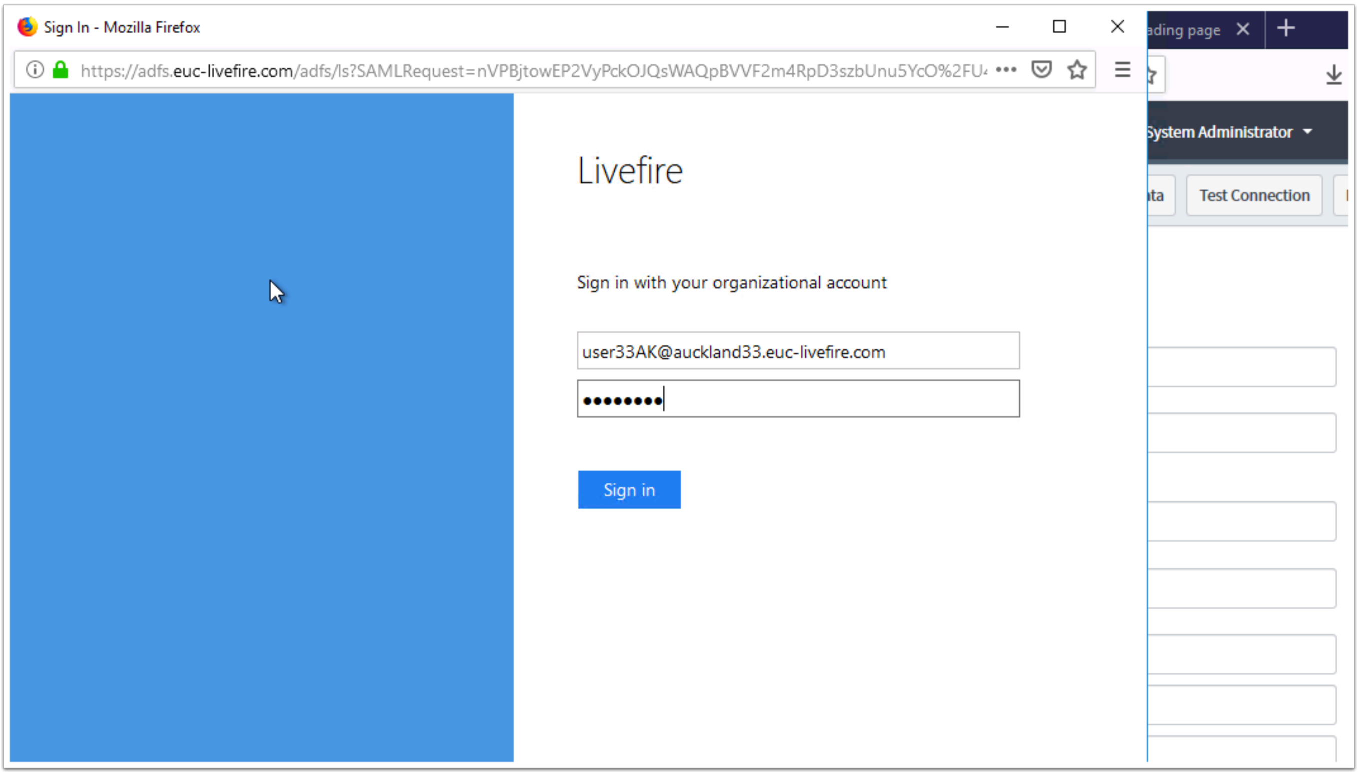
6. Notice at the top of the **ADFS Identity Provider** Screen . The status is now "**Active**".

7. Next to **Default**. Select the **checkbox** and select **Update** at the top.



* Name	ADFS	Active	☑
Default	☑	Auto Redirect IdP	□
* Identity Provider URL	http://adfs.euc-livefire.com/adfs/services/trust		
* Identity Provider's AuthnRequest	https://adfs.euc-livefire.com/adfs/ls		
Identity Provider's SingleLogoutRequest			
* ServiceNow Homepage	https://dev63664.service-now.com/navpage.do		
* Entity ID / Issuer	https://dev63664.service-now.com		
* Audience URI	https://dev63664.service-now.com		
* NameID Policy	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress		
External logout redirect	external_logout_complete.do		
Failed Requirement Redirect			

Signing/Encryption Key Alias		Signing Signature Algorithm	http://www.w3.org/2000/09/xmldsig#r
Signing/Encryption	••••••••	Sign AuthnRequest	□

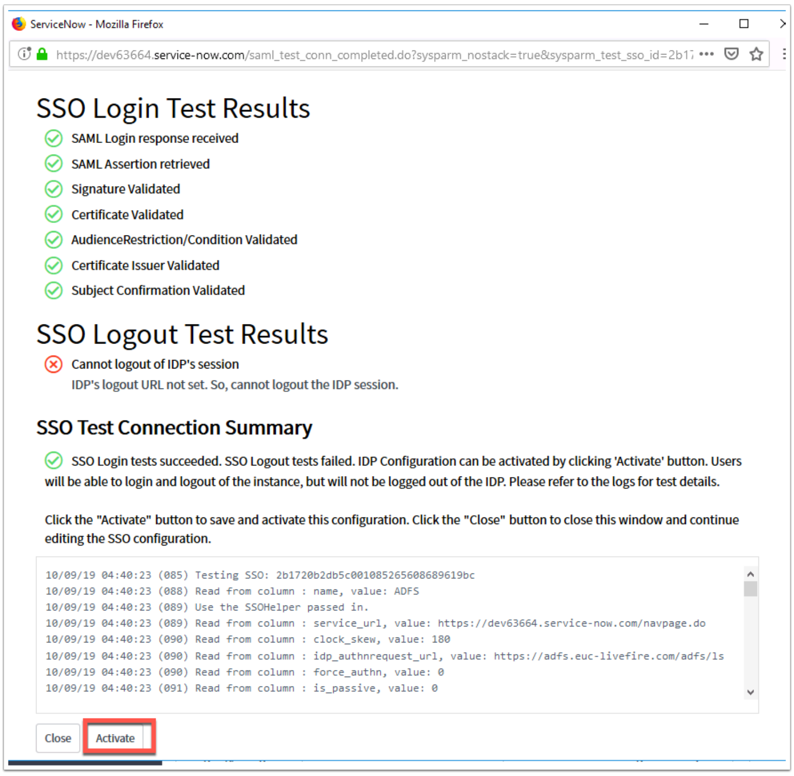

Sign In - Mozilla Firefox
https://adfs.euc-livefire.com/adfs/ls?SAMLRequest=nVPBjtowEP2VyPckOJQsWAQpBVVF2m4RpD3szbUnu5YcO%2FU
ading page
System Administrator
Test Connection

Livefire

Sign in with your organizational account

user33AK@auckland33.euc-livefire.com

••••••••


ServiceNow - Mozilla Firefox
https://dev63664.service-now.com/saml_test_conn_completed.do?sysparm_nostack=true&sysparm_test_sso_id=2b17

SSO Login Test Results

- ✓ SAML Login response received
- ✓ SAML Assertion retrieved
- ✓ Signature Validated
- ✓ Certificate Validated
- ✓ AudienceRestriction/Condition Validated
- ✓ Certificate Issuer Validated
- ✓ Subject Confirmation Validated

SSO Logout Test Results

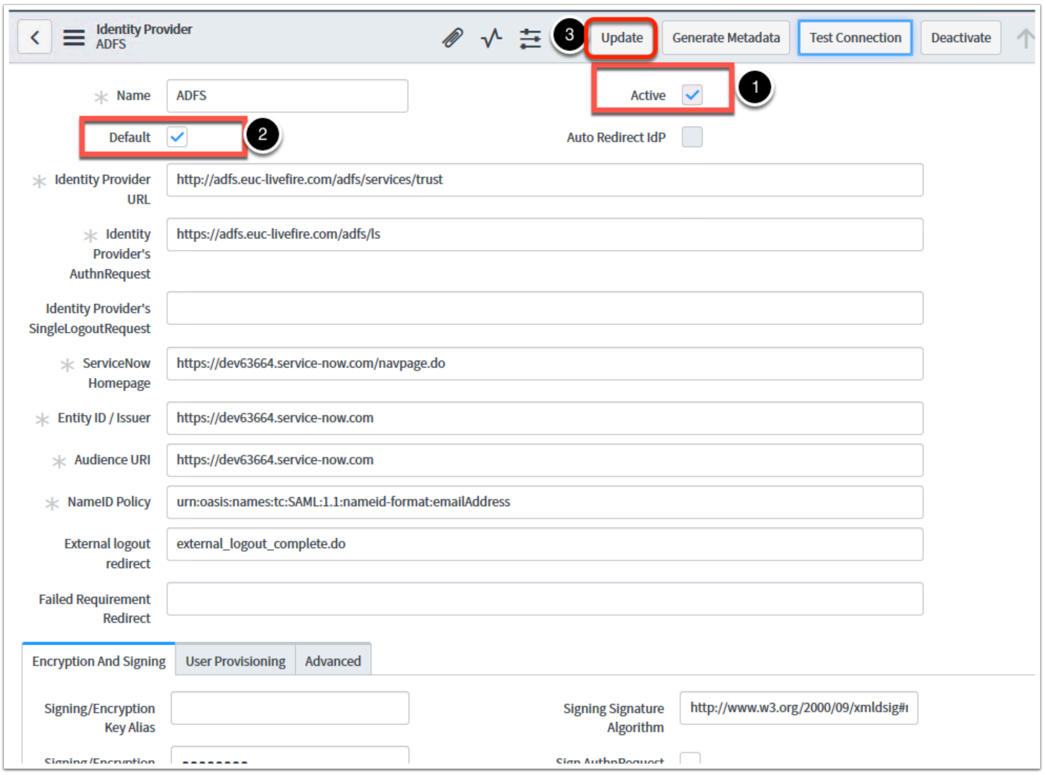
- ☒ Cannot logout of IDP's session
  IDP's logout URL not set. So, cannot logout the IDP session.

SSO Test Connection Summary

✓ SSO Login tests succeeded. SSO Logout tests failed. IDP Configuration can be activated by clicking 'Activate' button. Users will be able to login and logout of the instance, but will not be logged out of the IDP. Please refer to the logs for test details.

Click the "Activate" button to save and activate this configuration. Click the "Close" button to close this window and continue editing the SSO configuration.

```
10/09/19 04:40:23 (085) Testing SSO: 2b1720b2db5c0010852656086896l9bc
10/09/19 04:40:23 (088) Read from column : name, value: ADFS
10/09/19 04:40:23 (089) Use the SSOHelper passed in.
10/09/19 04:40:23 (089) Read from column : service_url, value: https://dev63664.service-now.com/navpage.do
10/09/19 04:40:23 (090) Read from column : clock_skew, value: 180
10/09/19 04:40:23 (090) Read from column : idp_authnrequest_url, value: https://adfs.euc-livefire.com/adfs/ls
10/09/19 04:40:23 (090) Read from column : force_authn, value: 0
10/09/19 04:40:23 (091) Read from column : is_passive, value: 0
```



Name: ADFS

Active ☑

Default ☑

Auto Redirect IdP □

Identity Provider URL: http://adfs.euc-livefire.com/adfs/services/trust

Identity Provider's AuthnRequest: https://adfs.euc-livefire.com/adfs/ls

Identity Provider's SingleLogoutRequest:

ServiceNow Homepage: https://dev63664.service-now.com/navpage.do

Entity ID / Issuer: https://dev63664.service-now.com

Audience URI: https://dev63664.service-now.com

NameID Policy: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

External logout redirect: external_logout_complete.do

Failed Requirement Redirect:

Signing/Encryption Key Alias:

Signing Signature Algorithm: http://www.w3.org/2000/09/xmldsig#

8. Navigate to the **Filter navigator** on the left hand side and type "**Multi**" > Now Select **Properties** under **Administration**

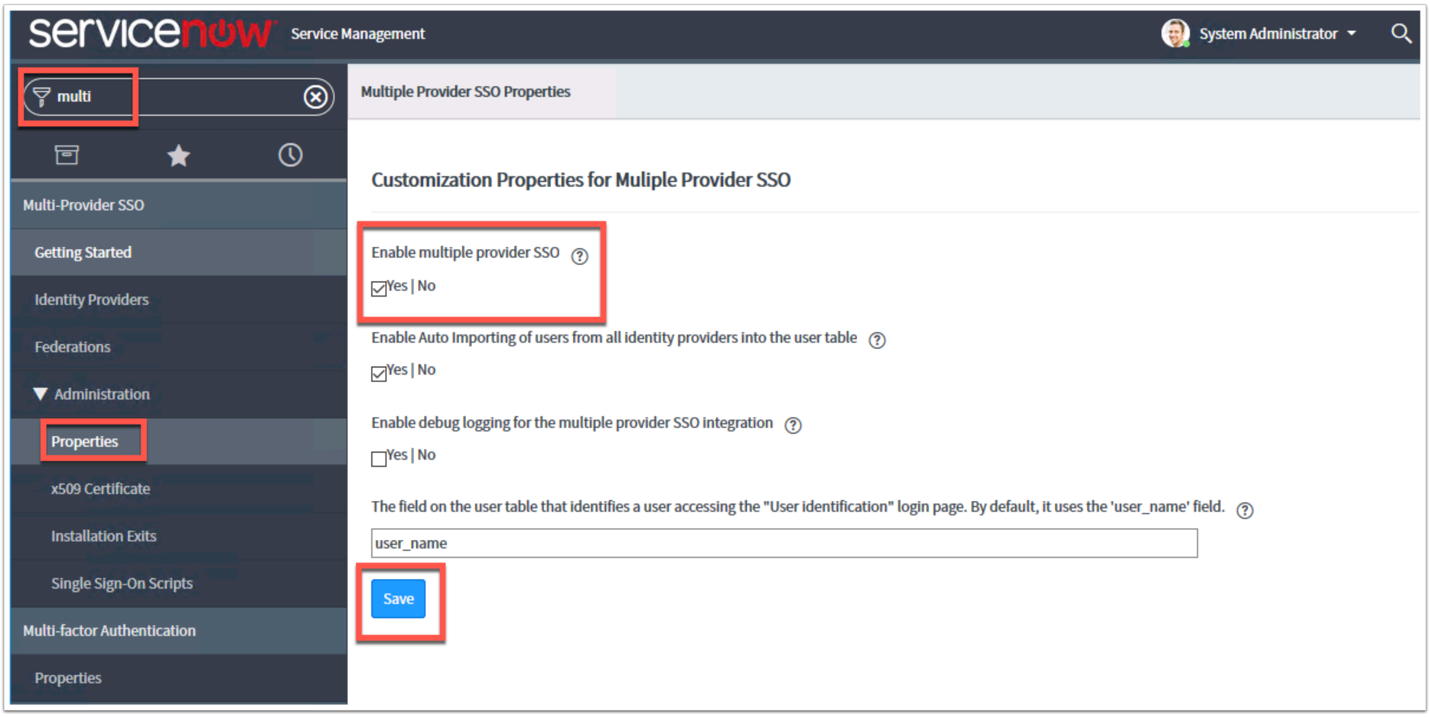
9. In the **Properties** window Under **Enable multiple provider SSO** select **Yes** check box. Select **Save** at the bottom of the page.

10. To do the final test open now a new browser on your **ControlCenter2** virtual machine. Navigate to your unique tenant (ie: https://dev92193.service-now.com) and click **Use external login.**

11. Now type in your **custom unique user account** ie **User35crsj**, created earlier in the users section. select **Submit**

12. You should now be redirected to your ADFS authentication page. Here put in your **UPN** e.g. **user35crsj@sanjose35.euc-livefire.com** and **password** from AD and select **Sign In**

You should be authenticated as the user now to ServiceNow



Customization Properties for Muliple Provider SSO

Enable multiple provider SSO

☑ Yes | No

Enable Auto Importing of users from all identity providers into the user table

☑ Yes | No

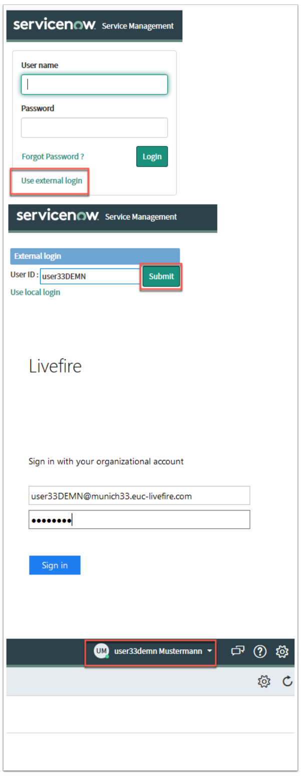
Enable debug logging for the multiple provider SSO integration

□ Yes | No

The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field.

user_name

Save



User ID : user33DEMN Submit

Sign in with your organizational account

user33DEMN@munich33.euc-livefire.com

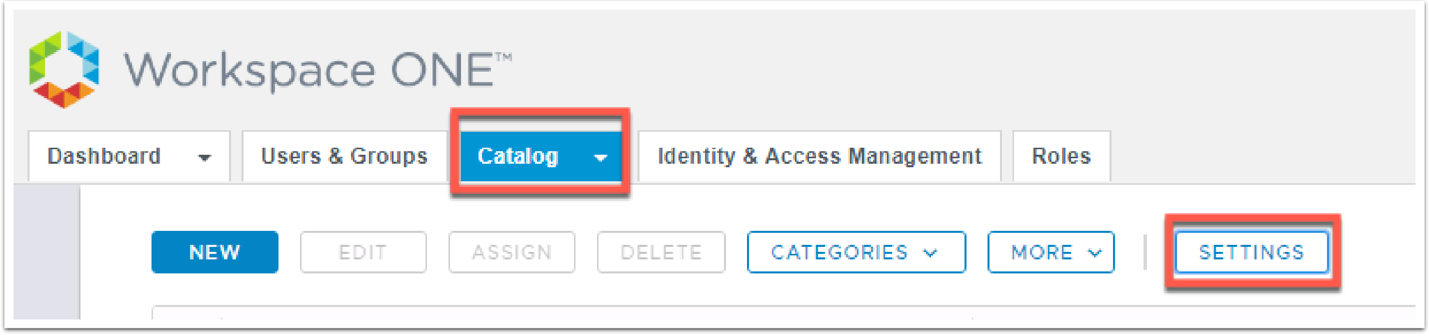
••••••••

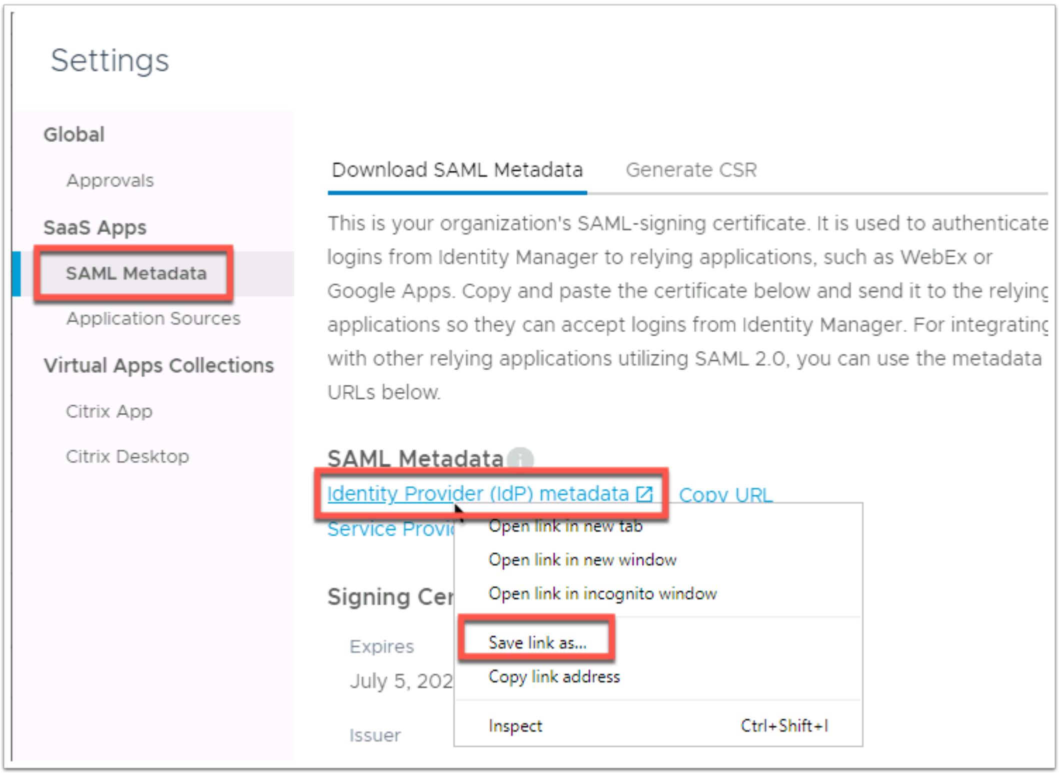
Sign in

Part 4: Adding Access as Claims Provider in ADFS

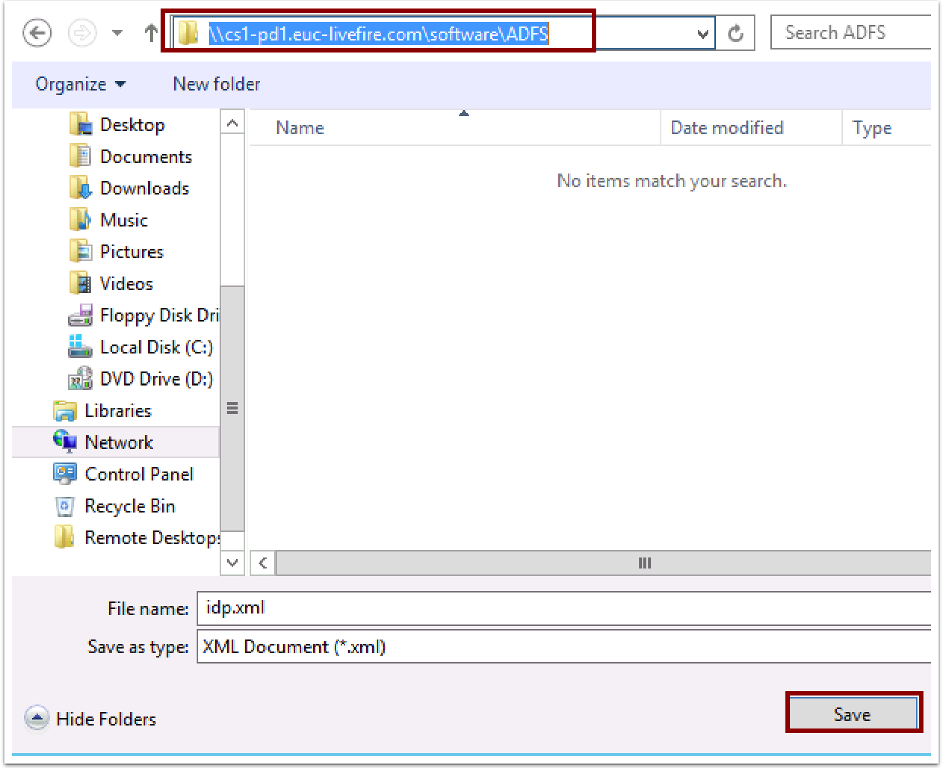
1. On your **controlcenter2** open FireFox and browse to your unique Workspace ONE Access Admin tenant.
2. **Select** the **System Domain** from the drop down domain drop down option and authenticate using the **administrator** account
3. In the admin console click on **catalog** and click **Settings**

4. In the Left Navigation column select **SAML metadata** under **SaaS Apps**
5. Right click the **Identity Provider (IdP) metadata** and select **save link as ...** IDP.xml
6. In the browser window that opens navigate to the **Software** folder on the desktop and open the **ADFS** folder and select **Save**





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.



File name: idp.xml

Save as type: XML Document (*.xml)

7. Open the **Remote Desktop** folder on the desktop and **RDP** to the **ADFS server**

8. In **Server Manager** and at the top, select **Tools** and select **AD FS Management**

9. When the AD FS Management interface is open navigate to **Claims Provider Trusts** (Only Active Directory should be present)

10 Right Click **Claims Provider Trust** and select **Add Claims Provider Trust...**

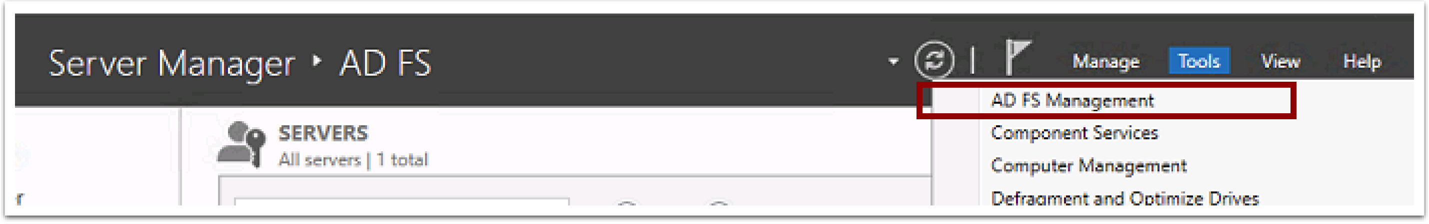
11. Click **Start** on the first Welcome page

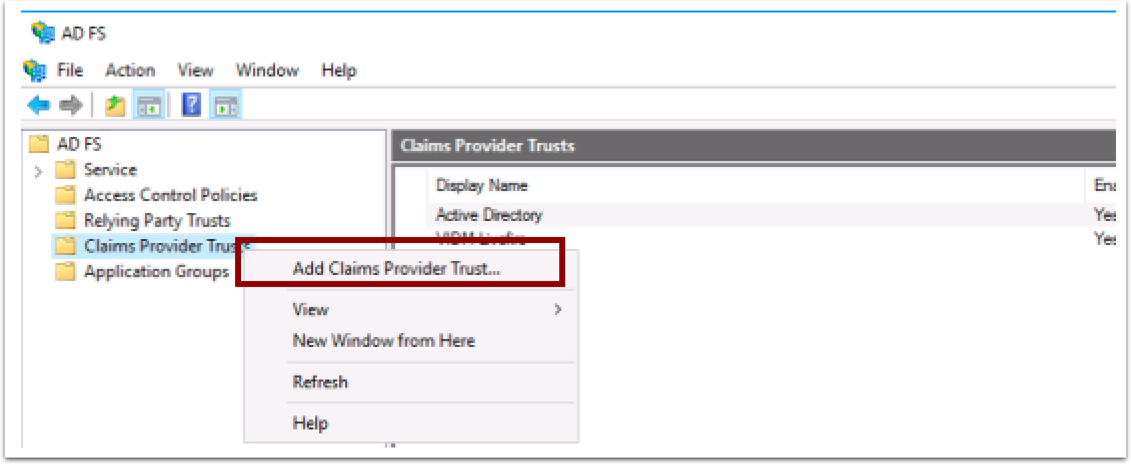
12.Then select **Import data about the claims provider from a file**

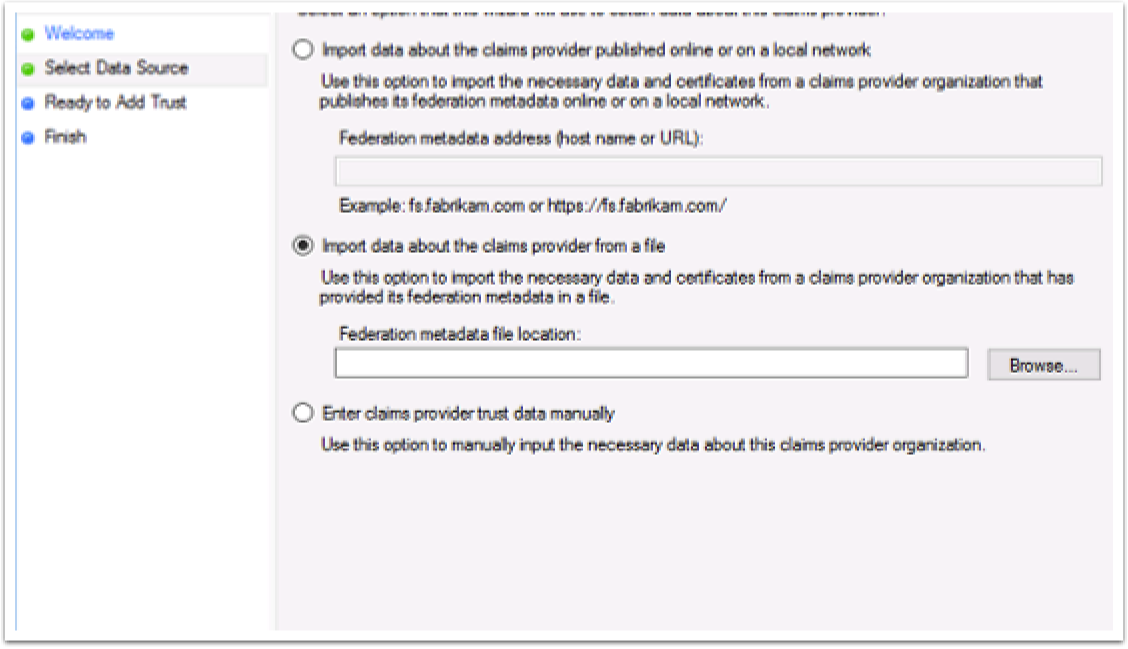
13. Select **Browse** and navigate to **Desktop** > Software > **ADFS** and select the **idp.xml** and click **Open.** Click **Next**

14. On the **Specify Display Name** page and write **Workspace ONE Access Livefire** in the Display name click **Next** > **Next** > **Close.** Now you will see **Active Directory** and **Workspace ONE Access Livefire** as Claims Providers

15. Right **Workspace ONE Access Livefire** and select **Edit Claim Rules...**







○ Import data about the claims provider published online or on a local network

Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.fabrikam.com or https://fs.fabrikam.com/

● Import data about the claims provider from a file

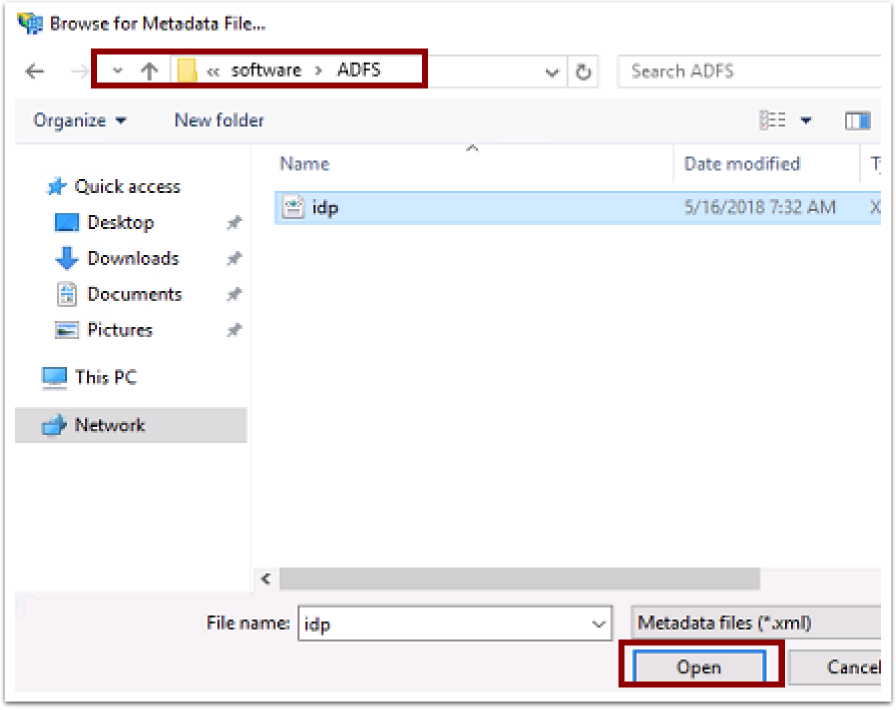
Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.

Federation metadata file location:

Browse...

○ Enter claims provider trust data manually

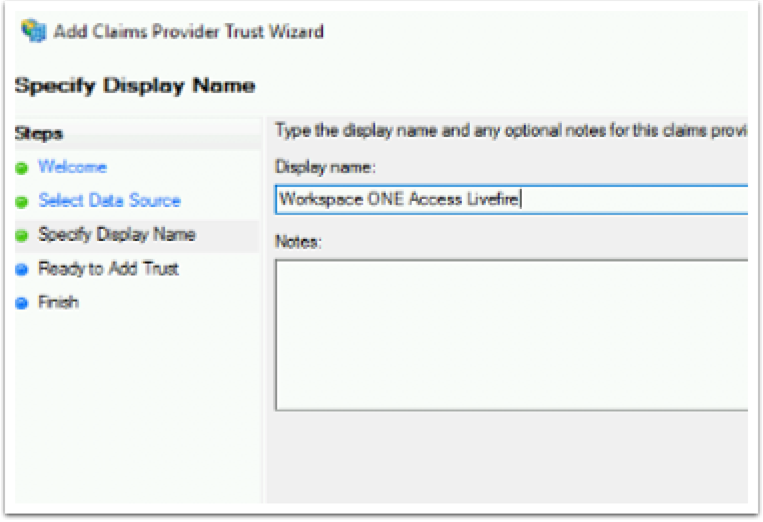
Use this option to manually input the necessary data about this claims provider organization.



idp 5/16/2018 7:32 AM

File name: idp

Metadata files (*.xml)

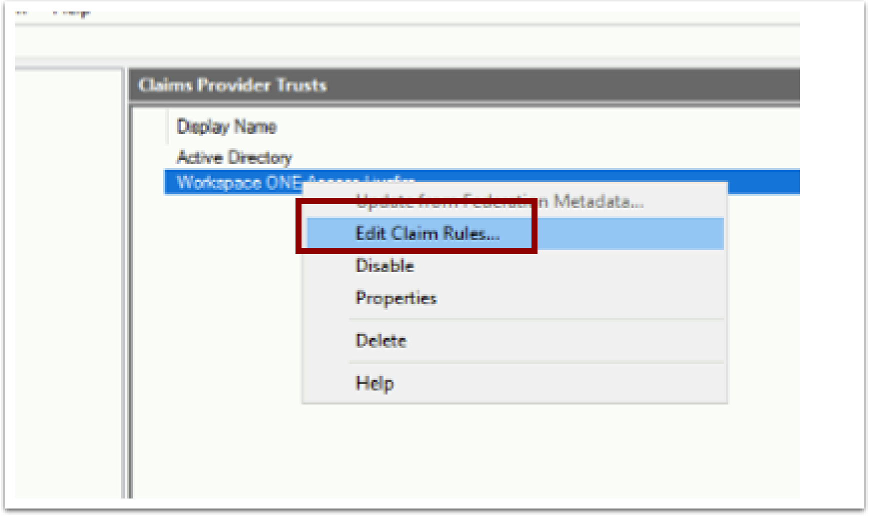


Specify Display Name

Type the display name and any optional notes for this claims provi

Display name: Workspace ONE Access Livefire

Notes:



16. Now Select **Add Rule...**

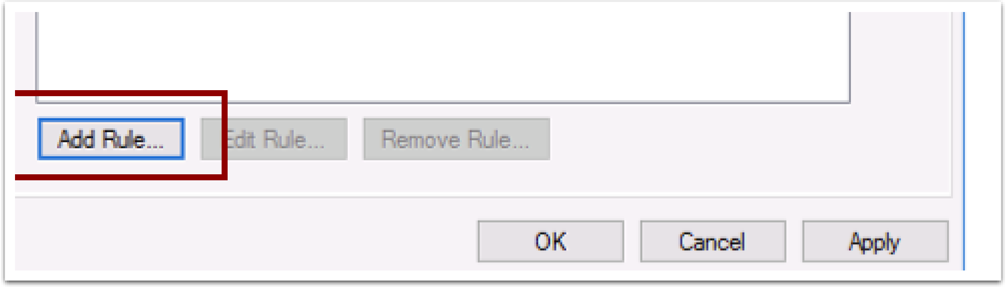
17 .From the next page select from the drop down **"Send Claim Using a Custom Rule"** select **Next**

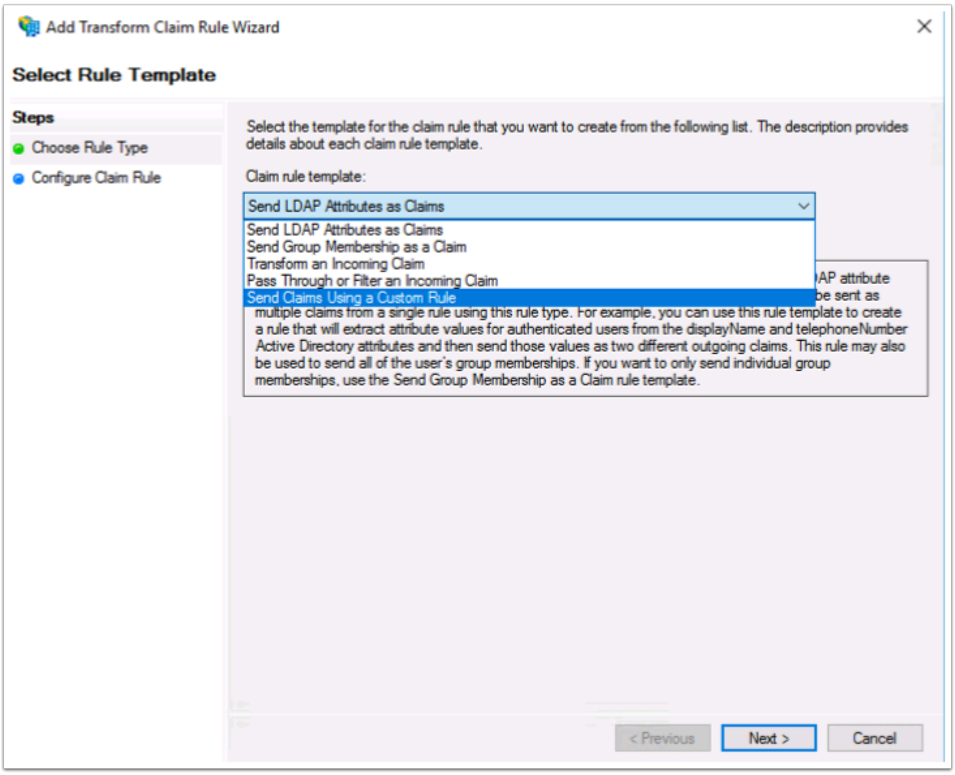
18 Type **Windows Accountname Claim** for the claim rule name

19 .Paste the below into the custom rule field:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] ==
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"] => issue(Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer =
"AD AUTHORITY", OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.
ValueType);
```

20. Select **Finish** and **OK**




Add Transform Claim Rule Wizard

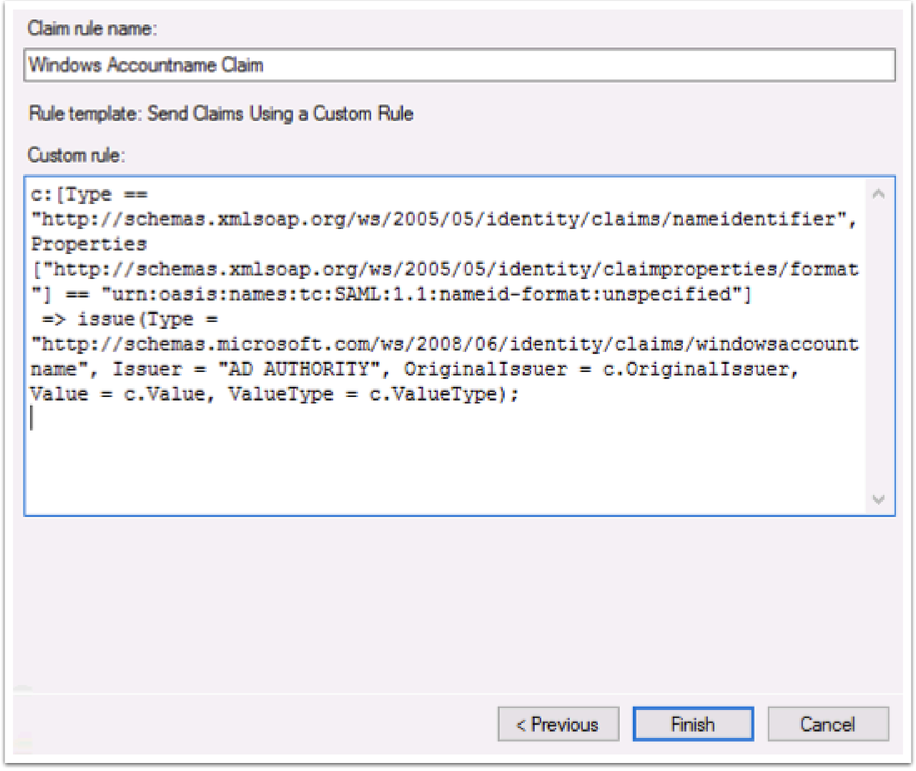
Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

AP attribute be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Steps
Choose Rule Type
Configure Claim Rule
Send LDAP Attributes as Claims
Send Group Membership as a Claim
Transform an Incoming Claim
Pass Through or Filter an Incoming Claim
Send Claims Using a Custom Rule
< Previous
Next >
Cancel



Claim rule name:

Windows Accountname Claim

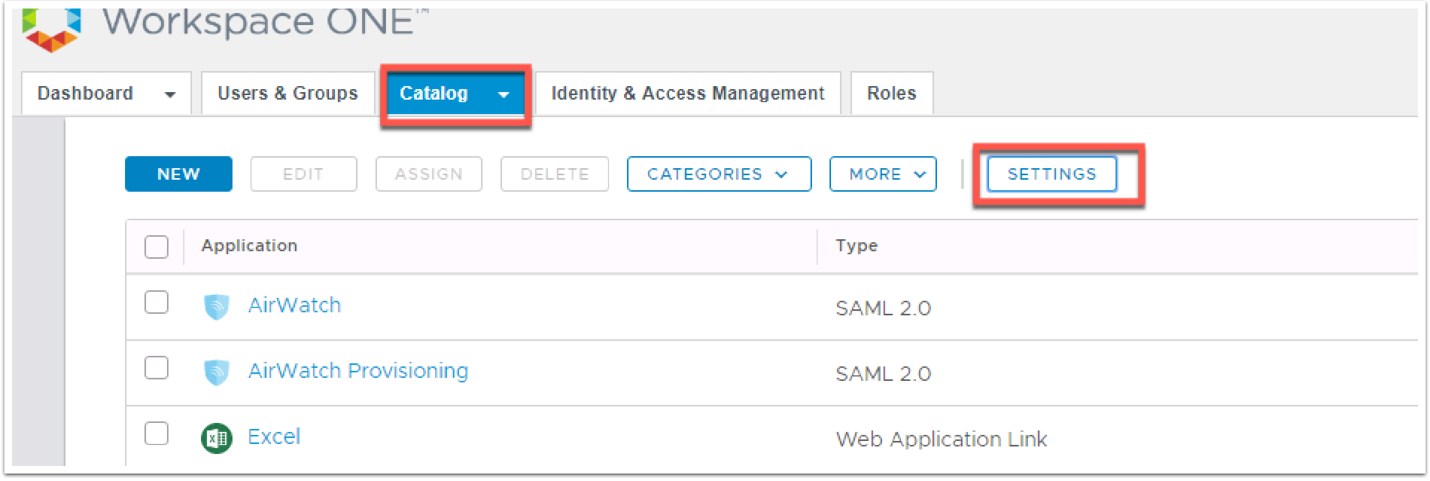
Rule template: Send Claims Using a Custom Rule

Custom rule:

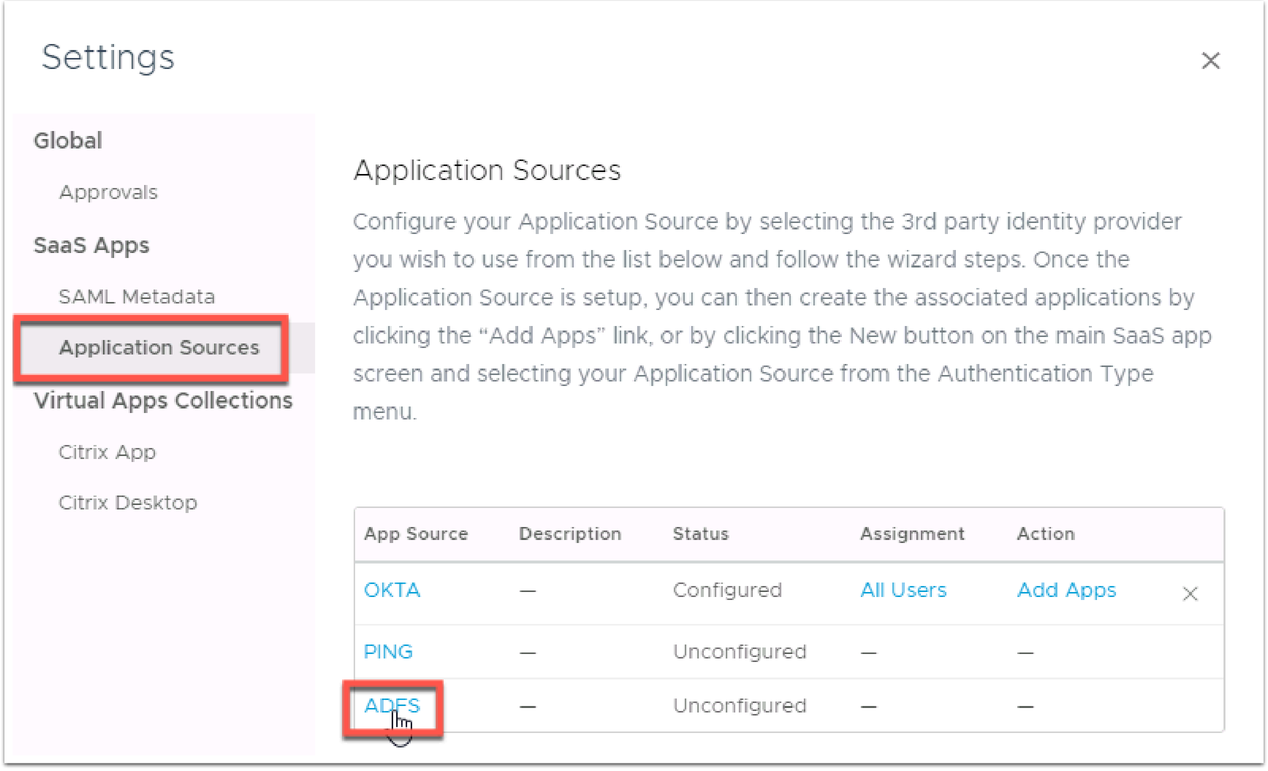
```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format
"] == "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"]
 => issue(Type =
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer = "AD AUTHORITY", OriginalIssuer = c.OriginalIssuer,
Value = c.Value, ValueType = c.ValueType);
```

Part 5:Add ADFS as Application source to Workspace ONE Access

1. Return to the **ControlCenter2** server and open **Firefox**
2. Using your browser go to **your unique Workspace ONE Access tenant**
3. Login with System Domain using user:**administrator** password:**VMware1!**
4. Now click on **Catalog** and select **Settings**
5. Navigate to **Application Sources** under the **Saas Apps** on the left hand side and select **ADFS** to configure the App Source.



Application	Type
AirWatch	SAML 2.0
AirWatch Provisioning	SAML 2.0
Excel	Web Application Link



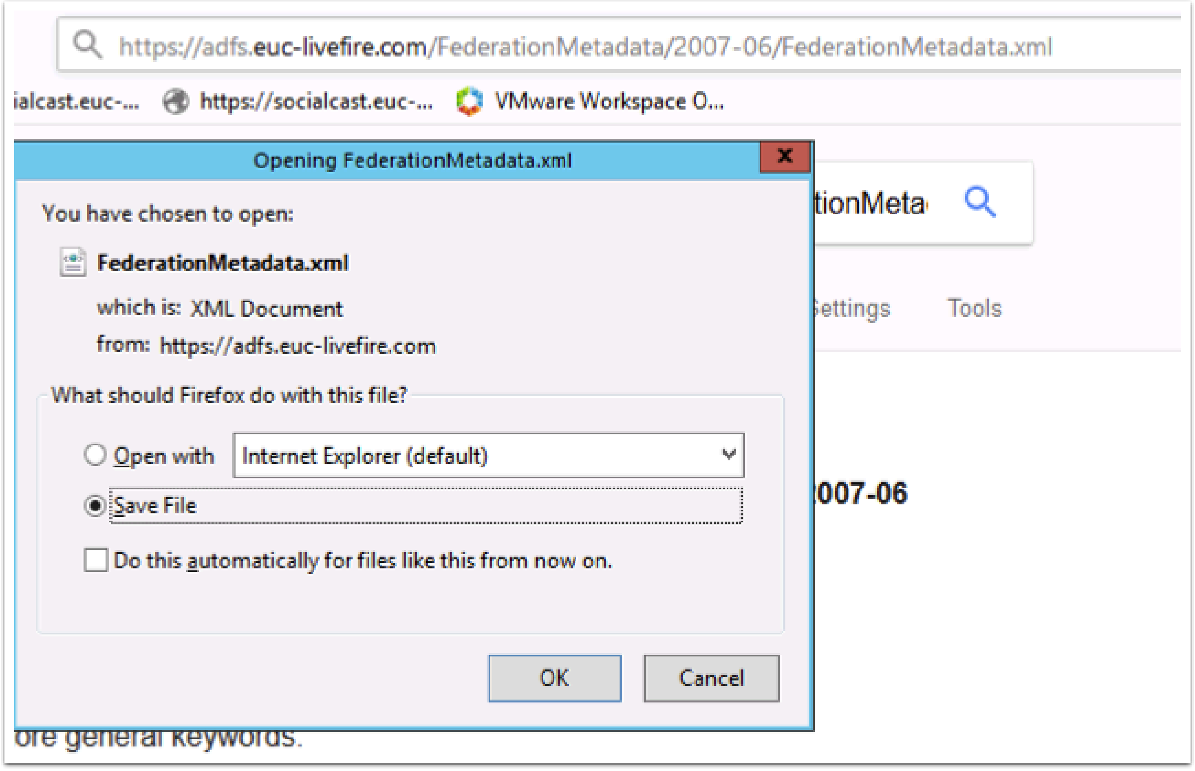
Settings

Application Sources

Configure your Application Source by selecting the 3rd party identity provider you wish to use from the list below and follow the wizard steps. Once the Application Source is setup, you can then create the associated applications by clicking the “Add Apps” link, or by clicking the New button on the main SaaS app screen and selecting your Application Source from the Authentication Type menu.

App Source	Description	Status	Assignment	Action
OKTA	—	Configured	All Users	Add Apps
PING	—	Unconfigured	—	—
ADFS	—	Unconfigured	—	—

1. Open the firefox browser on a new Tab and Browse to **https://adfs.euc-livefire.com/FederationMetadata/2007-06/FederationMetadata.xml**
2. Select **Save File** and go to the **Downloads** folder. (**Chrome** will download the file automatically)
3. Open the File using Notepad++ and **copy** the contents of the XML by pressing **ctrl + a** then **ctrl + c**
4. Then go back to the ADFS Application Source configuration on Workspace ONE Access and select **next**.
5. **Paste** the contents of the **FederationMetadata.xml** into the URL/XML field. Click **NEXT**
6. Click **Next** in the Access Policies and **SAVE** on the Summary Page



https://adfs.euc-livefire.com/FederationMetadata/2007-06/FederationMetadata.xml

Opening FederationMetadata.xml

You have chosen to open:

FederationMetadata.xml

which is: XML Document

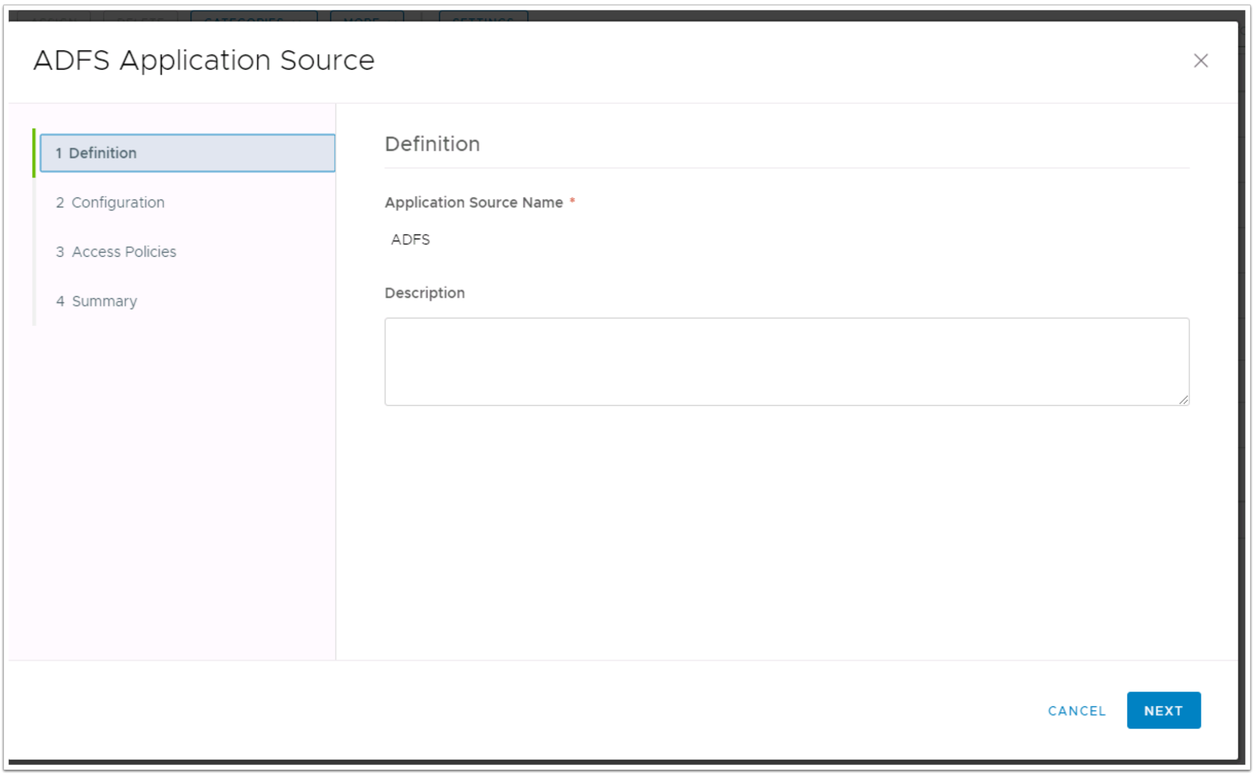
from: https://adfs.euc-livefire.com

What should Firefox do with this file?

○ Open with Internet Explorer (default)

● Save File

□ Do this automatically for files like this from now on.



ADFS Application Source

1 Definition

2 Configuration

3 Access Policies

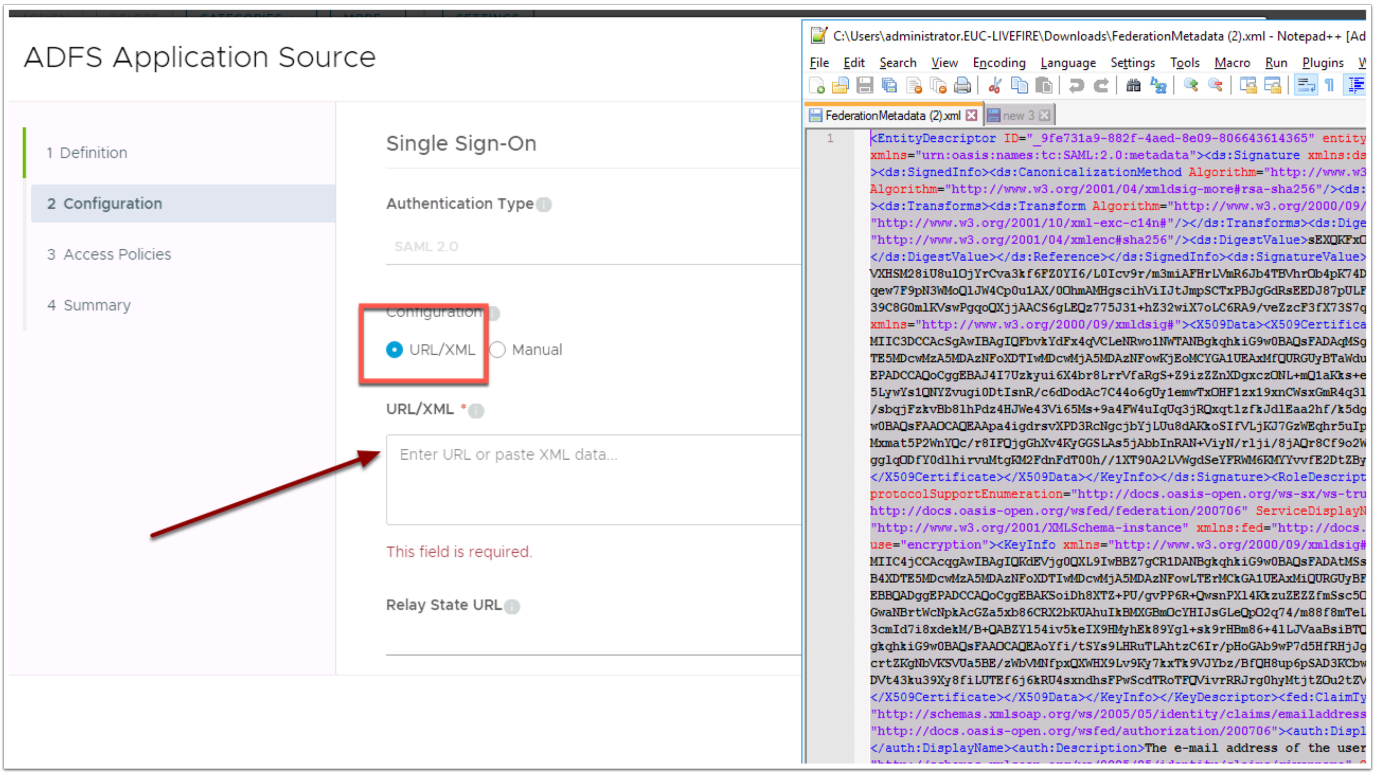
4 Summary

Definition

Application Source Name *

ADFS

Description



ADFS Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type

SAML 2.0

Configuration

● URL/XML ○ Manual

URL/XML *

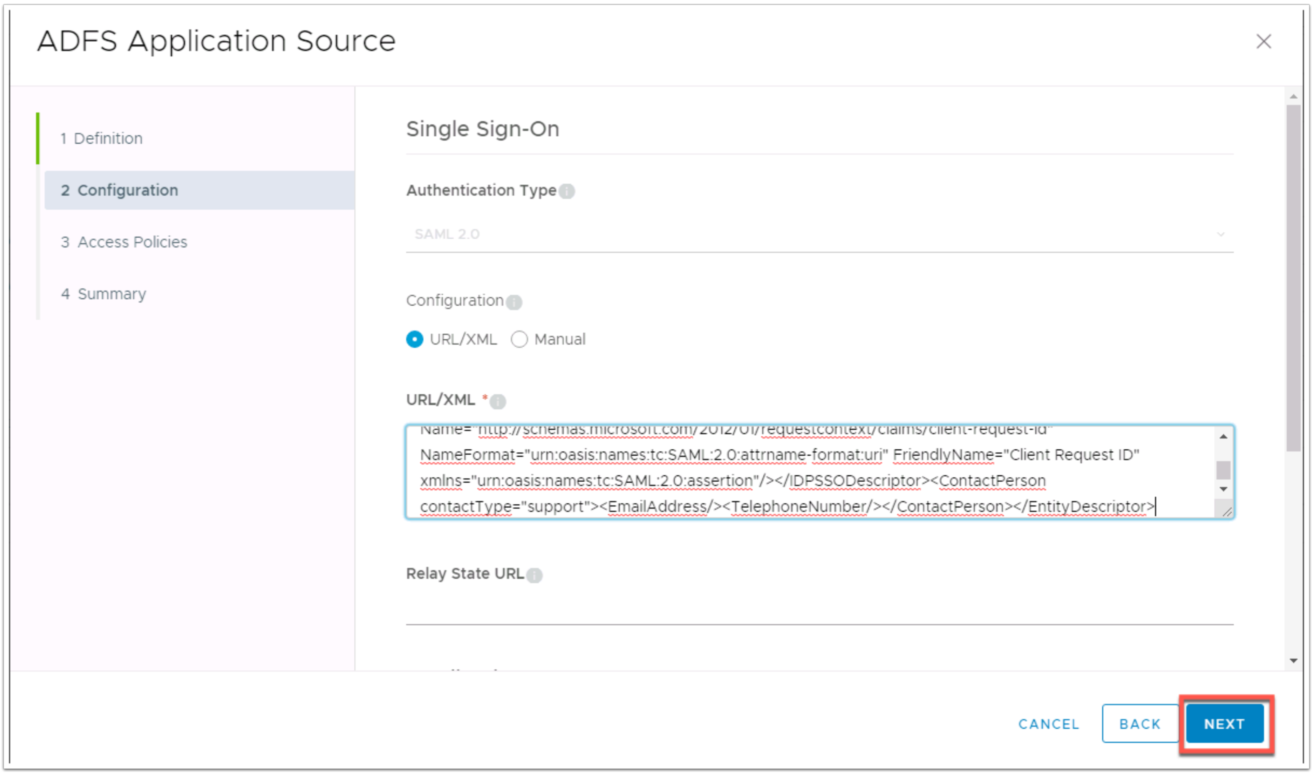
Enter URL or paste XML data...

This field is required.

Relay State URL

C:\Users\administrator.EUC-LIVEFIRE\Downloads\FederationMetadata (2).xml - Notepad++ [Ad
File Edit Search View Encoding Language Settings Tools Macro Run Plugins W
FederationMetadata (2).xml
new 3

```
<EntityDescriptor ID="_9fe731a9-882f-4aed-8e09-806643614365" entity
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><ds:Signature xmlns:ds
><ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:
><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/
"http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:Dige
"http://www.w3.org/2001/04/xmlenc#sha256"/><ds:DigestValue>sEXQKFxC
</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>
VXHSM28iU8ulOjYrCva3kf6FZ0YI6/L0Icv9r/m3miAFHrLVmR6Jb4TBVhrOb4pK74D
qew7F9pN3WMoQlJW4Cp0u1AX/0OhmAMHgscihViIJtJmpSCTxPBJgGdRsEEDJ87pULF
39C8G0mlKVswPgqoQXjjAACS6gLEQz775J31+hZ32wiX7oLC6RA9/veZzcF3fX73S7q
xmlns="http://www.w3.org/2000/09/xmldsig#"><X509Data><X509Certifica
MIIC3DCCAcSgAwIBAgIQFbvkYdFx4qVCLeNRwo1NWTANBgkqhkiG9w0BAQsFADAqMSg
TE5MDcwMzA5MDAzNFoXDTIwMDcwMjA5MDAzNFowKjEoMCYGA1UEAxMfQURGUyBTaWdu
EPADCCAQoCggEBAJ4I7Uzkyui6X4br8LrrVfaRgS+Z9izZZnXDgxczONL+mQ1aKks+e
5LywYs1QNYZvugi0DtIsnR/c6dDodAc7C44o6gUy1emwTxOHF1zx19xnCWsxGmR4q31
/sbqjFzkvBb8lhPdz4HJWe43Vi65Ms+9a4FW4uIqUq3jRQxqtlzfkJdlEaa2hf/k5dg
w0BAQsFAAOCAQEAApa4igdrsvXPD3RcNgcjbYjLUu8dAKkoSIfVLjKJ7GzWEqhr5uIp
Mxmat5P2WnYQc/r8IFQjgGhXv4KyGGSLAs5jAbbInRAN+ViyN/rlji/8jAQr8Cf9o2W
gglqODfY0dlhirvuMtgKM2FdnFdT00h//1XT90A2LVWgdSeYFRWM6KMYYvvfE2DtZBy
</X509Certificate></X509Data></KeyInfo></ds:Signature><RoleDescript
protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-tru
http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayN
"http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.
use="encryption"><KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#
MIIC4jCCAcqgAwIBAgIQKdEVjg0QXL9IwBBZ7gCR1DANBgkqhkiG9w0BAQsFADAtMSs
B4XDTE5MDcwMzA5MDAzNFoXDTIwMDcwMjA5MDAzNFowLTErMCkGA1UEAxMiQURGUyBF
EBBQADggEPADCCAQoCggEBAKSoiDh8XTZ+PU/gvPP6R+QwsnPXl4KkzuZEZZfmSsc5C
GwaNBrtWcNpkAcGZa5xb86CRX2bKUAhuIkBMXGBmOcYHIJsGLeQpO2q74/m88f8mTeL
3cmId7i8xdekM/B+QABZYl54iv5keIX9HMyhEk89Ygl+sk9rHBm86+4lLJVaaBsiBTQ
gkqhkiG9w0BAQsFAAOCAQEAoYfi/tSYs9LHRuTLAhtzC6Ir/pHoGAb9wP7d5HfRHjJg
crtZKgNbVKSVUa5BE/zWbVMNfpxQXWHX9Lv9Ky7kxTk9VJYbz/BfQH8up6pSAD3KCbw
DVt43ku39Xy8fiLUTEf6j6kRU4sxndhsFPwScdTRoTFQVivrRRJrg0hyMtjtZOu2tZV
</X509Certificate></X509Data></KeyInfo></KeyDescriptor><fed:ClaimTy
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
"http://docs.oasis-open.org/wsfed/authorization/200706"><auth:Displ
</auth:DisplayName><auth:Description>The e-mail address of the user
```



ADFS Application Source

1 Definition

2 Configuration

3 Access Policies

4 Summary

Single Sign-On

Authentication Type

SAML 2.0

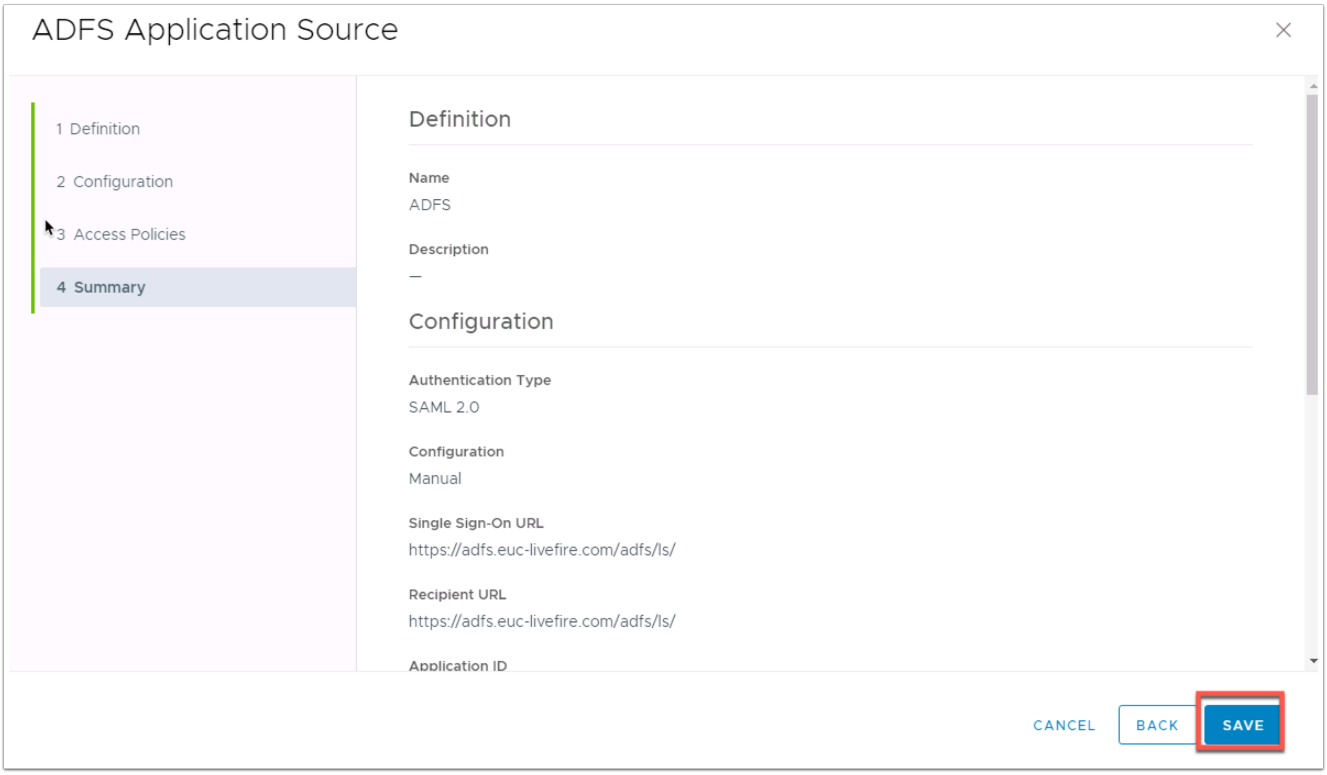
Configuration

● URL/XML ○ Manual

URL/XML *

```
Name="http://schemas.microsoft.com/2012/01/requestcontext/claims/client-request-id"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" FriendlyName="Client Request ID"
xmlns="urn:oasis:names:tc:SAML:2.0:assertion"/></IDPSSODescriptor><ContactPerson
contactType="support"><EmailAddress/><TelephoneNumber/></ContactPerson></EntityDescriptor>
```

Relay State URL



ADFS Application Source

Definition

Name
ADFS

Description
—

Configuration

Authentication Type
SAML 2.0

Configuration
Manual

Single Sign-On URL
https://adfs.euc-livefire.com/adfs/ls/

Recipient URL
https://adfs.euc-livefire.com/adfs/ls/

Application ID

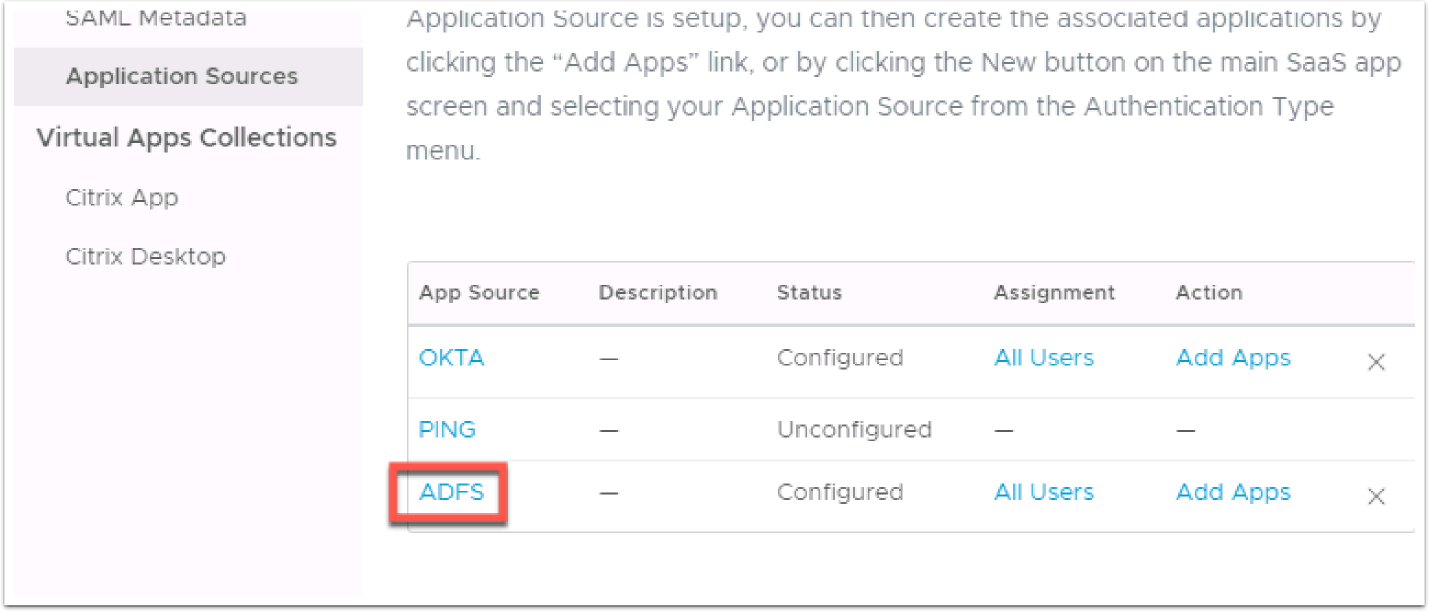
1. Now head back into the **ADFS settings** by selecting **ADFS** in the **Application Source** page.
2. Navigate to **Configuration** on the left hand side and change **Username Format** to **Unspecified**
3. Enter the following value under **Username Value**
   - **NB! there are no spaces in the below syntax**

```
${user.domain}\${user.userName}
```

4. Click on **Advanced Properties** and set **Signature Algorithm** to **SHA256 with RSA** and **Digest Algorithm** to **SHA256**

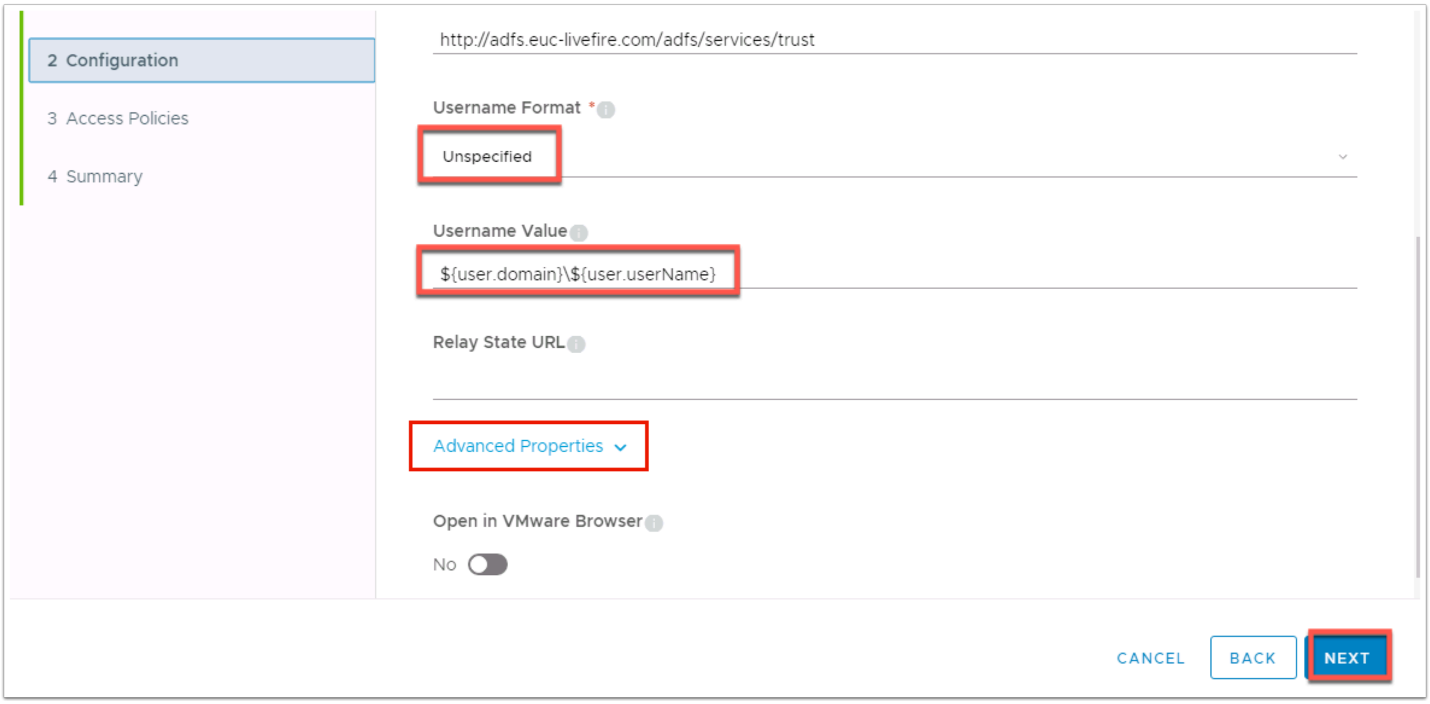
5. Select **NEXT** at the bottom of the page

6. Click **SAVE** on the Summary page



Application Source is setup, you can then create the associated applications by clicking the "Add Apps" link, or by clicking the New button on the main SaaS app screen and selecting your Application Source from the Authentication Type menu.

App Source	Description	Status	Assignment	Action	
OKTA	—	Configured	All Users	Add Apps	×
PING	—	Unconfigured	—	—	
ADFS	—	Configured	All Users	Add Apps	×



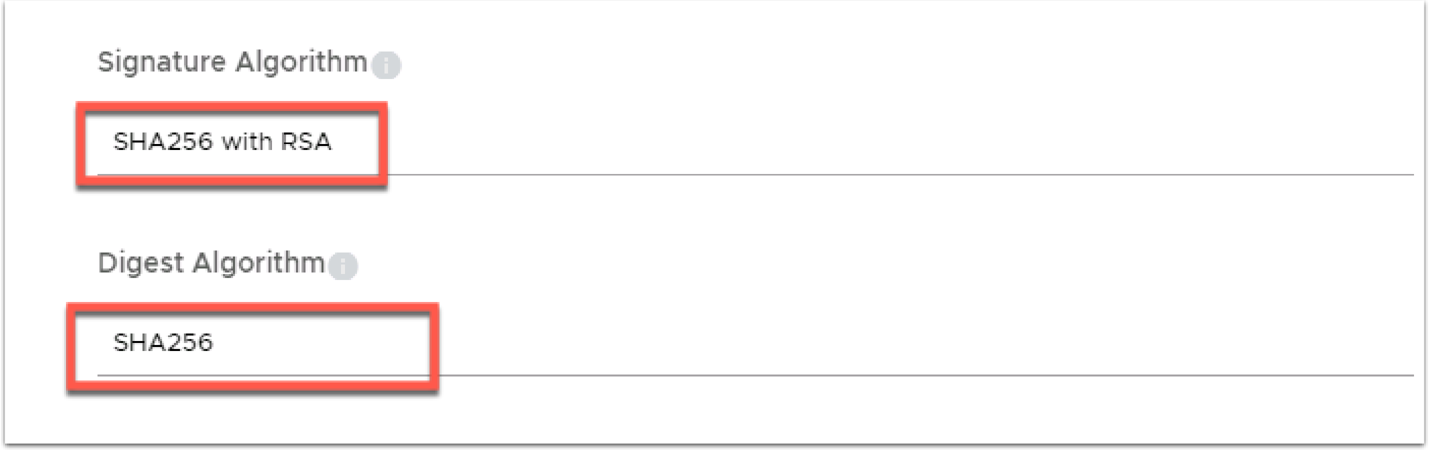
http://adfs.euc-livefire.com/adfs/services/trust

Username Format * Unspecified

Username Value ${user.domain}\${user.userName}

Relay State URL

Open in VMware Browser No



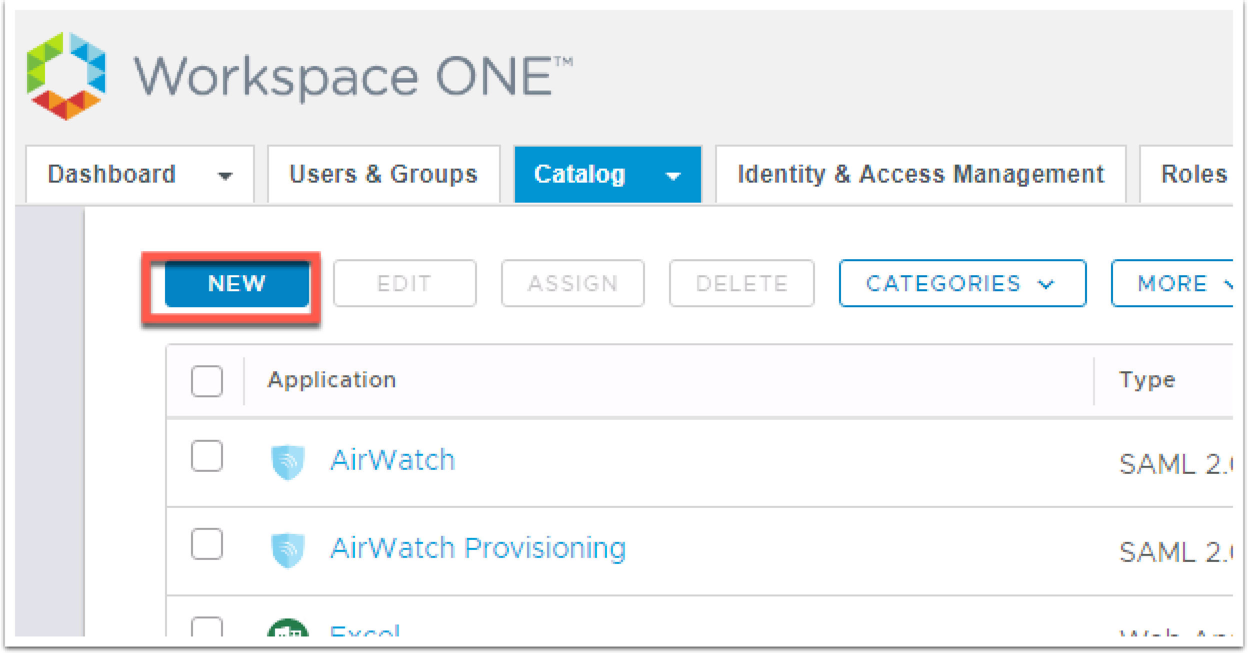
Signature Algorithm SHA256 with RSA

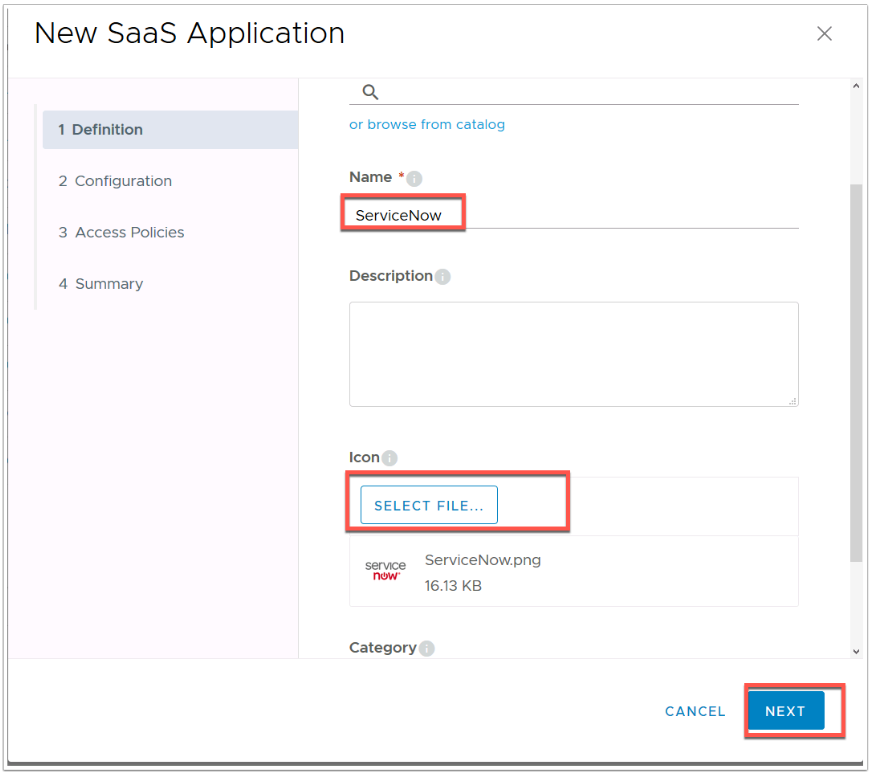
Digest Algorithm SHA256

Adding ADFS app to Workspace ONE Access

In certain scenarios admins might want to provide access to the Relying party configured in ADFS directly in the Workspace ONE catalog. This is made possible via the ADFS integration. We are essentially using a redirect to the Relying Party. Let's add the socialcast application to the catalog.

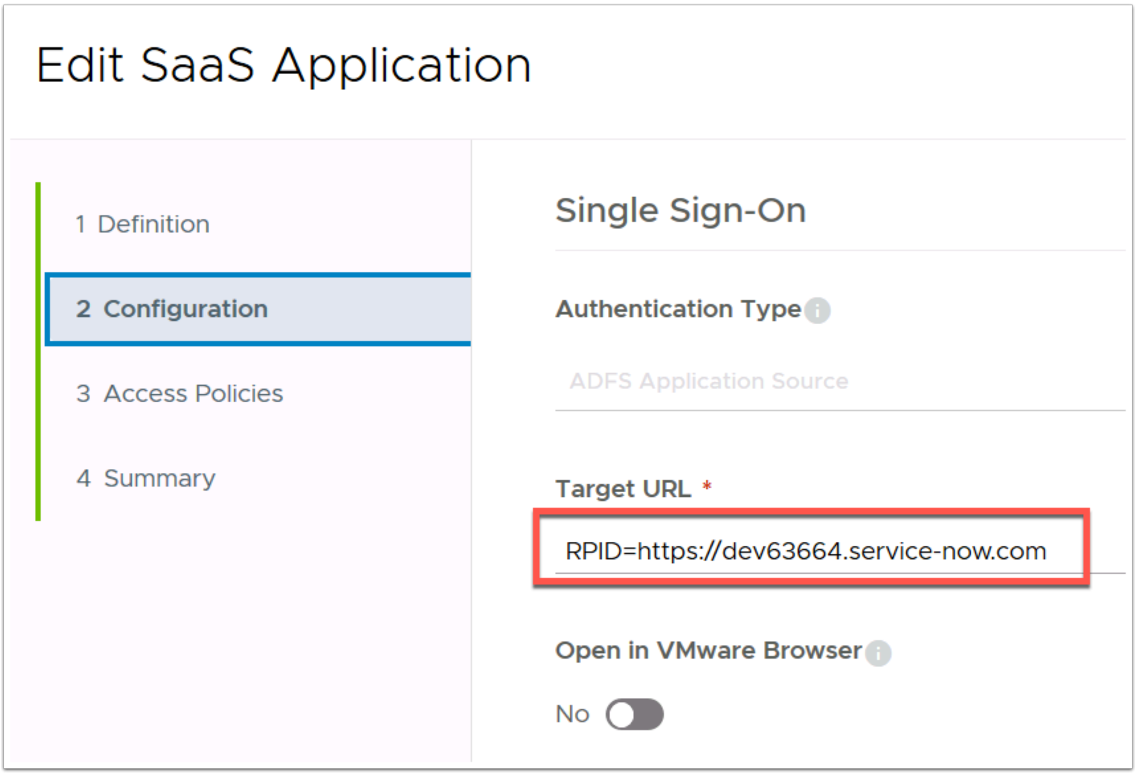
1. Log into you **unique Workspace ONE Access Admin** console using the local directory
2. Now navigate to **Catalog** then select **NEW** and give it the name: **ServiceNow**
3. Click on **Select File** below **Icon** and select the **ServiceNow.png** file in the **Downloads** folder and select **Open.** click **NEXT**
4. In the **Configuration page** select **ADFS Application Source** under Authentication Type.
5. Now type in the Target URL _RPID=https://DEVXXX.Service-Now.com (whereXXX is your unique tenant) and select **NEXT**
6. Click **NEXT** on the **Access Policies** Page, and **SAVE & ASSIGN** on the Summary page
7. In the **Assign page** assign the application to the **Marketing@euc-livefire.com** group
8. Start typing **marketing@euc-livefire.com** and you will see the Group showing up click it to confirm
9. Now set the **Deployment Type** group to **automatic** and select **SAVE**




New SaaS Application

Name *: ServiceNow

Icon: ServiceNow.png 16.13 KB


Edit SaaS Application

Single Sign-On

Authentication Type: ADFS Application Source

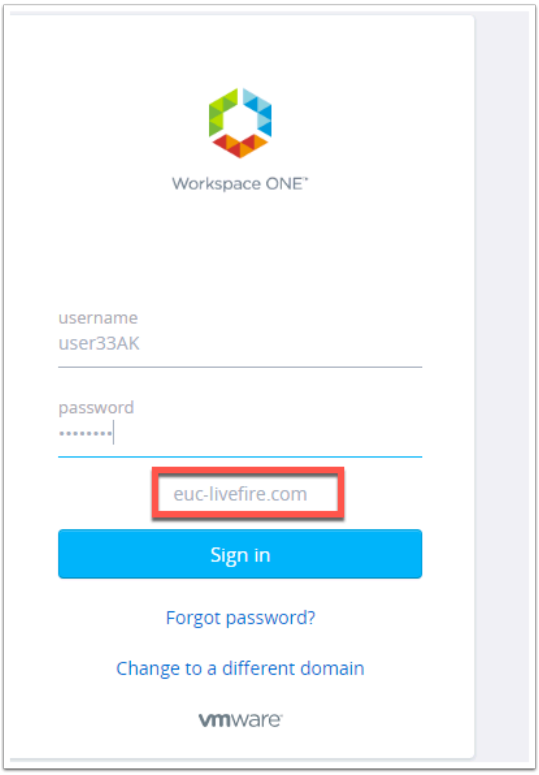
Target URL *: RPID=https://dev63664.service-now.com

Open in VMware Browser: No

1. **Close** the browser and all windows to ensure firefox or chrome has closed properly. Now **re-open** firefox and navigate to your u**nique Workspace ONE Access SaaS instance**.

2. Now log in as your **Unique User** in the domain **euc-livefire.com** you will then notice in the catalog the socialcast application.

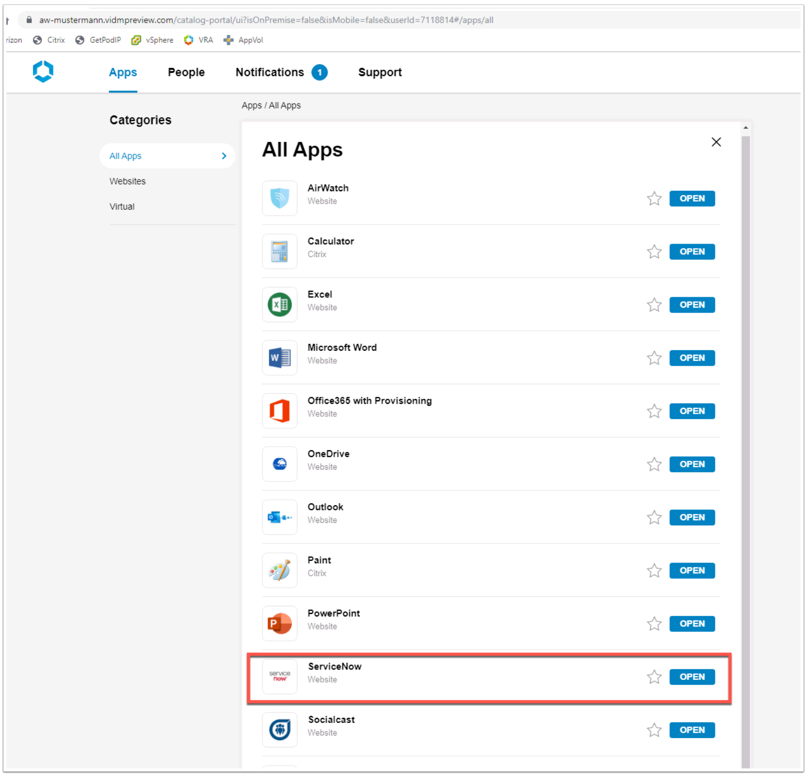
3. Now click on **Open** under ServiceNow icon and you will be redirected to ServiceNow and authenticated without additional credentials as your unique user.



username
user33AK

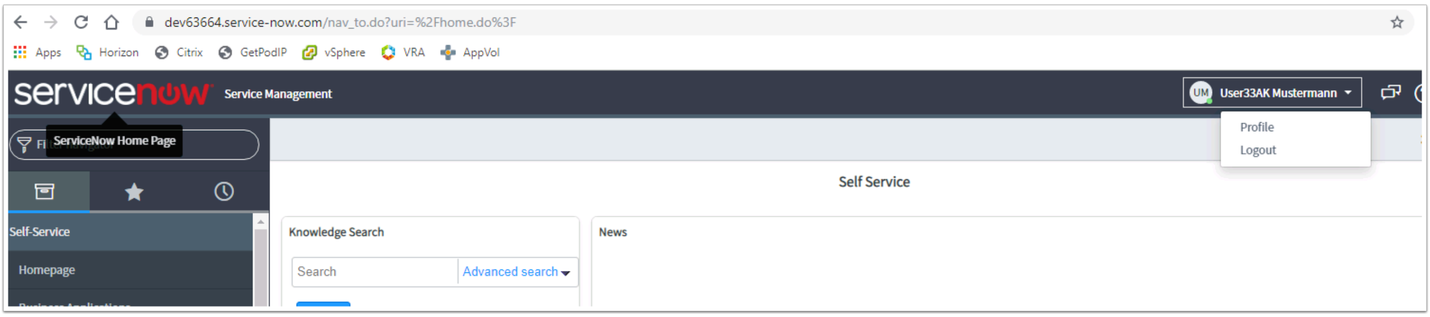
password
••••••••

euc-livefire.com


aw-mustermann.vidmpreview.com/catalog-portal/ui?isOnPremise=false&isMobile=false&userId=7118814#/apps/all

All Apps

AirWatch Website OPEN
Calculator Citrix OPEN
Excel Website OPEN
Microsoft Word Website OPEN
Office365 with Provisioning Website OPEN
OneDrive Website OPEN
Outlook Website OPEN
Paint Citrix OPEN
PowerPoint Website OPEN
ServiceNow Website OPEN
Socialcast Website OPEN



Part 6 : ExtraCurricular: Setting Workspace ONE Access as the default claim provider

There might be a use-case where an organisation in an SP-INIT Flow wants the configured relying party in ADFS always use a specific claims provider. Through powershell admins have the ability to set the **default claims provider** for specific **relying parties**.

On the **ADFS Server** do the following. Clear the cache on your Firefox browser and re-launch

1. navigating to https://devXXX.service-now.com/ (where XXX is your unique instance) and clicking on "use external login", then specify your **unique user** and click **Submit**.

You will be redirected and ADFS Claims providers screen and notice you have **WorkspaceONE Access** and **Active Directory** listed. We want to ensure that we are automatically redirected to WorkspaceONE Access instead of seeing this prompt.

2. Open powershell and type

```
Get-AdfsRelyingPartyTrust
```

3. You will now be able to see that ServiceNow is set to use both Active Directory and Workspace ONE Access LiveFire as the claims provider (IF empty it is set to use both)

4. Let's now set Workspace ONE Access as the default claims provider

In the same power shell windows now execute the below

```
Set-AdfsRelyingPartyTrust -TargetName "ServiceNow" -ClaimsProviderName @("WorkspaceONE
Access Livefire")
```

Plese note: the name of your claims provider should exactly match your adfs configuration

5. Confirm the changes by typing the same command to get the relying party trust information. You will notice now that **WorkspaceONE Access** is listed as the only ClaimsProvierName

```
Get-AdfsRelyingPartyTrust
```

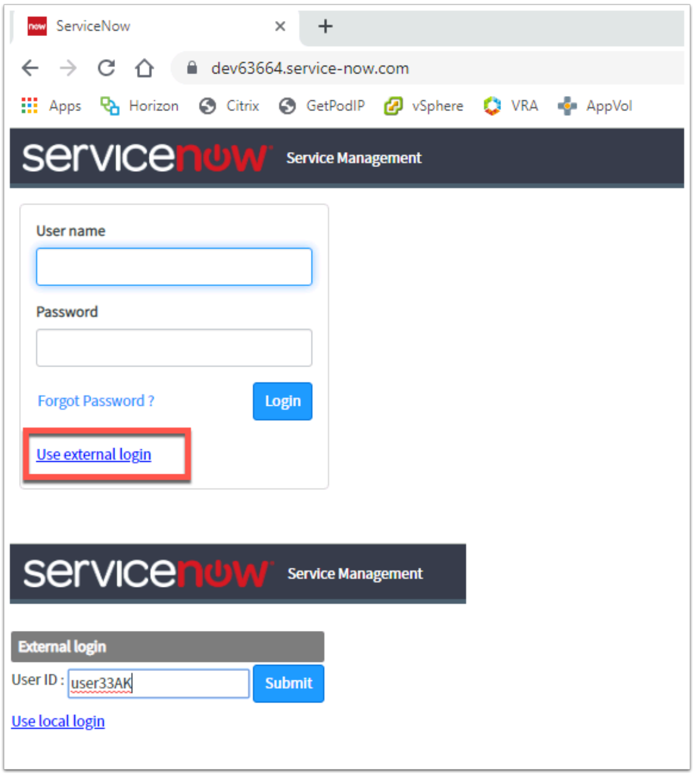
6. Now close your browser and re-open to https://devXXX.service-now.com (where XXX is your uniques instance)

7. Click on **Use External Login** on the next page type in your **unique user** notice now that you will automatically be re-directed to WorkspaceONE click **Next.** After authenticated you will automatically be logged into ServiceNow.

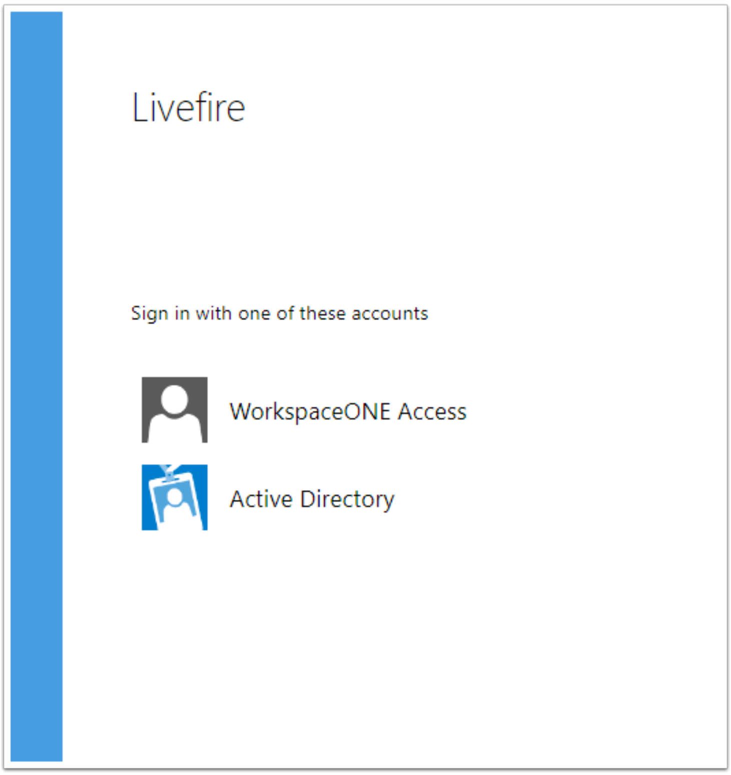
Observe you weren't prompted to chose the claim provider as in the original test.

NOTE: In order to reverse the above simply re-add Active Directory as another claims provider or leave blank to set to defualt.

```
 Set-AdfsRelyingPartyTrust -TargetName "ServiceNow" -ClaimsProviderName @("WorkspaceONE Access", "Active Directory")
```



User ID : user33AK

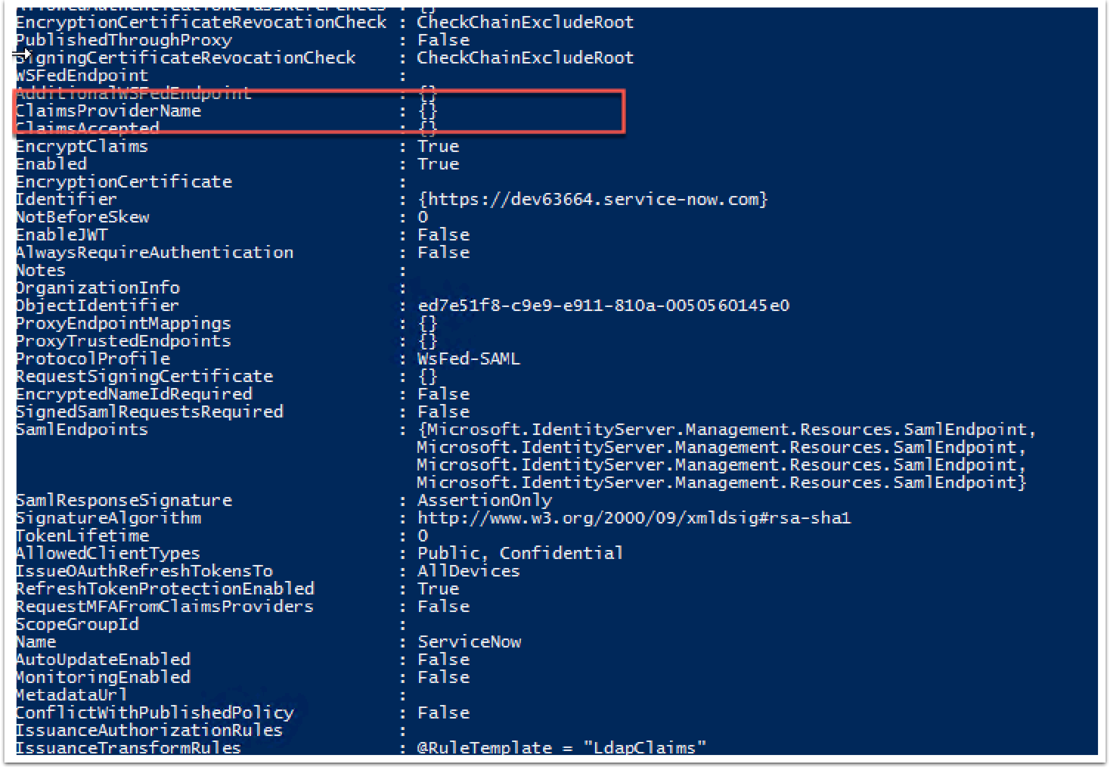


Livefire

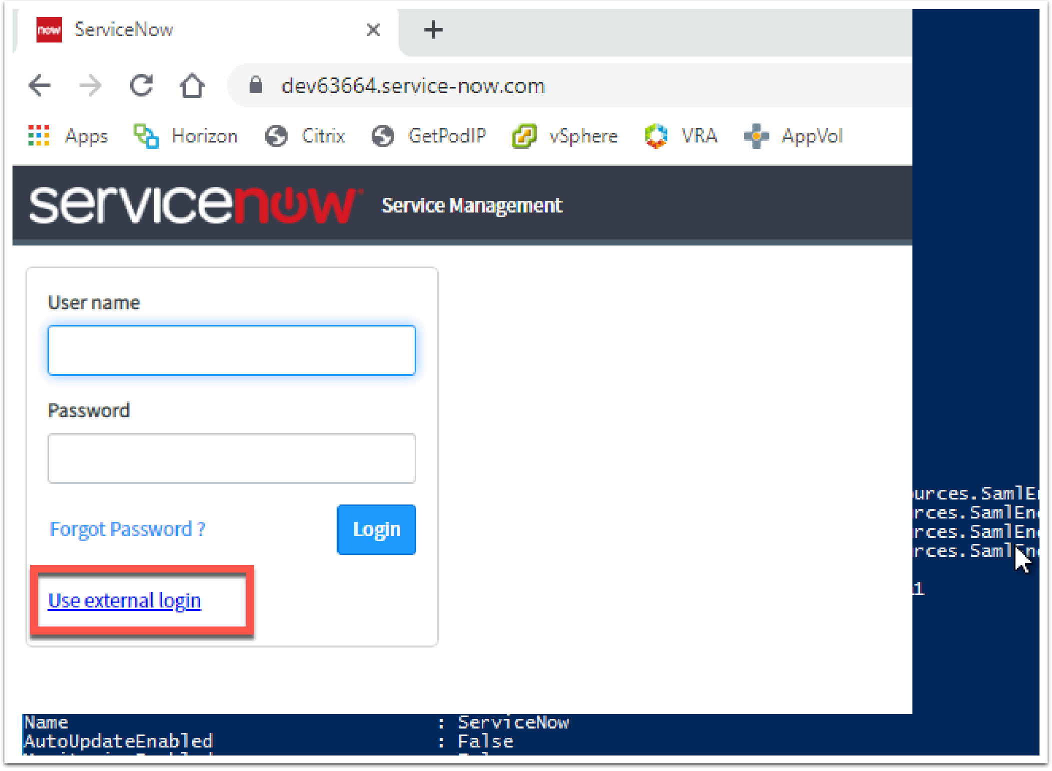
Sign in with one of these accounts

WorkspaceONE Access

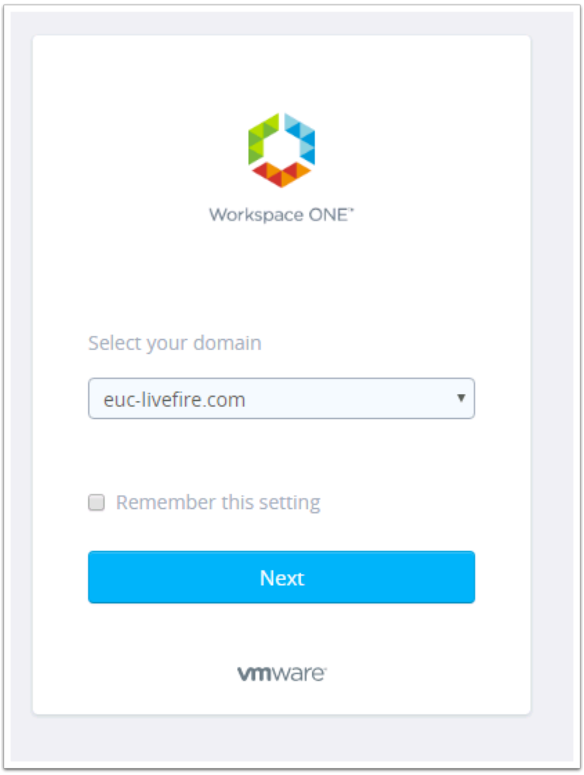
Active Directory



```
AllowedAuthenticationClassReferences : {}
EncryptionCertificateRevocationCheck : CheckChainExcludeRoot
PublishedThroughProxy                : False
SigningCertificateRevocationCheck    : CheckChainExcludeRoot
WSFedEndpoint                        :
AdditionalWSFedEndpoint              : {}
ClaimsProviderName                   : {}
ClaimsAccepted                       : {}
EncryptClaims                        : True
Enabled                              : True
EncryptionCertificate                :
Identifier                           : {https://dev63664.service-now.com}
NotBeforeSkew                        : 0
EnableJWT                            : False
AlwaysRequireAuthentication          : False
Notes                                :
OrganizationInfo                     :
ObjectIdentifier                     : ed7e51f8-c9e9-e911-810a-0050560145e0
ProxyEndpointMappings                : {}
ProxyTrustedEndpoints                : {}
ProtocolProfile                      : WsFed-SAML
RequestSigningCertificate            : {}
EncryptedNameIdRequired              : False
SignedSamlRequestsRequired           : False
SamlEndpoints                        : {Microsoft.IdentityServer.Management.Resources.SamlEndpoint,
                                       Microsoft.IdentityServer.Management.Resources.SamlEndpoint,
                                       Microsoft.IdentityServer.Management.Resources.SamlEndpoint,
                                       Microsoft.IdentityServer.Management.Resources.SamlEndpoint}

SamlResponseSignature                : AssertionOnly
SignatureAlgorithm                   : http://www.w3.org/2000/09/xmldsig#rsa-sha1
TokenLifetime                        : 0
AllowedClientTypes                   : Public, Confidential
IssueOAuthRefreshTokensTo            : AllDevices
RefreshTokenProtectionEnabled        : True
RequestMFAFromClaimsProviders        : False
ScopeGroupId                         :
Name                                 : ServiceNow
AutoUpdateEnabled                    : False
MonitoringEnabled                    : False
MetadataUrl                          :
ConflictWithPublishedPolicy          : False
IssuanceAuthorizationRules           :
IssuanceTransformRules               : @RuleTemplate = "LdapClaims"
```



```
Name                          : ServiceNow
AutoUpdateEnabled             : False
```



Day 3

Authentication Method - iOS SSO

Configuration for Single-Sign-On on native applications

In this section we will first configure the necessary pre-requirements for the last mile configuration of Mobile SSO.

There are two common options for a Certificate Authority:

1. Customers might want to use their own internal Certificate Authority for issuing certificates
2. Workspace ONE UEM can act as the certificate authority and issue certificates to devices for authentication against Workspace ONE Access.

In this specific lab we will leverage **option 2,** where Workspace ONE is the Certificate Authority and we will need to export the Root Certificate used for Single Sign on and Import it into Workspace ONE Access.

There are also two options for Key Distribution Center (KDC) :

1. Cloud Hosted, which means the KDC service is hosted by VMware in the cloud
2. On-Premise (LINUX only) where KDC service is running locally on the Workspace ONE Access server.

In this specific lab we will leverage **option 1**, as we are already leveraging the cloud hosted Workspace ONE Access server.

This lab is divided into 4 parts

Part 1 : Mobile Single Sign-On Configuration for IOS based Applications
Part 2:   IOS Device Configuration for Single Sign On
Part 3: IOS Device enrollment in Workspace ONE UEM
Part 4: Microsoft Word Single Sign On

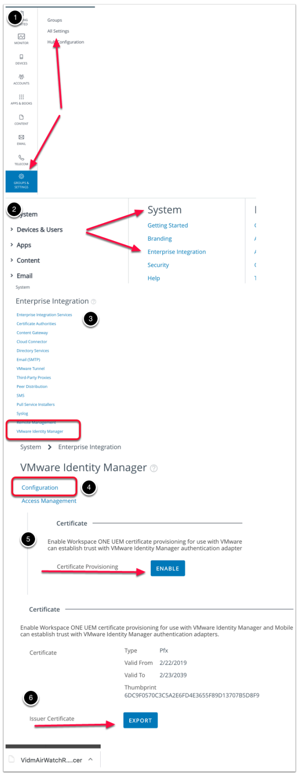
Part 1: Mobile Single Sign-On Configuration for IOS based Applications

1. **Mobile Single Sign-On Configuration for IOS based Applications**

- If you not already done so, navigate to the **WorkspaceONE UEM** console **https://cn-livefire.awmdm.com** and sign in with your **e-mail address** and **password**

1. In Admin Console select **Groups & Settings** > **All Settings**
2. Under **System > select Enterprise Integration**
3. Under **Enterprise Integration** select **VMware Identity Manager**
4. Under **VMware Identity Manager** select **Configuration**
5. Next to **Certificate Provisioning** select ENABLE (possibly already enabled)
6. Scroll down until you find the **Certificate** section and next to **Issuer Certificate** select **EXPORT**

   This will be the root certificate used to validate incoming certificate auth requests for IOS mobile devices. We need to now navigate to the Auth Adapter in Workspace ONE Access



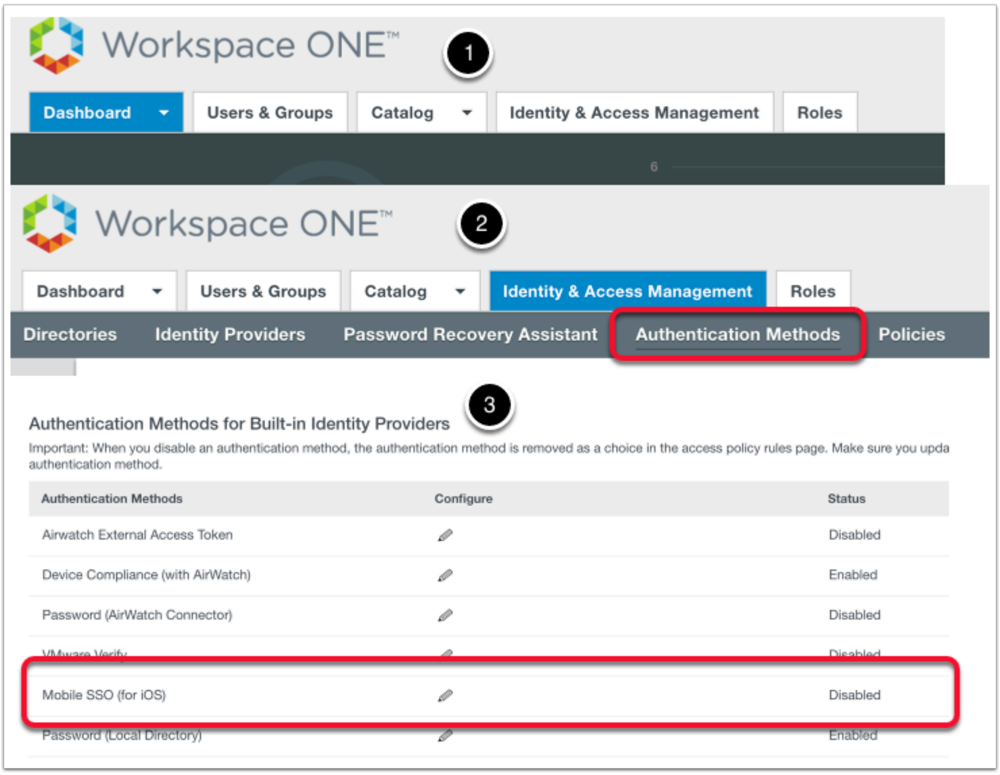
Enable Workspace ONE UEM certificate provisioning for use with VMware can establish trust with VMware Identity Manager authentication adapter

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile can establish trust with VMware Identity Manager authentication adapters.

Type Pfx
Valid From 2/22/2019
Valid To 2/23/2039
Thumbprint 6DC9F0570C3C5A2E6FD4E3655F89D13707B5D8F9

2. Mobile Single Sign-On Configuration for IOS based Applications...

- Navigate to your assigned Workspace ONE Access Server server and login the Admin Console using the local directory admin account. In the Tenant Admin Console select your **Administration Console**
  1. Select **Identity & Access Management**
  2. Under **Identity & Access Management > Manage** select **Authentication Methods**
  3. Under **Authentication Methods for Built-In Identity Providers** select then click the **Pencil** next to **Mobile SSO (for iOS)**



Authentication Methods for Built-in Identity Providers

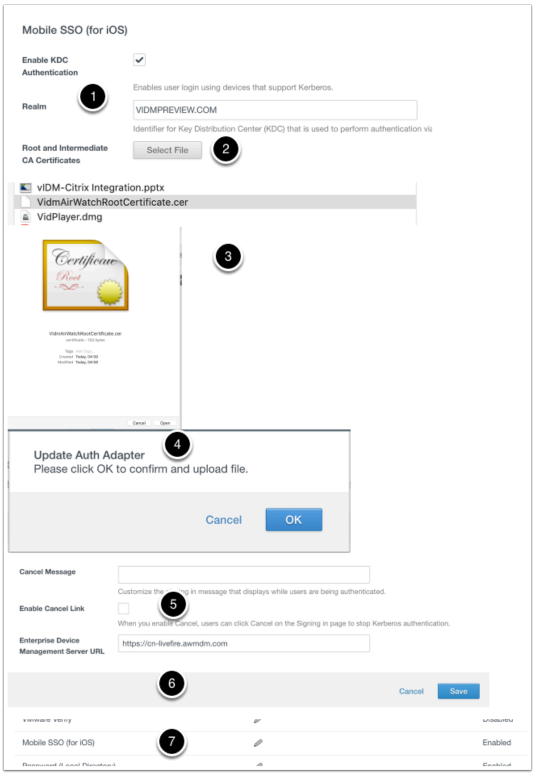
Important: When you disable an authentication method, the authentication method is removed as a choice in the access policy rules page. Make sure you upda authentication method.

Authentication Methods	Configure	Status
Airwatch External Access Token	✎	Disabled
Device Compliance (with AirWatch)	✎	Enabled
Password (AirWatch Connector)	✎	Disabled
VMware Verify	✎	Disabled
Mobile SSO (for iOS)	✎	Disabled
Password (Local Directory)	✎	Enabled

3. Mobile Single Sign-On Configuration for IOS based Applications...

- In the **Mobile SSO (for IOS)** window select the following:

1. Click **Enable KDC Authentication** **check box .** Leave as default next to **Realm:** as **VIDMPREVIEW.COM** (must be in all CAPS)
2. Next to **Root and Intermediate CA Certificates**, select **Select File** (step 1.6 earlier)
3. Select the **VidmAirWatchRootCertificate.cer** file and select **Open**
4. On the **Update Auth Adapter** window select **OK**
5. Next to **Enterprise Device Management Server URL** enter your Workspace ONE UEM url **https://cn-livefire.awmdm.com**
6. Select **Save**
7. **Mobile SSO (for IOS)** should now be enabled



Mobile SSO (for iOS)

Enable KDC Authentication ☑

Enables user login using devices that support Kerberos.

Realm: VIDMPREVIEW.COM

Identifier for Key Distribution Center (KDC) that is used to perform authentication vi

Root and Intermediate CA Certificates: Select File

vIDM-Citrix Integration.pptx
VidmAirWatchRootCertificate.cer
VidPlayer.dmg

Update Auth Adapter
Please click OK to confirm and upload file.

Cancel Message:

Customize the signing in message that displays while users are being authenticated.

Enable Cancel Link □

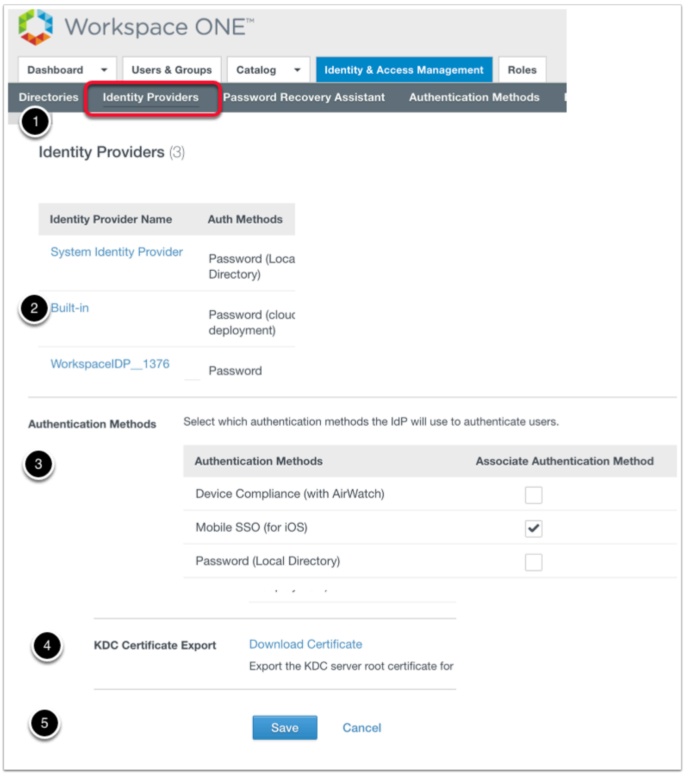
When you enable Cancel, users can click Cancel on the Signing in page to stop Kerberos authentication.

Enterprise Device Management Server URL: https://cn-livefire.awmdm.com

Mobile SSO (for iOS)	Enabled

4. **Mobile Single Sign-On Configuration for IOS based Applications...**

- We will now associate the Built-in IDP with the IOS Single Sign On method in order configure our Access Policies
  1. Under **Identity & Access Management > Manage** select **Identity Providers**
  2. Under **Identity Providers, select** the **Built-in** IDP
  3. Under **Authentication Methods** select the **Mobile SSO (for iOS) checkbox**
  4. Next to **KDC Certificate Export** select **Download Certificate**
  5. Scroll down and select **Save**



Identity Providers (3)

Identity Provider Name	Auth Methods
System Identity Provider	Password (Loca Directory)
Built-in	Password (clouc deployment)
WorkspaceIDP__1376	Password

Authentication Methods — Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Device Compliance (with AirWatch)	☐
Mobile SSO (for iOS)	☑
Password (Local Directory)	☐

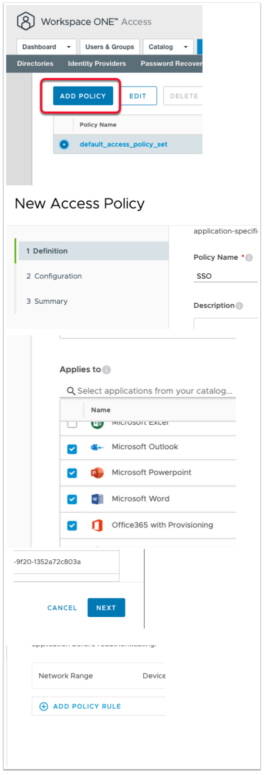
KDC Certificate Export — Download Certificate

Export the KDC server root certificate for

5. **Mobile Single Sign-On Configuration for IOS based Applications...**

- **We will now configure an Application Level Access Policy**
- Under **Identity & Access Policies > Manage** select **Policies**

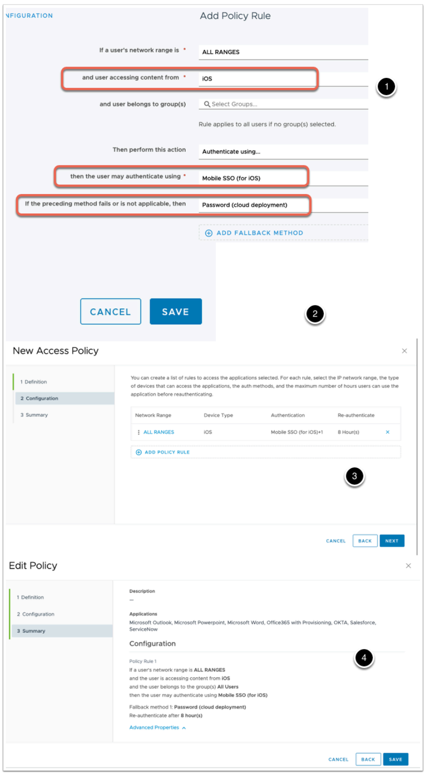
1. Select **ADD POLICY**
2. In the **New Access Policy** wizard under **Policy Name** type **SSO**
3. To the bottom of the Definition section under Applies to select the following **checkboxes**
   - Microsoft Outlook
   - Microsoft Powerpoint
   - Microsoft Word
   - Office 365 with Provisioning
   - OKTA
   - Onedrive
   - Salesforce
   - ServiceNow
4. Select **NEXT**
5. In the **Configuration** section select **+ ADD POLICY RULE**



6**. Mobile Single Sign-On Configuration for IOS based Applications...**

- Access Policies to support IOS devices continued...

1. On the **Add policy Rule** page next to **:**
   1. **"and user accessing content from"** select from the **dropdown** **iOS**
   2. **"then the user may authenticate using"** from the dropdown select **Mobile SSO (for iOS)**
   3. "i**f the preceding method fails or is not applicable then"** select from the dropdown **Password (Cloud Deployment)**
2. Select **Save**
3. On the **New Access Policy Configuration** window Select **Next**
4. On the **Summary** page, review your configurations and select **Save**



NFIGURATION

Add Policy Rule

If a user's network range is * ALL RANGES

and user accessing content from * iOS

and user belongs to group(s) Select Groups...

Rule applies to all users if no group(s) selected.

Then perform this action Authenticate using...

then the user may authenticate using * Mobile SSO (for iOS)

If the preceding method fails or is not applicable, then Password (cloud deployment)

New Access Policy

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
ALL RANGES	iOS	Mobile SSO (for iOS)+1	8 Hour(s)

Edit Policy

Description
—

Applications
Microsoft Outlook, Microsoft Powerpoint, Microsoft Word, Office365 with Provisioning, OKTA, Salesforce, ServiceNow

Configuration

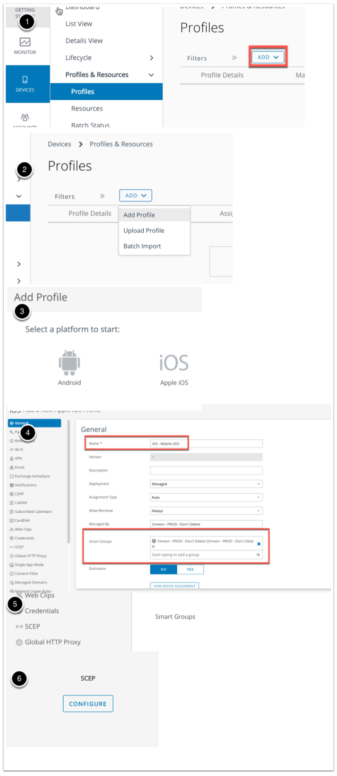
Policy Rule 1
If a user's network range is **ALL RANGES**
and the user is accessing content from **iOS**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **Mobile SSO (for iOS)**

Fallback method 1: **Password (cloud deployment)**
Re-authenticate after **8 hour(s)**

Part 2: IOS Device Configuration for Single Sign On

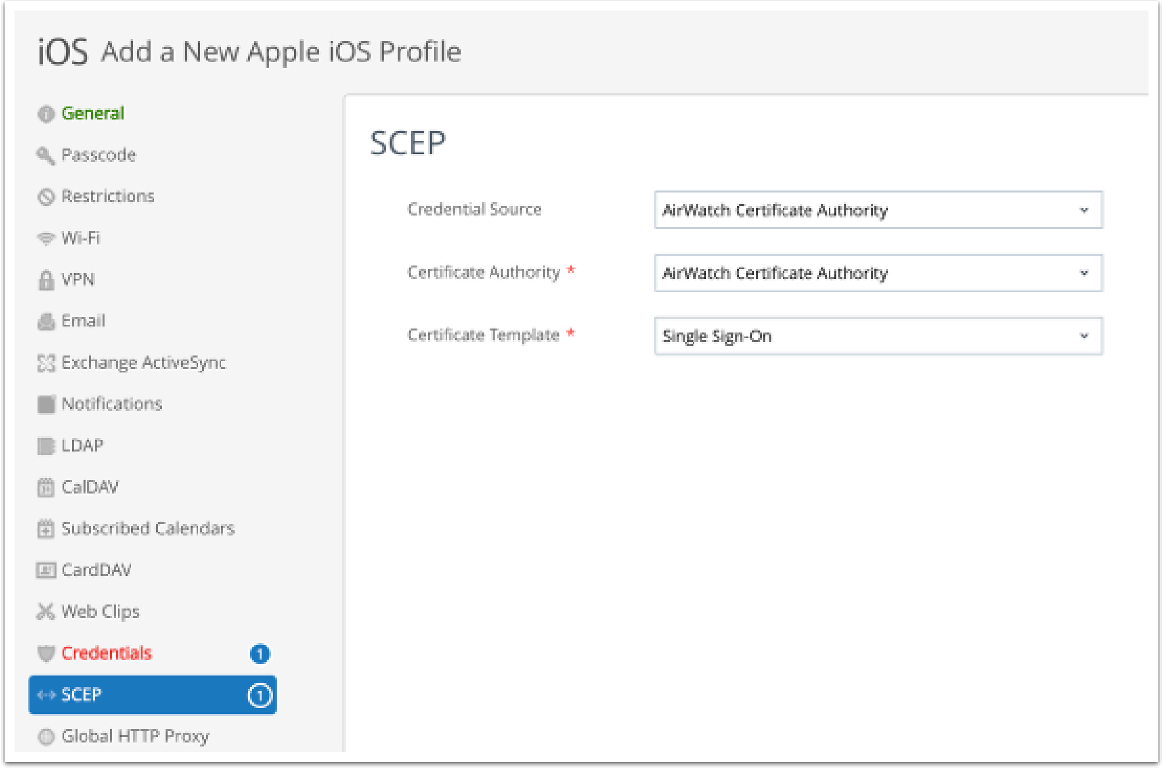
1. We will now ensure that the devices are receiving our certificates to authenticate to native mobile apps using iOS SSO.

- Return to the Workspace ONE UEM console **cn-livefire.awmdm.com**
  1. **Select Devices > Profiles & Resources >**
  2. Under **Profiles** click **ADD** > Add Profile
  3. Under **Add Profile**, select **Apple iOS**
  4. In the **IOS add a New Apple iOS Profile** under **General** add the following : Next to-
     1. Name the profile **iOS - Mobile SSO**
     2. Next to **Smart Groups** select **your Organisation Group**
  5. In the left navigation pane of the profile, select **SCEP**
  6. In the **SCEP** section in the middle of the pane select **CONFIGURE**



2. IOS Device Configuration for Single Sign On…

1. In the **SCEP window** add the following, next to:
    1. **Credential Source** : select **AirWatch Certificate Authority**,
    2. **Certificate Authority** select **AirWatch Certificate Authority**, **(it should default)**
    3. **Certificate Template** select **Single Sign-On** (it should default)



iOS Add a New Apple iOS Profile

SCEP

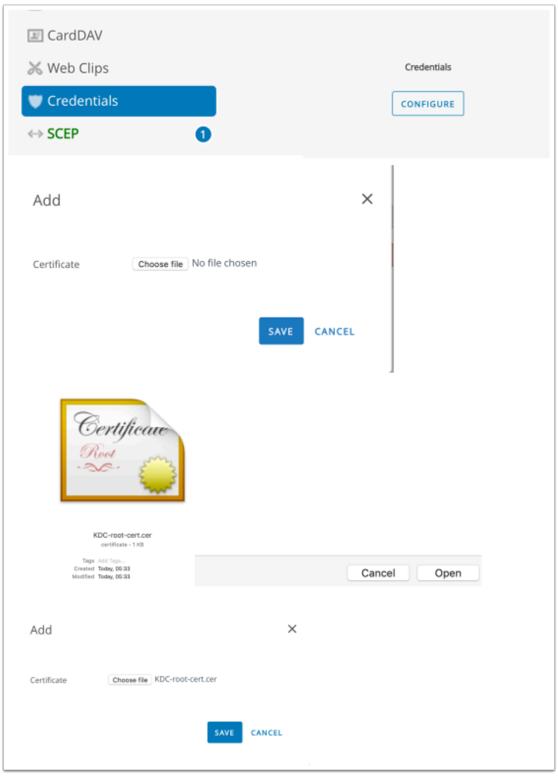
Credential Source: AirWatch Certificate Authority

Certificate Authority *: AirWatch Certificate Authority

Certificate Template *: Single Sign-On

3. IOS Device Configuration for Single Sign On…

- **iOS Add a New Apple iOS Profile cont…**
  1. On the left navigation pane above **SCEP** select **Credentials** select **configure**.
  2. In the **Credentials** window add the following, next to:-
     - Next to **Certificate** select **UPLOAD** , In the **Add** window, select **Choose file** select the **KDC-roo-cert.cer** file and select **Open**. In the **Add** window select **SAVE.** (Part 1 step 4.4 we downloaded the certificate)



4. IOS Device Configuration for Single Sign On…

- **iOS Add a New Apple iOS Profile cont…**
  1. In the left navigation pane ***scroll down*** and select **Single Sign-On**
  2. In the Single Sign-On section select **Configure**
  3. In the **Single Sign-On** window Fill in the Following information next to:-
     1. **Account Name**: **Kerberos**
     2. **Kerberos Principal Name** - **+ {EnrollmentUser}**
     3. **Realm** - **VIDMPREVIEW.COM** (ENSURE to do this in CAPS)
     4. **Renewal Certificate** - **SCEP #1**
     5. **URL Prefixes** - enter your unique vidm tenant (example https://aw-euclivefire.vidmpreview.com)
     6. Under the **Applications** section
        1. select **+ADD** below **Application Bundle ID** to add an extra line
        2. Under **Application Bundle ID** add each of these apps as separate lines

           com.microsoft.Office.Word

           com.air-watch.agent

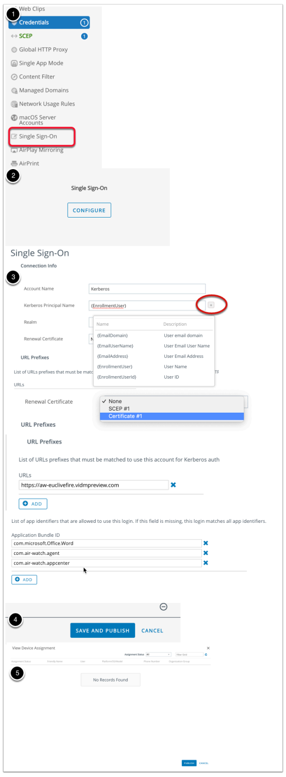
com.air-watch.appcenter

com.apple.mobilesafari

com.apple.SafariViewService

1. Select **SAVE AND PUBLISH**
2. On the **View Device Assignment** window select **PUBLISH**

Once an iOS Device is enrolled you will see the profile and the certificates appear in the settings of the device.



Single Sign-On

Connection Info

Account Name: Kerberos

Kerberos Principal Name: {EnrollmentUser}

Realm

Renewal Certificate

Name	Description
{EmailDomain}	User email domain
{EmailUserName}	User Email User Name
{EmailAddress}	User Email Address
{EnrollmentUser}	User Name
{EnrollmentUserId}	User ID

Renewal Certificate: ✓ None / SCEP #1 / Certificate #1

URL Prefixes

List of URLs prefixes that must be matched to use this account for Kerberos auth

URLs: https://aw-euclivefire.vidmpreview.com

List of app identifiers that are allowed to use this login. If this field is missing, this login matches all app identifiers.

Application Bundle ID:
com.microsoft.Office.Word
com.air-watch.agent
com.air-watch.appcenter

View Device Assignment

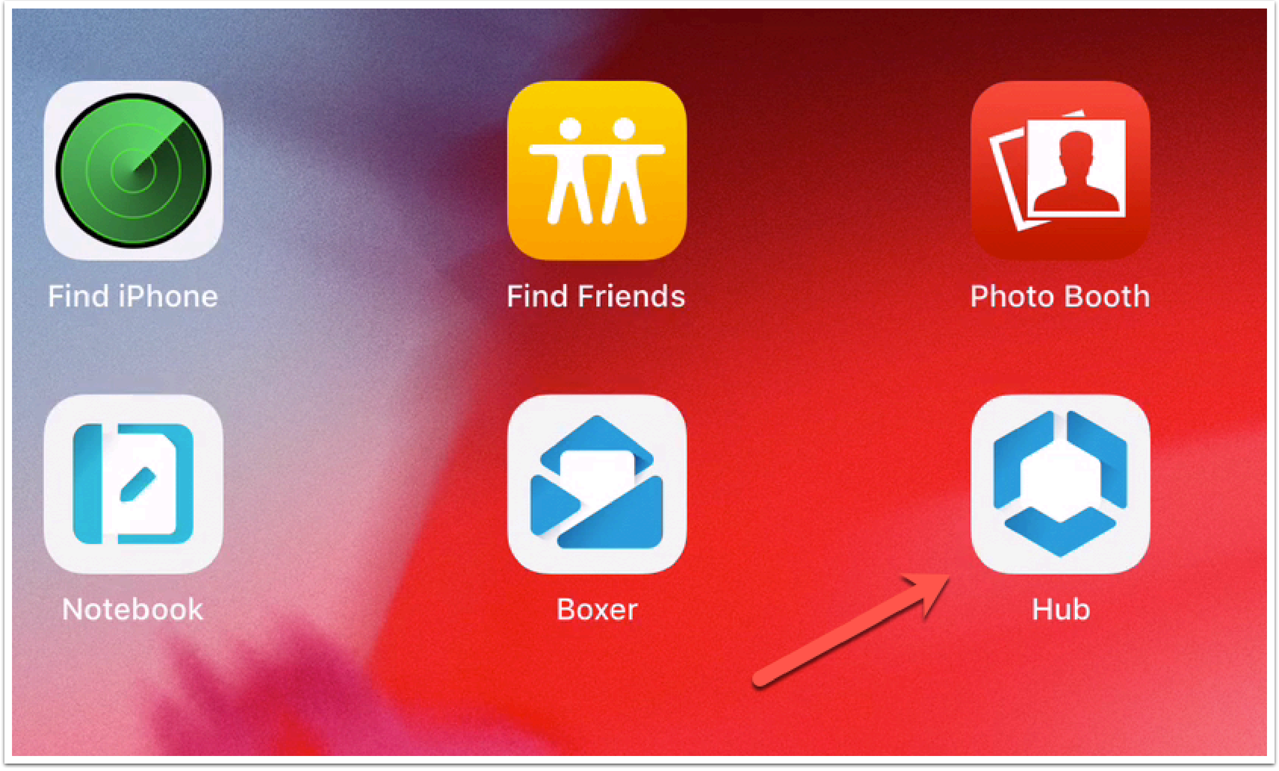
No Records Found

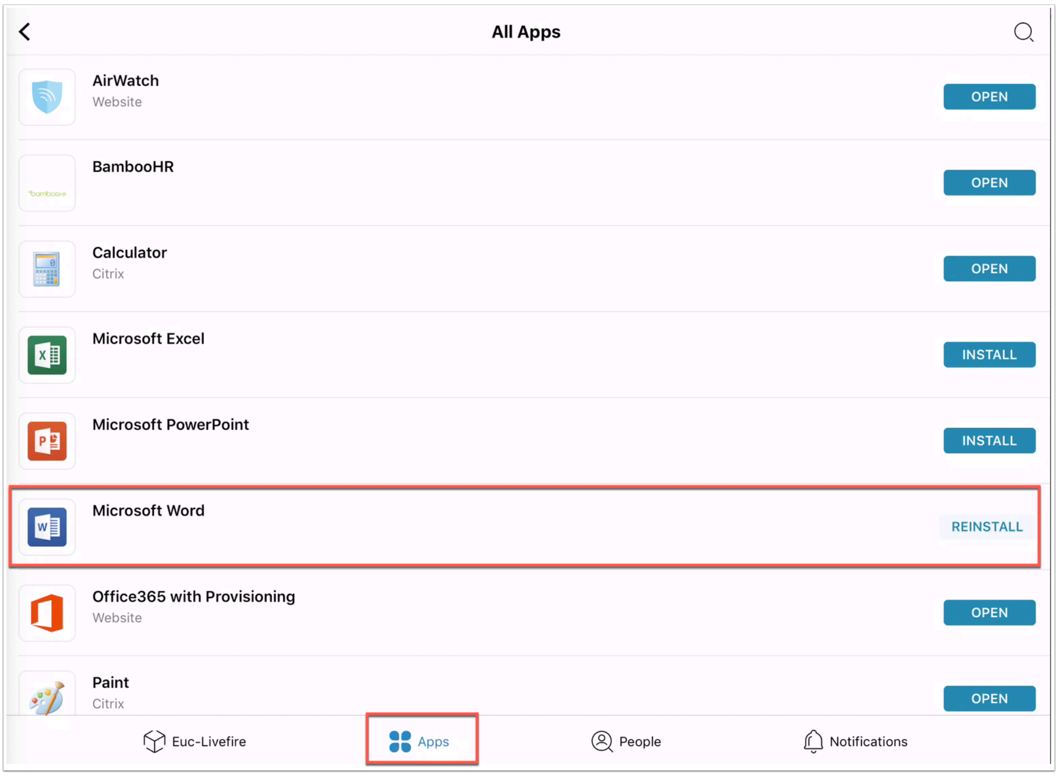
Part 3: Microsoft Word Single Sign On

Now the we have setup the device with the profile. Let's make sure we have the Microsoft Word Application installed.

1. Open the **Hub** application on your iOS device and authenticate using your biometrics or pin.

2. Select **Apps** at the bottom navigation and click **All Apps**. You will now see Microsoft Word - Click **Install** if it isn't already installed




All Apps

AirWatch Website	OPEN
BambooHR	OPEN
Calculator Citrix	OPEN
Microsoft Excel	INSTALL
Microsoft PowerPoint	INSTALL
Microsoft Word	REINSTALL
Office365 with Provisioning Website	OPEN
Paint Citrix	OPEN

1. Once the Microsoft Word application has installed you will now authenticate to the application using MobileSSO. Launch the Word application on your iOS device.

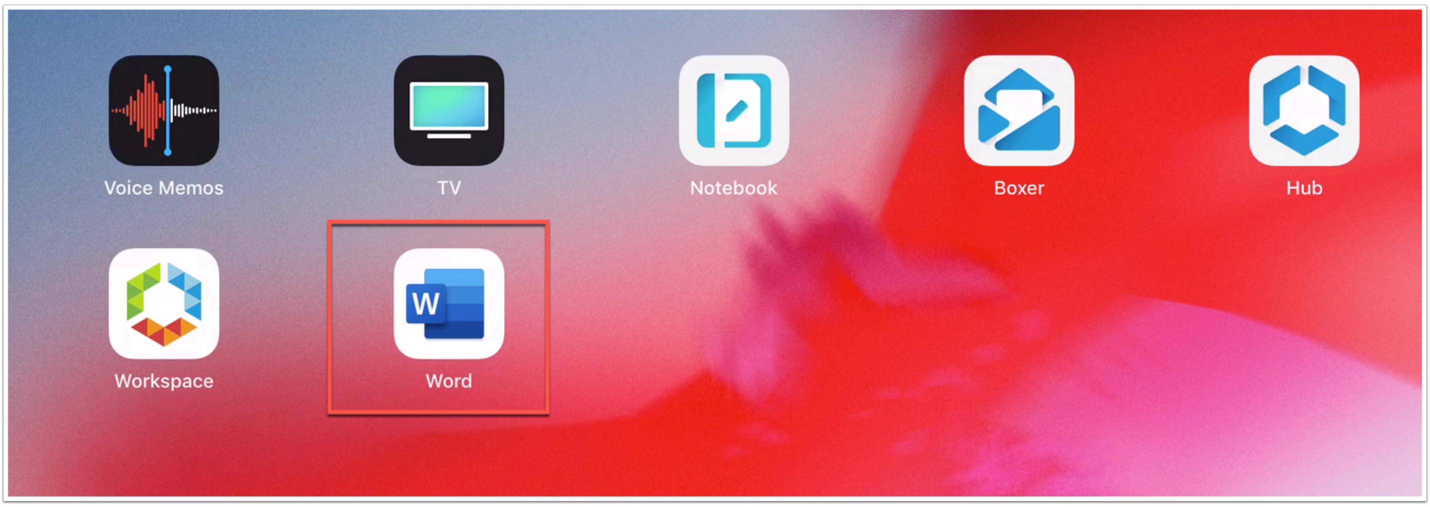
2. When prompted click **sign in.** Use the UPN of the unique user you create in the SFDC lab (ie user33buk@madrid33.euc-livefire.com) and click **Next**

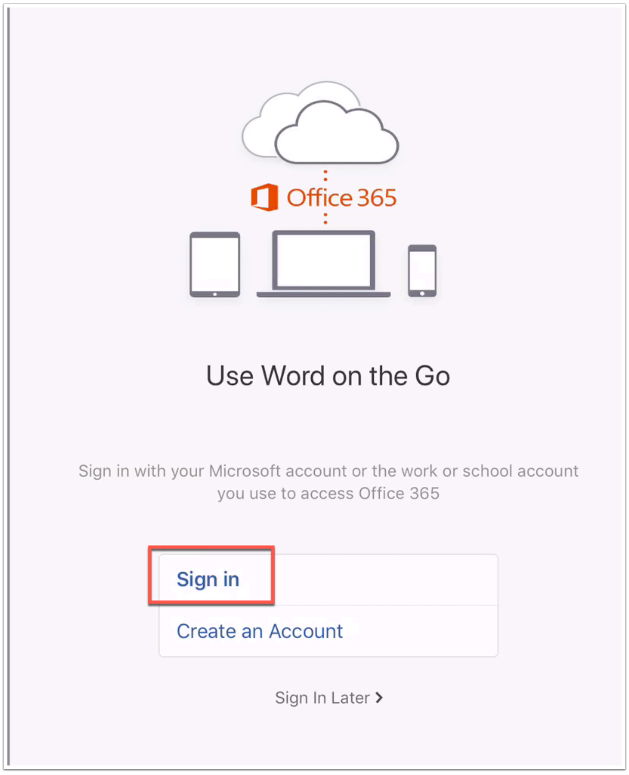
3. At his point the Mobile Single sign on for iOS will kick in and leverage the certificate on the device for authentication. You will see a screen that says activating.

4. On the Notification prompt click **Not Now**

5. Now click Create and Edit Documents to get started using the Word application

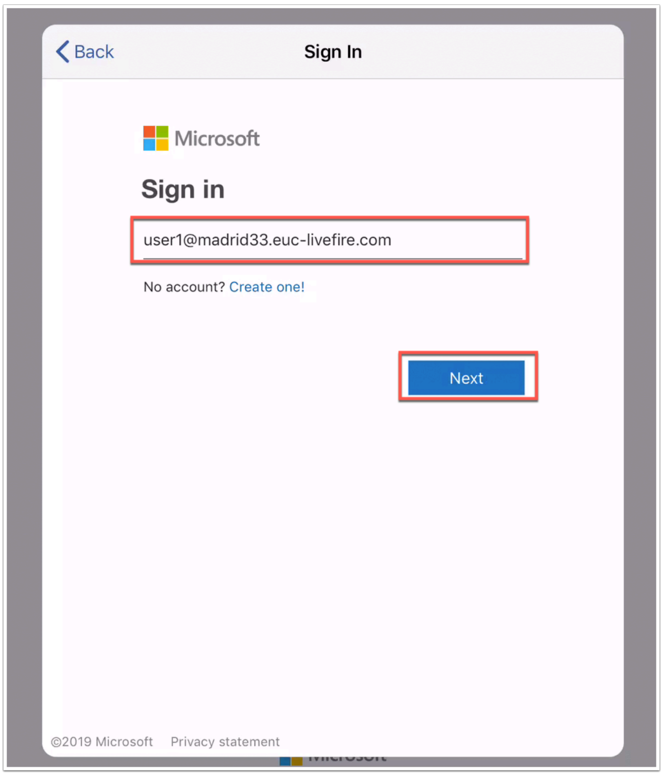
6. When you click on **Settings** you will see under **Account** the uniqueuser**@XXX.euc-livefire.com.** Notice you didn't have to use a username or password to authenticate. This is the user experience that so many enterprises desire for authentication.





Use Word on the Go

Sign in with your Microsoft account or the work or school account you use to access Office 365



Back

Sign In

Microsoft

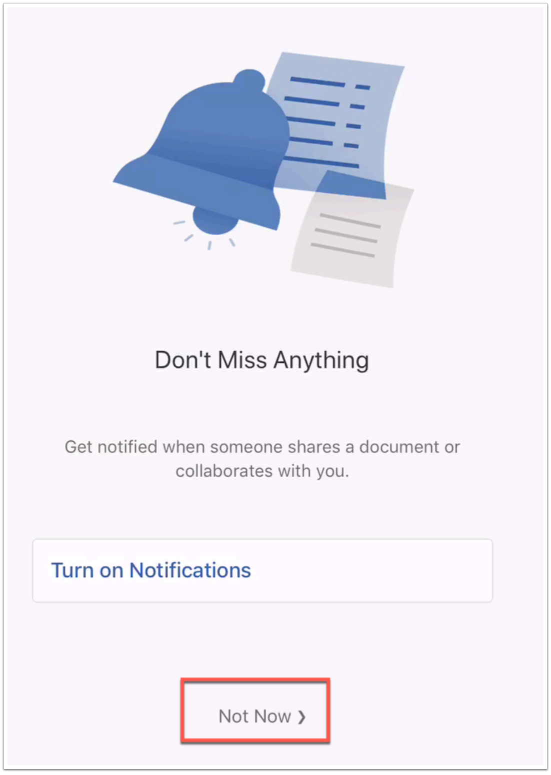
Sign in

user1@madrid33.euc-livefire.com

No account? Create one!

Next

©2019 Microsoft Privacy statement

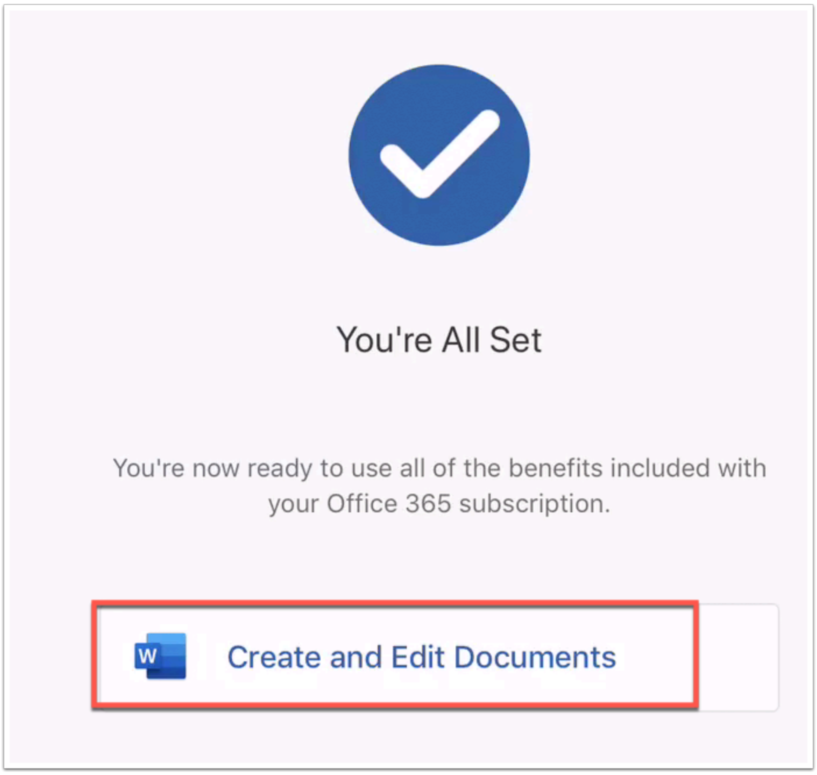


Don't Miss Anything

Get notified when someone shares a document or collaborates with you.

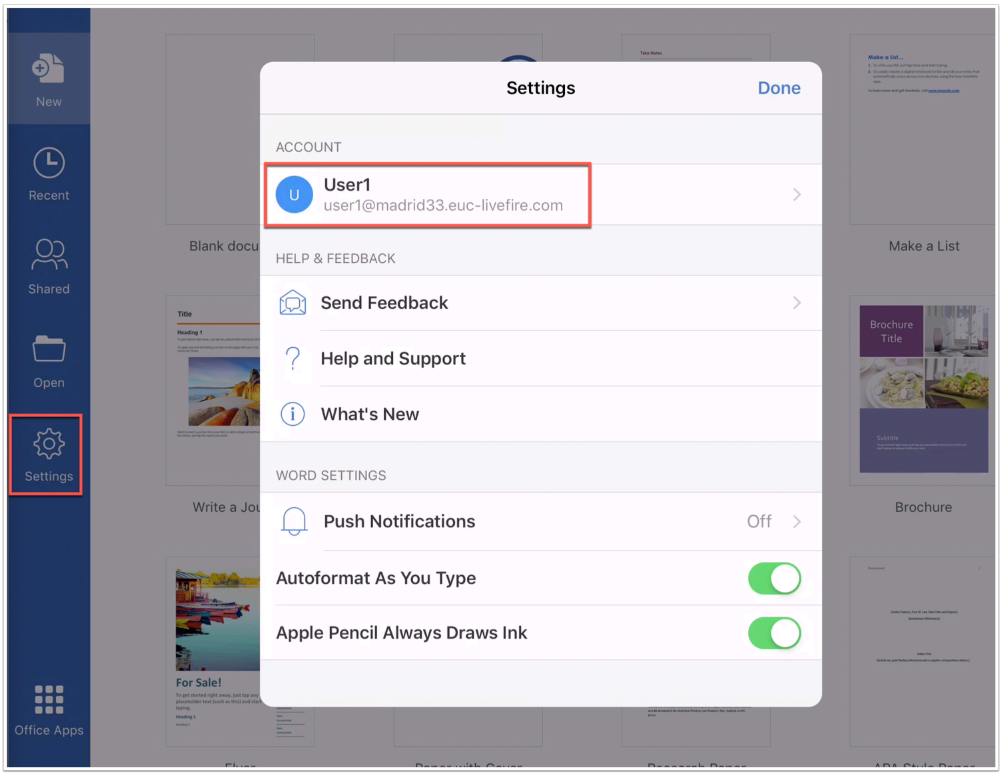
Turn on Notifications

Not Now ›



You're All Set

You're now ready to use all of the benefits included with your Office 365 subscription.



Settings

ACCOUNT

User1
user1@madrid33.euc-livefire.com

HELP & FEEDBACK

Send Feedback

Help and Support

What's New

WORD SETTINGS

Push Notifications Off

Autoformat As You Type

Apple Pencil Always Draws Ink

Authentication Method - Android SSO

Configure Single-Sign-on for Android Device from the Workspace ONE UEM Admin Console

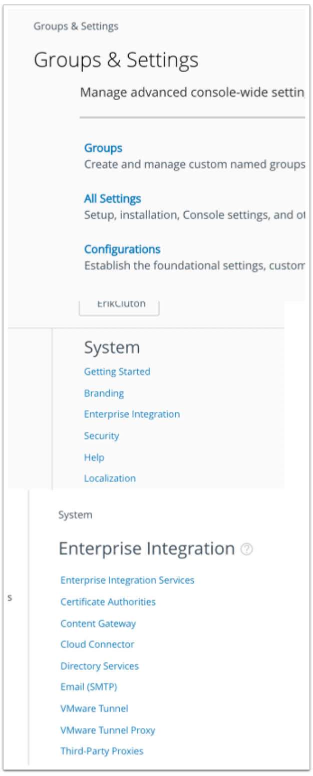
Pre-requisites to this lab

1. For this lab you will need an Android Device that you are willing to enroll into this lab environment.
2. If you do not have an Android test device, please complete Android emulator setup, from Day 1 lab, before proceeding.

Part 1: Configuring Workspace ONE Access for Android Mobile SSO

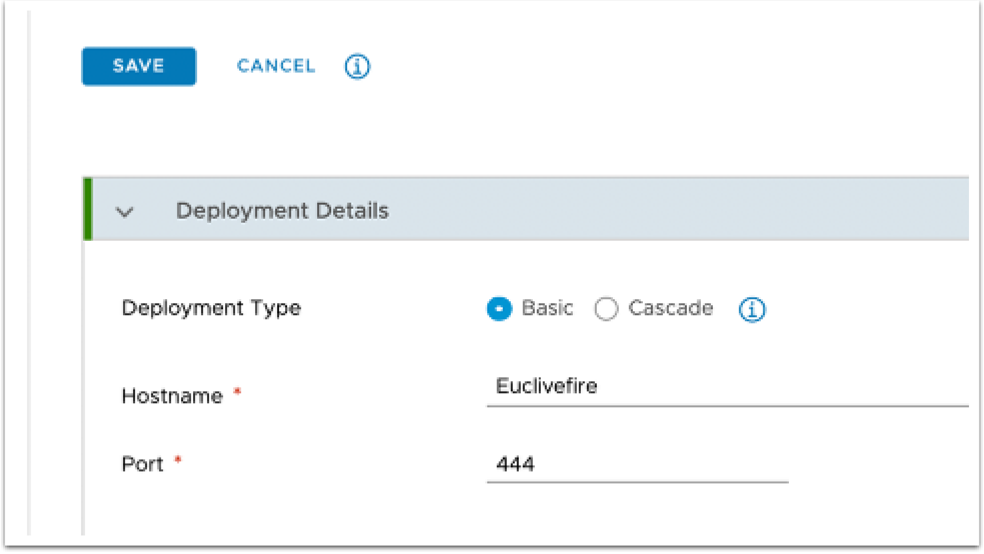
1.1 In this section we will download a certificate from WorkspaceONE UEM and use to configure Android Mobile SSO in Workspace ONE Access. After we will round all the remaining Workspace ONE Access configurations.

- Login to WorkspaceONE UEM with your custom credentials
  1. Select **GROUPS & SETTINGS** > **All Settings**
  2. Under **System** select **Enterprise Integration**
  3. Under **Enterprise Integration** select **VMware Tunnel**



1.2 On the **Tunnel Configuration** page enter the following

- Next to **Hostname**: **EUClivefire** (this can be anything)
- **Port: 444** (this can be anything)
- At the top of the page select **SAVE**



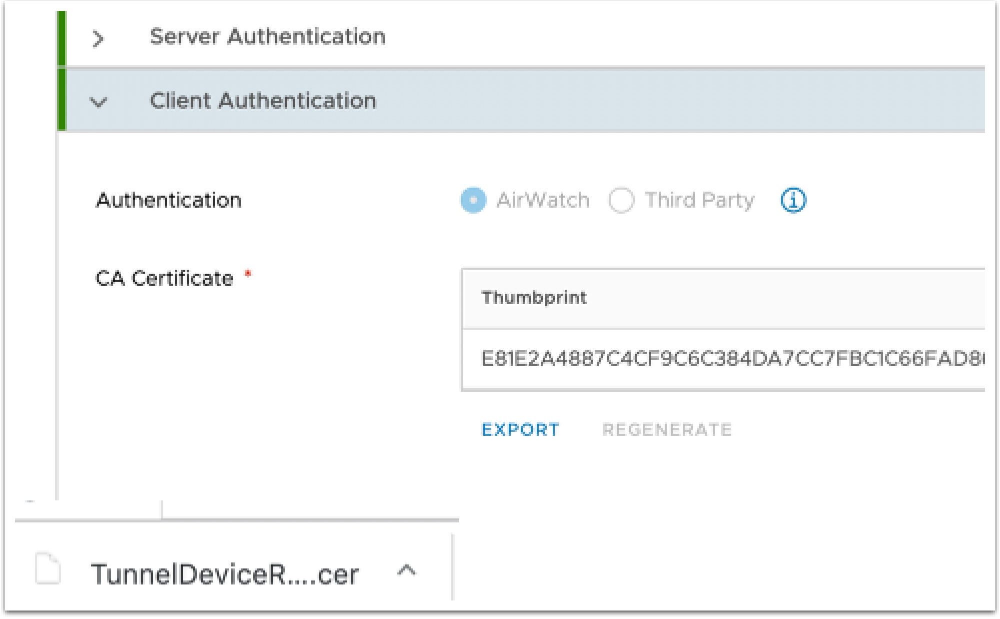
Deployment Type ● Basic ○ Cascade

Hostname * Euclivefire

Port * 444

1.3 Expand **Client Authentication**

- Below **Thumbprint** select **EXPORT**
- Note the name of the certificate is **TunnelDeviceRootCertificate.cer**



Authentication ● AirWatch ○ Third Party

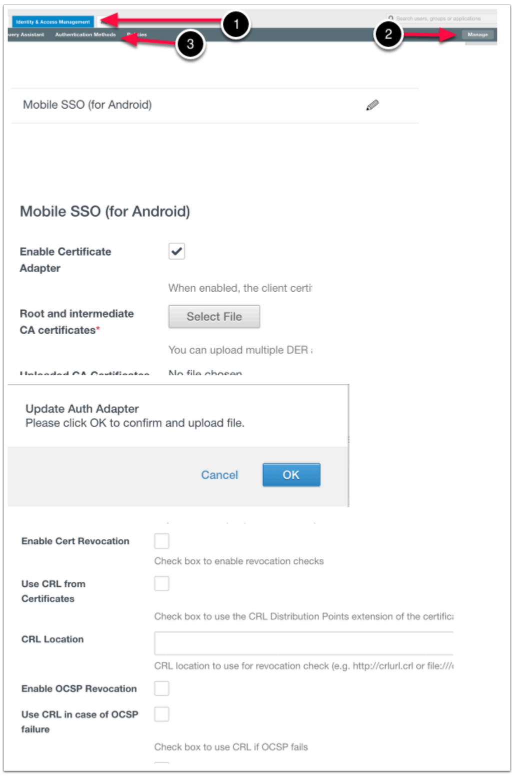
CA Certificate *

Thumbprint
E81E2A4887C4CF9C6C384DA7CC7FBC1C66FAD8

1.4 Login to your SaaS instance of Workspace ONE Access

1. Select the **Identity & Access Management** tab select **Manage** and then select **Authentication Methods**
2. Under **Authentication methods** select the **Pencil Icon** next to **Mobile SSO (for Android)**
3. On the **Mobile SSO (for Android)** window select the following: Next to

- **Enable Certificate Adapter:** select the **checkbox**
- **Root and Intermediate CA certificates** click on the **Select File** button, choose the **TunnelDeviceRootCertificate.cer** file you downloaded earlier and select **Open**. On the **Update Auth Adapter** window select **OK**
- **Use CRL from Certificates : Uncheck the checkbox**
- **Use CRL in case of OCSP failure: Uncheck the checkbox**
- At the bottom of the page select **Save**


Identity & Access Management
Search users, groups or applications
very Assistant
Authentication Methods
Policies
Manage
1
2
3

Mobile SSO (for Android)

Mobile SSO (for Android)

Enable Certificate Adapter ☑
When enabled, the client certi

Root and intermediate CA certificates* Select File
You can upload multiple DER

Uploaded CA Certificates No file chosen

Update Auth Adapter
Please click OK to confirm and upload file.

Cancel OK

Enable Cert Revocation □
Check box to enable revocation checks

Use CRL from Certificates □
Check box to use the CRL Distribution Points extension of the certific

CRL Location
CRL location to use for revocation check (e.g. http://crlurl.crl or file:///

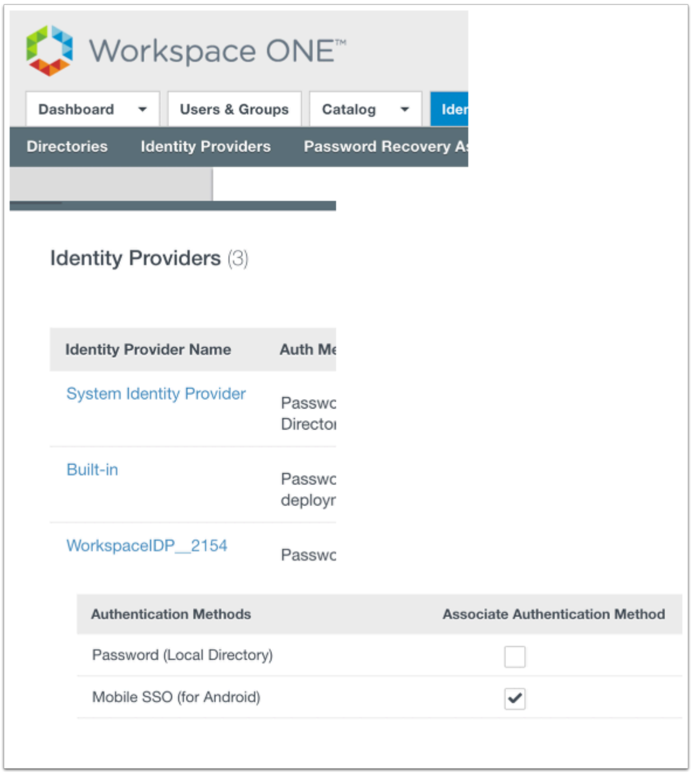
Enable OCSP Revocation □

Use CRL in case of OCSP failure □
Check box to use CRL if OCSP fails

1.5 On the **Identity & Access Management** tab > **Manage ...**

- , select **Identity Providers**

1. On the **Identity Providers** window, select **Built-in**
2. Under the **Authentication Methods** area select **Mobile SSO (for Android) checkbox**
3. Select **Save**



Identity Providers (3)

Identity Provider Name	Auth Me
System Identity Provider	Passwc Directoi
Built-in	Passwc deployr
WorkspaceIDP__2154	Passwc

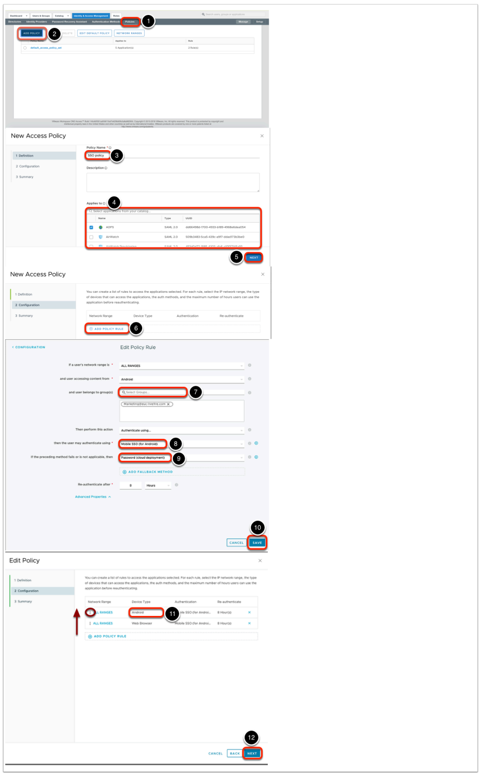
Authentication Methods	Associate Authentication Method
Password (Local Directory)	□
Mobile SSO (for Android)	☑

1.6 On the **Identity & Access Management** tab > **Manage**,

NOTE If you have done the **MOBILE SSO lab for IOS** previously, SKIP 1.6 and GO to Step 1.7 and we will **EDIT** the existing **SSO** Policy

- 1.Select **Policies**

1. Select **Add Policy.**
2. On the **New Access Policy** Page, enter a policy name: **SSO** Policy
3. Under **Applies to** section, select **ALL** the applications **except** AirWatch & AirWatch Provisioning.
4. Hit Next.
5. select **+ADD POLICY RULE**
6. On Add Policy Rule page add the following, next to:
   - **and user accessing content from *** : **Android**
   - and user belongs to group(s) : **Marketing@euc-livefire.com**
   - **then the user may authenticate using*** : **Mobile SSO (for Android)**
   - **if the preceding method fails or is not applicable, then *** : Password (cloud deployment)
   - Select **SAVE**
7. Ensure that **Android Mobile SSO** is the top of the order, above **Web Browser** (if present), if not select the **6 dots** next to **ALL RANGES**, and ***drag upwards*** select **NEXT**
8. On the **Summary** page select SAVE



	Policy Name	Applies to	Rule
○	default_access_policy_set	5 Application(s)	2 Rule(s)

New Access Policy

Policy Name *: SSO policy

	Name	Type	UUID
☑	ADFS	SAML 2.0	dd66498d-1700-4933-b189-4968e6dea054
□	AirWatch	SAML 2.0	509b3483-5ca5-439c-a9f7-ddad173b3be0

New Access Policy

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate

Edit Policy Rule

If a user's network range is *: ALL RANGES

and user accessing content from *: Android

and user belongs to group(s): Select Groups... Marketing@euc-livefire.com

Then perform this action: Authenticate using...

then the user may authenticate using *: Mobile SSO (for Android)

If the preceding method fails or is not applicable, then: Password (cloud deployment)

Re-authenticate after *: 8 Hours

Edit Policy

You can create a list of rules to access the applications selected. For each rule, select the IP network range, the type of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network Range	Device Type	Authentication	Re-authenticate
ALL RANGES	Android	Mobile SSO (for Androi...	8 Hour(s)
ALL RANGES	Web Browser	Mobile SSO (for Androi...	8 Hour(s)

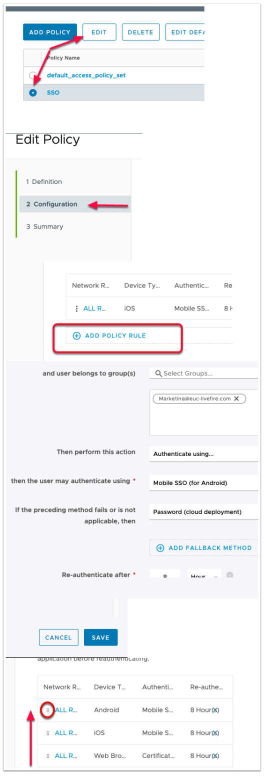
1.7 On the **Identity & Access Management** tab > **Manage**,

NOTE This section is for attendees that are doing both the Mobile IOS and Android lab.

- Select **Policies**

1. Select the **radio button** next ot **SSO** and select **EDIT.**
2. On the **Edit Policy** Page, select step **2 Configuration**
3. Select **+ADD POLICY RULE**
4. On Add Policy Rule page add the following, next to:
   - **and user accessing content from *** : **Android**
   - and user belongs to group(s) : **Marketing@euc-livefire.com**
   - **then the user may authenticate using*** : **Mobile SSO (for Android)**
   - **if the preceding method fails or is not applicable, then *** : Password (cloud deployment)
   - Select **SAVE**

5. Ensure that **Android Mobile SSO** is top of the order, above **Web Browser**, if not select the **6 dots** next to **ALL RANGES**, and ***drag upwards*** select **NEXT**
6. On the **Summary** page select **SAVE**



	Policy Name
○	default_access_policy_set
●	SSO

Edit Policy

1 Definition
2 Configuration
3 Summary

Network R...	Device Ty...	Authentic...	Re
ALL R...	iOS	Mobile SS...	8 H

and user belongs to group(s)
Select Groups...
Marketing@euc-livefire.com

Then perform this action
Authenticate using...

then the user may authenticate using *
Mobile SSO (for Android)

If the preceding method fails or is not applicable, then
Password (cloud deployment)

Re-authenticate after *
8 Hour

application before reauthenticating.

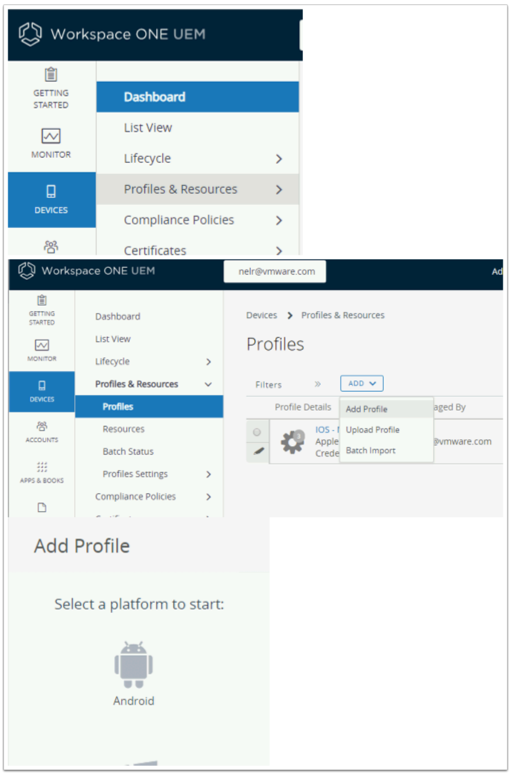
Network R...	Device T...	Authenti...	Re-authe...
ALL R...	Android	Mobile S...	8 Hour(s)
ALL R...	iOS	Mobile S...	8 Hour(s)
ALL R...	Web Bro...	Certificat...	8 Hour(s)

Part 2. Configuring Single-Sign-on for Android: Android VPN Profile

2.1. We have just configured the Workspace ONE Access Android SSO auth Adaptor, we will now configure the Android VPN profile and add a version to the profile in Workspace ONE UEM.

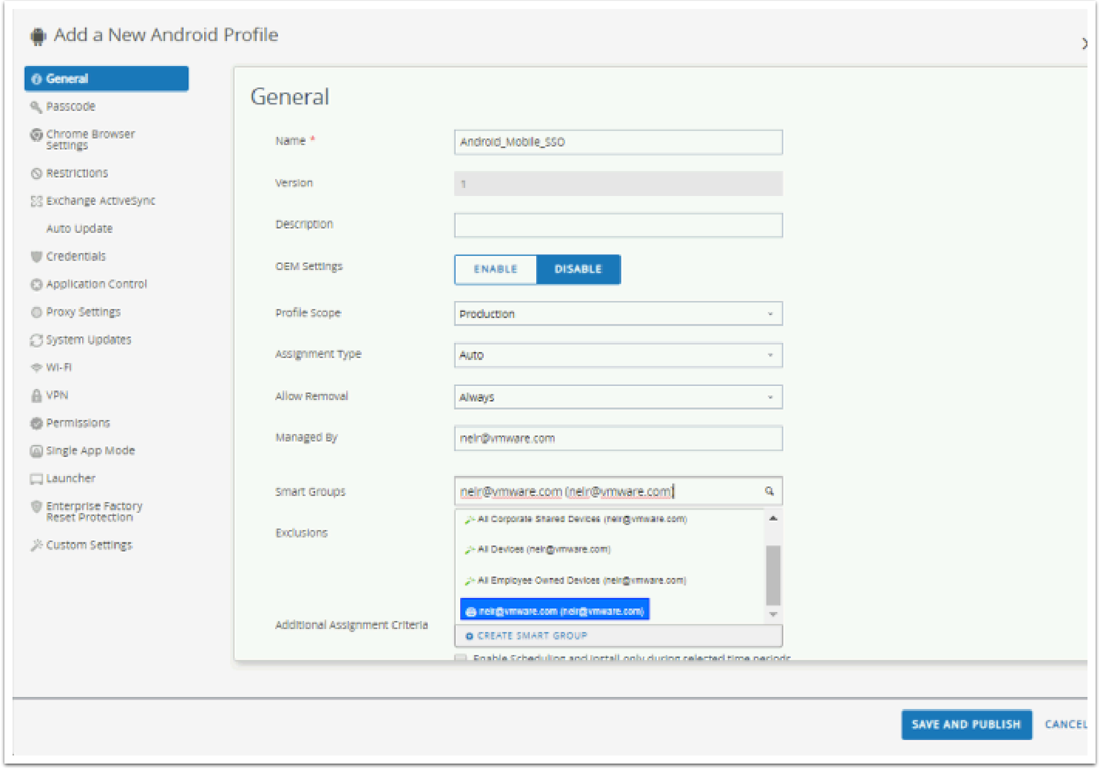
- **Login to your Saas Workspace ONE UEM Admin Console**
  - **Configuring Per App Tunnel Profile for Android**

1. In the **Workspace ONE UEM** admin console, select **Devices** > Profiles & Resources
2. Under **Profiles & Resources** select **Profiles**> **ADD** dropdown, then select **Add Profile**
3. On the **Add Profile** window, select **Android.**



2.2 Configuring Single-Sign-on for Android

- **Configuring Per App Tunnel Profile for Android cont..**
- In the **Add a New Android Profile** window configure the following...
  1. In the left column select **General** and configure only the following: Next to -
     1. **Name** type **Android_Mobile_SSO**
     2. **Smart Groups**: **YOUR ORGANISATIONAL GROUP**. (scroll to the bottom and select the line with the world)



General

Name * Android_Mobile_SSO

Version 1

Description

OEM Settings ENABLE [✓ DISABLE]

Profile Scope Production

Assignment Type Auto

Allow Removal Always

Managed By neir@vmware.com

Smart Groups neir@vmware.com (neir@vmware.com)

- All Corporate Shared Devices (neir@vmware.com)
- All Devices (neir@vmware.com)
- All Employee Owned Devices (neir@vmware.com)
- neir@vmware.com (neir@vmware.com)

CREATE SMART GROUP

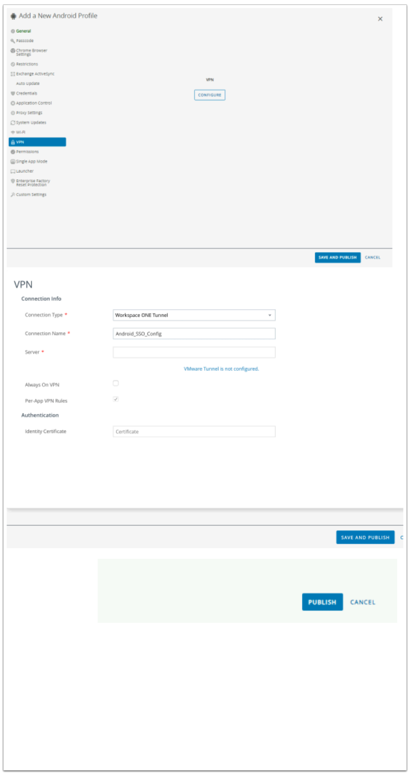
Exclusions

Additional Assignment Criteria

□ Enable Scheduling and install only during selected time periods

2.3 Configuring Single-Sign-on for Android

- **Configuring Per App Tunnel Profile for Android cont..**
- In the **Add a New Android Profile** window configure the following…
  1. In the left column, select **VPN** and select **Configure**.
     1. In the **VPN** window configure the following next to:-
        1. **Connection Type**: **Workspace ONE Tunnel**
        2. **Connection Name: Android_SSO_Config**
        3. **Server: (leave default)**
        4. Per-App VPN Rules: **checkbox enabled**
     2. Select **SAVE AND PUBLISH**
     3. On **View Device Assignment** window select **PUBLISH**



VPN

Connection Info

Connection Type * Workspace ONE Tunnel

Connection Name * Android_SSO_Config

Server *

VMware Tunnel is not configured.

Always On VPN □

Per-App VPN Rules ☑

Authentication

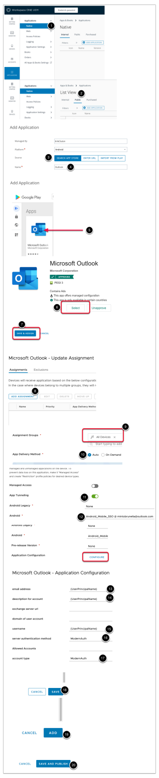
Identity Certificate Certificate

Part 3: Configuring an Android Native applications for a Per App VPN Profile in WorkspaceONE UEM for SSO

3.1

- Ensure you are logged into your Workspace ONE UEM admin console with your Admin credentials
  1. In the **Workspace ONE UEM** Admin Console select **APPS & BOOKS** > **Applications** > Native
  2. Under **Native** next to **Internal** select **Public** and then select **+ ADD APPLICATION**
  3. On the **Add Application** window add the following: -
     - Next to **Platform** select **Android**
     - Next to **Source** leave the default **SEARCH APP STORE**
     - Next **Name** type **Outlook**
     - At the bottom of the Page select **NEXT**
  4. In the A**dd Application** window select **Microsoft Outlook**
  5. On the **Microsoft Outlook:** window click on the **Select** button
  6. On the **Microsoft Outlook Access:** window click on the **APPROVE** button
  7. On the on the **Microsoft Outlook APPROVAL SETTINGS** window click on the **SAVE** button
  8. In the **Edit Application - Microsoft Outlook** window select **SAVE & ASSIGN**
  9. On the **Microsoft Outlook - Update Assignment** page . select **ADD ASSIGNMENT**
  10. On the **Microsoft Outlook - Add Assignment** page next to **Select Assignment Groups** select **All Devices** ,

11. Next to **App Delivery Method** select the AUTO **radio button**
12. Next to **App Tunneling** select **ENABLED**. Next to **Android*** select your **Android_Mobile_SSO@*** profile
13. Next **Application Configuration** select **Configure**
    - Next to the following add the respective configuration under the **Value** area
        - **email address** **{UserPrincipalName}**
        - **domain of user account** **{UserPrincipalName}**
        - **username** **{UserPrincipalName}**
        - **server authentication method** **ModernAuth**
        - **account type** **ModernAuth**
        - **Focused inbox** **Enable**
        - **Contact sync enabled** **Enable**
        - **Suggested replies enabled** **Enable**
14. Select **Save** > Select **ADD**
15. Select **SAVE AND PUBLISH** > **PUBLISH**
16. You should now have Outlook **for Android** in your **Apps & Books** > **Applications** console



Managed By: ErikCluton
Platform*: Android
Name*: Outlook

Devices will receive application based on the below configurati… In the case where devices belong to multiple groups, they will r…

Assignment Groups *: All Devices

App Delivery Method *: ● Auto ○ On Demand

managed and unmanaged applications on the device. To prevent data loss on this application, make it "Managed Access" and create "Restriction" profile policies for desired device types.

Managed Access: off

App Tunneling: on

Android Legacy *: None

Android *: Android_Mobile_SSO @ mintobrunella@outlook.com

Android Legacy *: None

Android *: Android_Mobile

Pre-release Version *: None

Application Configuration

email address: {UserPrincipalName}

description for account: {UserPrincipalName}

exchange server url:

domain of user account:

username: {UserPrincipalName}

server authentication method: ModernAuth

Allowed Accounts:

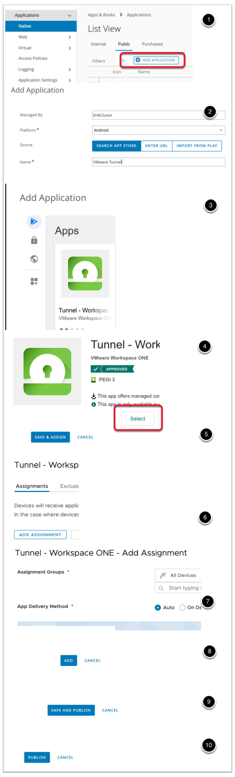
account type: ModernAuth

3.3

- In the **APPS & BOOKS** > **Applications** > **Native** > **Public** tab continued..
  1. Select **+ADD APPLICATION**
  2. In the **Add Application** window next to: Select
      - **Platform*** : **Android**
      - **Name*:** **VMware Tunnel**
      - select **NEXT**
  3. In the **Add Application** window select **Tunnel - Workspace ONE**

4. In the **Tunnel - Workspace ONE** section, click the **SELECT** button
5. Select **SAVE & ASSIGN**
6. On the **Tunnel - Workspace ONE- Update Assignment** window select **ADD ASSIGNMENT**
7. In the **VMware Workspace ONE Tunnel - Add Assignment** window next to
    - **Select Assignment Groups: All Devices**
    - **App Delivery Method: Auto** radio button

8. At the bottom of the page select **ADD**
9. Select **SAVE & PUBLISH**
10. Select **PUBLISH**



Managed By: ErikCluton

Platform*: Android

Name*: VMware Tunnel

Assignment Groups *: All Devices

App Delivery Method *: ● Auto ○ On De

3.4 Configuring Sales Force for native Android Single Sign-On

- In the **WorkspaceONE UEM** console, select **APPS & BOOKS** > **Applications** > **Native**

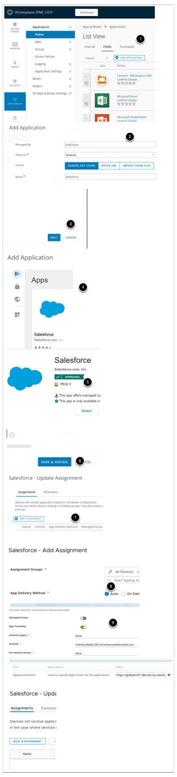
1. In the **List View** interface select **Public**, select **+ ADD APPLICATION**
2. In **Add Application** window, select the following, next to:-
    - **Platform*: Android**
    - **Name*: Salesforce**

3. At the bottom of the **Add Application** window, select **NEXT**
4. In the **Add Application** window under **Apps** select **Salesforce**
5. In the **Add Application** window under **Salesforce** click **SELECT**
6. On the **Edit Application - Salesforce** window, select **SAVE & ASSIGN**
7. On the **Salesforce - Update Assignment** window select **ADD ASSIGNMENT**
8. On the **Salesforce - Add Assignment** window select and update the following next to:-
    - **Select Assignment Groups**: **All Devices**
    - **App Delivery Method*: Auto radio button**

    - **App Tunneling:** toggle Enabled
        - **Android*:** Android_Mobile_SSO

9. Next to **Application Configuration** select **Configure**. You will notice a whole range of additional configurations now become available
10. Next to the Title **AppServiceHosts**
    - Under the middle area type in your **custom Salesforce domain**
    - e.g. **sanjose35-dev-ed.my.salesforce.com**
    - At the bottom of the **Salesforce - Application Configuration** page select **SAVE**
    - At the bottom of the **Salesforce - Add Assignment** window select **ADD**

11. On the **Salesforce - Update Assignment** window select **SAVE AND PUBLISH**
12. On the **Preview Assigned Devices** window select **PUBLISH**



3.5 Configuring BAMBOOHR for native Android Single Sign-On

1. In the **WorkspaceONE UEM** console, select **APPS & BOOKS** > **Applications** > **Native**
    - Under the Pubic select **+ADD APPLICATION**

2. In **Add Application** window, select the following, next to:-
    - **Platform*: Android**
    - **Name*: BAMBOOHR**
    - Select **NEXT**

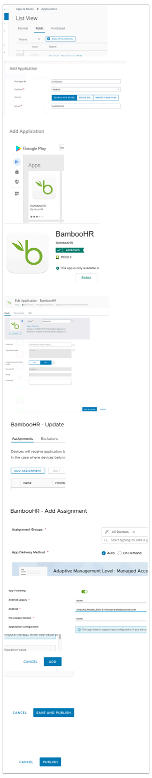
3. In the **Add Application** window under **Apps** select **BambooHR**
4. In the **Add Application** window under **BambooHR** click **Select**
5. On the **Edit Application - BambooHR** window, select **SAVE & ASSIGN**
6. On the **BambooHR - Update Assignment** window select **ADD ASSIGNMENT**
7. On the **BambooHR - Add Assignment** window select and update the following next to:-

  - **Assignment Groups**: **All Devices**
  - **App Delivery Method*: Auto radio button**
  - **App Tunneling: toggle** Enabled
    - **Android*:** Android_Mobile_SSO

  - Next to **Application Configuration:** NOTE **This App doesn't support app configuration...**

8. At the bottom of the **BambooHR - Add Assignment** window select **ADD**
9. On the **BambooHR - Update Assignment** window select **SAVE AND PUBLISH**
10. On the **Preview Assigned Devices** window select **PUBLISH**

- This application does not support the SDK we will therefore have to manually configure the native application settings on the device



Apps & Books > Applications

List View

Internal | Public | Purchased

Filters » ADD APPLICATION

Add Application

Managed By: ErikDaton

Platform*: Android

Source: SEARCH APP STORE | ENTER URL | IMPORT FROM PLAY

Name*: BAMBOOHR

Add Application

BambooHR

BambooHR

APPROVED

PEGI 3

This app is only available in

Select

Edit Application - BambooHR

BambooHR - Update

Assignments | Exclusions

Devices will receive application b

In the case where devices belong

ADD ASSIGNMENT | EDIT

BambooHR - Add Assignment

Assignment Groups *: All Devices

App Delivery Method *: ● Auto ○ On Demand

Adaptive Management Level : Managed Acce

App Tunneling: on

Android Legacy *: None

Android *: Android_Mobile_SSO @ mintobrunella@outlook.com

Pre-release Version *: None

Application Configuration: This app doesn't support app configuration. If you are us

CANCEL | ADD

CANCEL | SAVE AND PUBLISH

CANCEL | PUBLISH

3.6 Configuring your Chrome Browser for Single-Sign ON

- Certain Applications like Chrome integrate with your Browser. You will have to configure your browser for single-sign ON as well
  1. In the **APPS & BOOKS** > **Applications** > **Native** > **Public** tab continued..
  2. Select **+ADD APPLICATION**
  3. In the **Add Application** window next to: Select
     - **Platform*** : **Android**
     - **Name*: Chrome**

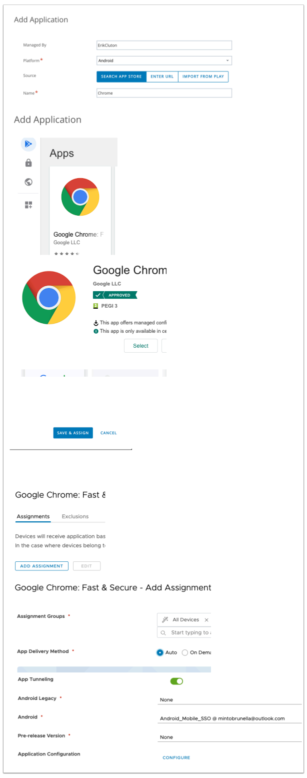
     1. select **NEXT**

  4. In the top of the **Add Application** window select **Google Chrome Fast & Secure**
  5. On the **Edit Application - Google Chrome Fast & Secure** select **SAVE & ASSIGN**

6. On the **Google Chrome: Fast & Secure -** Update Assignment window select **ADD ASSIGNMENT**
7. In the **Google Chrome** - Add Assignment window next to
   - **Select Assignment Groups: All Devices**
   - **App Delivery Method: Auto radio button**

8. Next to **App Tunneling** select **ENABLED** (two new sections are added)
   - **Android*** : **Android_Mobile_SSO**

9. At the bottom of the page select **ADD**
10. Select **SAVE & PUBLISH**
11. Select **PUBLISH**



Add Application

Managed By: ErikCluton

Platform*: Android

Source: SEARCH APP STORE | ENTER URL | IMPORT FROM PLAY

Name*: Chrome

Add Application

Google Chrome: Fast &

Devices will receive application bas
In the case where devices belong t

Google Chrome: Fast & Secure - Add Assignment

Assignment Groups *: All Devices ×

App Delivery Method *: ● Auto ○ On Dema

App Tunneling: ●

Android Legacy *: None

Android *: Android_Mobile_SSO @ mintobrunella@outlook.com

Pre-release Version *: None

Application Configuration: CONFIGURE

Part 4: Configuring VMware Tunnel Component

For this lab to work we need to ensure you have a Published Application like Microsoft Word. If you are comfortable with Workspace ONE UEM you can use any application you choose, but you will need to Publish it and ensure you have a native version on your Android Device.

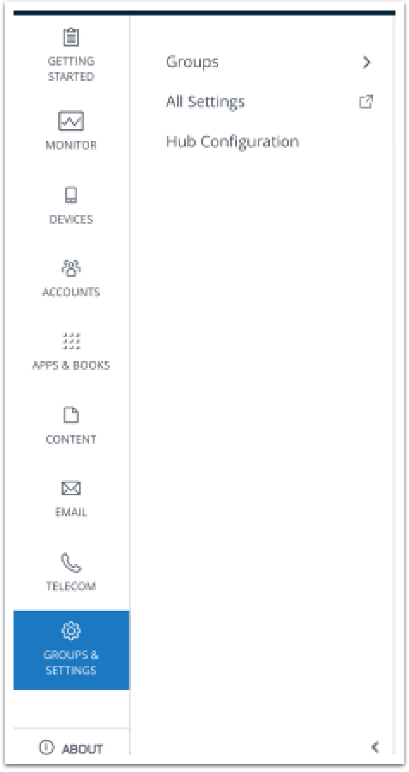
Configure single sign-on for Android devices to allow users to sign in securely to enterprise apps, without entering their password.

About this task

To configure single-sign-on for Android devices, you do not need to configure the VMware Tunnel, but you configure single sign-on using many of the same fields

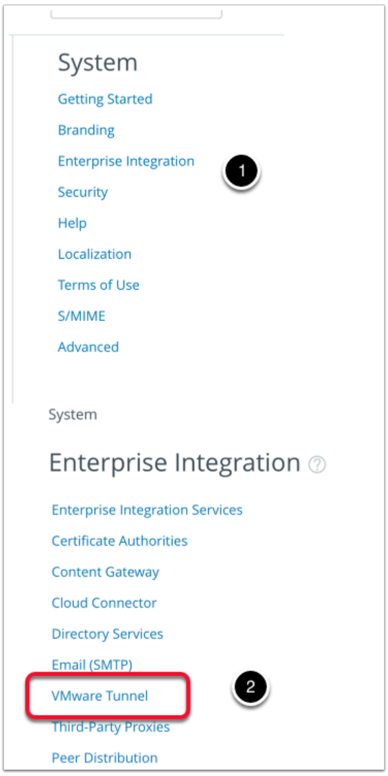
4.1

- **Configuring Single-Sign-on for Android**
  1. Ensure you launch your on your Control center desktop and launch your browser to enter **https://cn-livefire.awmdm.com**
  2. Log into your **Workspace ONE UEM** admin console with your Admin credentials.
  3. In the **Workspace ONE UEM** admin console, select **GROUPS & SETTINGS**, select **All Settings**



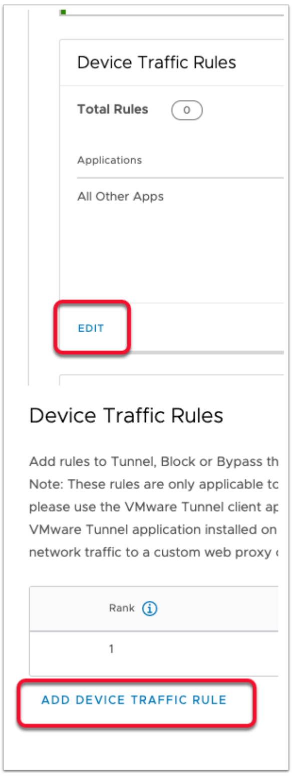
4.2 Configuring Single-Sign-on for Android.... continued

- **Configuring VMware Tunnel Component...**
  1. Under **System** select **Enterprise Integration**
  2. Select **VMware Tunnel.**



4.3 Configuring Single-Sign-on for Android.... continued

- In the **Device Traffic Rules section** section select **EDIT**
  - To the left of the **Device Traffic Rules** window select **ADD DEVICE TRAFFIC RULE**

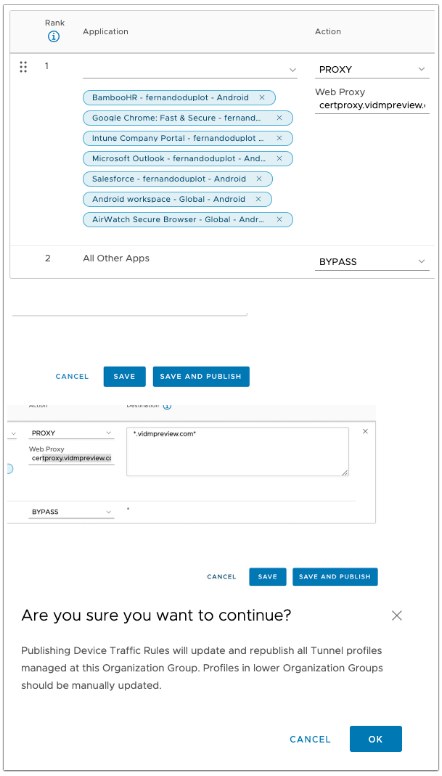


Add rules to Tunnel, Block or Bypass th
Note: These rules are only applicable tc
please use the VMware Tunnel client ap
VMware Tunnel application installed on
network traffic to a custom web proxy

4.4 Configuring Single-Sign-on for Android.... continued

- **Configuring VMware Tunnel Component...**

1.
    1. Next to **Rank # 1**, under **Application** in the **drop down** select BambooHR, Chrome: Fast & Secure, Intune Company Portal, **Microsoft Outlook**, Salesforce, Android Workspace and Airwatch Secure Browser.
        - Under **Action** from the **dropdown** select PROXY
        - Under **Web Proxy** type **certproxy.vidmpreview.com:5262**
        - Under **Destination** type ***.vidmpreview.com**
    2. Next to **Rank # 2,** under **Application** leave (**all other Apps**) under action select **BYPASS**
    3. Select **SAVE AND PUBLISH**
    4. On the **Are you sure you want to continue?** window select **OK**



Rank	Application	Action
1	BambooHR - fernandoduplot - Android × Google Chrome: Fast & Secure - fernand... × Intune Company Portal - fernandoduplot ... × Microsoft Outlook - fernandoduplot - And... × Salesforce - fernandoduplot - Android × Android workspace - Global - Android × AirWatch Secure Browser - Global - Andr... ×	PROXY Web Proxy certproxy.vidmpreview.(
2	All Other Apps	BYPASS

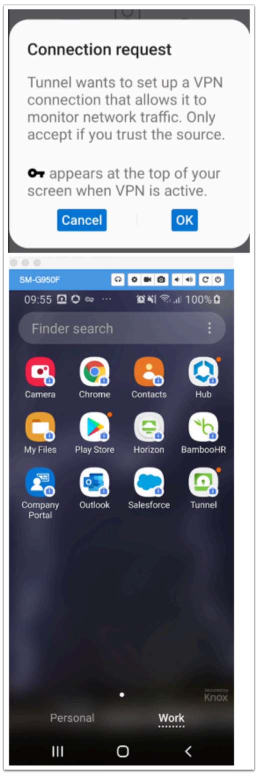
Action	Destination
PROXY Web Proxy certproxy.vidmpreview.cc	*.vidmpreview.com*
BYPASS	*

Are you sure you want to continue?

Publishing Device Traffic Rules will update and republish all Tunnel profiles managed at this Organization Group. Profiles in lower Organization Groups should be manually updated.

4.4

- On your Mobile Device, wait until all your apps have been deployed.That being **Microsoft Outlook; BambooHR; Salesforce, Intune Company Portal, Android Workspace, Airwatch Secure Browser** and **Chrome** and **VMware Tunnel**
- Look to be prompted for the following message : **Connection request**. **Tunnel wants to set up a VPN connection....** You have the option to select **Cancel** and **OK**. Select **OK**



Connection request

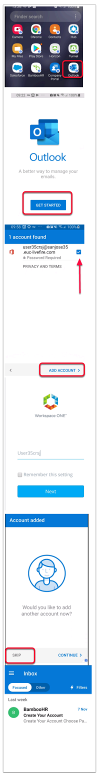
Tunnel wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

appears at the top of your screen when VPN is active.

Part 5: Testing Mobile SSO for Android

5.1 We will test Mobile SSO using the Microsoft OUTLOOK Application

- Ensure your Android Mobile device is enrolled into your custom environment
  1. On your Android device you should see a **Microsoft Outlook** application natively installed with a **Lock** as part of it. **Open** the **Microsoft Outlook** Application
  2. On the **Outlook** page select **GET STARTED**
  3. In the **Add account window** type your **email address,** eg. *user35crsj@sanjose35.euc-livefire.com* select **CONTINUE**
  4. On the User **Account found** select **the checkbox**
  5. To the bottom of the page select **ADD ACCOUNT**
  6. Enter your **username** in the **Workspace ONE Access** console, select **Next**
  7. If you are prompted for password , its an indication you **Mobile SSO for Android** has failed. Cancel the authentication. Do NOT Sign IN. (Possibly reach out to your instructor)
  8. On the **Account added** window select **SKIP**
  9. Notice you are now at your Outlook Inbox
  10. **Close** and **re-open** your Outlook client and you will see a seamless Mobile SSO experience.



A better way to manage your emails.

1 account found

user35crsj@sanjose35.euc-livefire.com

Password Required

User35crs

☐ Remember this setting

Account added

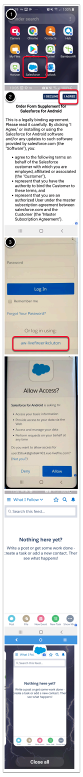
Would you like to add another account now?

Last week

BambooHR 7 Nov
Create Your Account
Create Your Account Choose Pa...

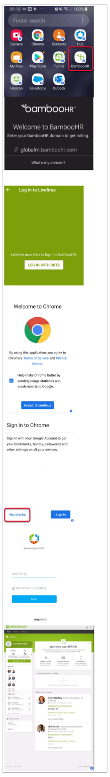
5.2. Testing Mobile SSO for Salesforce

- On your Android device, choose your **Work** profile
  1. Select the **Salesforce icon**
  2. On the terms and conditions select **I AGREE**
  3. On your login notice you have the option at the bottom **OR Log in using: *your custom domain.*** Select ***your custom domain***
  4. In the **Salesforce for Android** window select **Allow**
  5. Notice you are now in your Salesforce application for the first time. Close the application an re-open.



5.3 Testing Mobile SSO for BambooHR

- On your **Android** Device select your **BambooHR** application
  1. In the **bambooHR** window type in your ***custom domain*** in the **yourdomain**.boomboohr.com section
     - **eg. sanjose35.bamboohr.com**
     - select **Continue**
  2. Select the **LOG IN WITH OKTA** button
  3. On the **Welcome to Chrome** window select Accept & Continue
  4. On the **Sign in to Chrome** select **No thanks**
  5. On the **Workspace ONE** console enter your **username** and select **Next**
     1. Notice your Okta Routing rules redirect to Workspace ONE VIDM and authenticate and the you are granted access to BambooHR



Welcome to BambooHR

Enter your BambooHR domain to get rolling.

Livefiree uses Okta to log in to BambooHR.

Welcome to Chrome

By using this application, you agree to Chrome's Terms of Service and Privacy Notice.

☑ Help make Chrome better by sending usage statistics and crash reports to Google.

Sign in to Chrome

Sign in with your Google Account to get your bookmarks, history, passwords and other settings on all your devices.

Part 6. consolidating what we've larned

6.1

- Repeat part 3 and 4 for **Microsoft Word** , **Powerpoint** , **ONE drive** and **Excel**
  - We will do **Microsoft Word** as an example,

1. In the **APPS & BOOKS** > **Applications** > **Native** > **Public** tab continued..
2. Select **+ADD APPLICATION**
3. In the **Add Application** window next to: Select
4. **Platform*** : **Android**
5. **Name*:** Microsoft Word
6. select **NEXT**
7. In the **Add Application** window select **Microsoft Word**
8. In the **Microsoft Word** section, click the **SELECT** button
9. Select **SAVE & ASSIGN**
10. On the **Microsoft Word** - Update Assignment window select **+ADD ASSIGNMENT**
11. In the **Microsoft Word** - Add Assignment window next to
    - **Select Assignment Groups: All Devices**
    - **App Delivery Method: AUTO**
    - **App Tunneling:** ENABLED
      - **Android*** : **Android_Mobile_SSO**
12. At the bottom of the page select **ADD**
13. Select **SAVE & PUBLISH**

14. Select **PUBLISH**
    - *repeat this process for the rest of the applications*

6.2 . Configuring Network Traffic Rules

- In the **Workspace ONE UEM** console, select **GROUPS & SETTINGS** > **ALL Settings** > **Enterprise Integration** > **VMware Tunnel**
- In the **Device Traffic Rules** add **Microsoft Word, Excel, PowerPoint** and **OneDrive** to the existing **Webproxy** configuration

Windows 10 Certificate Single Sign On using an AirWatch Certificate Authority

In this lab you will be deploying a certificate to an enrolled Windows 10 virtual machine. This certificate will be generated by the built-in CA in Workspace ONE UEM.

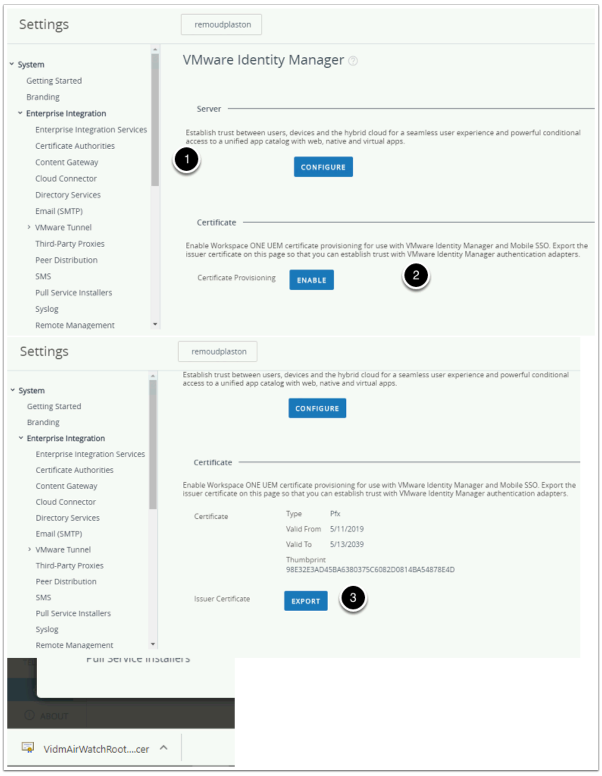
We will later configure Workspace ONE Access to trust certificates issues by UEM and configure the Certificate (Cloud Deployment) authentication adapter.

Finally we will test everything on a Windows 10 Machine to ensure we are able to have a seamless authentication experience.

Part 1: WorkspaceOne UEM - Certificate Profile

1

- Open Chrome on your **ControlCenter2** jumpbox and navigate to **https://cn-livefire.awmdm.com** Authenticate using your **e-mail address** and unique **password**
    1. Navigate to **Groups & Settings** > **All Settings** > **Enterprise Integration** > **VMware Identity Manager**> **Configuration**
    2. Under Certificate select **ENABLE** (this should be enabled from a previous lab)
    3. Under **Certificate** next to **Issuer Certificate** select **EXPORT**



VMware Identity Manager

Server

Establish trust between users, devices and the hybrid cloud for a seamless user experience and powerful conditional access to a unified app catalog with web, native and virtual apps.

Certificate

Enable Workspace ONE UEM certificate provisioning for use with VMware Identity Manager and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with VMware Identity Manager authentication adapters.

Certificate Provisioning

Certificate

Type: Pfx

Valid From: 5/11/2019

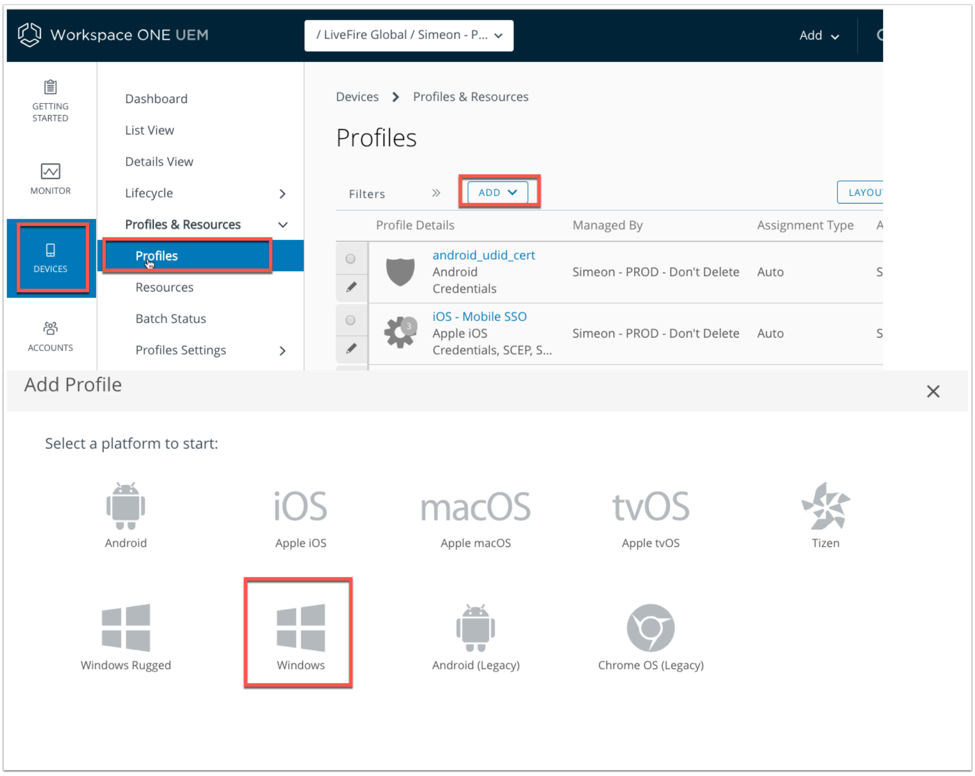
Valid To: 5/13/2039

Thumbprint: 98E32E3AD45BA6380375C6082D0814BA54878E4D

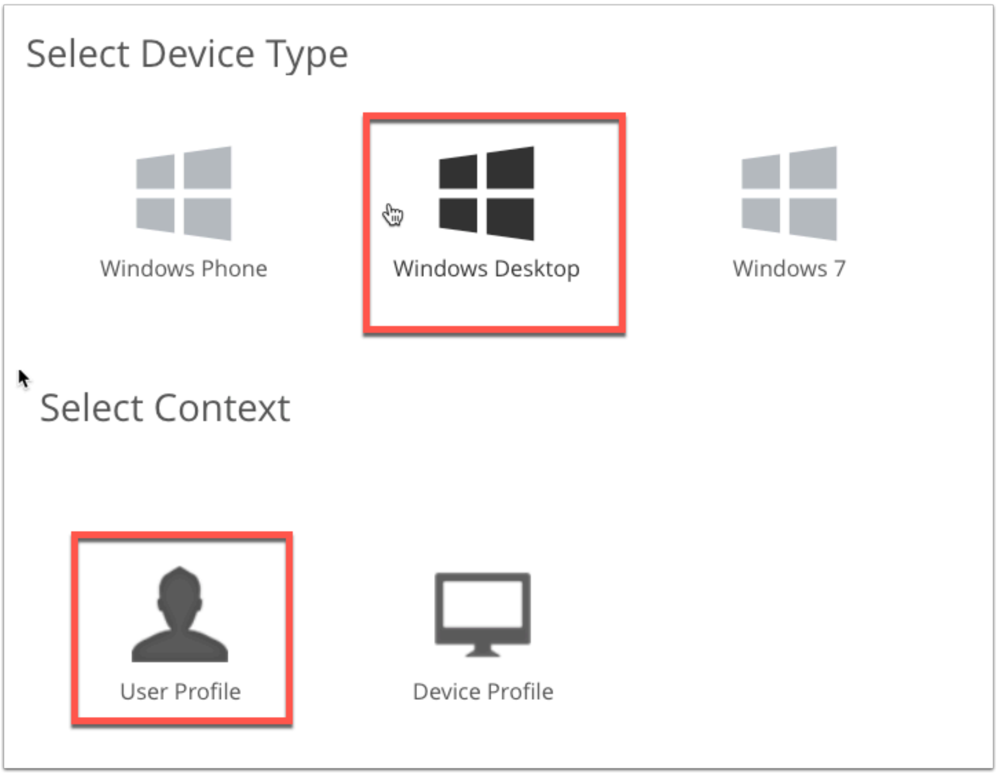
Issuer Certificate

2. WorkspaceOne UEM - Certificate Profile continued...

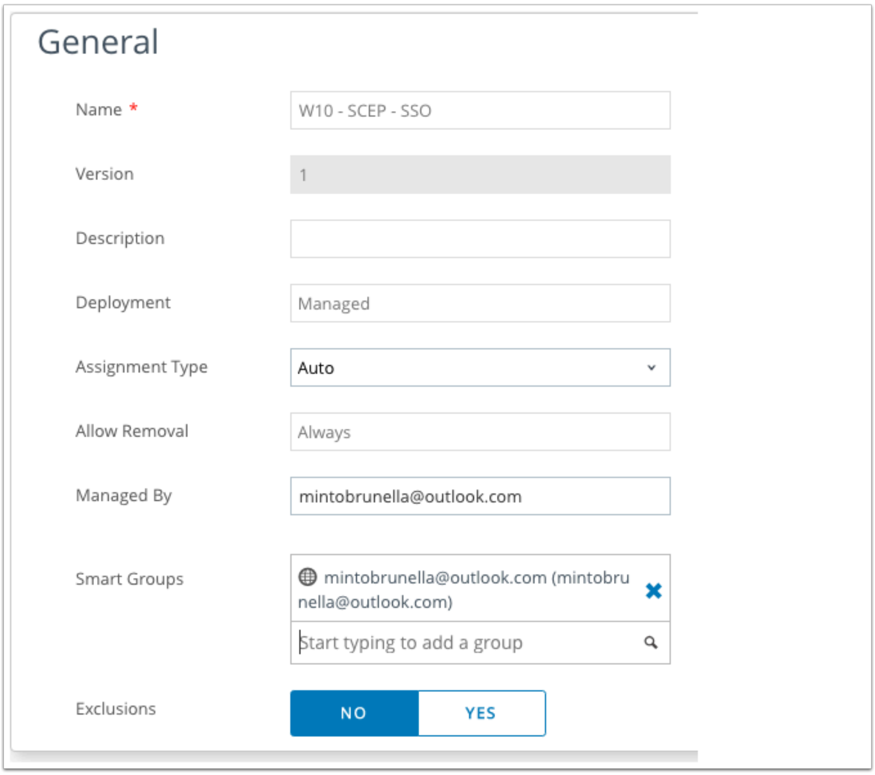
1. Then navigate to **Devices** > Profiles & Resources > Profiles > ADD > Add Profile > Windows > Windows Desktop > User Profile Give it a name : **W10 - SCEP - SSO** .
2. Select your **Smart Group** with the **World icon** for the Smart Group
3. Select the **SCEP** payload on the left hand navigation panel.
4. Select **CONFIGURE**
5. Set the following
   - Credential Source: **AirWatch Certificate Authority**
   - Certificate Template: **Certificate (Cloud Deployment)**
   - Issuer: **LiveFire**
   - Click **SAVE AND PUBLISH**
6. In the **Device Assignment** notice your device in the list of device being added. Then click **PUBLISH**



Workspace ONE UEM
/ LiveFire Global / Simeon - P...
Add
GETTING STARTED
MONITOR
DEVICES
ACCOUNTS
Dashboard
List View
Details View
Lifecycle
Profiles & Resources
Profiles
Resources
Batch Status
Profiles Settings
Devices > Profiles & Resources
Profiles
Filters
ADD
LAYOUT
Profile Details
Managed By
Assignment Type
android_udid_cert
Android
Credentials
Simeon - PROD - Don't Delete
Auto
iOS - Mobile SSO
Apple iOS
Credentials, SCEP, S...
Simeon - PROD - Don't Delete
Auto
Add Profile
Select a platform to start:
Android
iOS
Apple iOS
macOS
Apple macOS
tvOS
Apple tvOS
Tizen
Windows Rugged
Windows
Android (Legacy)
Chrome OS (Legacy)

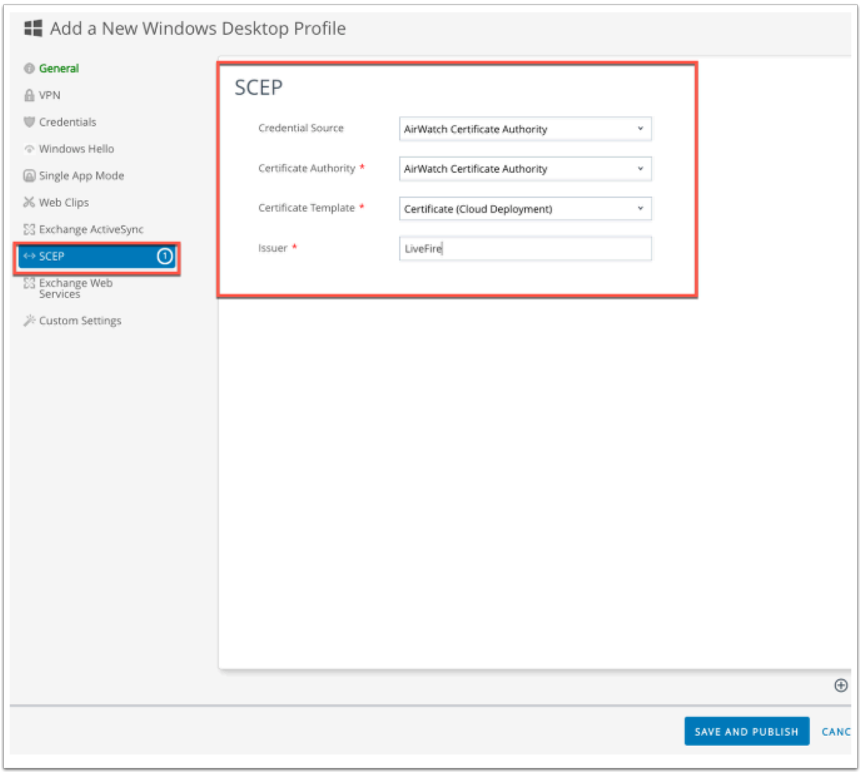


Select Device Type
Windows Phone
Windows Desktop
Windows 7
Select Context
User Profile
Device Profile



General

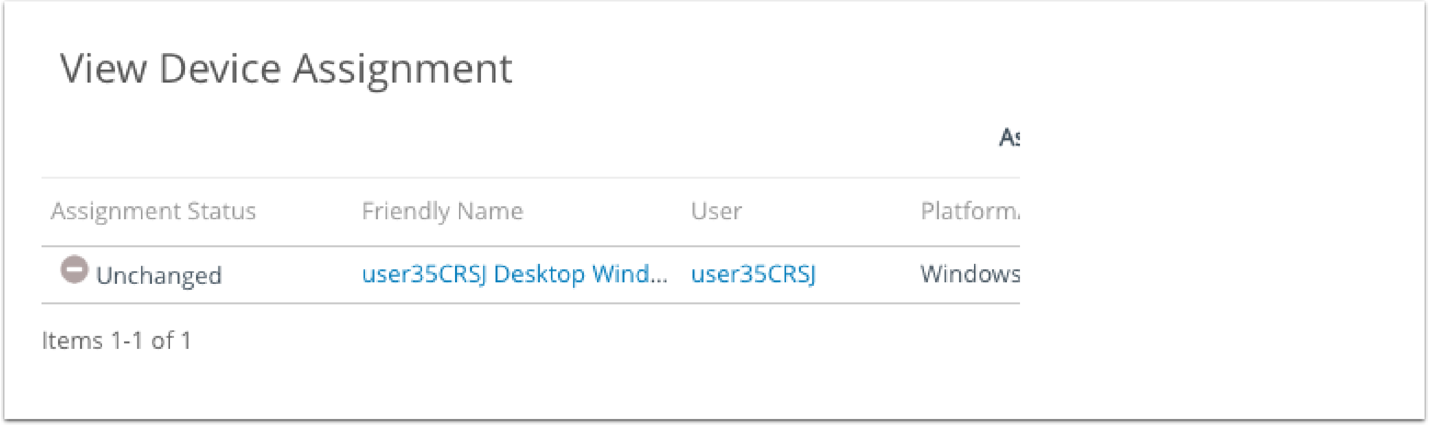
Name *	W10 - SCEP - SSO
Version	1
Description	
Deployment	Managed
Assignment Type	Auto
Allow Removal	Always
Managed By	mintobrunella@outlook.com
Smart Groups	mintobrunella@outlook.com (mintobrunella@outlook.com) Start typing to add a group
Exclusions	NO YES



Add a New Windows Desktop Profile

SCEP

Credential Source	AirWatch Certificate Authority
Certificate Authority *	AirWatch Certificate Authority
Certificate Template *	Certificate (Cloud Deployment)
Issuer *	LiveFire



View Device Assignment

As

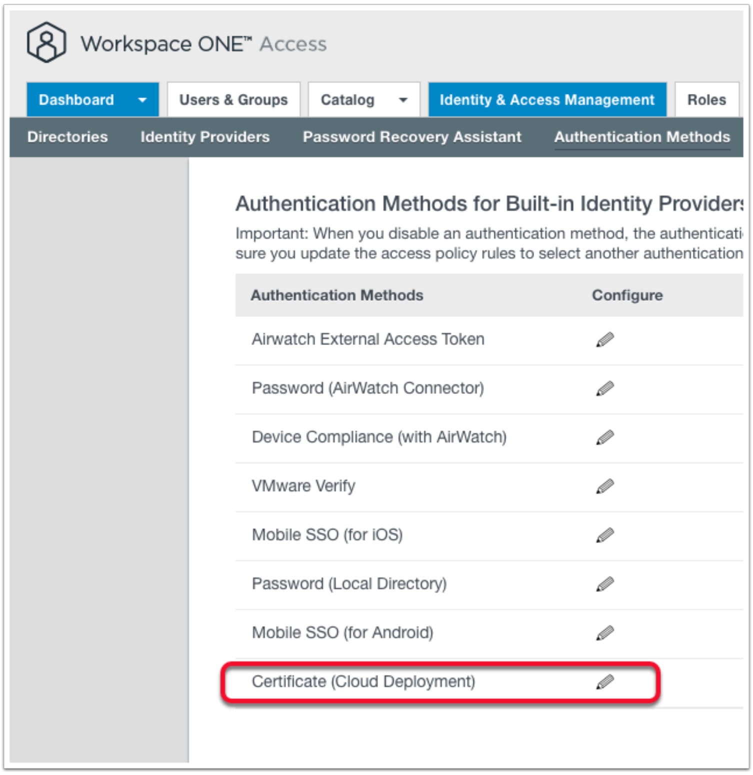
Assignment Status	Friendly Name	User	Platform
Unchanged	user35CRSJ Desktop Wind...	user35CRSJ	Windows

Items 1-1 of 1

Part 2: Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication

1. **Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication**

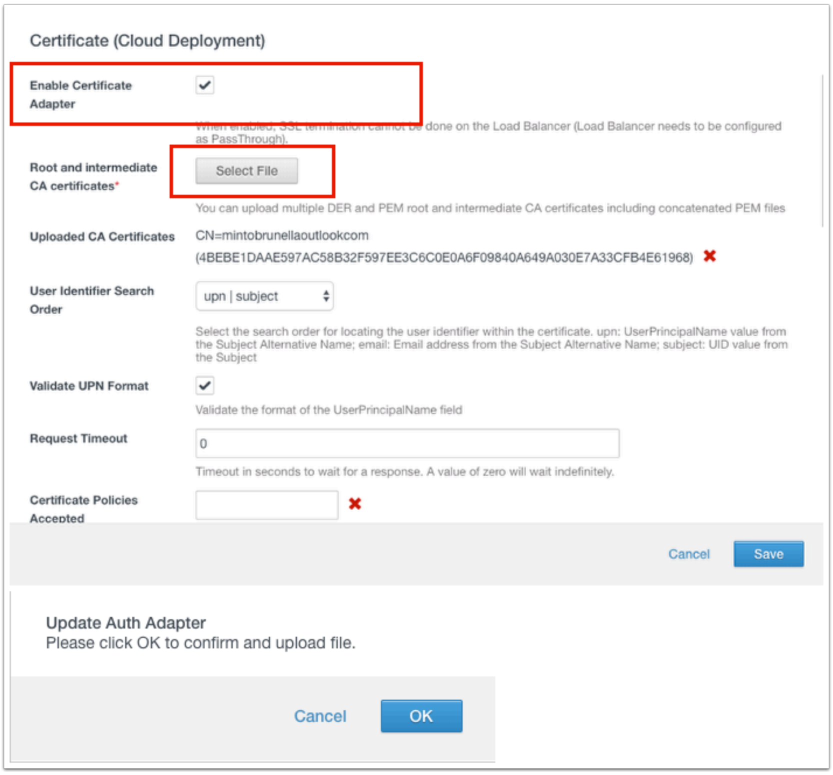
- In this next section, we will configure Workspace ONE Access Certificate Auth Adaptor to trust the certificates being presented by the devices.
  1. On your **ControlCenter** server, use your **unique Workspace ONE Access** server and authenticate to the local directory using administrator account and password.
  2. Under Identity & Access Management > Manage select **Authentication Methods**
  3. Click on the **Pencil** to Configure the **Certificate (Cloud Deployment)** authentication method.
  4. Select the **checkbox** **Enable Certificate Adapter** and click **Select File** to **upload the Certificate** (**VidmAirWatchRootCertificate.cer**) you downloaded above in the UEM console.
  5. On the **Update Auth Adapter** window select **OK**
  6. Leave everything else in here as default and click **Save.**
  7. Now navigate **Identity Providers** under **Identity & Access Management** click on **Built-in**
  8. Navigate to the **Authentication Methods** area and select the **check box** next to **Certificate (Cloud Deployment)** and select **Save** at the bottom of the page.



Authentication Methods for Built-in Identity Provider

Important: When you disable an authentication method, the authenticati
sure you update the access policy rules to select another authentication

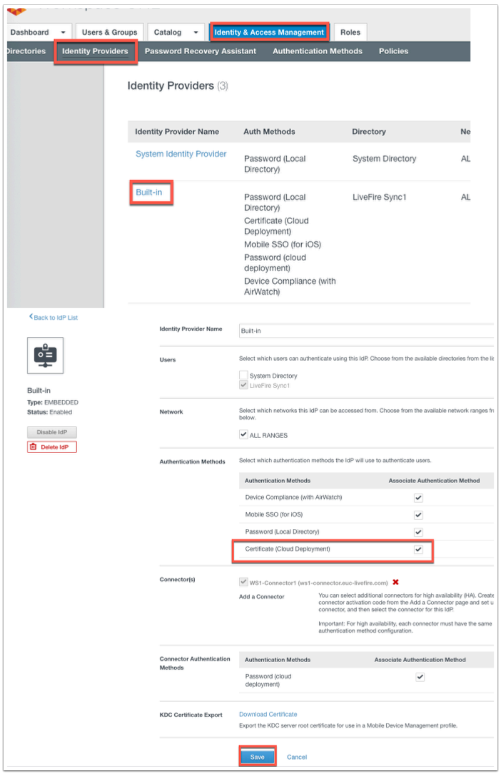
Authentication Methods	Configure
Airwatch External Access Token	✎
Password (AirWatch Connector)	✎
Device Compliance (with AirWatch)	✎
VMware Verify	✎
Mobile SSO (for iOS)	✎
Password (Local Directory)	✎
Mobile SSO (for Android)	✎
Certificate (Cloud Deployment)	✎



Certificate (Cloud Deployment)

Enable Certificate Adapter	☑ When enabled, SSL termination cannot be done on the Load Balancer (Load Balancer needs to be configured as PassThrough).
Root and intermediate CA certificates*	Select File You can upload multiple DER and PEM root and intermediate CA certificates including concatenated PEM files
Uploaded CA Certificates	CN=mintobrunellaoutlookcom (4BEBE1DAAE597AC58B32F597EE3C6C0E0A6F09840A649A030E7A33CFB4E61968) ✖
User Identifier Search Order	upn | subject Select the search order for locating the user identifier within the certificate. upn: UserPrincipalName value from the Subject Alternative Name; email: Email address from the Subject Alternative Name; subject: UID value from the Subject
Validate UPN Format	☑ Validate the format of the UserPrincipalName field
Request Timeout	0 Timeout in seconds to wait for a response. A value of zero will wait indefinitely.
Certificate Policies Accepted	✖

Update Auth Adapter
Please click OK to confirm and upload file.



Identity Providers (3)

Identity Provider Name	Auth Methods	Directory	Ne
System Identity Provider	Password (Local Directory)	System Directory	AL
Built-in	Password (Local Directory) Certificate (Cloud Deployment) Mobile SSO (for iOS) Password (cloud deployment) Device Compliance (with AirWatch)	LiveFire Sync1	AL

Built-in
Type: EMBEDDED
Status: Enabled

Identity Provider Name Built-in

Users Select which users can authenticate using this IdP. Choose from the available directories from the lis

□ System Directory
☑ LiveFire Sync1

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

☑ ALL RANGES

Authentication Methods Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Device Compliance (with AirWatch)	☑
Mobile SSO (for iOS)	☑
Password (Local Directory)	☑
Certificate (Cloud Deployment)	☑

Connector(s) ☑ WS1-Connector1 (ws1-connector.euc-livefire.com)

Add a Connector You can select additional connectors for high availability (HA). Create connector activation code from the Add a Connector page and set u connector, and then select the connector for this IdP.

Important: For high availability, each connector must have the same authentication method configuration.

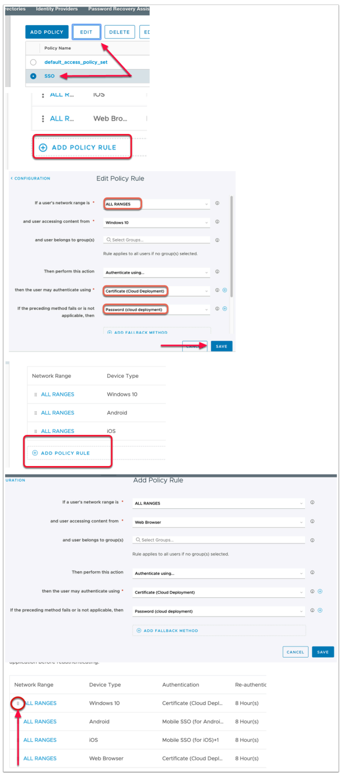
Connector Authentication Methods

Authentication Methods	Associate Authentication Method
Password (cloud deployment)	☑

KDC Certificate Export Download Certificate
Export the KDC server root certificate for use in a Mobile Device Management profile.

2.

- **Configuring Workspace ONE Access Certificate (Cloud Deployment) Authentication....continued**
  1. Navigate to **Policies** under **Identity & Access Management** then click on the **SSO** policy.
  2. Select **Edit**
  3. Next to **Configuration** select **+ADD POLICY RULE.**
  4. In the **Add Policy Rule** window add the following, next to : -
     - '**and user accessing content from**' to Select Windows 10 from the drop down
     - **then the user may authenticate using*** change to **Certificate (Cloud Deployment)**
     - "**if the preceding method fails or is not applicable, then"** change **Select failback method...** to **Password (Cloud Deployment)**
  5. Select **SAVE**
  6. Select **+ADD POLICY RULE.**
  7. In the **Add Policy Rule** window add the following, next to : -
     - '**and user accessing content from**' select Web Browser from the drop down
     - **then the user may authenticate using*** change to **Certificate (Cloud Deployment)**
     - "**if the preceding method fails or is not applicable, then"** change **Select failback method...** to **Password (Cloud Deployment)**
  8. Select **SAVE,**
  9. Next to **ALL RANGES for Windows 10** on the left select the **6 DOTS** and drag to the top
  10. Select **NEXT,** select **SAVE.**



Policy Name
default_access_policy_set
SSO

ALL R...	iOS
ALL R...	Web Bro...

Edit Policy Rule

If a user's network range is *: ALL RANGES

and user accessing content from *: Windows 10

and user belongs to group(s): Select Groups...

Rule applies to all users if no group(s) selected.

Then perform this action: Authenticate using...

then the user may authenticate using *: Certificate (Cloud Deployment)

If the preceding method fails or is not applicable, then: Password (cloud deployment)

Network Range	Device Type
ALL RANGES	Windows 10
ALL RANGES	Android
ALL RANGES	iOS

Add Policy Rule

If a user's network range is *: ALL RANGES

and user accessing content from *: Web Browser

and user belongs to group(s): Select Groups...

Rule applies to all users if no group(s) selected.

Then perform this action: Authenticate using...

then the user may authenticate using *: Certificate (Cloud Deployment)

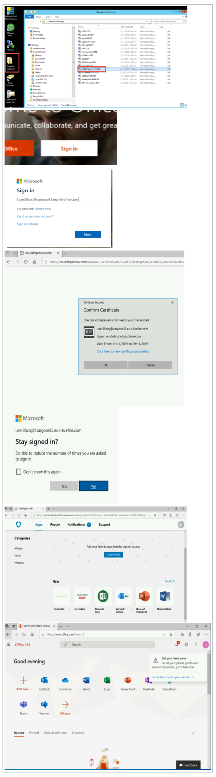
If the preceding method fails or is not applicable, then: Password (cloud deployment)

Network Range	Device Type	Authentication	Re-authentic
ALL RANGES	Windows 10	Certificate (Cloud Depl...	8 Hour(s)
ALL RANGES	Android	Mobile SSO (for Androi...	8 Hour(s)
ALL RANGES	iOS	Mobile SSO (for iOS)+1	8 Hour(s)
ALL RANGES	Web Browser	Certificate (Cloud Depl...	8 Hour(s)

Part 3: Windows 10 Single Sign On using Certificates

- Now that the administrative elements are in place we will now test the authentication flow from our Windows 10 VM.
  1. On the **ControlCenter2** VM on the desktop you will find the **Remote Desktop** folder. In this folder click double click on **w10client01.RDP**
  2. Inside the Windows 10 Virtual Machine **open** **Microsoft Edge** from the desktop and type **OFFICE.COM** in the address bar
  3. In the **Office.com** page select **Sign In**
  4. In the **Sign in** window, type your **email address**. eg user35crsj@sanjose35.euc-livefire.com.
  5. Select **Next**
  6. Notice now that you are being re-directed to **cas.vidmpreview.com** in the URL field and you are prompted for a **Certificate.**
  7. Click **OK** on the pop-up for your certificate and notice your are straight into your WorkspaceOne bookmarks Tab.
  8. Now click on any one of your **Office365 deeplinks** and notice your are authenticated without further credentials. If you get prompted to "Stay Signed in?" simply click **No.**
  9. You are now authenticated to your O365 environment using a certificate based authentication method.

This completes this lab.



User35crsj@sanjose35.euc-livefire.com

https://cas.vidmpreview.com/cas/t/AW-LIVEFIREMB/API/1.0/REST/landing?EAB_CALLBACK_URL=%2Fauth%2

Confirm Certificate

Site cas.vidmpreview.com needs your credentials:

user35crsj@sanjose35.euc-livefire.com

Issuer: mintobrunellaoutlookcom

Valid From: 11/11/2019 to 09/11/2029

user35crsj@sanjose35.euc-livefire.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

Windows 10 Compliance Workspace One UEM + Workspace ONE Access

Part 1: Workspace One UEM Compliance Rules

WorkspaceOne allows administrators to check the device posture in addition to the credentials provided for authentication. This ensure's that not only the provided credentials are valid, but also the device being used to access corporate resources is deemed secure and compliant. WorkspaceOne UEM has a robust compliance engine that allows administrator to set a standard for security on devices.

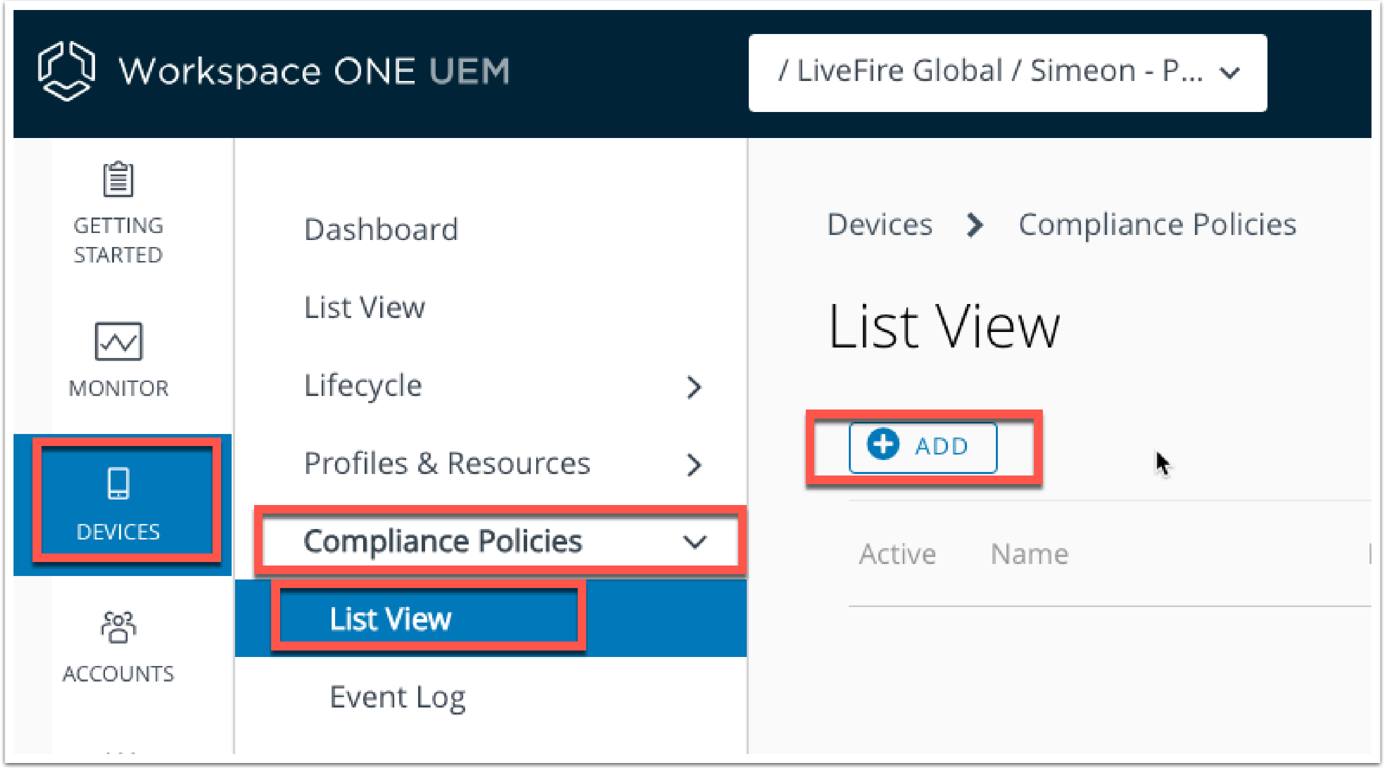
First you will be configuring a standard for compliance on Windows 10 using WorkspaceOne UEM

Second, you will be configuring Workspace ONE Access Access Policies to check the device compliance during the authentication process.

Third, you will bring this to life by authenticating to O365 using Workspace ONE Access certificate adapter in conjunction with device compliance.

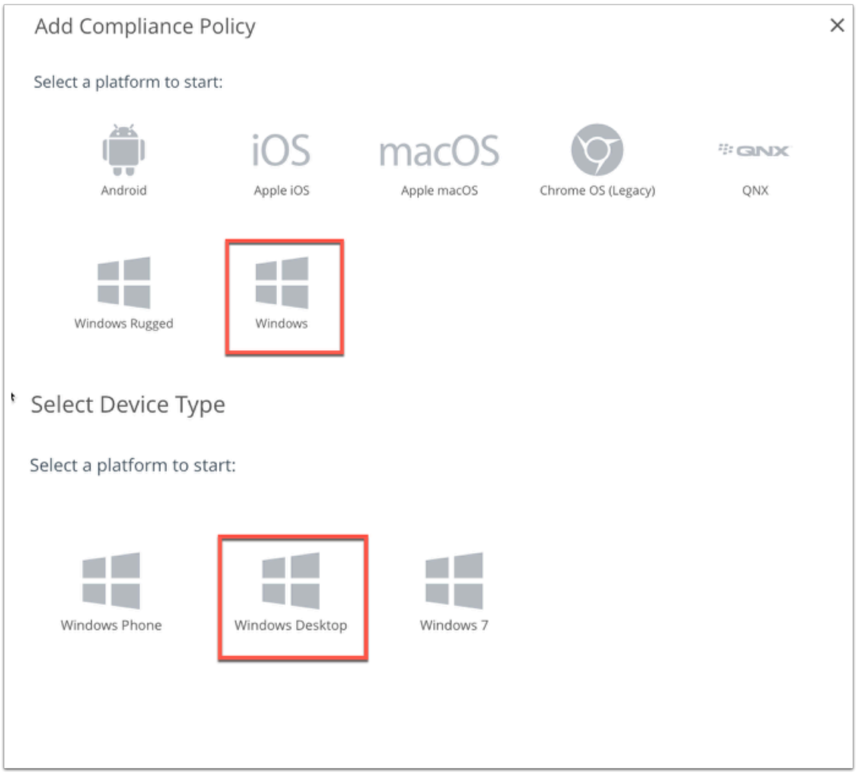
1. Let's begin with configuring our UEM compliance rules for Windows 10.
(**Note**: that the same procedure can be used for Android and iOS, but in our scenario we will be dealing with Windows 10)

- Open the Workspace One UEM console on **cn-livefire.awmdm.com** and authenticate using your unique credentials. Navigate to **Devices** > **Compliance Policies** > **List View** and click **+ ADD**



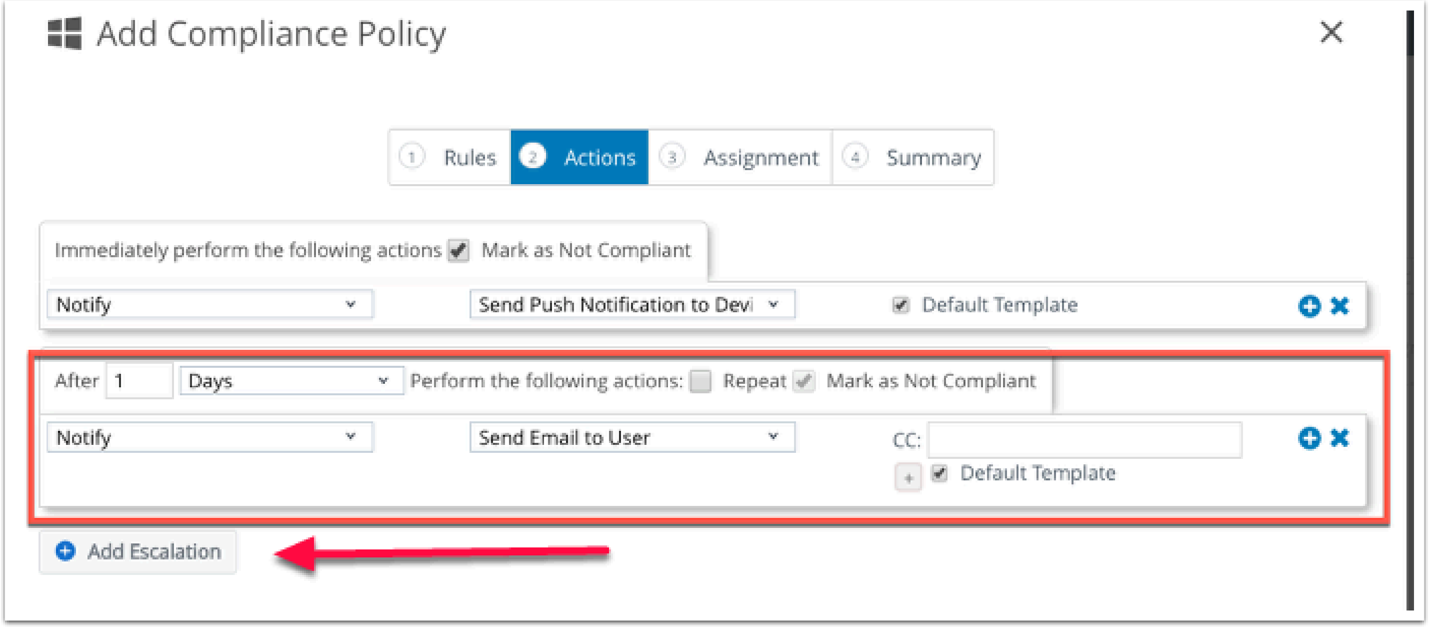
2. Select **Windows** from the **"Select a platform to start:"** window and select **Windows Desktop** from the next page as this one relates to Windows10 specifically.

- Select **NEXT** at the bottom of the page. We have now set our rule we will now select an action.



3. In the **Actions** tab validate the check box next to **"Mark as Not Compliant"** is selected.

- This will ensure that if our device does not follow the rules set in the previous page it will be flagged as not compliant. Now notice the drop down for the actions you can take. You could go as harsh as performing an enterprise wipe, or as subtle as notifying the user via a push notification.
- In the left dropdown leave **Notify** as the default and change **Send Email to User** to **"Send Push Notification to Device"** from the the action dropdown.
- Select + **Add Escalation** and leave as default. Notice you the user will be e-mailed after 1 day of the rule still being broken. Click **NEXT** at the bottom of the page



Add Compliance Policy

① Rules ② Actions ③ Assignment ④ Summary

Immediately perform the following actions ☑ Mark as Not Compliant

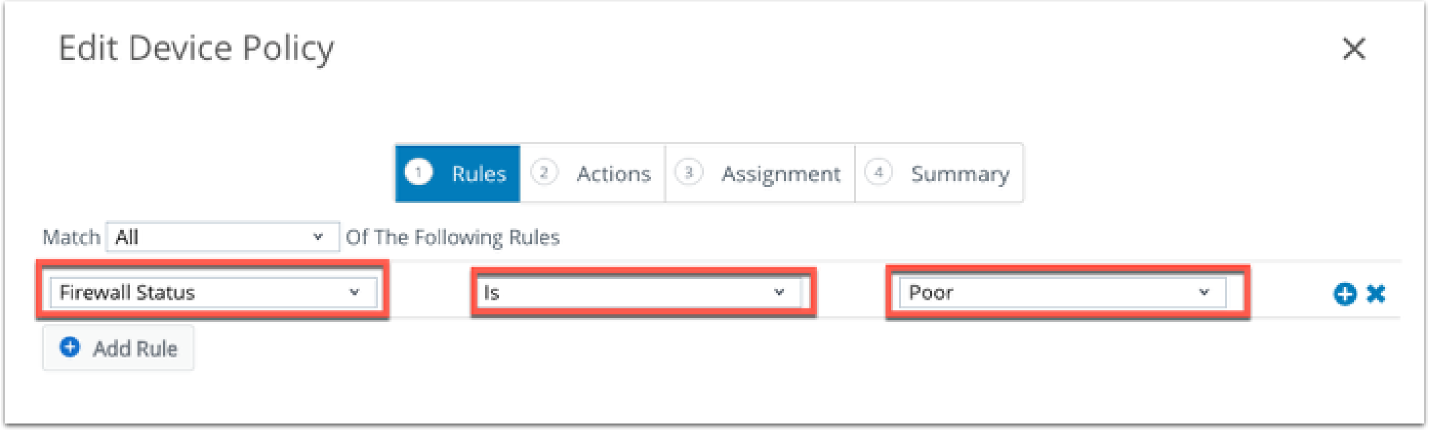
Notify | Send Push Notification to Devi | ☑ Default Template

After 1 Days Perform the following actions: □ Repeat ☑ Mark as Not Compliant

Notify | Send Email to User | CC: | ☑ Default Template

4. In the **Add Compliance Policy** page notice all the rules your can set in the left hand drop down. These are all the parameters an admin can set to determine whether a device is compliant with the organizations security rules. For this particular lab we will be dealing with the **Firewall Status**. Configure the following:-

- On the left under **Match** select the **dropdown** and change **MDM Terms of Use Acceptance** to **Firewall Status**
- In the 2nd drop down, this should automatically change to **Is**
- in the 3rd dropdown change **Good** to **"Poor".**

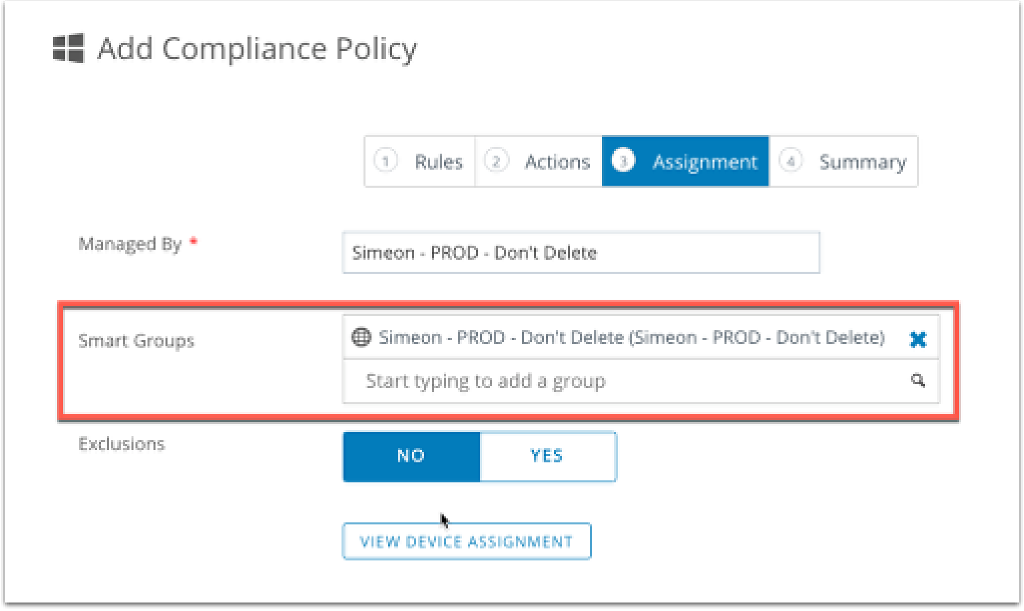

Edit Device Policy

Match All Of The Following Rules

Firewall Status | Is | Poor

5. Under the **Assignment** tab next **Smart Groups** select your unique **Organization Group** marked with the **world** symbol.

Click **NEXT**


Add Compliance Policy

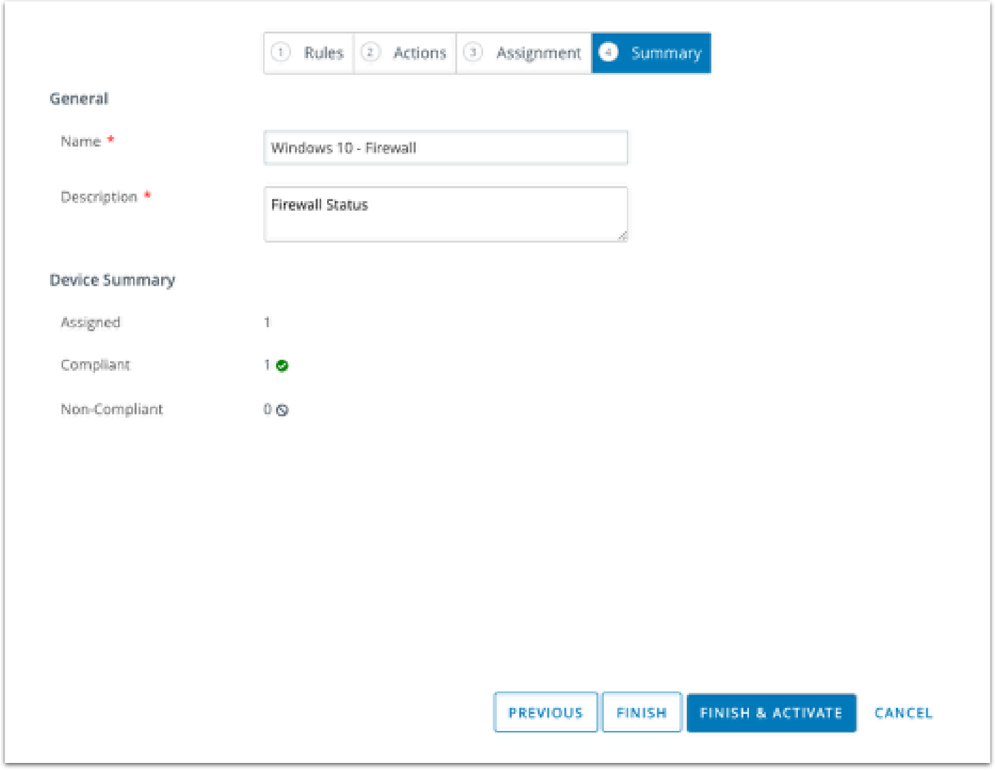
Managed By * Simeon - PROD - Don't Delete

Smart Groups Simeon - PROD - Don't Delete (Simeon - PROD - Don't Delete)

Start typing to add a group

Exclusions NO YES

6. Under the **Summary** Tab change the default Name **Firewall Status** to - **Windows 10 - Firewall** and click **FINISH & ACTIVATE** at the bottom of the page.



General

Name * Windows 10 - Firewall

Description * Firewall Status

Device Summary

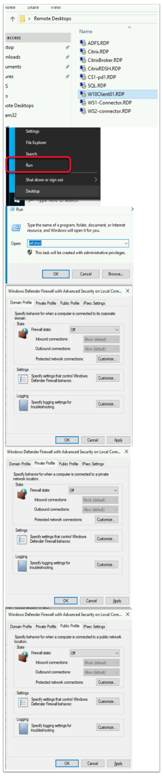
Assigned 1

Compliant 1 ✓

Non-Compliant 0

7. On your **Controlcenter** desktop, open the **Remote Desktop** folder.

- Select and RDP to the **W10Client01** with username **Administrator** and password **VMware1!**
  1. On the windows 10 desktop select **Start** > **Run**
  2. In the **Run** window type **WF.msc**
  3. In the **Windows Defender for Firewall for Advanced Security** select the **Domain**, **Private** and **Public Profile** and change the **Firewall state** from **ON (recommended)** to **OFF,** Select **OK** to close the **Windows Defender Firewall** window



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

This task will be created with administrative privileges.

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to a private network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

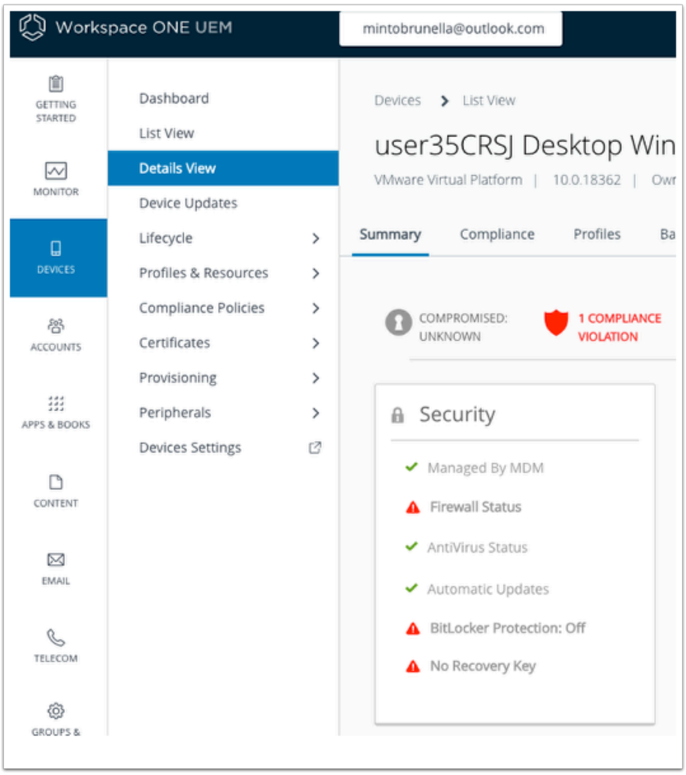
Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

8. Note! The Compliance Engine will now run (runs every 5 minutes by default) a check against the devices assigned to the Compliance Rule and report back to the Admin whether there are any device that have not passed the test. Since the Firewall is disabled on the Windows 10 Device we should get a flag stating it's non-compliant. This might take a while, so move on to the next section of the lab.

- Go back to your **Workspace ONE UEM** console, select **Devices** > **Details View**
- Notice now there is **1 COMPLIANCE VIOLATION** and the **Firewall Status** is red



COMPROMISED: UNKNOWN

1 COMPLIANCE VIOLATION

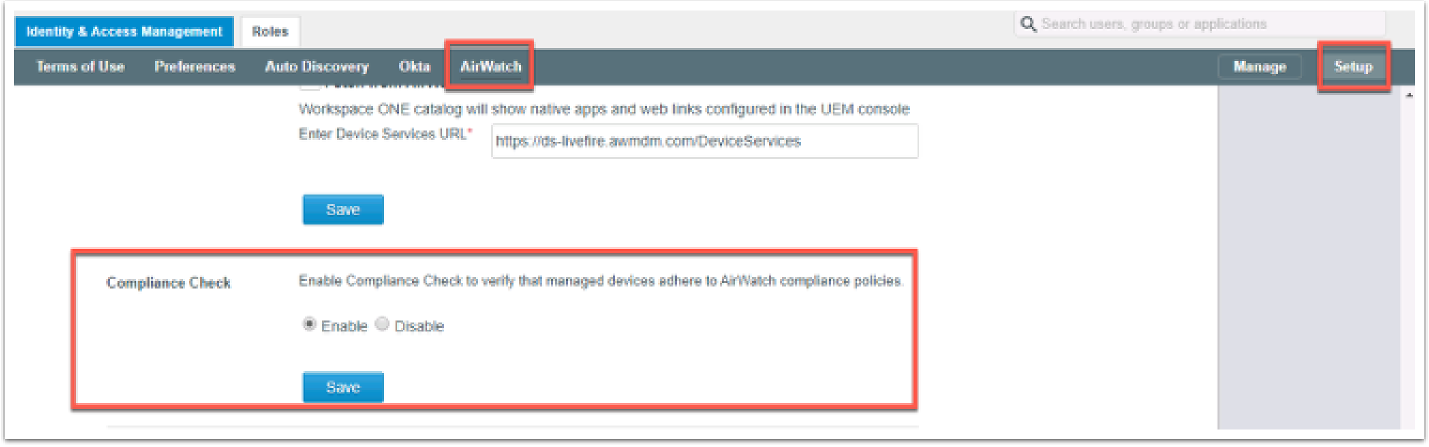
Security

- ✓ Managed By MDM
- ⚠ Firewall Status
- ✓ AntiVirus Status
- ✓ Automatic Updates
- ⚠ BitLocker Protection: Off
- ⚠ No Recovery Key

Part 2: Workspace ONE Access Access Policy Device Compliance

1.

- Let's enable Device Compliance from AirWatch then enable Authentication Method in the **Built-In** Identity Providers .
  1. Navigate to your unique **Workspace ONE Access** tenant and authenticate as **System Admin**
  2. Navigate to **Identity & Access Management** Tab > **Setup** > **AirWatch**
  3. Scroll down to Compliance Check, select the **Enable** **radio button** and select **Save**



Workspace ONE catalog will show native apps and web links configured in the UEM console

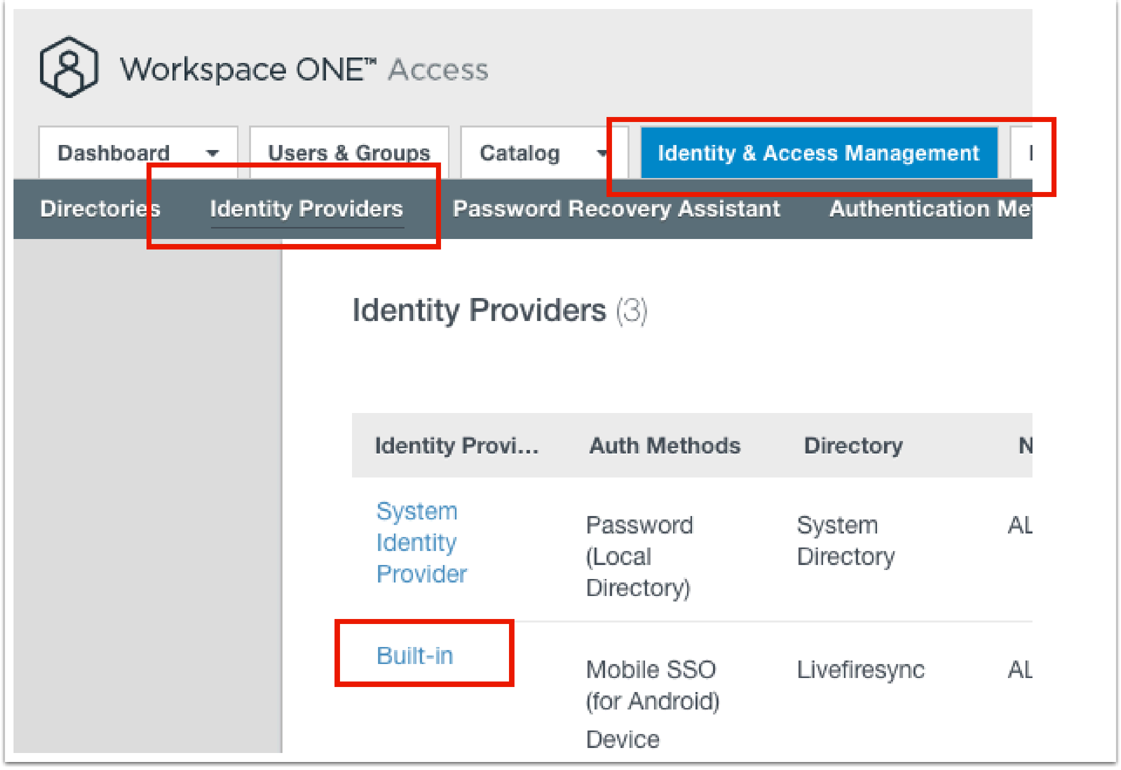
Enter Device Services URL* https://ds-livefire.awmdm.com/DeviceServices

Compliance Check

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

● Enable ○ Disable

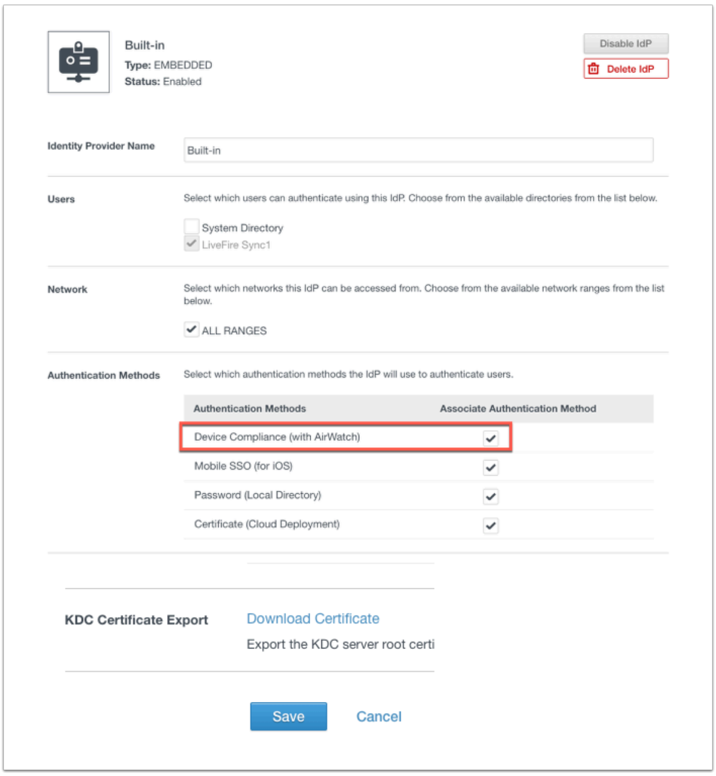
2. Open **Identity & Access Management** tab and select **Identity Providers**. On the page **Identity Providers** window select **Built-in**



Identity Providers (3)

Identity Provi...	Auth Methods	Directory	N
System Identity Provider	Password (Local Directory)	System Directory	AL
Built-in	Mobile SSO (for Android) Device	Livefiresync	AL

3. Scroll down to **Authentication Methods** and enable the **Device Compliance (with AirWatch)** checkbox and scroll down and select **Save** at the bottom of the page.



Built-in
Type: EMBEDDED
Status: Enabled

Identity Provider Name Built-in

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

□ System Directory
☑ LiveFire Sync1

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

☑ ALL RANGES

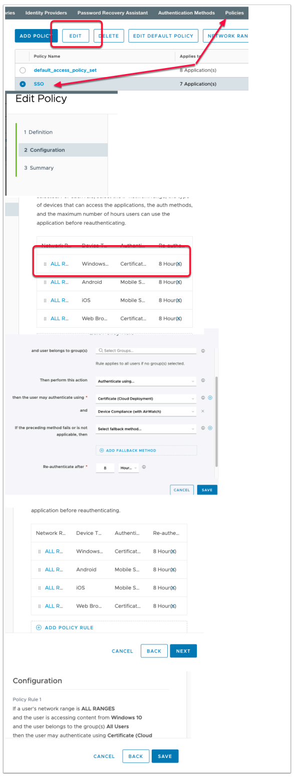
Authentication Methods Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Device Compliance (with AirWatch)	☑
Mobile SSO (for iOS)	☑
Password (Local Directory)	☑
Certificate (Cloud Deployment)	☑

KDC Certificate Export Download Certificate
Export the KDC server root certi

4.

- Now Navigate and select **Policies** in the **Identity & Access Management** tab
  1. Next to the **SSO** policy select the **radio button** and select **EDIT**
  2. In the **Edit Policy** window select **Configuration**
  3. Select **ALL RANGES** next to the policy that applies to **"Windows 10"**
  4. In this policy you will see that **Certificate (Cloud Deployment)** is the primary authentication method that is being used. We will now add device compliance, as an additional Access requirement, to allow user access. Select the **+** next to **Certificate (Cloud Deployment)**
  5. Next to **If the preceding method fails or is not applicable, then** CHANGE **Password (cloud deployment)** to **Select fallback method....**
  6. You will now have an **"and"** clause. In the dropdown select **Device Compliance (AirWatch)** .
  7. Select **SAVE** at the bottom of the page.
  8. Select **NEXT** on the following page and **SAVE** again on the **Summary** of the **Edit Policy** page.



Policy Name	Applies to
○ default_access_policy_set	8 Application(s)
● SSO	7 Application(s)

of devices that can access the applications, the auth methods, and the maximum number of hours users can use the application before reauthenticating.

Network R...	Device T...	Authenti...	Re-authe...
ALL R...	Windows...	Certificat...	8 Hour(s)
ALL R...	Android	Mobile S...	8 Hour(s)
ALL R...	iOS	Mobile S...	8 Hour(s)
ALL R...	Web Bro...	Certificat...	8 Hour(s)

and user belongs to group(s): Select Groups...

Rule applies to all users if no group(s) selected.

Then perform this action: Authenticate using...

then the user may authenticate using *: Certificate (Cloud Deployment)

and: Device Compliance (with AirWatch)

If the preceding method fails or is not applicable, then: Select fallback method...

Re-authenticate after *: 8 Hour...

application before reauthenticating.

Network R...	Device T...	Authenti...	Re-authe...
ALL R...	Windows...	Certificat...	8 Hour(s)
ALL R...	Android	Mobile S...	8 Hour(s)
ALL R...	iOS	Mobile S...	8 Hour(s)
ALL R...	Web Bro...	Certificat...	8 Hour(s)

Configuration

Policy Rule 1
If a user's network range is **ALL RANGES**
and the user is accessing content from **Windows 10**
and the user belongs to the group(s) **All Users**
then the user may authenticate using **Certificate (Cloud**

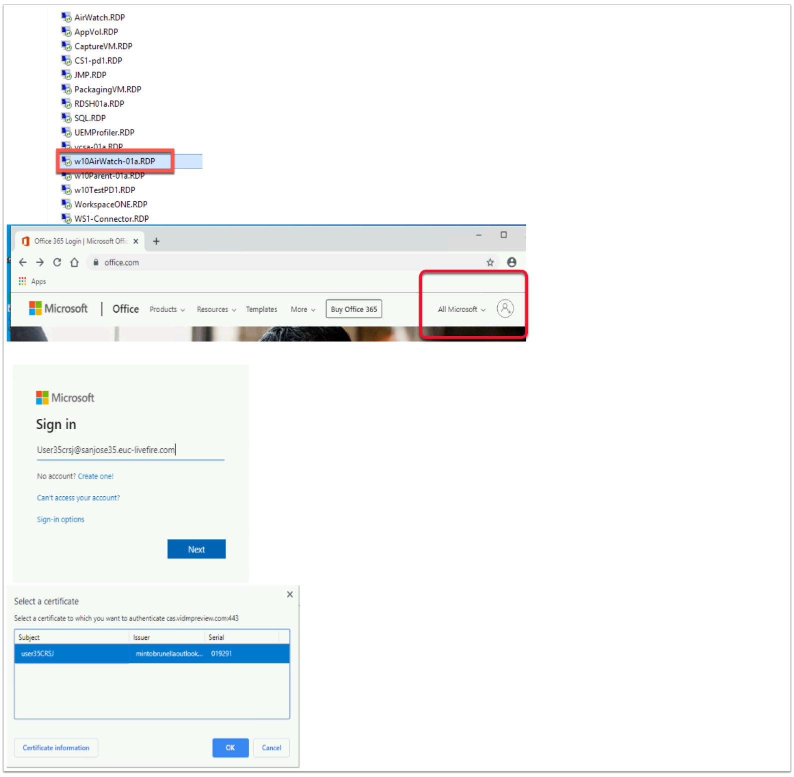
Part 3: Windows 10 Compliance in Action

1. Windows 10 Compliance in Action

- We will now test for Compliance as an authentication method.
  1. Navigate to the Desktop of the **ControlCenter2** and open the **Remote Desktop** folder and launch an RDP session using the **W10client01.RDP** client.
  2. Open **Chrome** within the **W10** machine that was enrolled. Now type in **Office.com** . Select the **sign-in to your account** **ICON** on the right-hand side of the page.

3. On the **Sign In** window type your **custom user** eg user35crsj@sanjose35.euc-livefire.com, select **Next**
    - You will get a **pop up** from Chrome that will request you to select the appropriate certificate to use for authentication.
4. On the **Select a certificate** window select **OK**

- At this point Workspace ONE Access will check the validity of the certificate, but also send an API compliance query to Workspace ONE UEM to ensure the device is compliant (This is using the **UDID** that is present to vIDM in the certificate)



User35crsj@sanjose35.euc-livefire.com

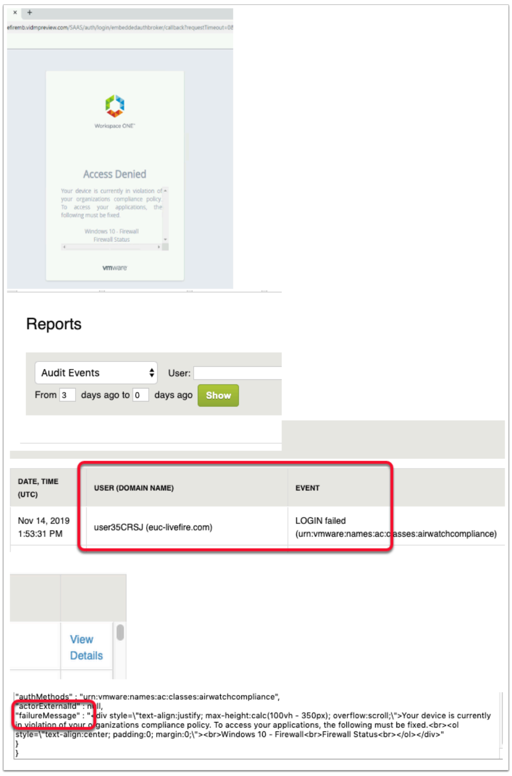
Select a certificate

Select a certificate to which you want to authenticate cas.vidmpreview.com:443

Subject	Issuer	Serial
user35CRSJ	mintobrunellaoutlook...	019291

2.

- You will notice an **Access Denied** message. We can also see this in the Event audits in Workspace ONE Access.
  1. In your Workspace ONE Access tenant. Navigate to **Dashboard** > Reports > Audit Events and select **Show**
  2. Look for an event that is **LOGIN failed** with your custom user,
  3. To the right select **View Details.** Scroll down until you find the area **"failuremessage"** and read what it says.



efiremb.vidmpreview.com/SAAS/auth/login/embeddedauthbroker/callback?requestTimeout=08

Workspace ONE

Access Denied

Your device is currently in violation of your organizations compliance policy. To access your applications, the following must be fixed.

Windows 10 - Firewall
Firewall Status

Reports

Audit Events User:

From 3 days ago to 0 days ago Show

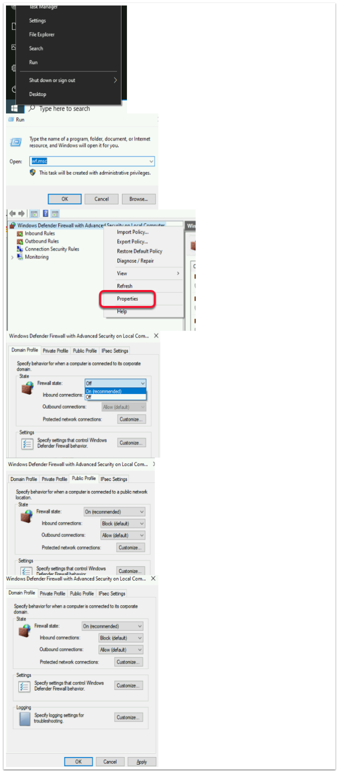
DATE, TIME (UTC)	USER (DOMAIN NAME)	EVENT
Nov 14, 2019 1:53:31 PM	user35CRSJ (euc-livefire.com)	LOGIN failed (urn:vmware:names:ac:classes:airwatchcompliance)

View Details

```
"authMethods" : "urn:vmware:names:ac:classes:airwatchcompliance",
"actorExternalId" : null,
"failureMessage" : "<div style=\"text-align:justify; max-height:calc(100vh - 350px); overflow:scroll;\">Your device is currently
in violation of your organizations compliance policy. To access your applications, the following must be fixed.<br><ol
style=\"text-align:center; padding:0; margin:0;\"><br>Windows 10 - Firewall<br>Firewall Status<br></ol></div>"
}
}
```

3. Windows 10 Compliance in Action continued...

- Use your RDP connection and go back and enable the Windows Firewall on the Windows 10 machine.
  1. Select **Start** > **RUN** and type **wf.msc**
  2. Right click **Windows Defender Firewall with Advanced Security on Local Computer** and select **Properties**
  3. Re-enable the **Domain**, **Private** and **Public Profiles** by selecting the **dropdown** next **Firewall state** and change **Off** to **On (recommended)**
  4. Select **OK** to close the **Windows Defender Firewall with Advanced Settings on Local Computer**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

This task will be created with administrative privileges.

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

On (recommended)

Off

Inbound connections:

Outbound connections: Allow (default)

Protected network connections:

Settings

Specify settings that control Windows Defender Firewall behavior.

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to a public network location.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:

Settings

Specify settings that control Windows Defender Firewall behavior.

Windows Defender Firewall with Advanced Security on Local Com...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections:

Settings

Specify settings that control Windows Defender Firewall behavior.

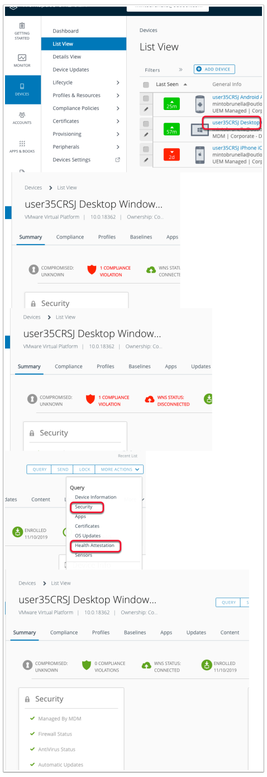
Logging

Specify logging settings for troubleshooting.

4.

- Navigate back to your Workspace ONE UEM Console
  1. Select **Devices** > **List View** > and select your **Windows 10 device**
  2. It take about 5 minutes for your Status to change in Workspace ONE UEM. **Keep refreshing** your screen
     1. If **WNS status: Disconnected** shows then try rebooting your Windows 10 machine.
     2. If this does not work Select **Query** > **Security** and **Query** > **Health Attestation**

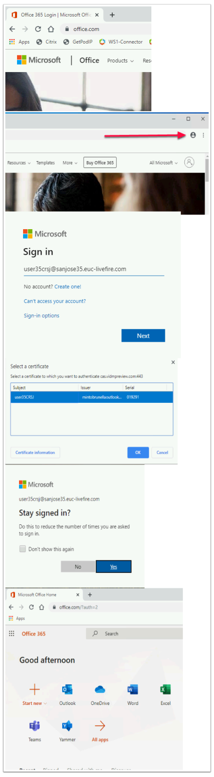
  3. You should now see the device listed as **compliant** and the **Firewall status** as green in the WorkspaceOne UEM console.



5

- Revert back to your Windows 10 virtual machine

1. Open a browser and type **Office.com**
2. On the right of the page select the **Sign into your accounts** ICON
3. On the **Sign in** type your **custom user email address** eg. user35crsj@sanjose35.euc-livefire.com select **Next**
4. On the **Select a certificate** window select **OK**
5. On the **Stay signed In?** window select **NO**
6. Notice the Single Sign-On using the **Certificate + the Compliance Check** against UEM worked successfully and you now have access to the application



Office 365 Login | Microsoft Off...
office.com
Microsoft | Office Products
Resources Templates More Buy Office 365 All Microsoft

Microsoft

Sign in

user35crsj@sanjose35.euc-livefire.com

No account? Create one!

Can't access your account?

Sign-in options

Next

Select a certificate

Select a certificate to which you want to authenticate cas.vidmpreview.com:443

Subject	Issuer	Serial
user35CRSJ	mintobrunellaoutlook...	019291

Certificate information OK Cancel

Microsoft

user35crsj@sanjose35.euc-livefire.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

No Yes

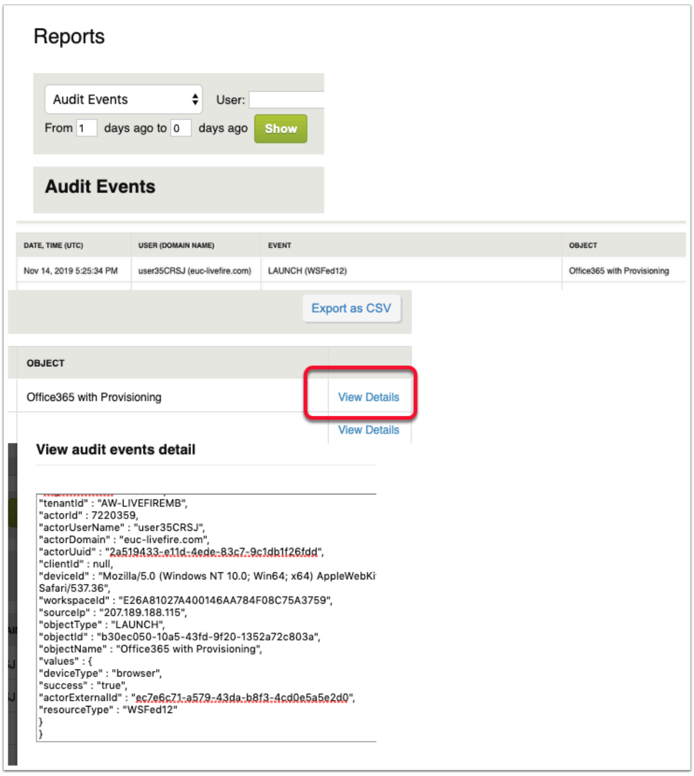
Good afternoon

6.

- If you go to Workspace ONE Access , select the **Dashboard** > **Reports** > **Audit Events**
  1. Select **Show** ,
     - notice the **EVENT** is **LAUNCH** and your **User** , the **OBJECT** is **Office365 with Provisioning**,
  2. Select **View Details**
  3. Notice Audit Events are reporting a successful login using Certificate (Cloud Deployment) and Device Compliance (with AirWatch).

-

This completes the **Windows 10 Compliance** with **Workspace ONE Access** and **Workspace ONE UEM Lab**. This is a single example of the many options for compliance that could be used not restricted to Windows 10, but also other platforms



Audit Events

DATE, TIME (UTC)	USER (DOMAIN NAME)	EVENT	OBJECT
Nov 14, 2019 5:25:34 PM	user35CRSJ (euc-livefire.com)	LAUNCH (WSFed12)	Office365 with Provisioning

OBJECT	
Office365 with Provisioning	View Details
	View Details

View audit events detail

```
"tenantId" : "AW-LIVEFIREMB",
"actorId" : 7220359,
"actorUserName" : "user35CRSJ",
"actorDomain" : "euc-livefire.com",
"actorUuid" : "2a519433-e11d-4ede-83c7-9c1db1f26fdd",
"clientId" : null,
"deviceId" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
Safari/537.36",
"workspaceId" : "E26A81027A400146AA784F08C75A3759",
"sourceIp" : "207.189.188.115",
"objectType" : "LAUNCH",
"objectId" : "b30ec050-10a5-43fd-9f20-1352a72c803a",
"objectName" : "Office365 with Provisioning",
"values" : {
"deviceType" : "browser",
"success" : "true",
"actorExternalId" : "ec7e6c71-a579-43da-b8f3-4cd0e5a5e2d0",
"resourceType" : "WSFed12"
}
}
```

Securing O365 with Workspace One UEM

Part 1: Configure Azure for Integration with Workspace ONE UEM

In this lab you will configure and apply data loss prevention (DLP) application policies to the Microsoft Intune App Protection applications and data in the Workspace ONE UEM console. Workspace ONE UEM does not directly enforce policies on applications. The Microsoft SDK controls and enforces the policies.

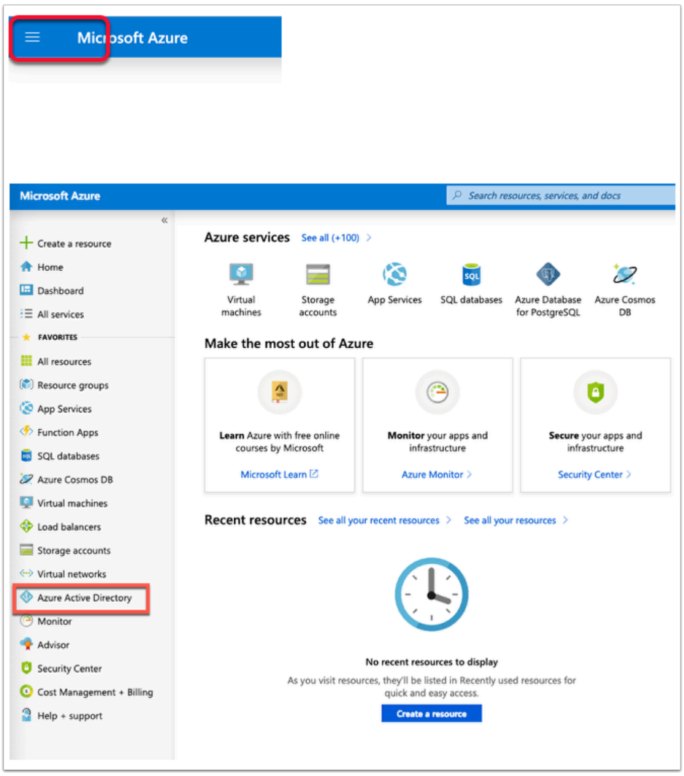
Pre-requisites:

1. Enterprise Mobility + Security E5 License (EM+S E5)

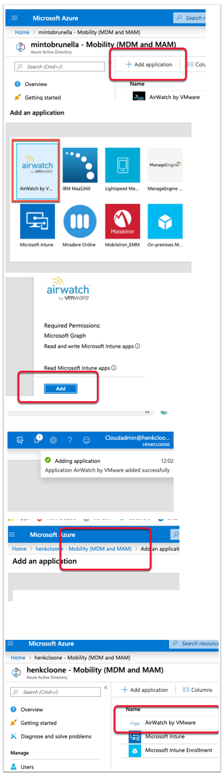
2. Admin credentials with access to Azure Active Directory with permissions to add enterprise applications and with the Group.Read.All and Group.ReadWrite.All permissions.

Note: Graph API does not support modern authentication. Hence can only use non federated Admin credential. Use *onmicrosoft.com domain.

1. Login to **portal.azure.com** using your onmicrosoft admin account created in an earlier lab.
   1. On the landing page select the ☰ 3 **horizontal lines** in the top-left hand corner to open the **admin menu**
   2. Select the **Azure Active Directory** from the left hand navigation pane.



2. In the left pane select **Mobility (MDM and MAM)**
   1. In the **Mobility (MDM and MAM)** select **+ Add application**
   2. Select the **AirWatch by VMware** application, **scroll down** to the bottom right-hand corner
   3. Select **Add** on the side panel that pops-up.
      - You should notice a brief **Added application** message with a green tick next to it
   4. Go back to **Mobility (MDM and MAM)** by selecting the **Mobility (MDM and MAM)** at the top of the screen
      - Notice you now have an **AirWatch by VMware** Application

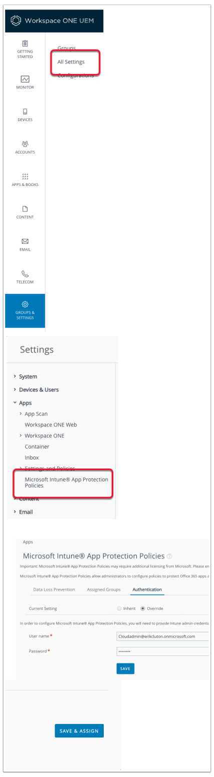


Required Permissions:
Microsoft Graph
Read and write Microsoft Intune apps
Read Microsoft Intune apps

Adding application 12:02
Application AirWatch by VMware added successfully

Part 2: Configure Workspace ONE UEM for Application Protection Policy

1. Configuring Data Loss Prevention using Microsoft Intune® App Protection Policies for Android and IOS Mobile devices
    1. Switch to your **Workspace ONE UEM** console and login as **Admin**
    2. Go to **GROUPS & SETTINGS** > **ALL SETTINGS**
    3. Under **APPS** , select **Microsoft Intune App Protection Policies**
    4. In the **Microsoft Intune App Protection Policies** console. Select the **Authentication** tab. Next to : -
        - **Username** : your **office 365 CloudAdmin username**
        - **Password** : your **cloud admin off365 password**
    5. Select **SAVE & ASSIGN**



Microsoft Intune® App Protection Policies

Important: Microsoft Intune® App Protection Policies may require additional licensing from Microsoft. Please en

Microsoft Intune® App Protection Policies allow administrators to configure policies to protect Office 365 apps a

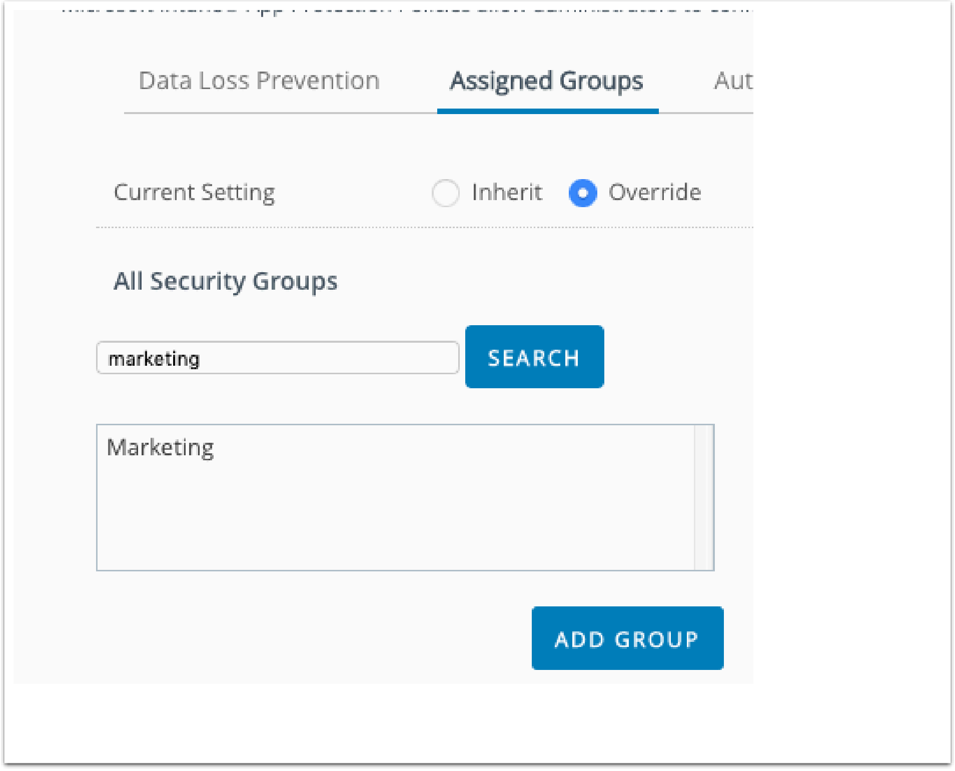
Current Setting ○ Inherit ● Override

In order to configure Microsoft Intune® App Protection Policies, you will need to provide Intune admin credenti

User name * Cloudadmin@erikcluton.onmicrosoft.com

Password * ••••••••

2. In the **Microsoft Intune App Protection Policies** console
   1. Next to the **Authentication** tab to the left, select the **Assigned Groups** Tab
   2. Under **All Security Groups** select **SEARCH** Marketing
   3. Select **Marketing** select **ADD GROUP**
   4. Close the window by selecting the **X** in the top right-hand corner.



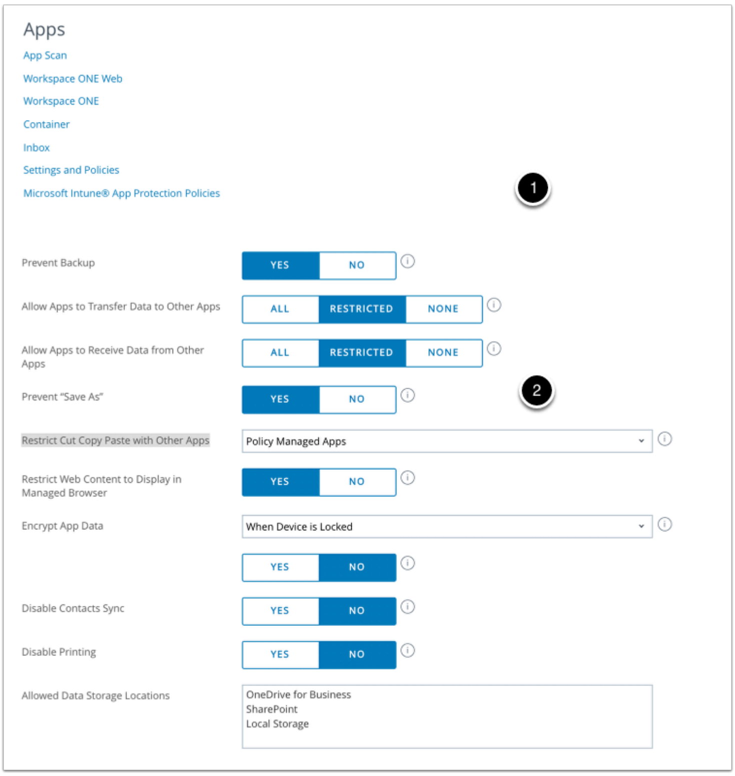
Current Setting ○ Inherit ● Override

All Security Groups

marketing

Marketing

3. Ensure you are still logged into your **Workspace ONE UEM** admin console
    1. Select **GROUPs & SETTINGS** > **All Settings**
    2. In the **Apps Section** select **Microsoft Intune® App Protection Policies**
    3. Select the **Data `Loss Protection** tab, under **Data Relocation** section configure the following:-
        - **Allow Apps to Transfer Data to Other Apps : RESTRICTED**
        - **Allow Apps to Receive Data from Other Apps : RESTRICTED**
        - **Restrict Cut Copy Paste with Other Apps : Policy Managed Apps**
    4. Select **SAVE & ASSIGN**



Prevent Backup: [✓ YES] NO

Allow Apps to Transfer Data to Other Apps: ALL [✓ RESTRICTED] NONE

Allow Apps to Receive Data from Other Apps: ALL [✓ RESTRICTED] NONE

Prevent "Save As": [✓ YES] NO

Restrict Cut Copy Paste with Other Apps: Policy Managed Apps

Restrict Web Content to Display in Managed Browser: [✓ YES] NO

Encrypt App Data: When Device is Locked

YES [✓ NO]

Disable Contacts Sync: YES [✓ NO]

Disable Printing: YES [✓ NO]

Allowed Data Storage Locations: OneDrive for Business
SharePoint
Local Storage

> For Intune Policies to be applied on **Android devices** we have to install the **Microsoft Intune company Portal app.**

Part 2.1: Installing the Microsoft Intune Company Portal App (Android Only)

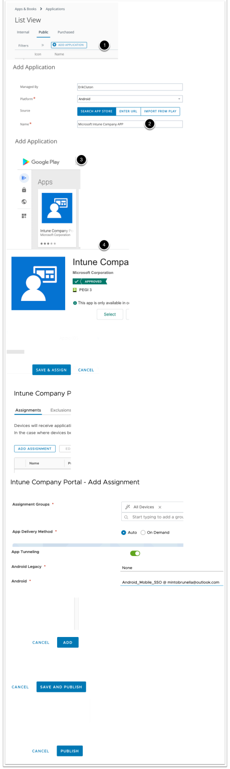
In the**APPS & BOOKS**>**Applications**>**Native**>**Public**tab

1. Select **+ADD APPLICATION**
2. In the **Add Application**window next to: Select
    - **Platform***: **Android**
    - **Name*:** **Microsoft Intune Company Portal App**

- select **NEXT**

3. In the **Add Application** window select **Intune Company Portal**
4. In the **Intune Company Portal** section, click the **Select** button
5. Select **SAVE & ASSIGN**
6. On the **Intune Company Portal- Update Assignment** window select **ADD ASSIGNMENT**
7. In the **Intune Company Portal- Add Assignment** window next to:-
   - **Select Assignment Groups: All Devices**
   - **App Delivery Method: AUTO** radio button
   - **App Tunneling :** ENABLED (notice two extra lines are added)
     - **Android*** Android_Mobile_SSO

8. At the bottom of the page select **ADD**
9. Select **SAVE & PUBLISH**
10. Select **PUBLISH**



Managed By: ErikCluton

Platform*: Android

Source: SEARCH APP STORE

Name*: Microsoft Intune Company APP

Assignment Groups *: All Devices

App Delivery Method *: ● Auto ○ On Demand

App Tunneling: enabled

Android Legacy *: None

Android *: Android_Mobile_SSO @ mintobrunella@outlook.com

Part 3: Test App Protection Policies

> Now that the settings have been setup in the Workspace ONE UEM console, we must actually see these policies in effect on the device to enhanced security.
>
> Wait 5 to 10 minutes for those policies to be applied to your device.

Part 3: Is divided into 2 sections

Section 1 : We test with an IOS device

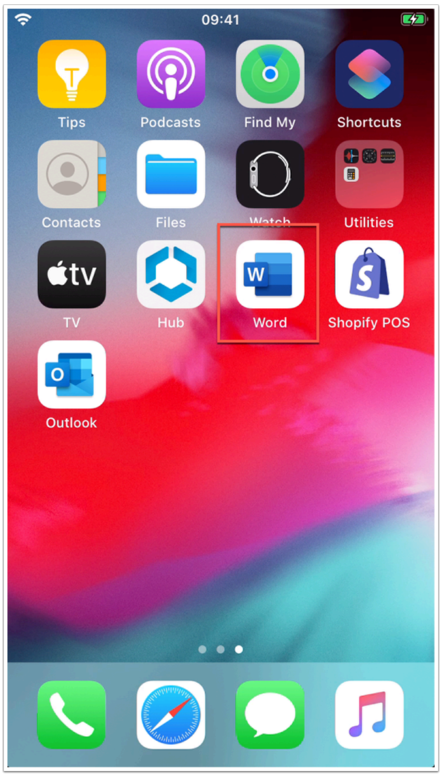
Section 2 : We test using an Android device

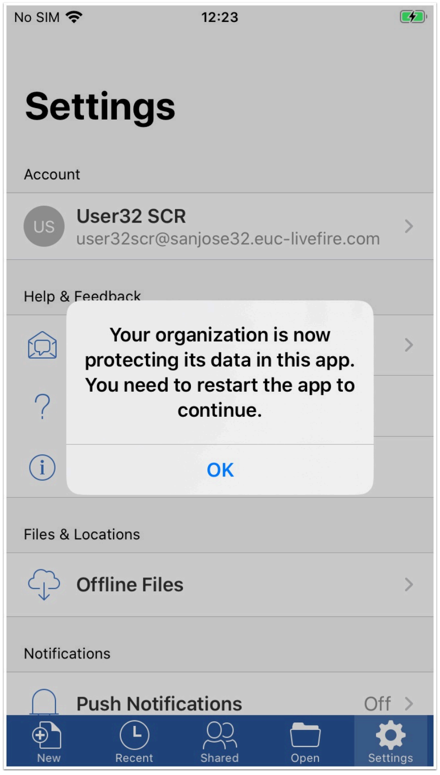
If you have not done any IOS configuration move on to Section 2 in Part 3 of this Lab.

Section 1: IOS TEST

Note: The following steps have been written assuming you have NO previously installed Native Office 365 Applications on your IOS device prior to enrolling your device. If you suspect you have, for consistent results, that are in line with the instructions in this Lab, remove these native applications, and install Microsoft Word and Microsoft Excel through the Workspace ONE HUB application.

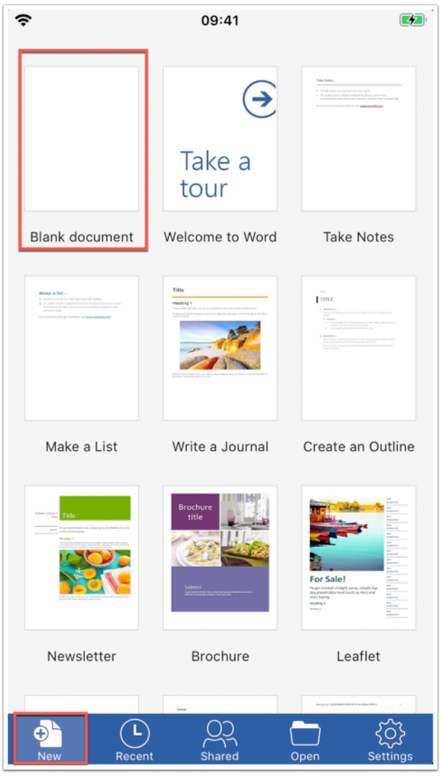
1. Ensure your IOS device is enrolled your lab environment and all previous parts of these labs have been completed successfully
    1. On your **IOS** device launch **Microsoft Word**
        - You will now see a prompt that the application has received additional Company Policies, select **OK** to close the window
    2. You will be prompted to set a passcode in accordance with the policy. Set a **4 digit pin** e.g. **2019**

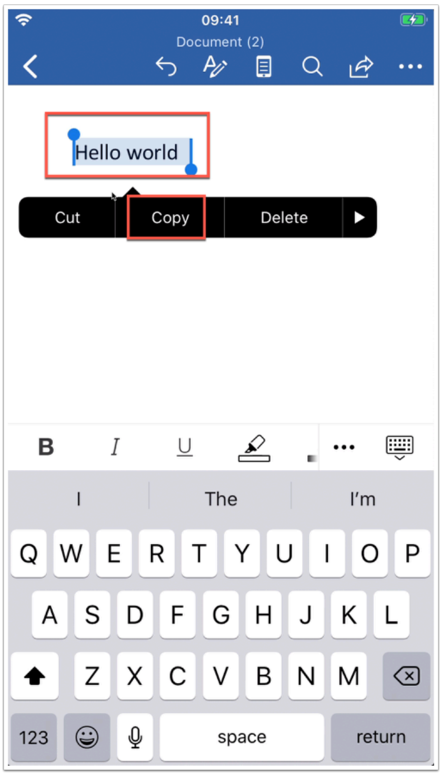


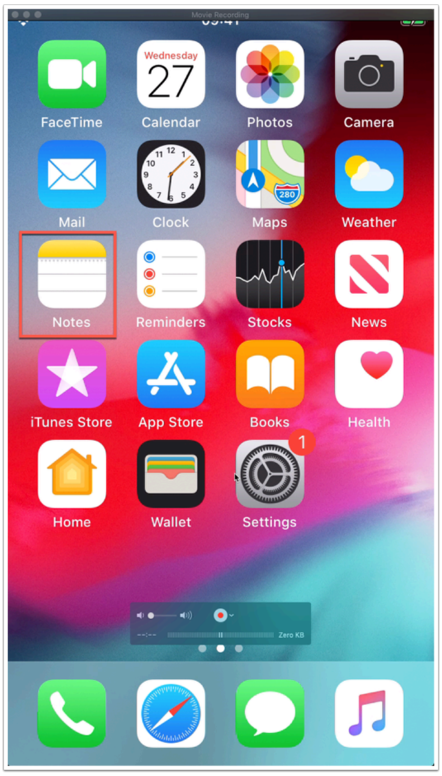


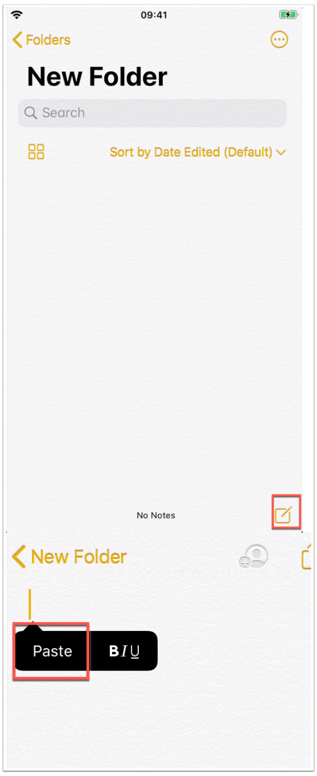
Your organization is now protecting its data in this app. You need to restart the app to continue.

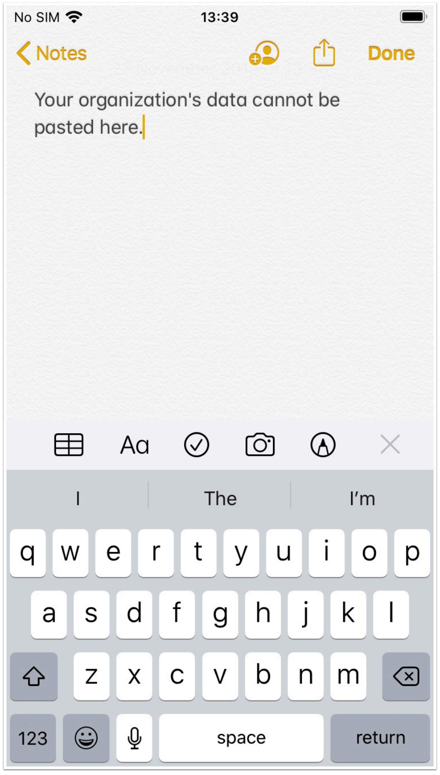
2. Let's now look at the Data Loss Prevention feature.
    1. In the **Word app** on your iOS device click on **New** at the bottom left to create a new document.
    2. Click on **Blank Document** in the top left corner.
    3. Now type **Hello World**, then **select** and click **copy**
    4. Now open **Notes** as an application on the device
    5. Click the **Pen on paper icon** in the bottom right corner of the application for a new note.
    6. Now **press and hold** to select **Paste.** You will get a message saying **"Your Organisation's data cannot be pasted here.**"


09:41
Take a tour
Blank document
Welcome to Word
Take Notes
Make a List
Write a Journal
Create an Outline
Newsletter
Brochure
Leaflet
New
Recent
Shared
Open
Settings


09:41
Document (2)
Hello world
Cut
Copy
Delete
B
I
U
I
The
I'm
space
return
123


Movie Recording
09:41
Wednesday
27
FaceTime
Calendar
Photos
Camera
Mail
Clock
Maps
Weather
Notes
Reminders
Stocks
News
iTunes Store
App Store
Books
Health
Home
Wallet
Settings
Zero KB

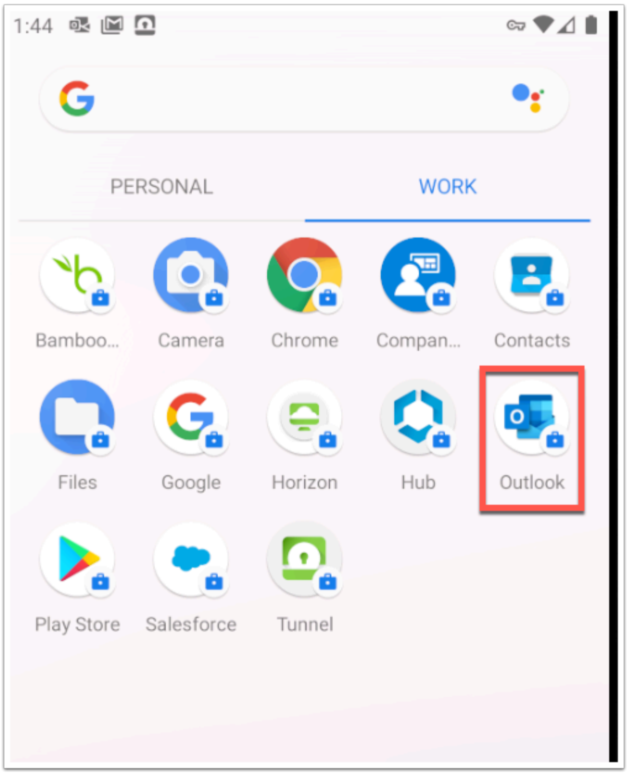

09:41
Folders
New Folder
Search
Sort by Date Edited (Default)
No Notes
New Folder
Paste
B I U

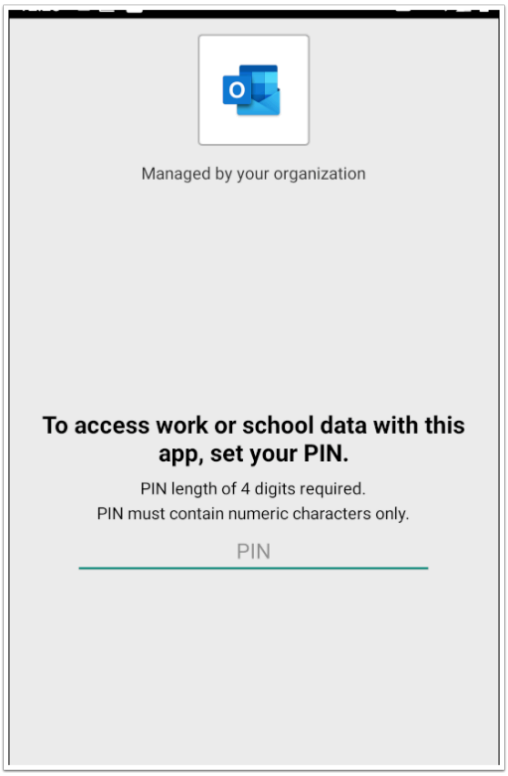


Your organization's data cannot be pasted here.

Section 2: Android OS Test

1. Ensure your Android device is enrolled your lab environment and all previous parts of these labs have been completed successfully.
   1. On your Android Device. Open the managed **Outlook** application
      - Notice the application is managed by your organization and you will be required to set a pin. Type **2019** or any four digit pin.
   2. Once you are in the **Outlook** application and you have entered the pin to authenticate, click on the **pencil icon** in the bottom right.
   3. Now in the body area of the new message type **Hello World**.
   4. **Select** the text and click **copy**



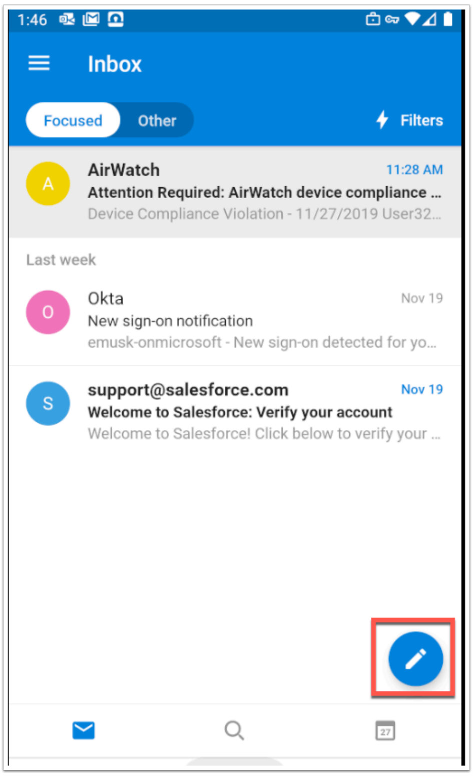


Managed by your organization

To access work or school data with this app, set your PIN.

PIN length of 4 digits required.
PIN must contain numeric characters only.

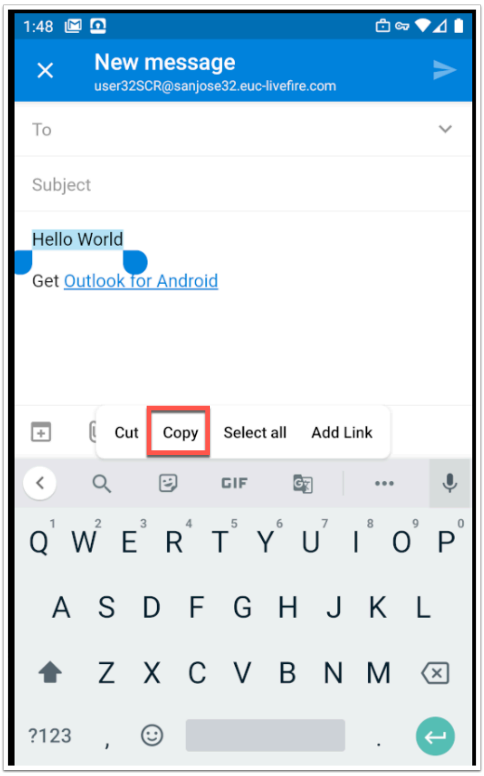
PIN



AirWatch 11:28 AM
Attention Required: AirWatch device compliance ...
Device Compliance Violation - 11/27/2019 User32...

Okta Nov 19
New sign-on notification
emusk-onmicrosoft - New sign-on detected for yo...

support@salesforce.com Nov 19
Welcome to Salesforce: Verify your account
Welcome to Salesforce! Click below to verify your ...

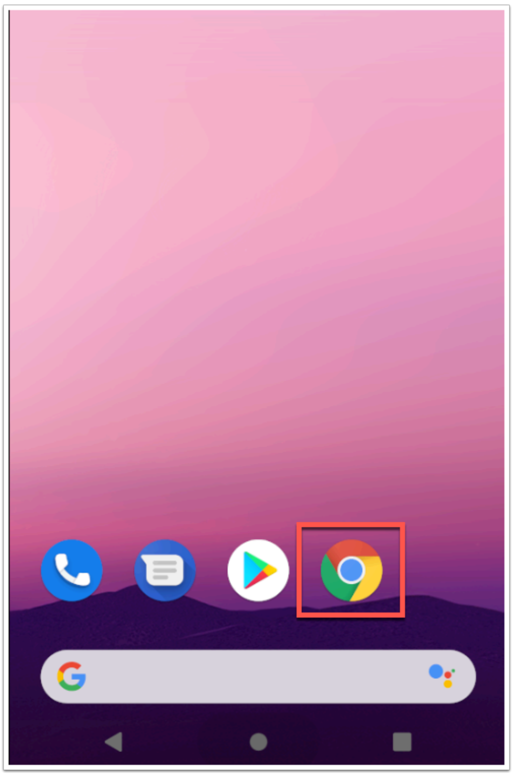


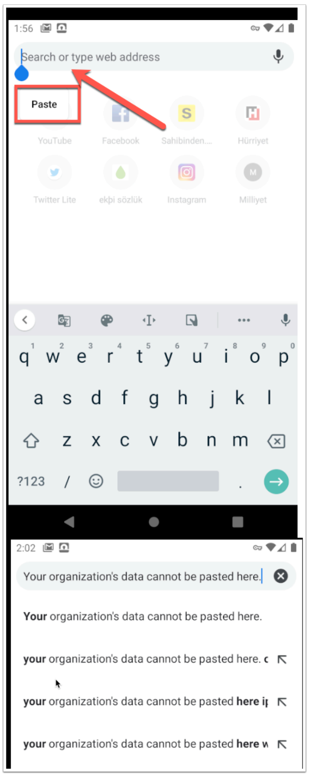
Hello World

Get Outlook for Android

2. Now click **home** and click on the **Chrome** application that does not have the suitcase.
    1. In the **Chrome application** click on the address bar and click **Paste**
    2. You will note that it will not paste this text from Outlook. You will get a message "**Your organisation's data cannot be pasted here.**"

- This concludes the Securing O365 with Workspace ONE UEM - you have seen the integration with Microsoft securing the digital workplace.





Your organization's data cannot be pasted here.

Your organization's data cannot be pasted here.

your organization's data cannot be pasted here. c

your organization's data cannot be pasted **here** i

your organization's data cannot be pasted **here** w

Day 4

Reporting, Analytics and Automation WorkspaceOne Intelligence

Part 1: Overview

VMware Workspace ONE Intelligence gives you insights into your digital workspace. At the moment Intelligence can aggregate information from three different sources: Workspace ONE Access, Workspace ONE UEM, and Apteligent.

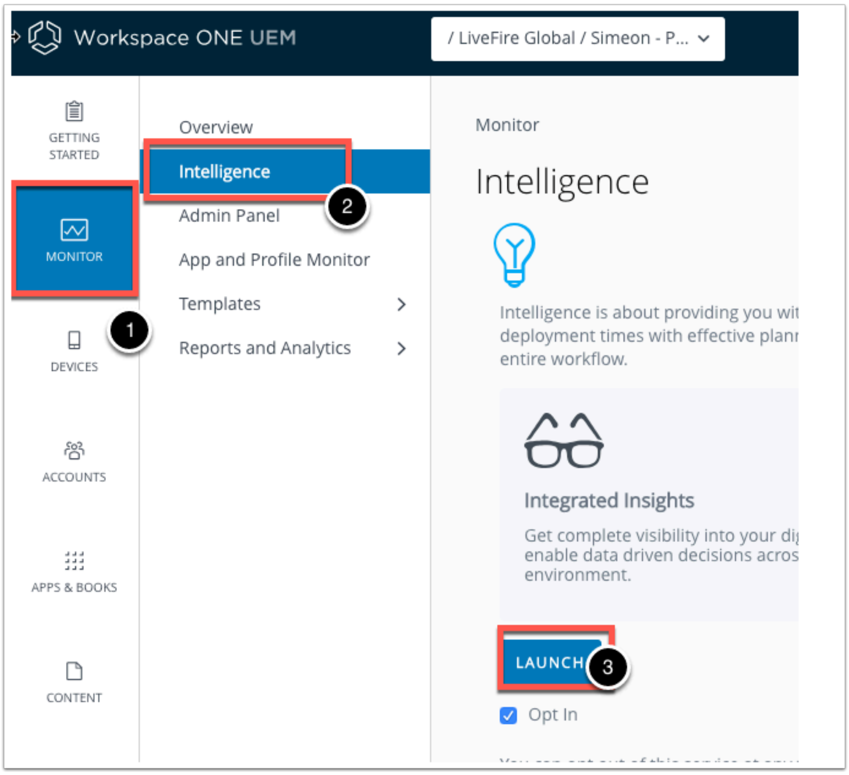
Components

Workspace ONE Intelligence aggregates data from Workspace ONE UEM and Apteligent by VMware. It includes **Dashboards**, **Reports**, and **Automation** to analyze data and perform actions for efficiency and remediation. It integrates with third-party connection services like Slack and ServiceNow for notifications.

In this lab we will look at how to create reports, dashboards and build automation based on this information.

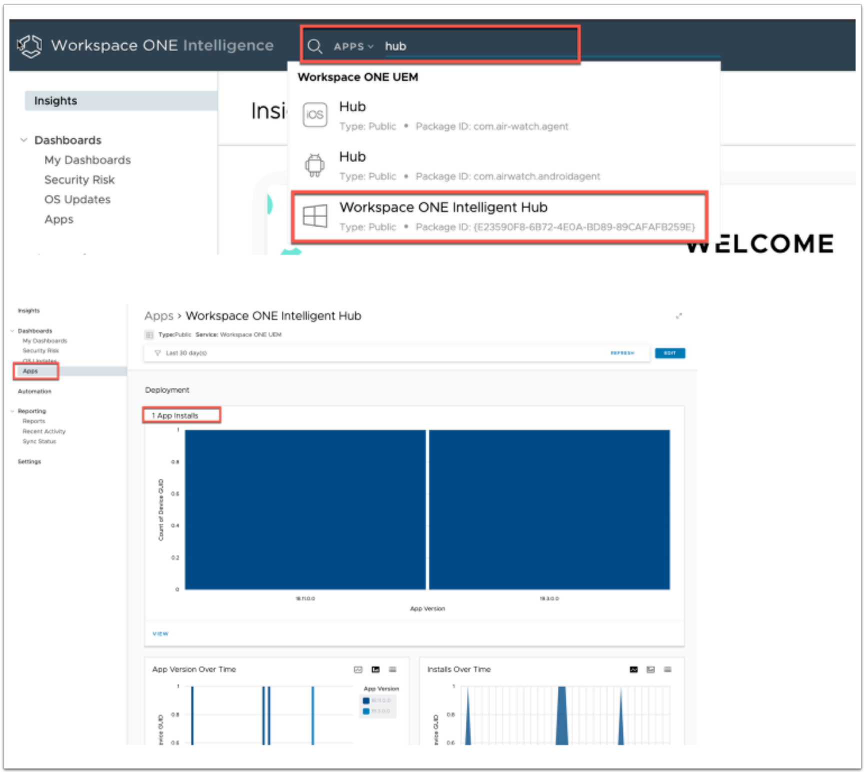
1. Accessing **Workspace ONE Intelligence** from the **Workspace ONE UEM** console:

1. Open a browser and navigate to **cn-livefire.awmdm.com** and authenticate using your **username** and **password.**
2. Navigate to **MONITOR** in the **Workspace ONE UEM Admin** console > Select **Intelligence** and select **LAUNCH**

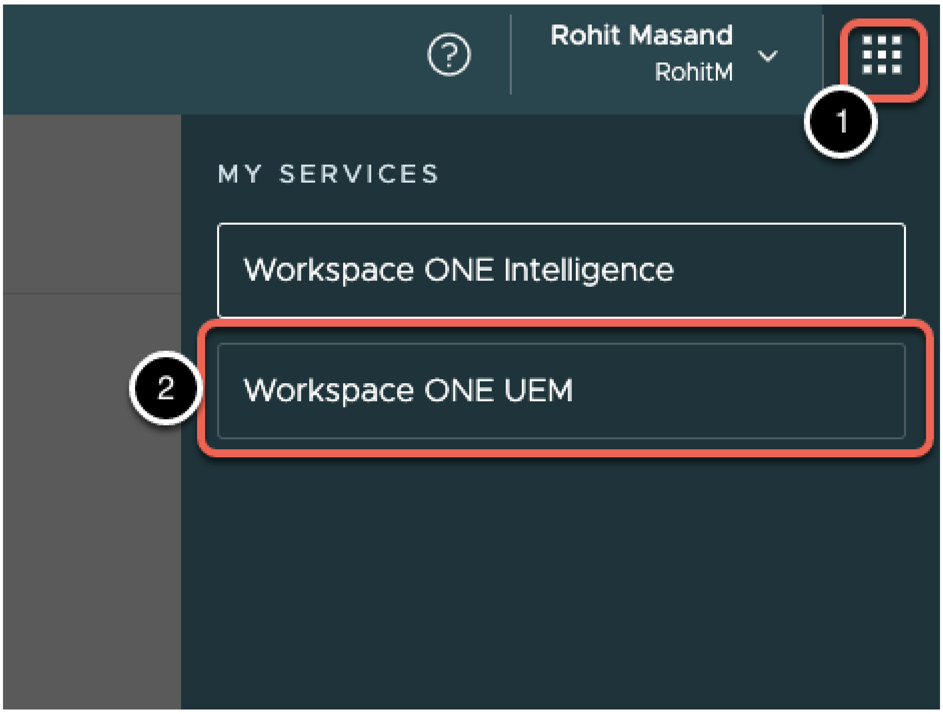


2. You will now be redirected to the **Workspace ONE Intelligence** server.
   - Here you will find ***at the top*** a **search function** which allows you to search for **Apps**, Automations **Reports**, **Automation**, **Dashboards**, **OS, Reports** and **Widgets**.

1. Select **Apps**. This is very useful if you want to just look for something quickly.
2. In the **Search** area type "**Hub**". Notice the devices that you have the hub installed.
3. Click on **Windows**, or any other that you have installed. You will now get a glimpse into the devices this app is installed on, the version of the application, the time it was installed etc.
   - Notice you are also directed in the left hand navigation bar to **Apps** under **Dashboards**. We will come back to **Dashboards** at a later stage in the lab.


Workspace ONE Intelligence
APPS hub
Workspace ONE UEM
Hub
Type: Public • Package ID: com.air-watch.agent
Hub
Type: Public • Package ID: com.airwatch.androidagent
Workspace ONE Intelligent Hub
Type: Public • Package ID: {E23590F8-6B72-4E0A-BD89-89CAFAFB259E}
Insights
Dashboards
My Dashboards
Security Risk
OS Updates
Apps
WELCOME
Apps › Workspace ONE Intelligent Hub
Deployment
1 App Installs
App Version
App Version Over Time
Installs Over Time

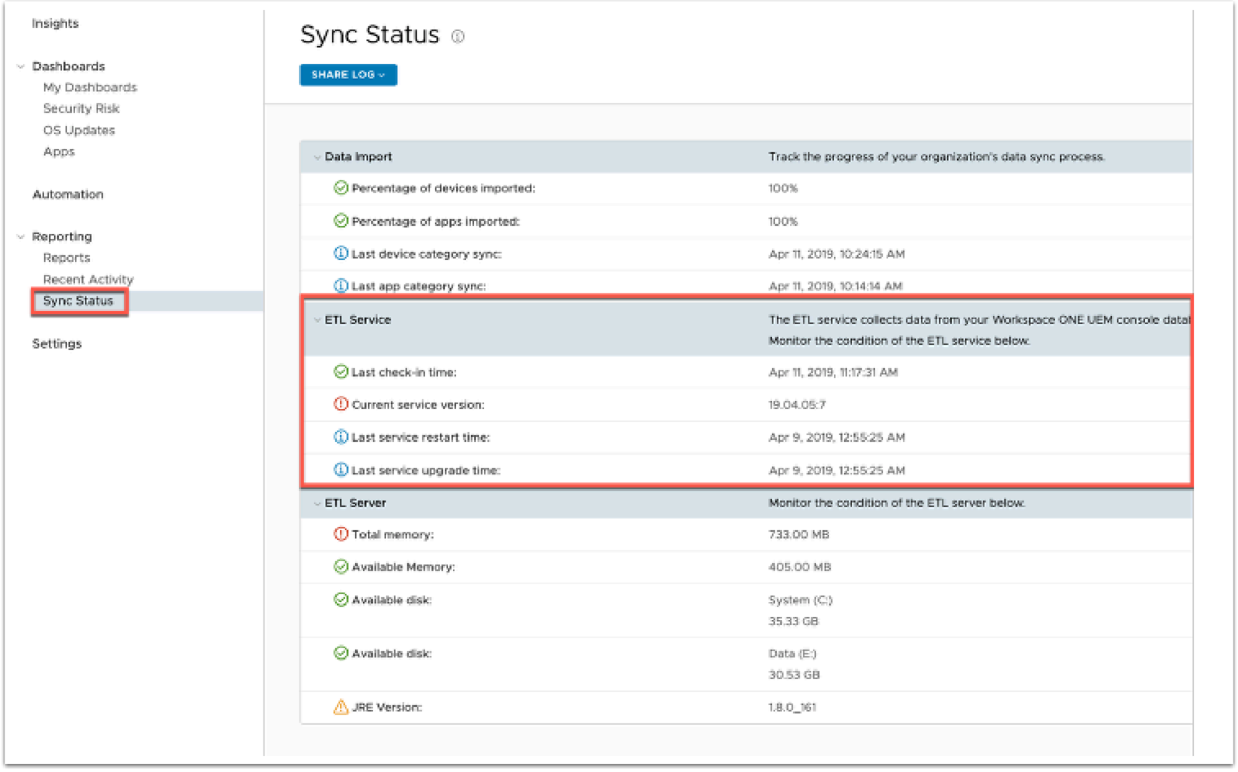
3. Return to the **Workspace ONE UEM** console:
    1. Select the **square menu** for **MY SERVICES** in the top right corner of the UI.
    2. Select **Workspace ONE UEM** from the **MY SERVICES** menu.



Part 2: Reporting

1. Under **Reporting** Click on **Sync Status**

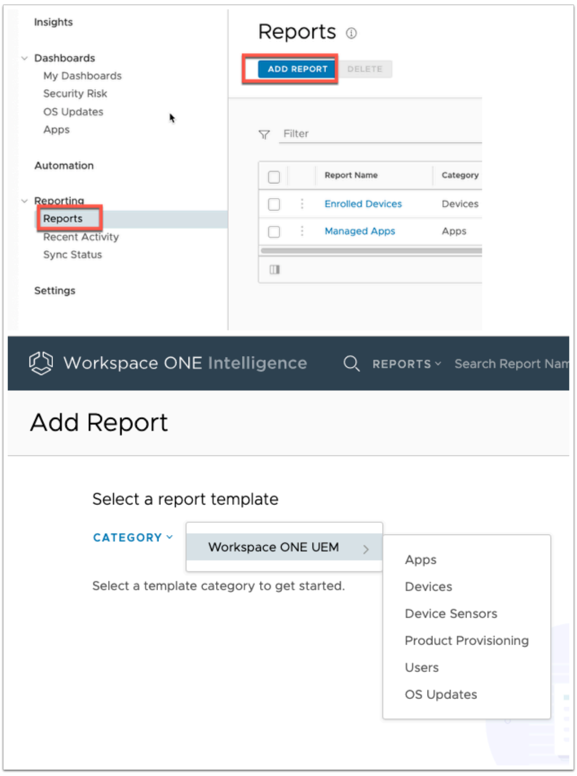
Reports tie in directly into the database of the WorkspaceOne Workspace ONE UEM environment. For SaaS environment no additional setup required. However for on-premise Workspace ONE UEM deployments you will require the ETL (extract, transform, load) service which pushed data from the Workspace ONE UEM database to the Intelligence Cloud Service on AWS. This would have to be installed on a separate server. In order to see the current Status of the ETL service.



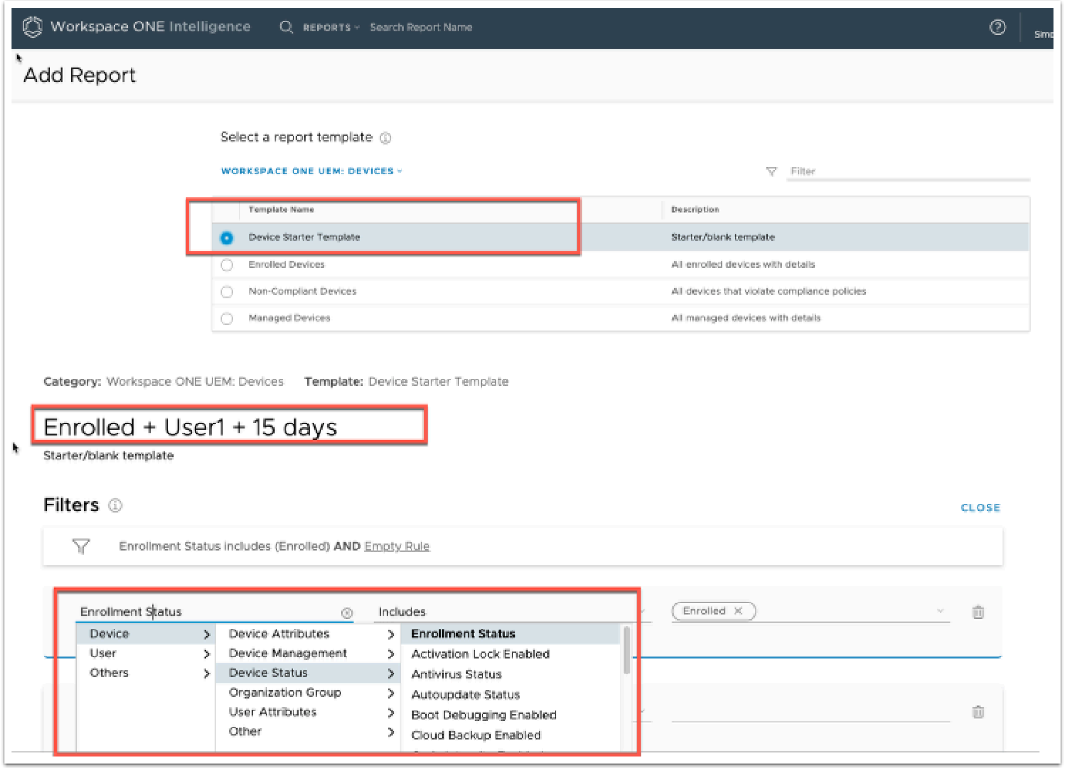
Sync Status

Data Import	Track the progress of your organization's data sync process.
✓ Percentage of devices imported:	100%
✓ Percentage of apps imported:	100%
ⓘ Last device category sync:	Apr 11, 2019, 10:24:15 AM
ⓘ Last app category sync:	Apr 11, 2019, 10:14:14 AM
ETL Service	The ETL service collects data from your Workspace ONE UEM console data Monitor the condition of the ETL service below.
✓ Last check-in time:	Apr 11, 2019, 11:17:31 AM
ⓘ Current service version:	19.04.05.7
ⓘ Last service restart time:	Apr 9, 2019, 12:55:25 AM
ⓘ Last service upgrade time:	Apr 9, 2019, 12:55:25 AM
ETL Server	Monitor the condition of the ETL server below.
ⓘ Total memory:	733.00 MB
✓ Available Memory:	405.00 MB
✓ Available disk:	System (C:) 35.33 GB
✓ Available disk:	Data (E:) 30.53 GB
⚠ JRE Version:	1.8.0_161

2. Under **Reporting**
   1. Click on **Reports** and click on **ADD REPORT**
      - You will now have the option to select category of report you would like to create.
   2. In the **Add Report** window expand the **dropdown arrow** next to **CATEGORY**, Click on **Workspace ONE UEM** > **Devices**
      - Notice here you have a few reports already pre-populated for the admin to use.



3. Select the **radio button** next to **Device Starter Template**
    1. Select **NEXT** at the bottom of the page.
    2. Where it says **Device Starter Template** re-name it to **Enrolled + CustomUser + 15 days**.
    3. Below **Empty Rule,** In the **Search** field select on **Search ,** select **Device** > **Device Status** > **Enrollment Status**
    4. To the right of **Enrollment Status** using the **drop-down** to the right of **Includes**. Replace **Includes** with **Equals .**
    5. To the right of **Equals**, from the drop down select **Enrolled.**



Add Report

Select a report template

	Template Name	Description
●	Device Starter Template	Starter/blank template
○	Enrolled Devices	All enrolled devices with details
○	Non-Compliant Devices	All devices that violate compliance policies
○	Managed Devices	All managed devices with details

Category: Workspace ONE UEM: Devices **Template:** Device Starter Template

Enrolled + User1 + 15 days

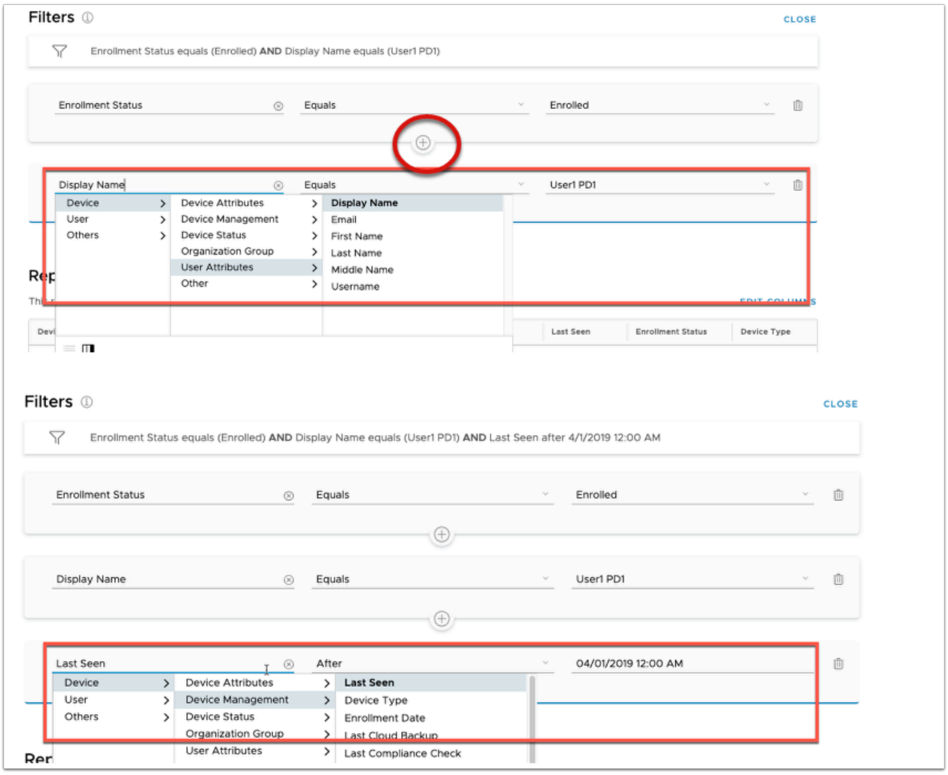
Starter/blank template

Filters

Enrollment Status includes (Enrolled) **AND** Empty Rule

Enrollment Status Includes Enrolled

4. Under your first Filter in the middle, select the **+** to add another filter
    1. In the **Search** area area select **Device** > **User Attributes** > **User Name**
        1. In the area to the right of **Display,** select the **drop down** on the right side of **Includes** and select **Equals**
        2. In the area to the right of **Equals** select the **drop down** and select your **Custom User.**
    2. Below the filter in the middle select the **+** to add another filter and click **Device** > Device Management > Last Seen
        1. In the area to the right of **Last Seen,** select the **drop down** on the right side of **Includes** and select **After**
        2. In the area to the right of **After** select the **drop down** and select select **04/01/2019** (April 1 2019)



Filters ⓘ CLOSE

Enrollment Status equals (Enrolled) **AND** Display Name equals (User1 PD1)

Enrollment Status — Equals — Enrolled

Display Name — Equals — User1 PD1

Filters ⓘ CLOSE

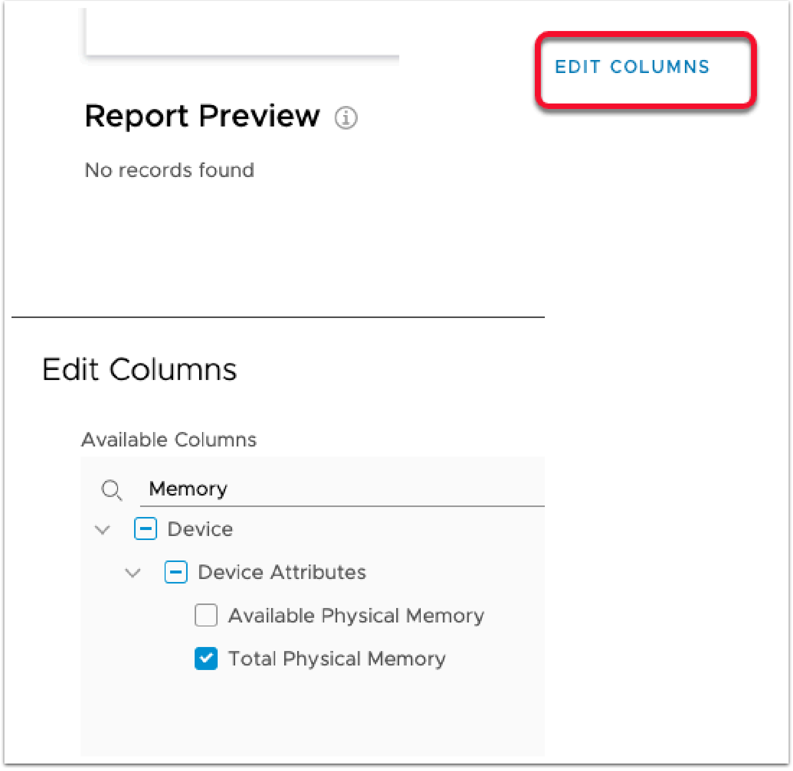
Enrollment Status equals (Enrolled) **AND** Display Name equals (User1 PD1) **AND** Last Seen after 4/1/2019 12:00 AM

Enrollment Status — Equals — Enrolled

Display Name — Equals — User1 PD1

Last Seen — After — 04/01/2019 12:00 AM

5. Below your fliters, In the **Report Preview** section,
    1. In the far-right side of **Report Preview** click on **EDIT COLUMNS**. note. Intelligence allows you to customize the results to your business requirements.
    2. In the Edit Columns window, under **Available Columns** in the **Search** area type **Memory** and select **Total Physical Memory**.
    3. In the bottom left-hand corner select **ADD (1)**. You will see the column **Total Physical Memory** is added.
        - Note, you can re-arrange the order in which columns are presented in the report by dragging the column.
    4. Select **SAVE** to close the **EDIT COLUMNS** window
    5. Select **SAVE** at the botom right to save your **custom Report**



EDIT COLUMNS

Report Preview ⓘ

No records found

Edit Columns

Available Columns

Memory

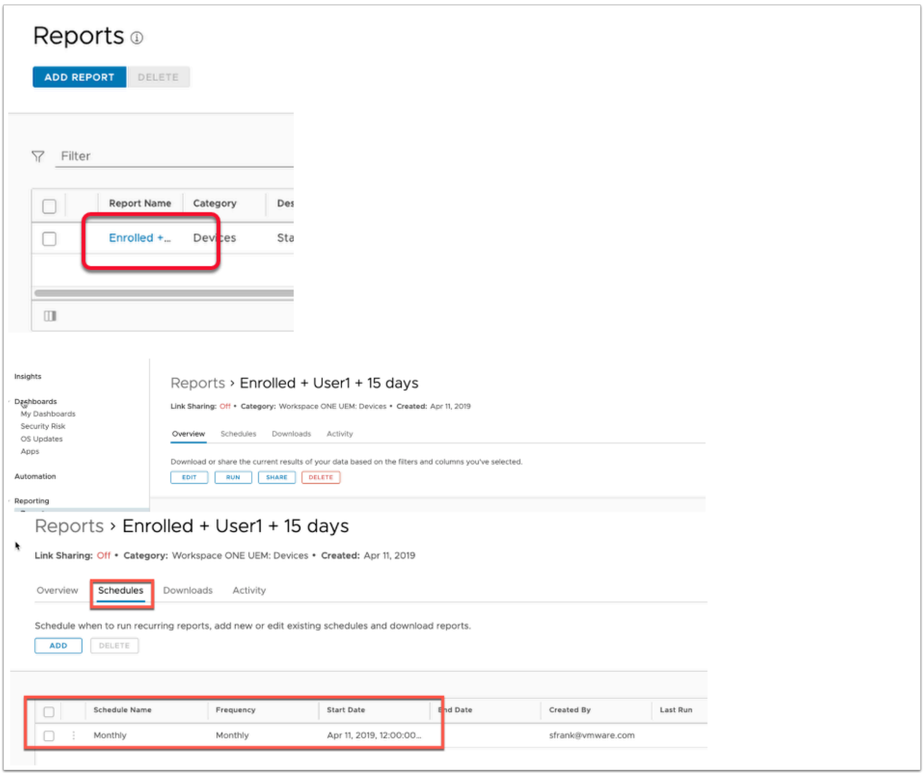
⊟ Device

⊟ Device Attributes

□ Available Physical Memory

☑ Total Physical Memory

6. Go back into your Custom Report by select **Enrolled +..** under **Report Name**
   - Notice you have 4 tabs at the top **Overview**, **Schedules**, **Downloads**, and **Activity**
   - You have the ability to **Edit** the report, **Run** the report and **Share** and **delete** the report.
   - Share is a great feature as you can e-mail various parties or even make it available via an external link to someone outside the organisation.
   - The second tab is **Schedules**, this is where you can set when the report should run. It can be setup **hourly, daily**, **weekly**, or **monthly**.



□	Report Name	Category	Des
□	Enrolled +...	Devices	Sta

Reports › Enrolled + User1 + 15 days

Link Sharing: Off • Category: Workspace ONE UEM: Devices • Created: Apr 11, 2019

Download or share the current results of your data based on the filters and columns you've selected.

Reports › Enrolled + User1 + 15 days

Link Sharing: Off • Category: Workspace ONE UEM: Devices • Created: Apr 11, 2019

Schedule when to run recurring reports, add new or edit existing schedules and download reports.

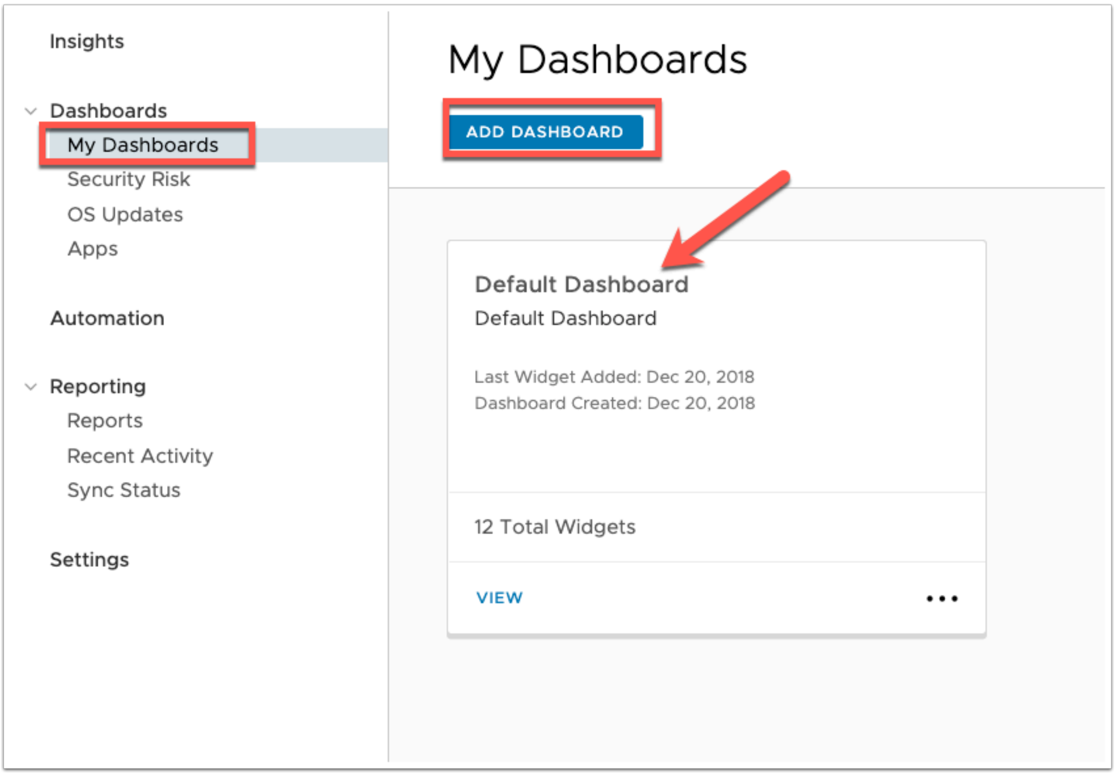
□	Schedule Name	Frequency	Start Date	End Date	Created By	Last Run
□	Monthly	Monthly	Apr 11, 2019, 12:00:00...		sfrank@vmware.com	

Part 3: Dashboards

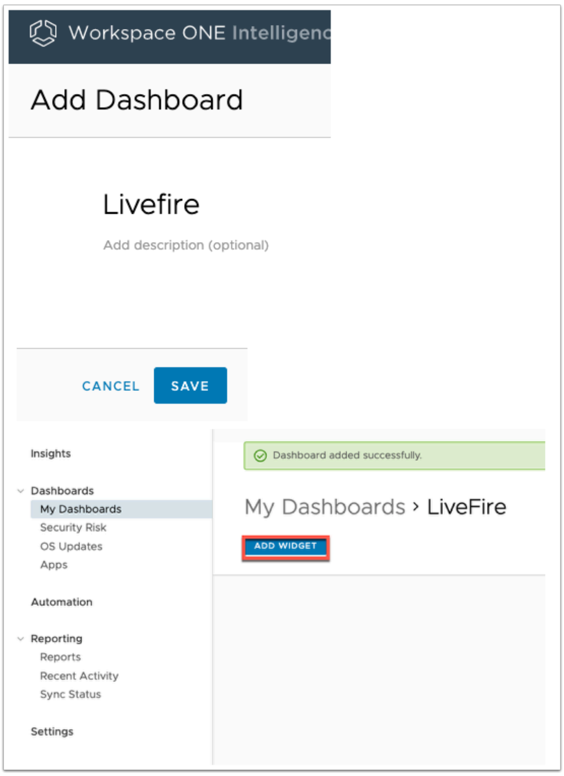
My Dashboards powered by Workspace ONE Intelligence, displays data you customize with applied widgets. Display data as graphics and analyze the trends occurring in areas within your Workspace ONE platform by App, Device, or Operating system (OS) update. Data in this view are consolidated from other dashboards.

1. In the Workspace ONE Intelligence window
   1. In left hand-hand pane, select to **Dashboards** > **My Dashboards**
   2. Select **ADD DASHBOARD**

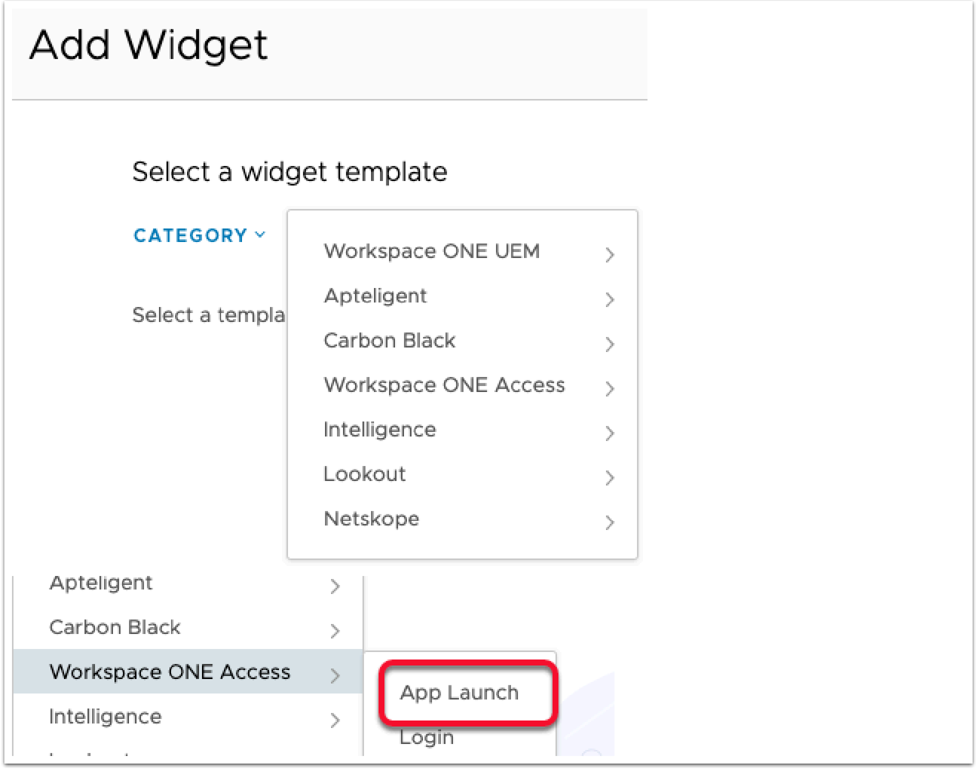
- Notice there is already a **Default Dashboard** setup with 12 widgets, this can also be view. For this lab we will create a new Dashboard.



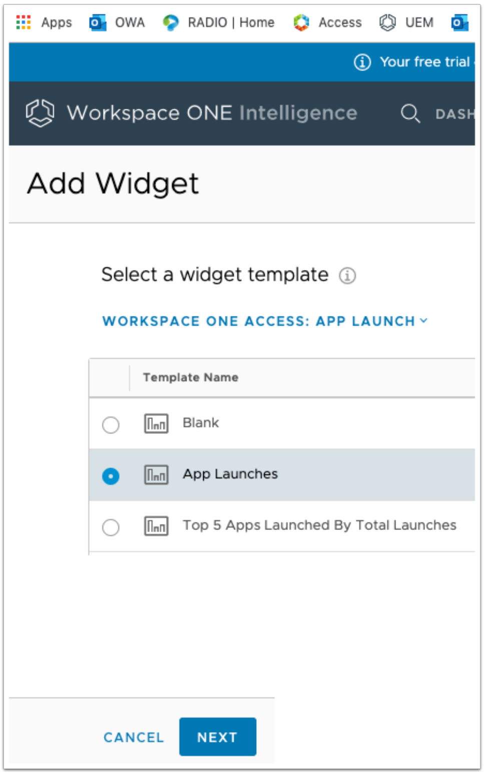
2. In the **Add Dashboard** window,
   1. In the **Name your Dashboard** area type **LiveFire** and select **SAVE** in the bottom right.
   2. In the **My Dashboards > Lifefire** window select **ADD WIDGET**



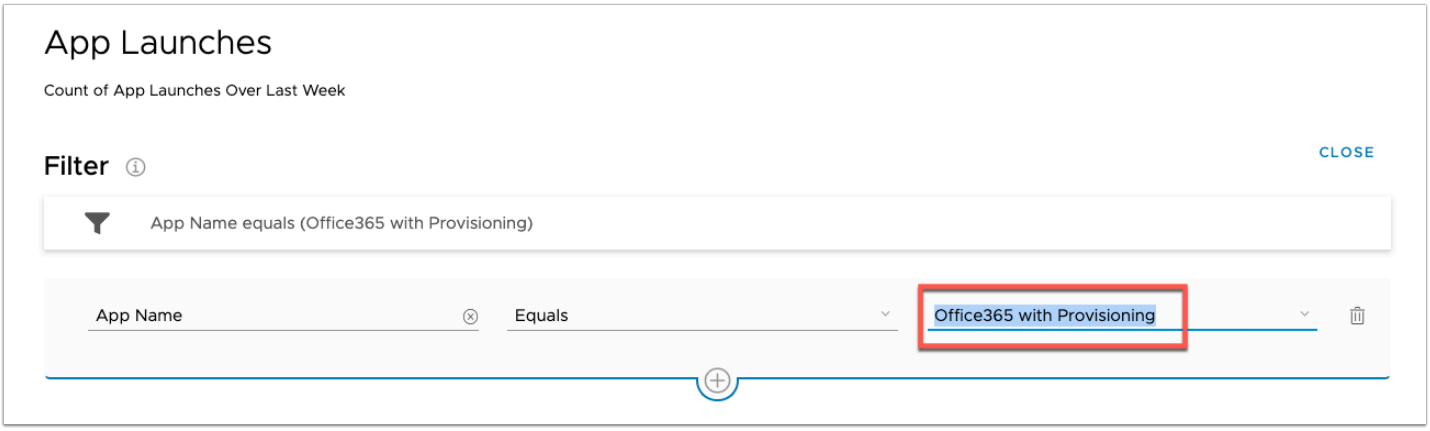
3. In the **ADD WIDGET** window
   1. Next to **CATEGORY** select the **drop down**
   2. Select **Workspace ONE Access** > **APP LAUNCH**



4. We will now have the option to create from blank widget or existing widget.
   1. In the Template Name Column select the radio button next to **App Launches** (second one from the top)
   2. Select **NEXT** in the bottom right corner.



5. In the **App Launches** window under the **Filter** heading
   - Select **App Name** > **Equals** > **Office 365 with Provisioning**. (**NOTE**: If you have done the Deep Links lab, Select **Word**)



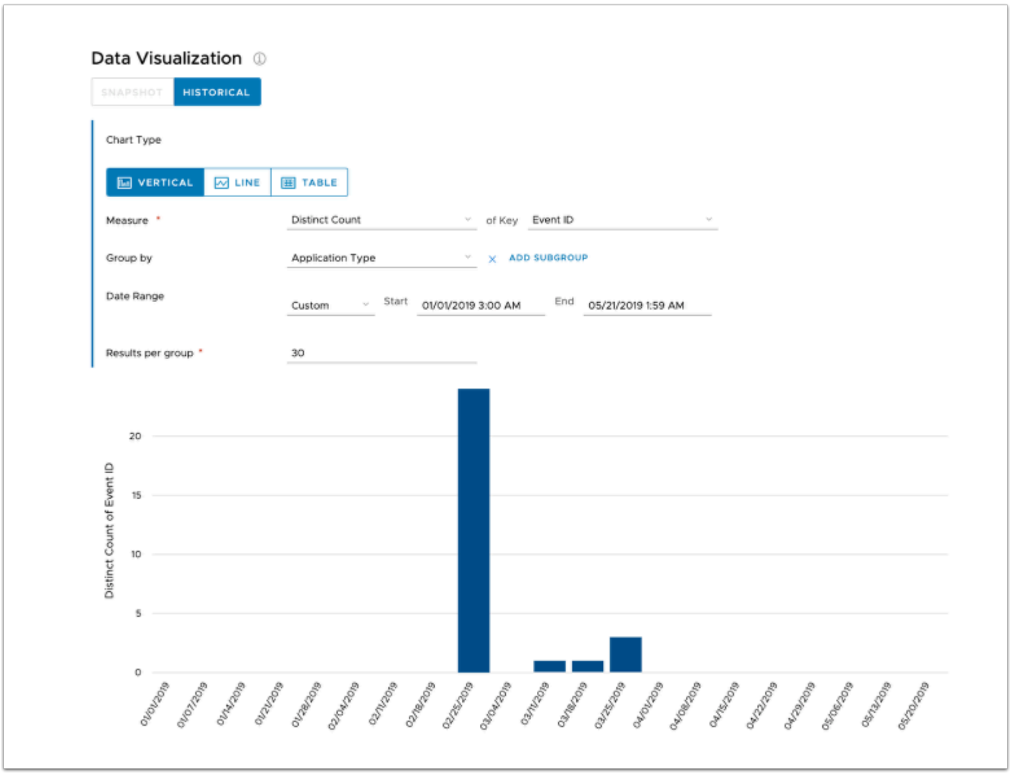
App Name equals (Office365 with Provisioning)

App Name | Equals | Office365 with Provisioning

6. Under **Data Visualization**
   1. Next to **SNAPSHOT** select **HISTORICAL**
   2. Under the **VERTICAL** tab enter the following filter: -
      1. Next to **Measure** - from the **dropdown** select **Distinct Count** and next to **of Key** from the **dropdown** select **Event ID**
      2. Next to **Group by** - from the **dropdown** select **Application Type**
      3. Next to **Date Range** - from the **dropdown** select **Custom** next to **Start 05/01/2019** next to **End {todays date}**
      4. Next to **Results per group** - type **30**

- You will now get a data visualization of the times someone access this particular application within a give time period.

3. Select **SAVE** at the bottom right to close the wizard.



Data Visualization

Chart Type

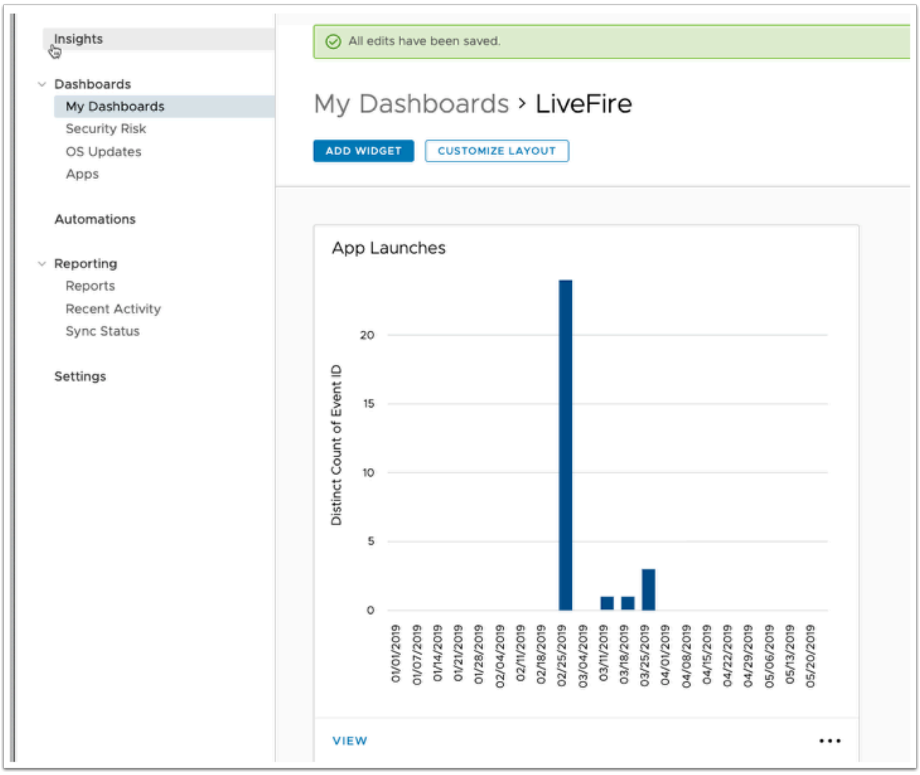
Measure * Distinct Count of Key Event ID

Group by Application Type

Date Range Custom Start 01/01/2019 3:00 AM End 05/21/2019 1:59 AM

Results per group * 30

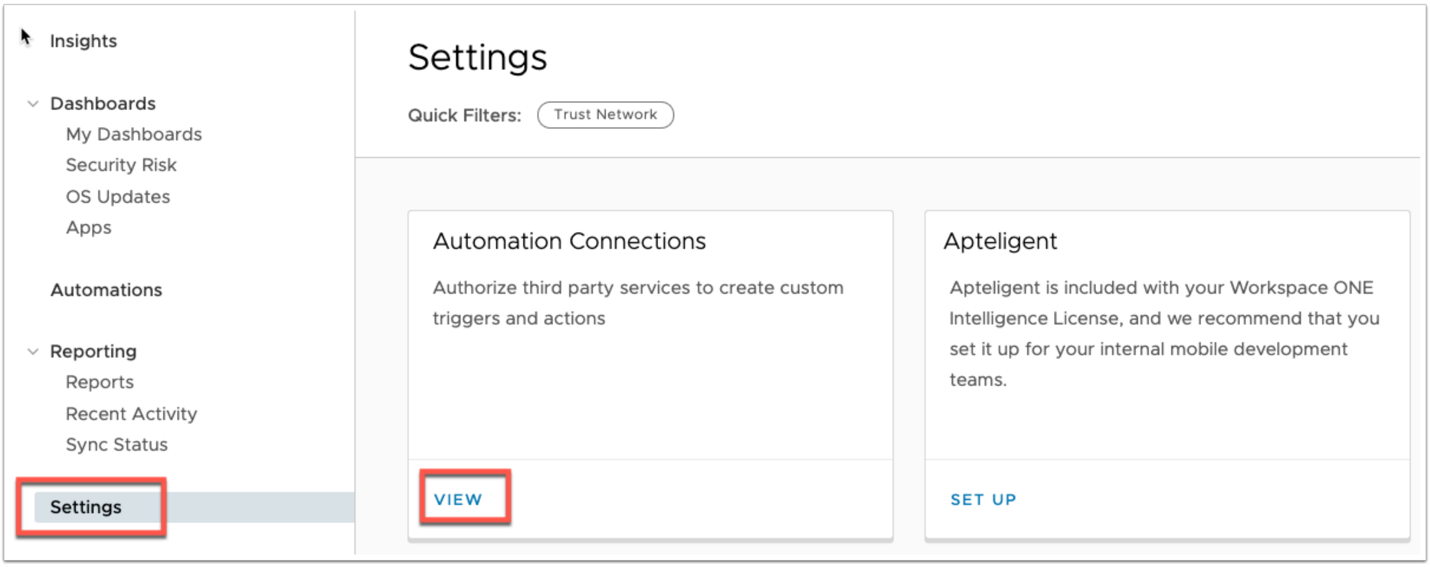
7. You will now see the the LiveFire Dashboard has one widget "App Launches" with very specific data visualized for the admin to consume.



Part 4: Automation

Automation requires the use of "Connectors" to connect to other services via API to execute a sub set of commands based on the input. Currently, Automation is possible out of box with Workspace ONE UEM, Slack and ServiceNow. You can create a custom connection as well. In this example, we will use Workspace ONE UEM as a connector to trigger actions based on the aggregated information.

1. In **Workspace ONE Intelligence**
    1. In the left pane under **Insights**, go to the **Settings** section, select **Integrations**
    2. Under **Automation Connections** select **VIEW**
        - Notice there are three connectors there by default Slack, Workspace ONE UEM, and ServiceNow. This is an ever growing link as VMware continue to partner with vendors.



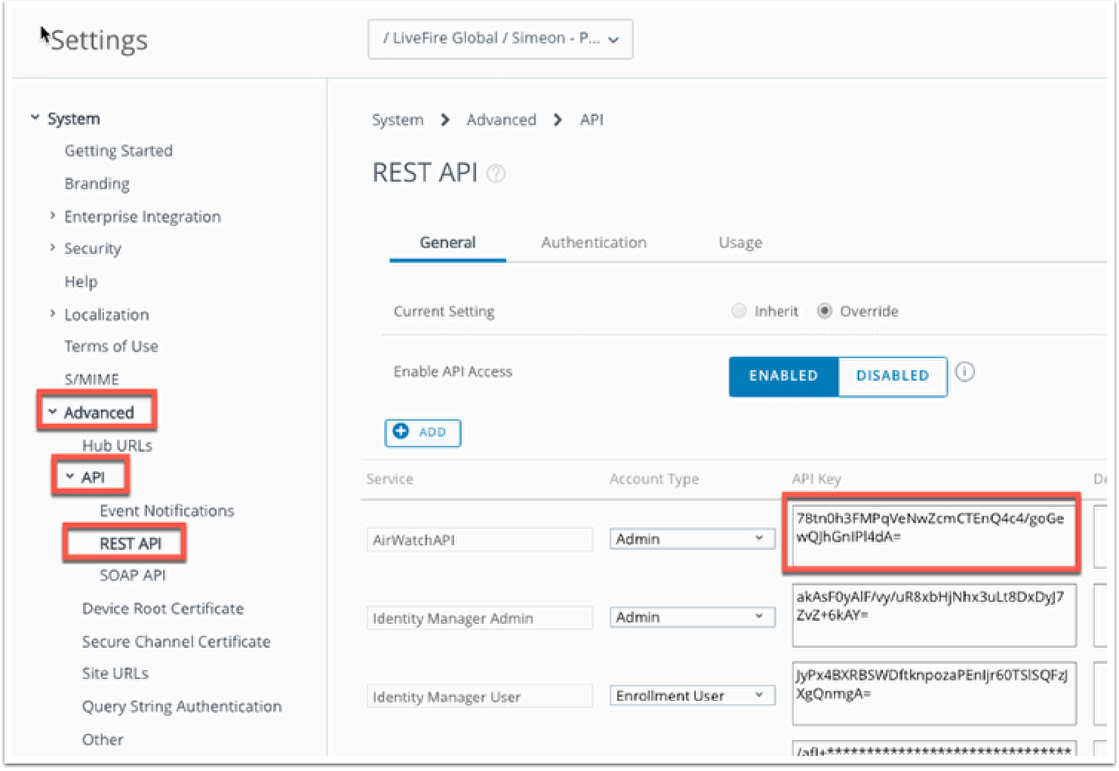
Automation Connections

Authorize third party services to create custom triggers and actions

Apteligent

Apteligent is included with your Workspace ONE Intelligence License, and we recommend that you set it up for your internal mobile development teams.

2. Open a **new tab** if necessary in your browser and revert back to the **Workspace ONE UEM** Console
   1. Select **Groups & Settings** > **All Settings** > **System** > **Advanced**
   2. Expand **API** select **REST API.**
   3. Under **Service** next to **AirWatchAPI** copy the **API key** to Notepad or an equivalent text editor



Current Setting ○ Inherit ● Override

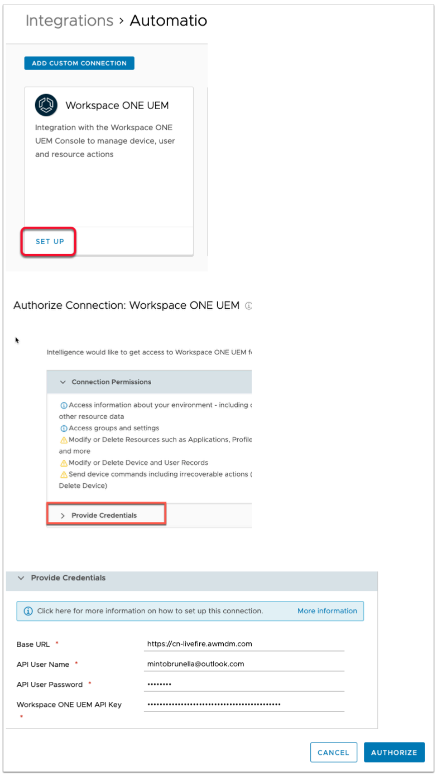
Enable API Access ENABLED DISABLED

Service	Account Type	API Key	De
AirWatchAPI	Admin	78tn0h3FMPqVeNwZcmCTEnQ4c4/goGewQJhGnIPl4dA=	
Identity Manager Admin	Admin	akAsF0yAlF/vy/uR8xbHjNhx3uLt8DxDyJ7ZvZ+6kAY=	
Identity Manager User	Enrollment User	JyPx4BXRBSWDftknpozaPEnIjr60TSlSQFzJXgQnmgA=	
		/afl+********************************	

3. Revert back to **Workspace ONE Intelligence.** In the **Integrations > Automation Connections** section

1. Under the **Workspace ONE UEM** connector, select **SET UP**
2. In the **Authorize Connection: Workspace ONE UEM**, select **Provide Credentials**
3. Fill in the information with your Workspace ONE UEM credentials:
   - **BASE URL :** https://cn-livefire.awmdm.com
   - **API User Name** : **Your login credentials for your Workspace ONE Tenant**
   - **API user Password** : **Password of your Workspace ONE UEM Tenant**
   - **Workspace ONE UEM Tenant Code** : **API Admin Key from Workspace ONE UEM**

4. Select **Authorize**



Integration with the Workspace ONE UEM Console to manage device, user and resource actions

Authorize Connection: Workspace ONE UEM

Intelligence would like to get access to Workspace ONE UEM f

Connection Permissions

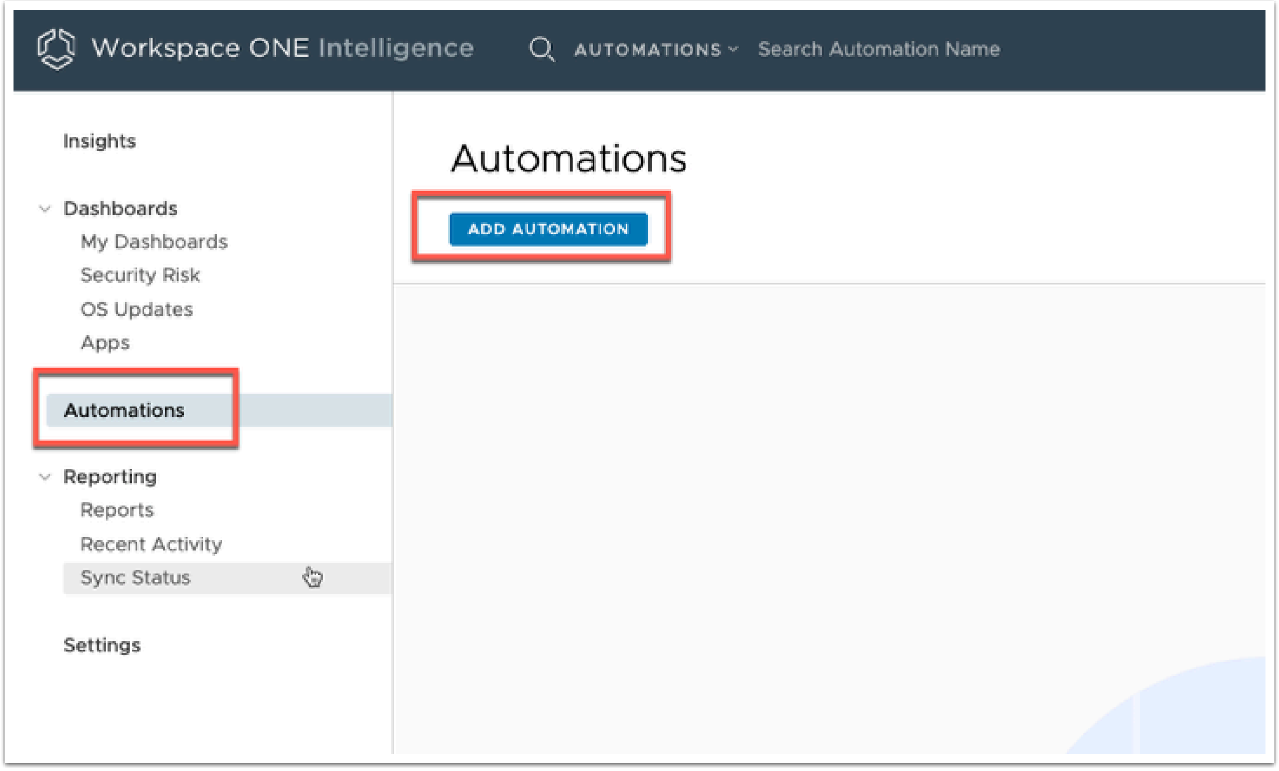
- Access information about your environment - including other resource data
- Access groups and settings
- Modify or Delete Resources such as Applications, Profile and more
- Modify or Delete Device and User Records
- Send device commands including irrecoverable actions (Delete Device)

Provide Credentials

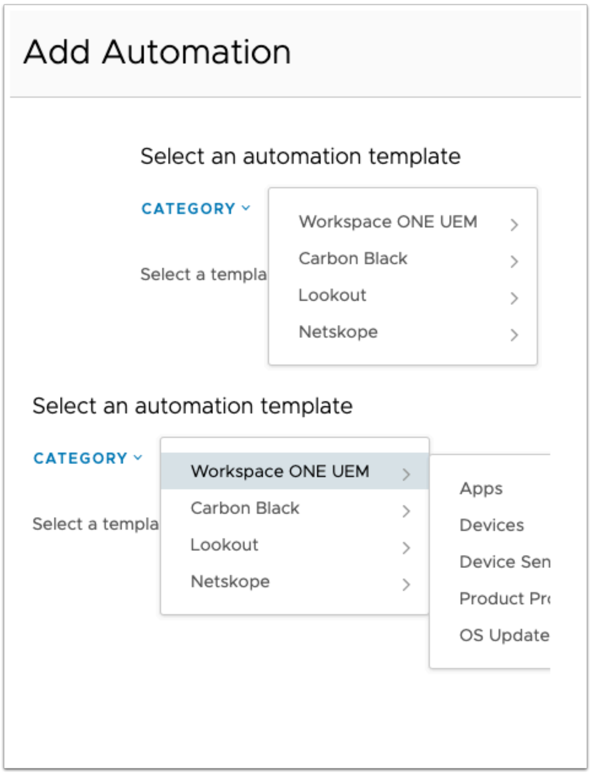
Click here for more information on how to set up this connection. More information

Base URL *	https://cn-livefire.awmdm.com
API User Name *	mintobrunella@outlook.com
API User Password *	••••••••
Workspace ONE UEM API Key *	••

4. Now that the connector for WorkspaceOne Workspace ONE UEM has been configured for Automation. Let's build an Automation!
   - Navigate inside the Workspace ONE Intelligence Console click Automations **ADD AUTOMATION**

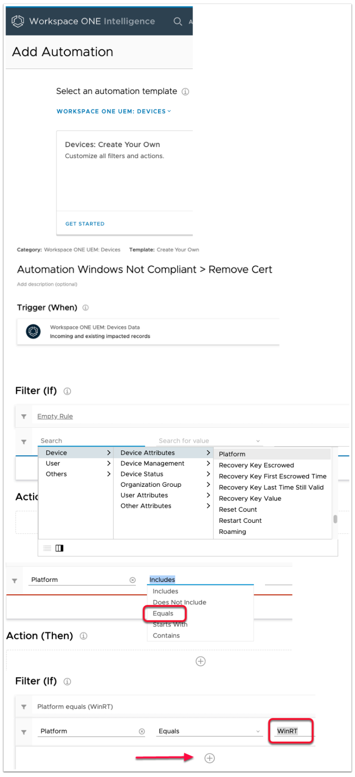


5. In the **Add Automation** window
    1. Next to **Category** select the **drop down**
    2. Select **Workspace ONE UEM** > Devices



6. In the Add Automation window
    1. In the **Devices: Create Your Own** section select **GET STARTED**

2. In the **Name your automation** section type **Automation Windows Not Compliant > Remove Cert**
3. Under **Filter (If)**
    - In the **Search** area select **Device** > **Device Attributes** > **Platform**
    - To the right of **Platform** select the **Includes** **dropdown** and change to **Equals**
    - In the area to the right of **Includes** select **WinRT**
    - Just below your **first filter** in the middle select the **?**



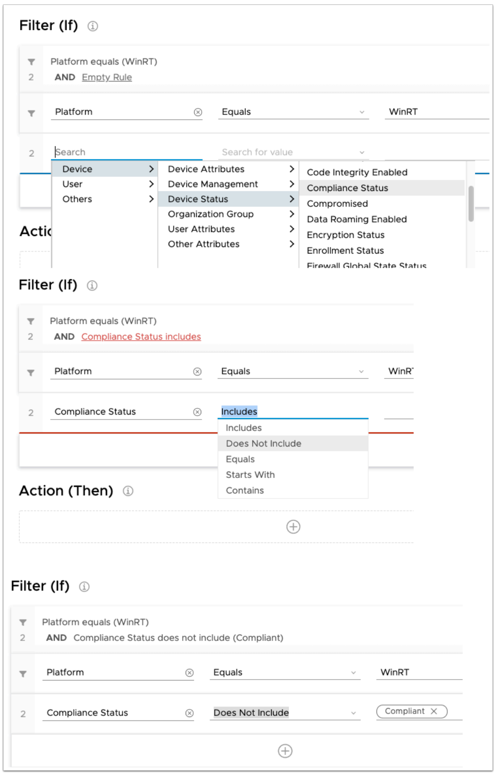
Category: Workspace ONE UEM: Devices **Template:** Create Your Own

Automation Windows Not Compliant > Remove Cert

Platform equals (WinRT)

Platform Equals WinRT

7. Under **Filter (If)** under **Platform** in the **Search** area
    1. In the **Search** area select **Device** > **Device Status** > **Compliance Status**
    2. To the right of **Compliance Status** select the **Includes** **dropdown** and change to **Does not Include**
    3. In the area to the right of **Does not Include** select **Compliant**



Filter (If)

Platform equals (WinRT)
2 AND Empty Rule

Platform | Equals | WinRT

2 Search | Search for value

Filter (If)

Platform equals (WinRT)
2 AND Compliance Status includes

Platform | Equals | WinRT

2 Compliance Status | Includes

Filter (If)

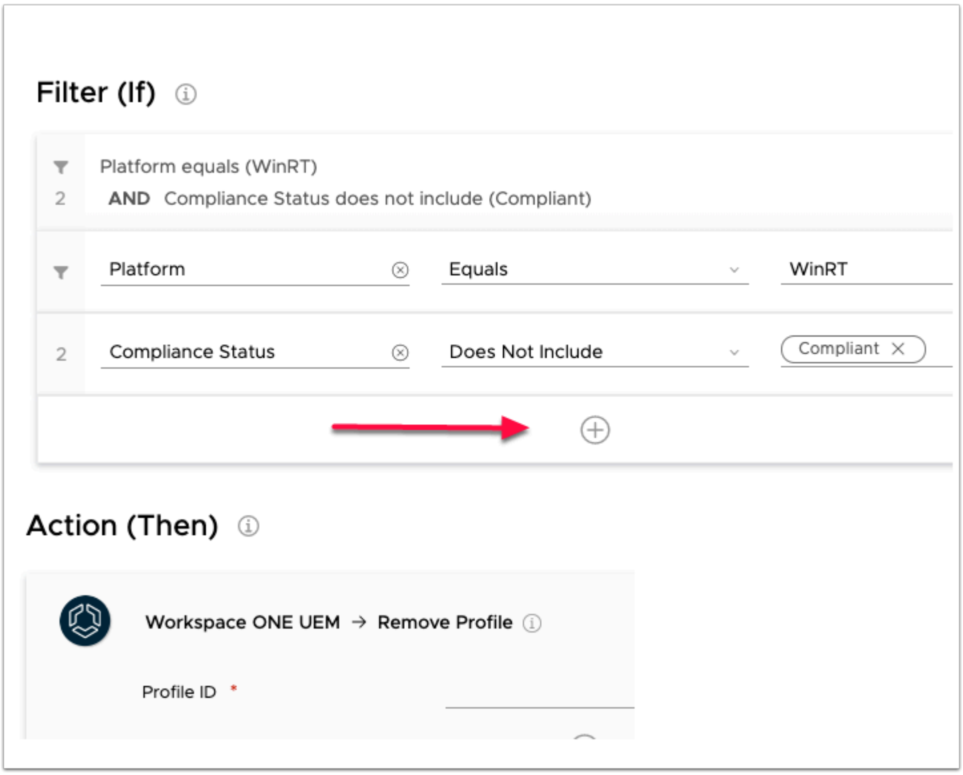
Platform equals (WinRT)
2 AND Compliance Status does not include (Compliant)

Platform | Equals | WinRT

2 Compliance Status | Does Not Include | Compliant

8. Below your filters In the **Action (Then**) area
   1. Select the **?**
   2. Under **Action (Then)** in the **Search fot trigger or connections area**, in the **drop down** select **Workspace ONE UEM ---> Remove Profile**

- We now need to get the **Profile ID**. Get this from the **Workspace ONE UEM** Console



Filter (If)

Platform equals (WinRT)
2 AND Compliance Status does not include (Compliant)

Platform | Equals | WinRT

2 Compliance Status | Does Not Include | Compliant

Action (Then)

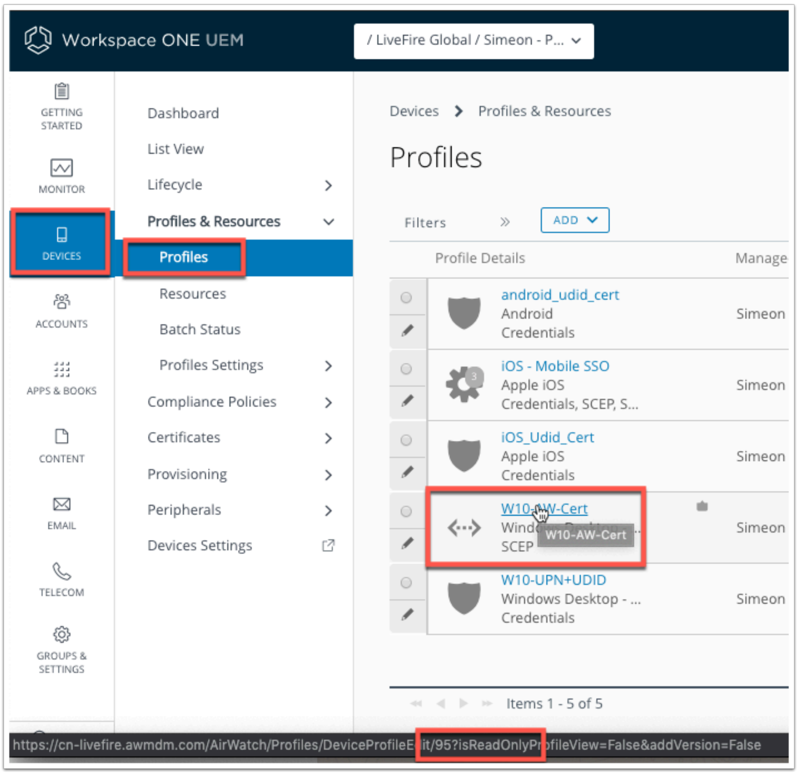
Workspace ONE UEM → Remove Profile

Profile ID *

9. In the Workspace ONE UEM Console
    1. Go to **Devices**> Profiles & Resources > **Profiles**.
    2. Point to the applicable Windows SSO profile in the Profiles List View to display the item's URL in the bottom left of the browser.
        - Find the ID number located in the middle of the string.

An example of the string is:

https://<Workspace_ONE_Workspace ONE UEM>/AirWatch/Profiles/DeviceProfileEdit/**95**?isReadOnlyProfileView=x.

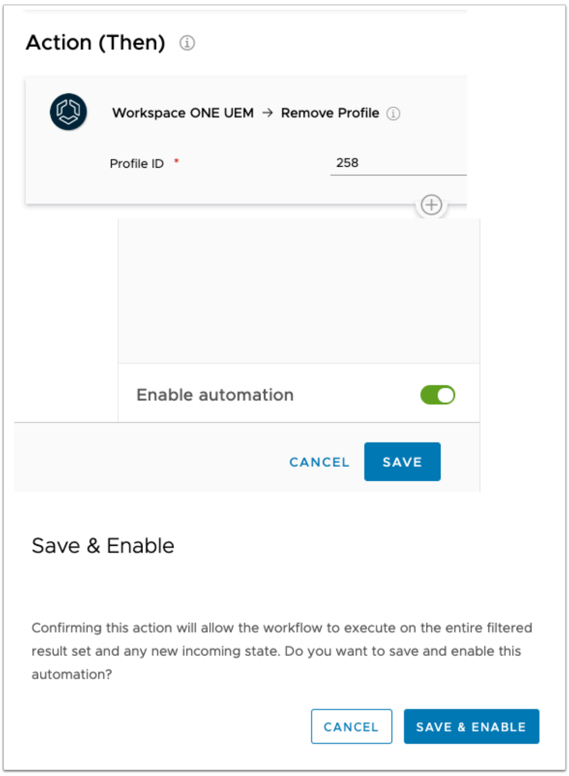


https://cn-livefire.awmdm.com/AirWatch/Profiles/DeviceProfileEdit/95?isReadOnlyProfileView=False&addVersion=False

10. Go back to your Workspace ONE Intelligence Console
    1. Use the unique number in your URL string and next to **Profile ID** type in the **UNIQUE NUMBER**
    2. In the far right next to **Enable automation** change the to **Toggle** from **OFF** to **ON**
    3. Select **SAVE**
    4. Select **Save and Enable**

You have now finished the Automation that lets us Automate actions into WorkspaceOne Workspace ONE UEM based on triggers. This completes the Intelligence lab.

Note, you can choose to take multiple actions like emailing the user, changing organization group or even removing multiple applications and profiles from the device.



Action (Then)

Workspace ONE UEM → Remove Profile

Profile ID * 258

Enable automation

Save & Enable

Confirming this action will allow the workflow to execute on the entire filtered result set and any new incoming state. Do you want to save and enable this automation?

Advanced API Automation

Overview

This lab will provide hands on training to leverage APIs to perform Automation task in your Workspace ONE UEM Environment. We will use POSTMAN to demonstrate the API automation.

In the industry today, DevOps, Operations and Support teams are leveraging API capability to automate application releases, minimize human interaction and achieve faster troubleshooting. In this lab we will learn how to use these APIs by making a collection of API calls for our DevOps use case.

Use Case: Developer team releases weekly updates to business critical application. Built an automation for this application release to our production devices.

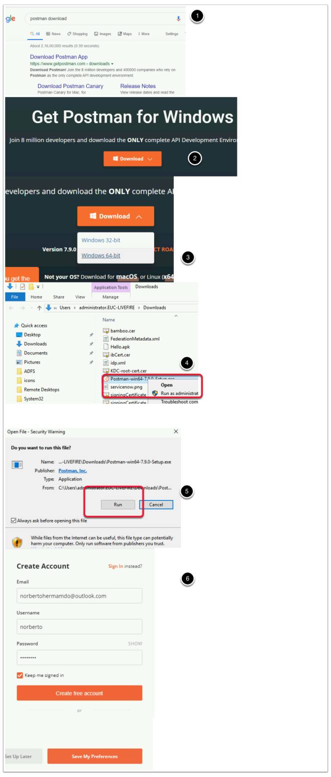
This section has 2 parts

- Setting UP Postman•
- Accessing the Workspace ONE UEM ApI

Part 1: Setting Up Postman

Log in to your **Controlcenter** server with your administrative credentials

1. Open your **chrome browser** in the google search type **Postman download.** Select the option to **Download Postman App**
2. In the Get Postman for Windows select **Download**
3. Select the **Windows 64bit** version to download
4. Open your **Downloads** folder on select and **Open** the **Postman-win64. xx** installer
5. Select **Run**
6. After the installer has finished you will be prompted to **Sign UP**
   1. In the **Email** section type an **email** (possibly a dummy email you used in previous labs)
   2. Fill in **Username**
   3. **Password** VMware1!
   4. Select **Create free account**
7. On the Welcome to Postman page select **Save My Preferences**



About 2,16,00,000 results (0.39 seconds)

Download Postman App
https://www.getpostman.com › downloads
Download Postman! Join the 8 million developers and 400000 companies who rely on Postman as the only complete API development environment.

Download Postman Canary
Postman Canary for Mac. for

Release Notes
View release dates and read the

Get Postman for Windows

Join 8 million developers and download the ONLY complete API Development Enviro

Version 7.9.0

Not your OS? Download for macOS or Linux (x64

Users › administrator.EUC-LIVEFIRE › Downloads

bamboo.cer
FederationMetadata.xml
Hello.apk
ibCert.cer
idp.xml
KDC-root-cert.cer
Postman-win64-7.9.0-Setup.exe
servicenow.png
signingCertificate
signingCertificate

Open File - Security Warning

Do you want to run this file?

Name: ...-LIVEFIRE\Downloads\Postman-win64-7.9.0-Setup.exe
Publisher: Postman, Inc.
Type: Application
From: C:\Users\administrator.EUC-LIVEFIRE\Downloads\Post...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.

Create Account — Sign In instead?

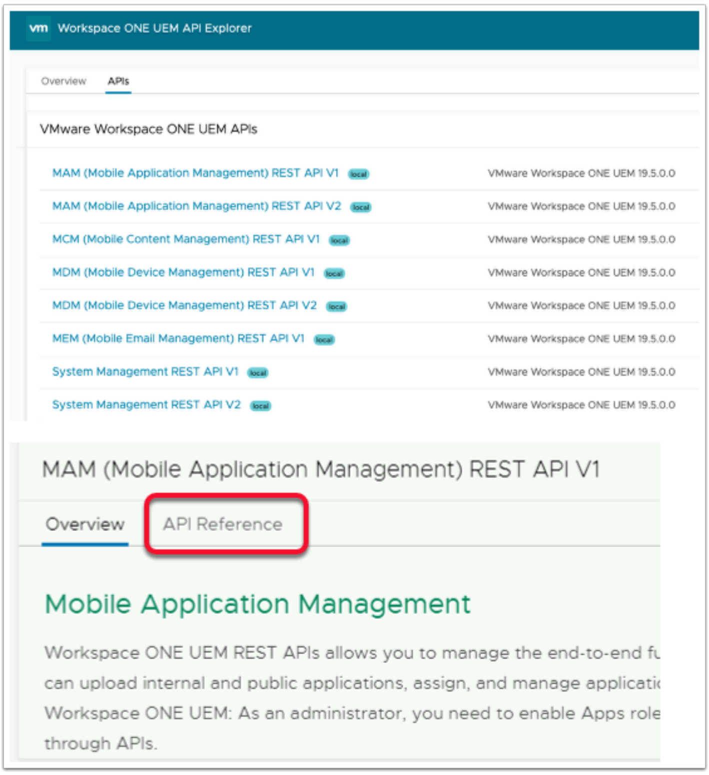
Email: norbertohermamdo@outlook.com
Username: norberto
Password: •••••••• SHOW
☑ Keep me signed in

or

Part 2: Accessing the Workspace ONE UEM API

All the REST API calls are listed in the API portal. You can access the portal by navigating to https://<WorkspaceONE *UEM URL*>/api/help.

1. On your **ControlCenter** server, open your browser and navigate to **https://cn-livefire.awmdm.com/api/help**
2. You will notice you are the default **Overview** page. Click on the **APIs.** tab.
3. Select and open the **MAM (Mobile Application Management) REST API V1** module.
   - One can use the search capability to search for desired API calls' using the **Search APIs/** Method field and then typing the name of the API.
4. In the **MAM (Mobile Application Management) REST API V1** you will land on the **Overview** page, select the **API Reference tab**



VMware Workspace ONE UEM APIs

MAM (Mobile Application Management) REST API V1 local	VMware Workspace ONE UEM 19.5.0.0
MAM (Mobile Application Management) REST API V2 local	VMware Workspace ONE UEM 19.5.0.0
MCM (Mobile Content Management) REST API V1 local	VMware Workspace ONE UEM 19.5.0.0
MDM (Mobile Device Management) REST API V1 local	VMware Workspace ONE UEM 19.5.0.0
MDM (Mobile Device Management) REST API V2 local	VMware Workspace ONE UEM 19.5.0.0
MEM (Mobile Email Management) REST API V1 local	VMware Workspace ONE UEM 19.5.0.0
System Management REST API V1 local	VMware Workspace ONE UEM 19.5.0.0
System Management REST API V2 local	VMware Workspace ONE UEM 19.5.0.0

MAM (Mobile Application Management) REST API V1

Mobile Application Management

Workspace ONE UEM REST APIs allows you to manage the end-to-end fu
can upload internal and public applications, assign, and manage applicati
Workspace ONE UEM: As an administrator, you need to enable Apps role
through APIs.

Part 3: DevOps Automation

- To meet our use case, DevOps needs the capability of uploading the application to the UEM console, create and assign smart group and publish to specific devices. We will use a total of 4 API calls to achieve the same.

Step 1: Upload Application

> ℹ Uploading the application in the console comprises of two POST API commands.
>
> 1. uploadblob: Uploads the apk as a blob to the database server.
> 2. begininstall: Creates an internal application using the uploaded file blob.

1. Search **uploadblob** in the **Search APIs/** Method field.

2. Next to **POST**, Click on **blobs/uploadblob**

3. Scroll down to the Parameters field and Enter the required fields next to

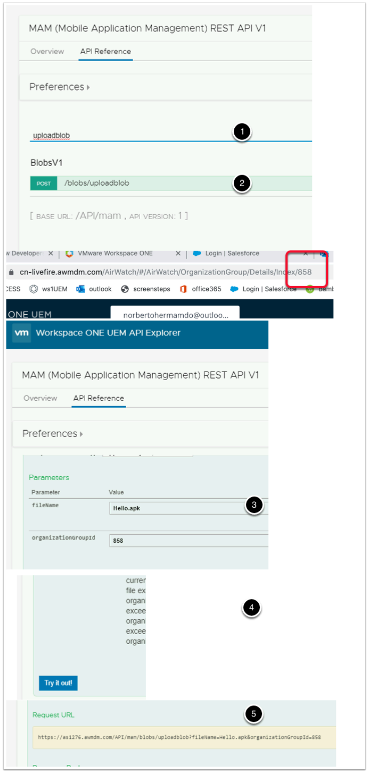
- **filename** : **Hello.apk**
- **organizationGroupId: your oganizationGroupID**

Note: In your **Workspace ONE UEM** Console, browse to **Groups & Settings** > Groups > Organization Groups > Details. Look in the address bar of your browser and the last digits will be a /number combination . **Copy the ID** from **the Browser** URL. For example: **https://cn-**

livefire.awmdm.com/AirWatch/#/AirWatch/OrganizationGroup/Details/Index/722. In this case, 722 is the **organizationGroupId**, **copy this number** to **organizationGroupID** field

4. Scroll right down to the bottom of the page and Click **Try it out!**.

5. Scroll down to see the response of your API call. **Copy** and **Paste** the **Request URL** in the response to **Notepad++.**



MAM (Mobile Application Management) REST API V1

Overview | API Reference

Preferences ▸

uploadblob

BlobsV1

POST /blobs/uploadblob

[BASE URL: /API/mam , API VERSION: 1]

cn-livefire.awmdm.com/AirWatch/#/AirWatch/OrganizationGroup/Details/Index/858

Workspace ONE UEM API Explorer

Parameters

Parameter	Value
fileName	Hello.apk
organizationGroupId	858

Request URL

```
https://as1276.awmdm.com/API/mam/blobs/uploadblob?fileName=Hello.apk&organizationGroupId=858
```

Note: We will use Postman tool to make our API calls and create Automation.

6. Navigate to the **ControlCenter2** Server. Find the Postman icon on your desktop screen. **Open** Postman application.

7. Click **Request.**

8. In the **SAVE REQUEST** Window in the **Request Name** section type **DevOps Upload Blob**.

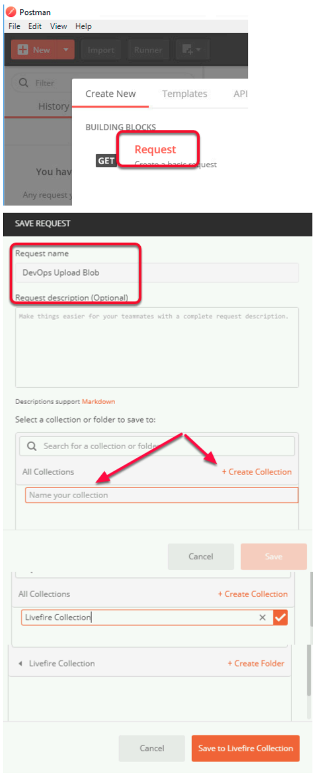
This is the first API call you are creating.

9. Scroll down to **+Create Collection**. and click on **+Create Collection**

10. In the **Name your Collection** area name it **Livefire collection.**

11. Select the **orange tick box** to the right of your entry

12 Click **Save to Livefire Collection.**



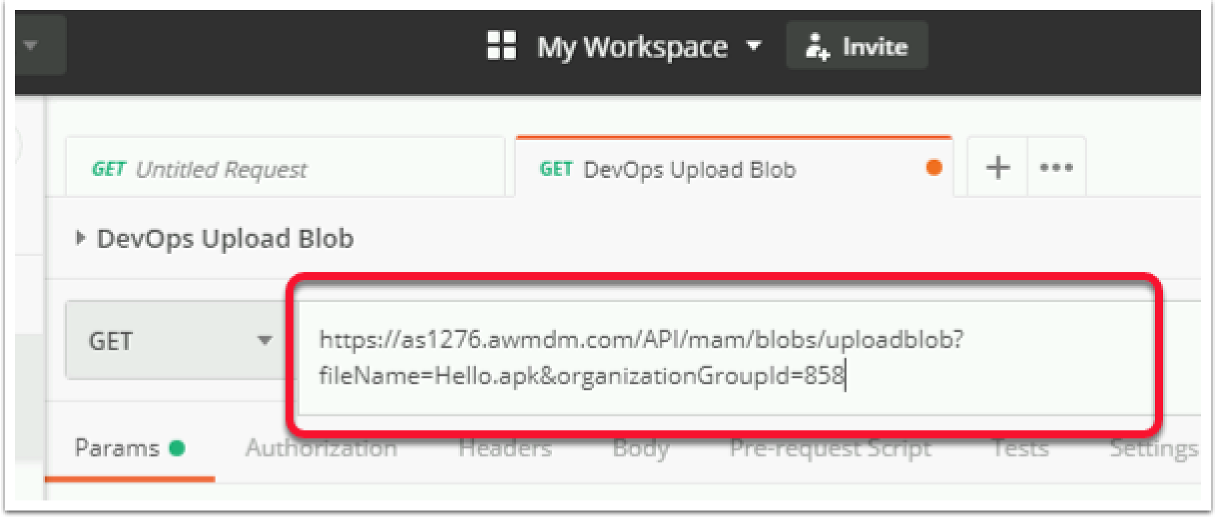
Request name: DevOps Upload Blob

Request description (Optional): Make things easier for your teammates with a complete request description.

Select a collection or folder to save to:

Name your collection: Livefire Collection

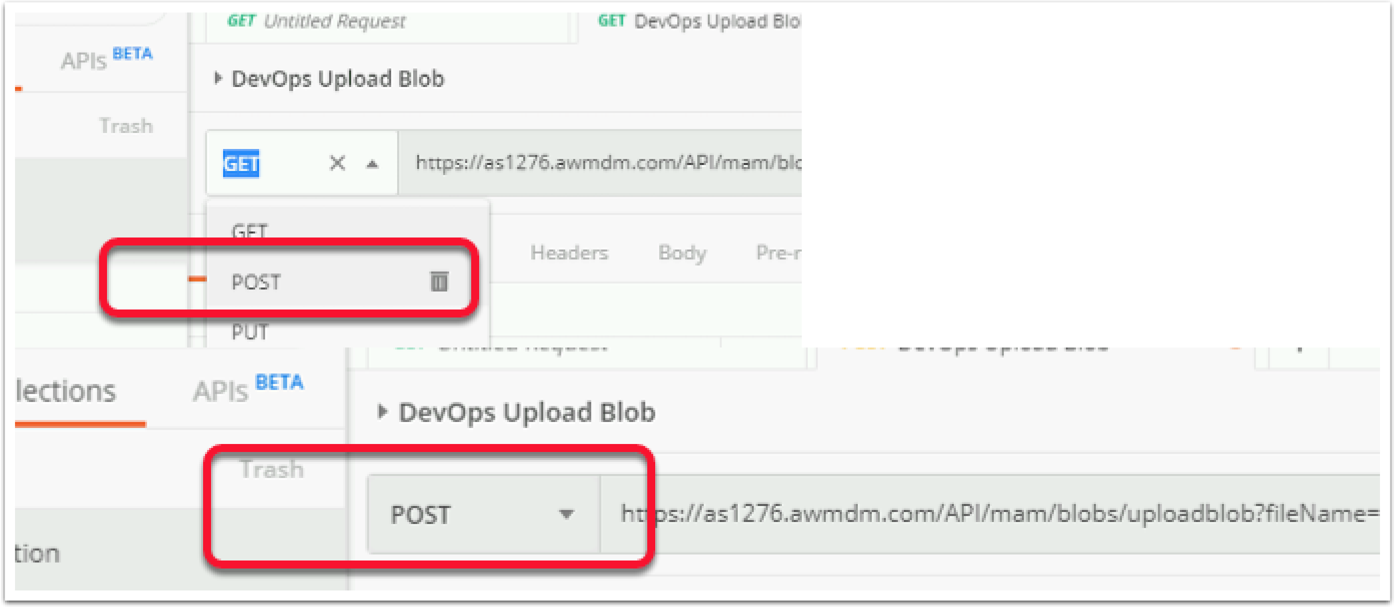
12. Next to **GET**, Paste the copied **Request URL** in the **Enter Request URL** field in Postman.



```
https://as1276.awmdm.com/API/mam/blobs/uploadblob?fileName=Hello.apk&organizationGroupId=858
```

13. Change the Request type from **GET** to **POST**.

    Note the Params value is now populated.

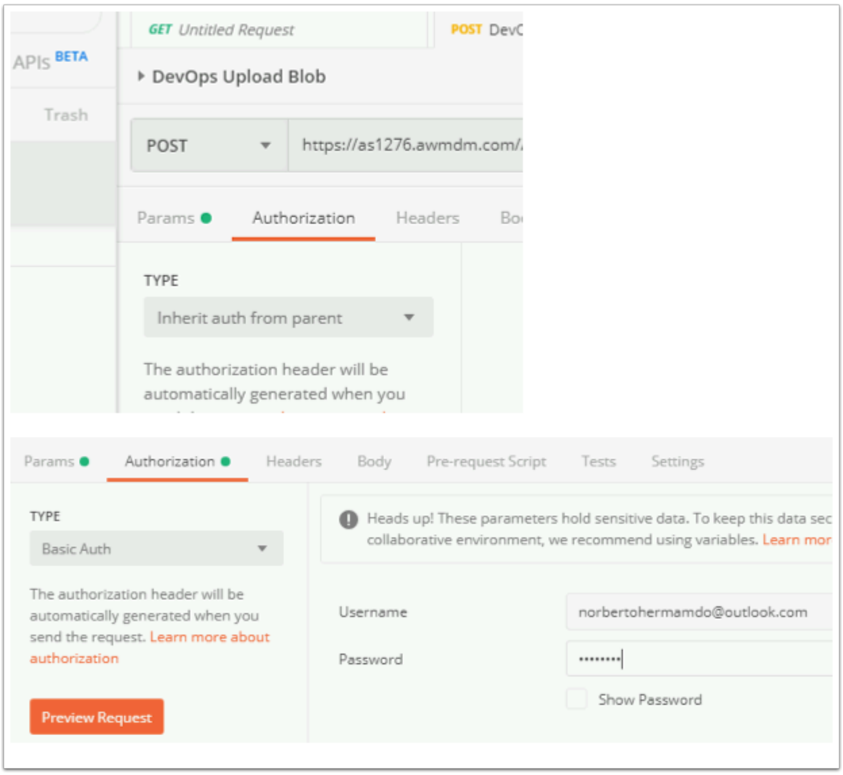


POST https://as1276.awmdm.com/API/mam/blobs/uploadblob?fileName=

14. Below **POST** next to **Params** select the **Authorization** tab,

15. Below the **TYPE** area select the **drop down** and change **inherit auth from parent** to Basic Auth.

16. Provide your **Workspace ONE UEM admin credentials** in the **Username** and **Password** field.



TYPE: Inherit auth from parent

The authorization header will be automatically generated when you

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data sec collaborative environment, we recommend using variables. Learn mor

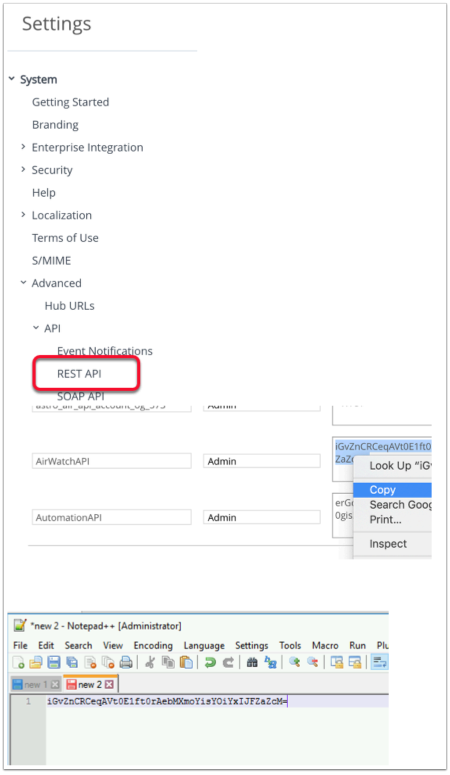
Username: norbertohermamdo@outlook.com

Password: ••••••••

□ Show Password

17. Switch back to the Workspace ONE UEM console

- Go **Groups & Settings** > **ALL Settings** > **System** > **Advanced** > **API** > **REST API**
- In the **REST API** section next the **AirWatchAPI - ADMIN** section **select** and **copy** the **API KEY**
- **Note Save** the API key to **Notepad++**



Settings

- System
  - Getting Started
  - Branding
  - Enterprise Integration
  - Security
  - Help
  - Localization
  - Terms of Use
  - S/MIME
  - Advanced
    - Hub URLs
    - API
      - Event Notifications
      - REST API
      - SOAP API

AirWatchAPI	Admin	iGvZnCRCeqAVt0E1ft0 ZaZ
AutomationAPI	Admin	erG 0gis

Look Up "iG
Copy
Search Goog
Print...
Inspect

*new 2 - Notepad++ [Administrator]

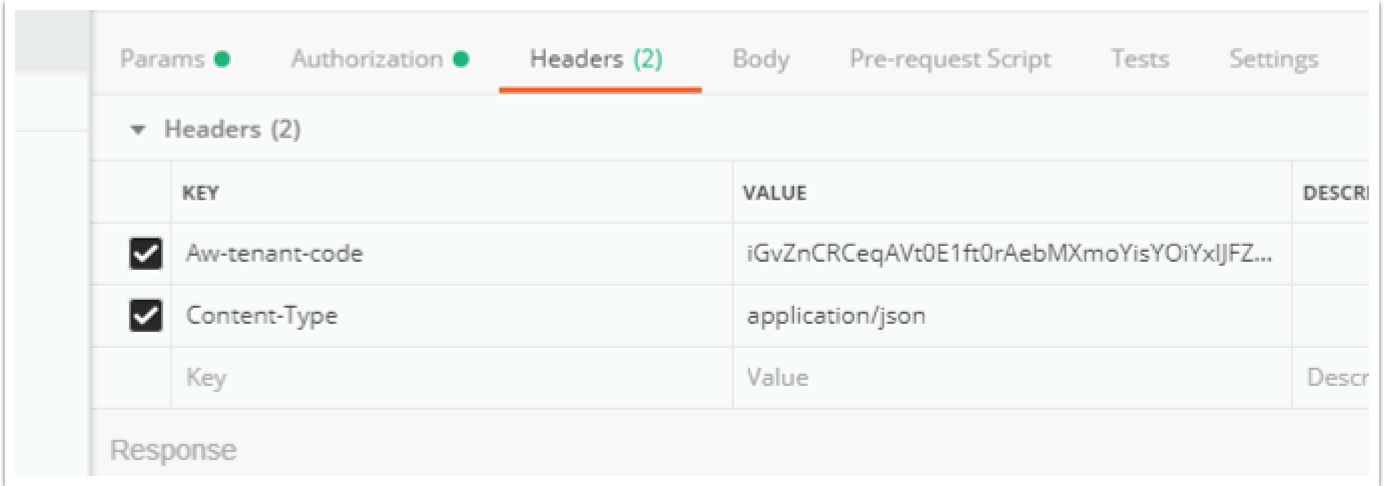
File Edit Search View Encoding Language Settings Tools Macro Run Plu
new 1
new 2

```
iGvZnCRCeqAVt0E1ft0rAebMXmoYisYOiYxIJFZaZcM=
```

18. Switch back to **PostMan** . On the next tab next to **Authorization** select **Headers,**

- Add the following under the **KEY** and **VALUE** areas

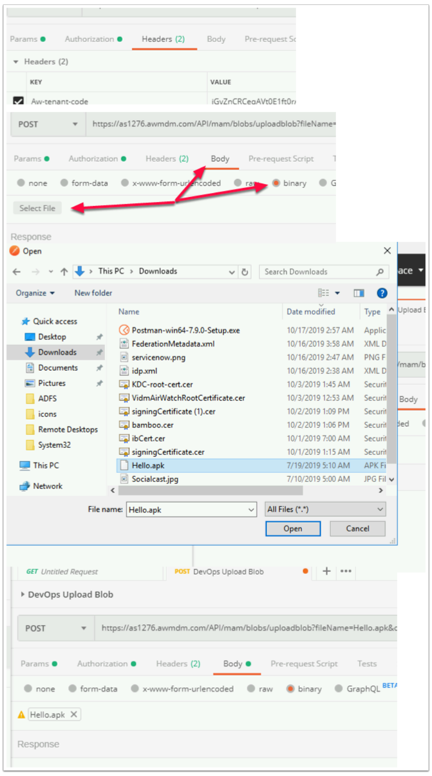
KEY	**VALUE**
Aw-tenant-code	*YOUR API ADMIN KEY*
Content-Type	application/json



	KEY	VALUE	DESCRI
☑	Aw-tenant-code	iGvZnCRCeqAVt0E1ft0rAebMXmoYisYOiYxIJFZ...	
☑	Content-Type	application/json	
	Key	Value	Descr

19. Next to the **Headers** tab, switch to the **Body** tab

- In the **Body** section select the **Binary** radio button
- In the **Binary** section click on **Select File**.
- Browse to the **Downloads** folder and select the **Hello.apk** file. Select **Open.**



POST https://as1276.awmdm.com/API/mam/blobs/uploadblob?fileName=

KEY	VALUE
☑ Aw-tenant-code	iGvZnCRCeqAVt0E1ft0r

Name	Date modified	Type
Postman-win64-7.9.0-Setup.exe	10/17/2019 2:57 AM	Applic
FederationMetadata.xml	10/16/2019 3:58 AM	XML D
servicenow.png	10/16/2019 2:47 AM	PNG F
idp.xml	10/16/2019 2:38 AM	XML D
KDC-root-cert.cer	10/3/2019 1:45 AM	Securi
VidmAirWatchRootCertificate.cer	10/3/2019 12:53 AM	Securi
signingCertificate (1).cer	10/2/2019 1:09 PM	Securi
bamboo.cer	10/2/2019 1:06 PM	Securi
ibCert.cer	10/1/2019 7:00 AM	Securi
signingCertificate.cer	10/1/2019 1:15 AM	Securi
Hello.apk	7/19/2019 5:10 AM	APK Fi
Socialcast.jpg	7/10/2019 5:00 AM	JPG Fil

File name: Hello.apk

All Files (*.*)

DevOps Upload Blob

POST https://as1276.awmdm.com/API/mam/blobs/uploadblob?fileName=Hello.apk&c

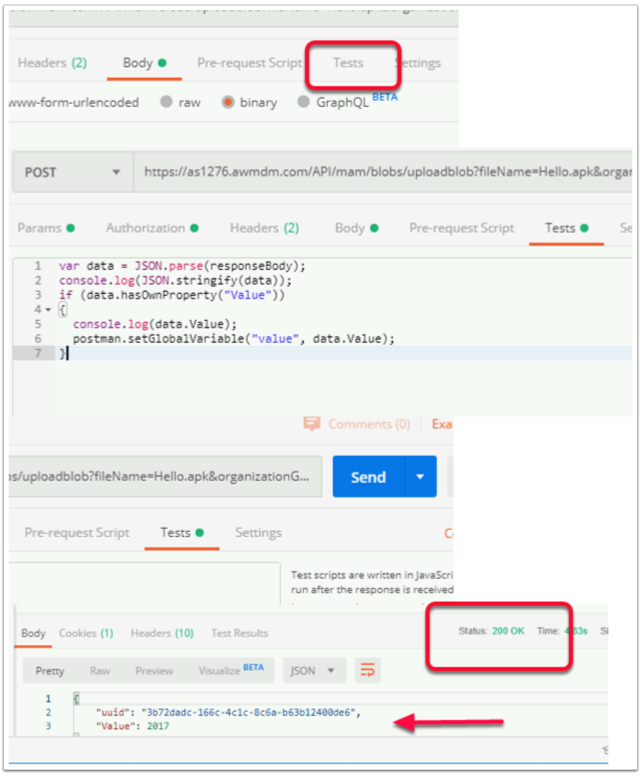
○ none ○ form-data ○ x-www-form-urlencoded ○ raw ● binary ○ GraphQL BETA

Hello.apk

20. From the **Body** section switch two tabs across and select the **Tests** tab

- Under **Tests**, **copy** and **paste** the below ***json script.***
  - This will create a global variable **Value** and assign the response result of the blob update to this global variable.
- Click **SEND**.
  - You should see a **200 OK** next to **Status.**
  - In the body of the response, you will see **uuid** and **value** of the uploaded blob

```
var data = JSON.parse(responseBody);
console.log(JSON.stringify(data));
if (data.hasOwnProperty("Value"))
{
  console.log(data.Value);
  postman.setGlobalVariable("value", data.Value);
}
```

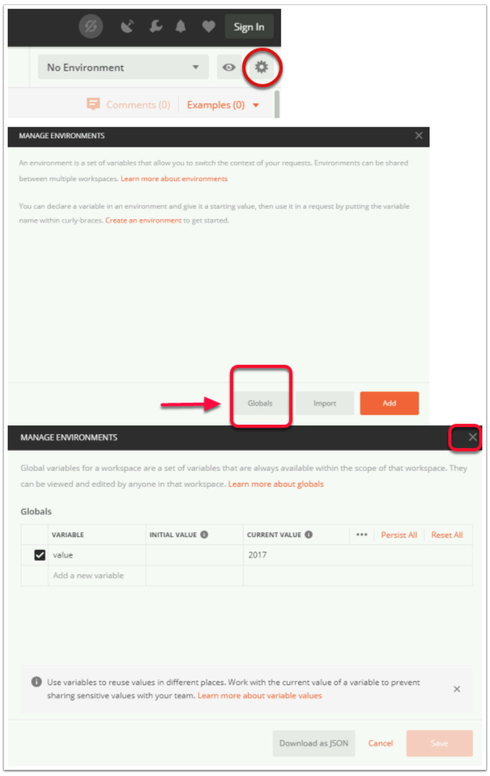


```
var data = JSON.parse(responseBody);
console.log(JSON.stringify(data));
if (data.hasOwnProperty("Value"))
{
  console.log(data.Value);
  postman.setGlobalVariable("value", data.Value);
}
```

```
{
    "uuid": "3b72dadc-166c-4c1c-8c6a-b63b12400de6",
    "Value": 2017
```

21. Before we move forward, we will check to confirm the global parameter from our previous call is created.

1. In PostMan navigate to **Settings** (Top Right cog wheel)
2. Select **Globals**
3. Check in the list if there exist an entry called **'value'** and its **CURRENT VALUE** matches the output in the response body. We will use this value in the next call.
4. Click **X** to Close the **MANAGE ENVIRONMENTS** window



MANAGE ENVIRONMENTS

An environment is a set of variables that allow you to switch the context of your requests. Environments can be shared between multiple workspaces. Learn more about environments

You can declare a variable in an environment and give it a starting value, then use it in a request by putting the variable name within curly-braces. Create an environment to get started.

MANAGE ENVIRONMENTS

Global variables for a workspace are a set of variables that are always available within the scope of that workspace. They can be viewed and edited by anyone in that workspace. Learn more about globals

Globals

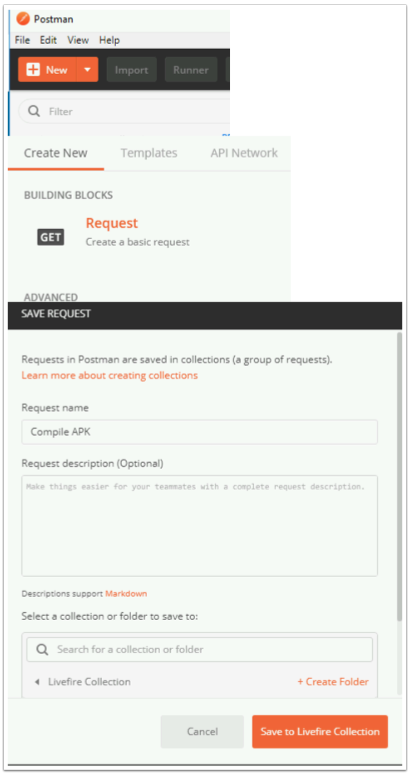
	VARIABLE	INITIAL VALUE	CURRENT VALUE	••• Persist All Reset All
☑	value		2017	
	Add a new variable			

Use variables to reuse values in different places. Work with the current value of a variable to prevent sharing sensitive values with your team. Learn more about variable values

Part 4: Creating the next API Call

Once Uploadblob is successfully executed, we will pass this blob **"value"** parameter in the next API call to save as an internal app on the console.

1.
   1. In **PostMan** Create a new tab by selecting the **+New** on the top left hand corner
   2. In the **Create New** window select **GET Request**
   3. In the **SAVE REQUEST** window under **Request name** type **Compile APK**.
   4. Select **Save to Livefire Collection.**



SAVE REQUEST

Requests in Postman are saved in collections (a group of requests).
Learn more about creating collections

Request name: Compile APK

Request description (Optional): Make things easier for your teammates with a complete request description.

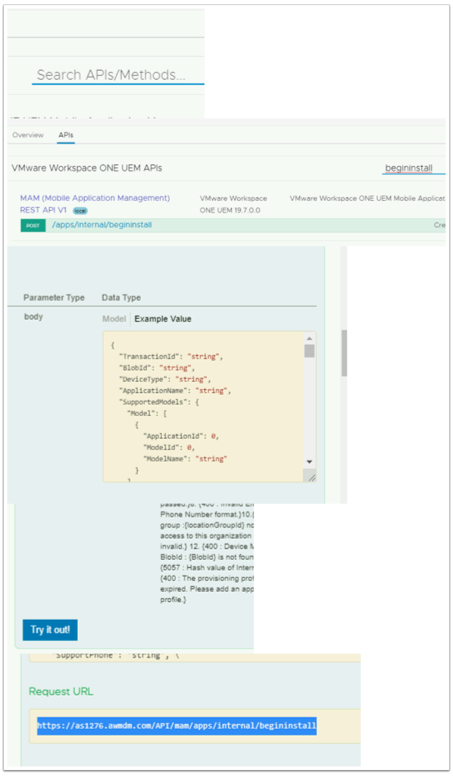
Descriptions support Markdown

Select a collection or folder to save to:

Search for a collection or folder
Livefire Collection
+ Create Folder
Cancel
Save to Livefire Collection

2. On your ControlCenter server, revert back to your browser In the address bar **https://cn-livefire.awmdm.com/api/help**

1. Under the **APIs** tab to the right in the **Search APIs/Methods** area type **begininstall**.
2. Click on **/apps/internal/begininstall** API.
3. Scroll down to **Parameters**. In the right part of **Parameters** next to **Parameter Type** you will see **Data Type**, Hover your mouse over the **yellow Data Type** box and **Click.** You will see the **appChunkTransaction** field populated on the left.
4. Scroll down and Click **Try it out!**
5. Scroll down. **Copy** the **Request URL** field in the response.



Search APIs/Methods...
Overview
APIs
VMware Workspace ONE UEM APIs
begininstall
MAM (Mobile Application Management) REST API V1
local
VMware Workspace ONE UEM 19.7.0.0
VMware Workspace ONE UEM Mobile Applicat
POST
/apps/internal/begininstall
Cre
Parameter Type
Data Type
body
Model
Example Value
Try it out!
Request URL

```
{
  "TransactionId": "string",
  "BlobId": "string",
  "DeviceType": "string",
  "ApplicationName": "string",
  "SupportedModels": {
    "Model": [
      {
        "ApplicationId": 0,
        "ModelId": 0,
        "ModelName": "string"
      }
```

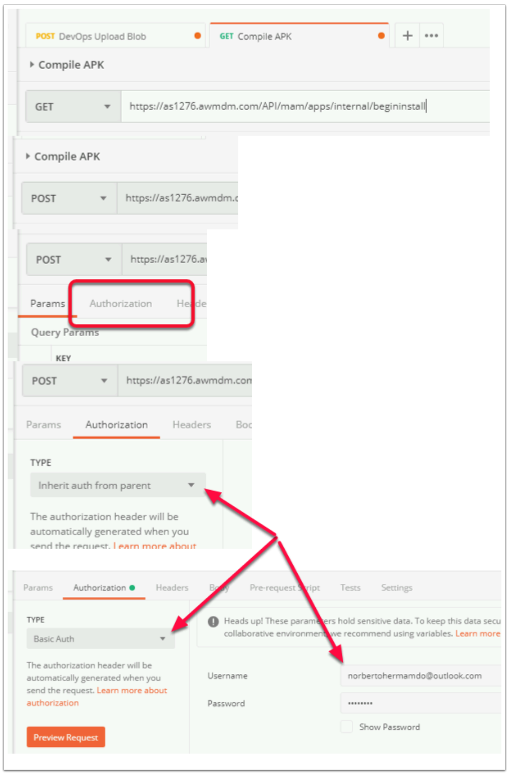
Phone Number format.}10.{
group :{locationGroupId} nc
access to this organization
invalid.} 12. {400 : Device M
BlobId : {BlobId} is not foun
{5057 : Hash value of Interr
{400 : The provisioning prof
expired. Please add an app
profile.}

"SupportPhone": "string", \

https://as1276.awmdm.com/API/mam/apps/internal/begininstall

3.

- Navigate back to **Postman**,
  1. Under the **Compile APK** tab next to **GET** in the **Enter Request URL** area, **paste the copied Request URL**.
  2. Change the command type from **GET** to **POST.**
  3. Under the newly selected **POST**. To the right of the **Params** tab select the **Authorization** tab
  4. In the **Authorization** section under **TYPE** change **Inherit auth from parent** to **Basic Auth**
  5. To the right fill in your **Workspace ONE UEM** **username** and **password**. (this might autofill as its round number 2)



GET https://as1276.awmdm.com/API/mam/apps/internal/begininstall

POST https://as1276.awmdm.com

TYPE: Inherit auth from parent

The authorization header will be automatically generated when you send the request. Learn more about

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secu collaborative environment, we recommend using variables. Learn more

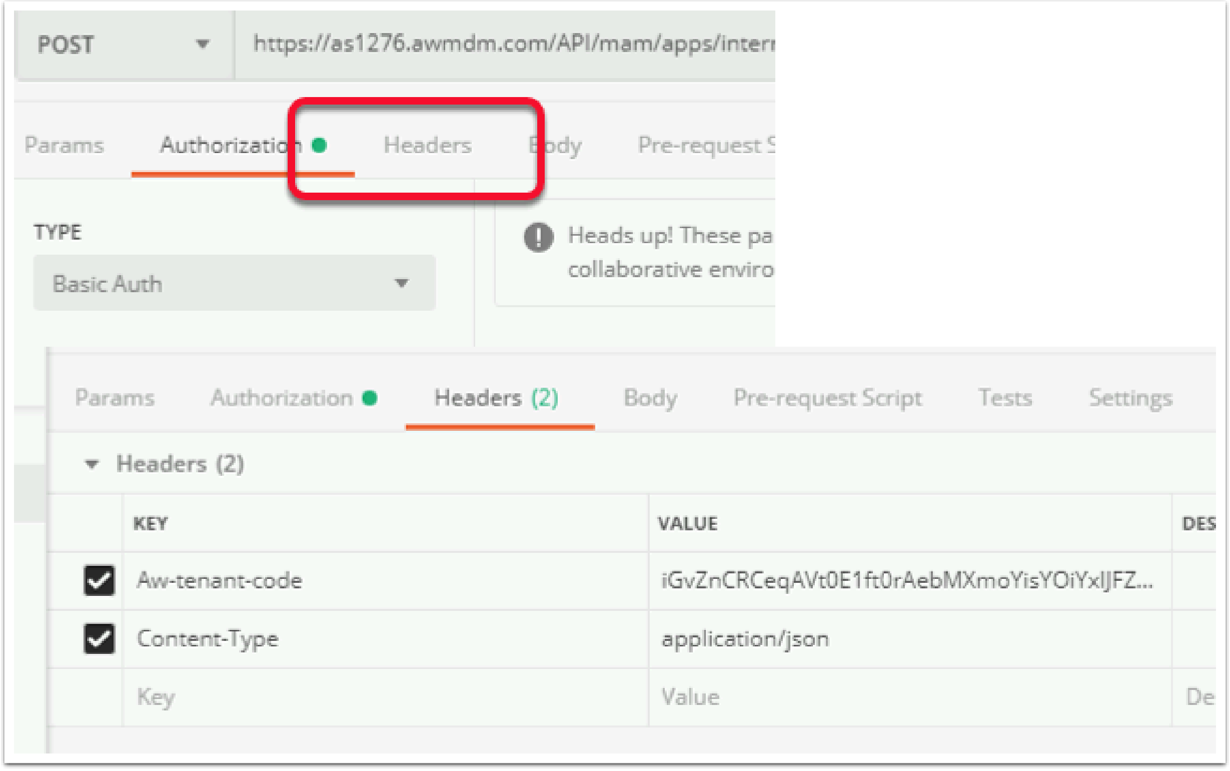
Username: norbertohermamdo@outlook.com

Password: ••••••••

4.

- Next to the **Authorization** tab select the **Headers** tab
- Under the **Headers** tab under **KEY** and **VALUE** fill in the **following values** using the table below.

KEY	**VALUE**
Aw-tenant-code	*YOUR API ADMIN KEY*
Content-Type	application/json



https://as1276.awmdm.com/API/mam/apps/interr

TYPE

Basic Auth

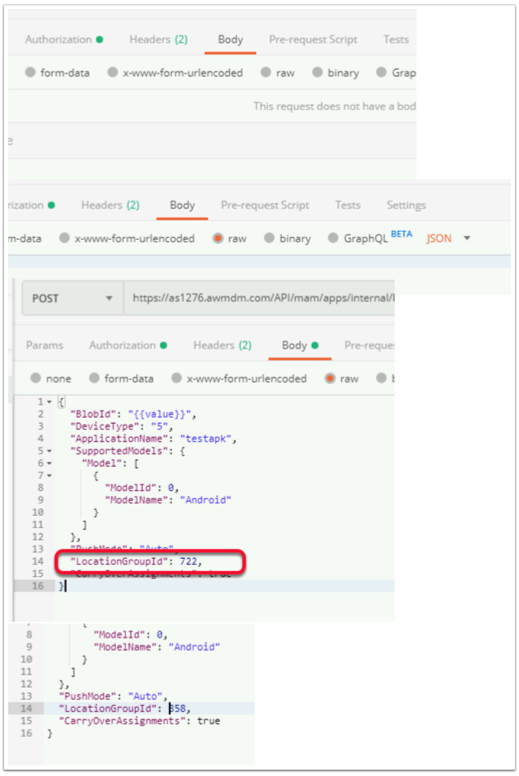
Heads up! These pa
collaborative enviro

	KEY	VALUE	DES
☑	Aw-tenant-code	iGvZnCRCeqAVt0E1ft0rAebMXmoYisYOiYxIJFZ...	
☑	Content-Type	application/json	
	Key	Value	De

5.

- Next to **Header** select the **Body** Tab ,
  1. select the **RAW** radio button
     - Ensure that **JSON** is select instead of **TEXT.** (JSON should be default)
  2. **Copy** and **Paste** the below sample script.
     - In this example, we have simplified to only include device type Android (Device type-5),
       Push mode and Organization group.
  3. Replace the **LocationGroupId** in the sample script with your **LocationGroupId** documented in Notepad++
     - You could edit the **ApplicationName**. Leave **PushMode** in the body of the API call to **"Auto".**

```
{
  "BlobId": "{{value}}",
  "DeviceType": "5",
  "ApplicationName": "testapk",
  "SupportedModels": {
    "Model": [
      {
        "ModelId": 0,
        "ModelName": "Android"
      }
    ]
  },
  "PushMode": "Auto",
  "LocationGroupId": 722,
  "CarryOverAssignments": true
}
```



```
{
  "BlobId": "{{value}}",
  "DeviceType": "5",
  "ApplicationName": "testapk",
  "SupportedModels": {
    "Model": [
      {
        "ModelId": 0,
        "ModelName": "Android"
      }
    ]
  },
  "PushMode": "Auto",
  "LocationGroupId": 722,
  "CarryOverAssignments": true
}
```

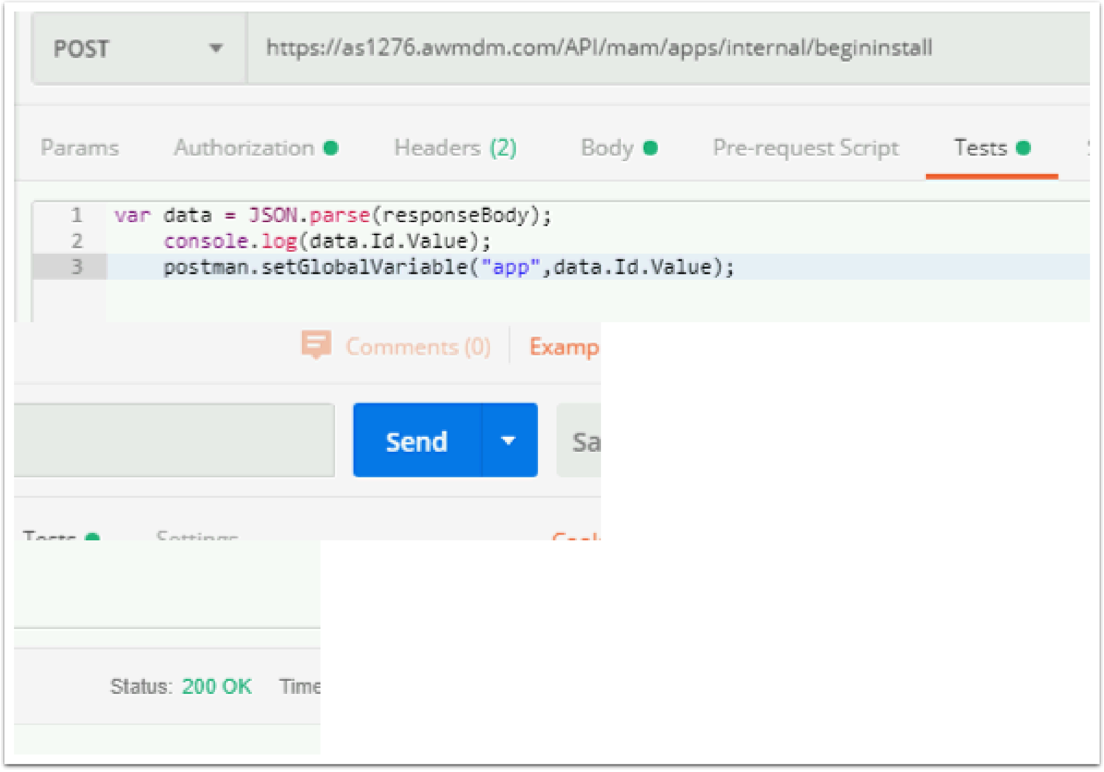
```
        "ModelId": 0,
        "ModelName": "Android"
      }
    ]
  },
  "PushMode": "Auto",
  "LocationGroupId": 858,
  "CarryOverAssignments": true
}
```

6.

- Two tabs down from **Body** select the **Tests** tab
  - In the **Tests** Tab, we will create a new global variable for our application id.
    - This Application id will be passed in the future to assign the smart group to this application.

```
var data = JSON.parse(responseBody);
    console.log(data.Id.Value);
    postman.setGlobalVariable("app",data.Id.Value);
```

- Click **SEND.** Confirm the response is **200 OK.**

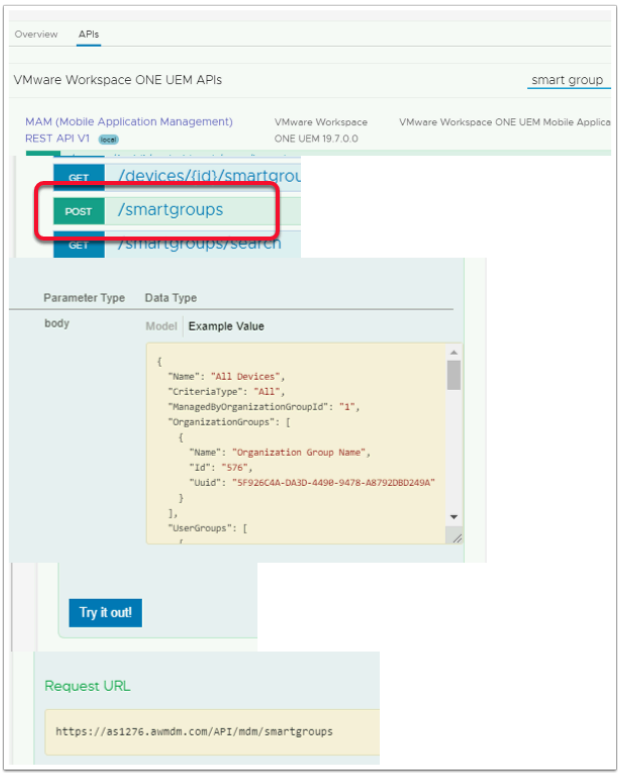


```
var data = JSON.parse(responseBody);
    console.log(data.Id.Value);
    postman.setGlobalVariable("app",data.Id.Value);
```

Part 5 : Create a Smart Group

1.

- Navigate back to your Workspace ONE UEM API console, https://cn-livefire.awmdm.com/api/help
  1. Switch to the **APIs** tab, in the **Search APIs/Methods** type **Smart Group.**
  2. Click on **POST /smartgroups**.
  3. **Scroll down** to find the expanded view of the API, under **Parameters**, to the right under **Data Type** **click** over the **yellow box**
     - This will populate the **SmartGroupEditModel** field.
  4. **Scroll down** and click **Try It Out!** button.
  5. Scroll until you find the **Request URL** field, **Copy your Request URL** https://as1276.awmdm.com/API/mdm/smartgroups.


Overview
APIs
VMware Workspace ONE UEM APIs
smart group
MAM (Mobile Application Management) REST API V1
local
VMware Workspace ONE UEM 19.7.0.0
VMware Workspace ONE UEM Mobile Applica
GET
/devices/{id}/smartgrou
POST
/smartgroups
GET
/smartgroups/search
Parameter Type
Data Type
body
Model
Example Value
Try it out!

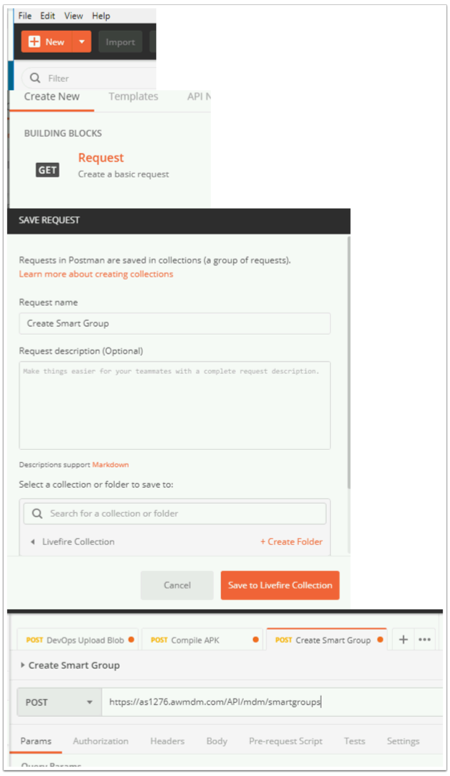
```
{
  "Name": "All Devices",
  "CriteriaType": "All",
  "ManagedByOrganizationGroupId": "1",
  "OrganizationGroups": [
    {
      "Name": "Organization Group Name",
      "Id": "576",
      "Uuid": "5F926C4A-DA3D-4490-9478-A8792DBD249A"
    }
  ],
  "UserGroups": [
```

Request URL

```
https://as1276.awmdm.com/API/mdm/smartgroups
```

2

- Switch back to **Postman**.
  1. In the top left-hand corner select **+New**
  2. Next to **GET** select **Request**
  3. In the **SAVE REQUEST** window, Under **Request name** type **Create Smart Group**. Select **Save to Livefire Collection**
  4. Change the **Request type** from **GET** to **POST.**
  5. In the **Enter request URL** area **Copy** and **Paste** your copied *request URL*



Requests in Postman are saved in collections (a group of requests).
Learn more about creating collections

Request name: Create Smart Group

Request description (Optional): Make things easier for your teammates with a complete request description.

Descriptions support Markdown

Select a collection or folder to save to:

Search for a collection or folder

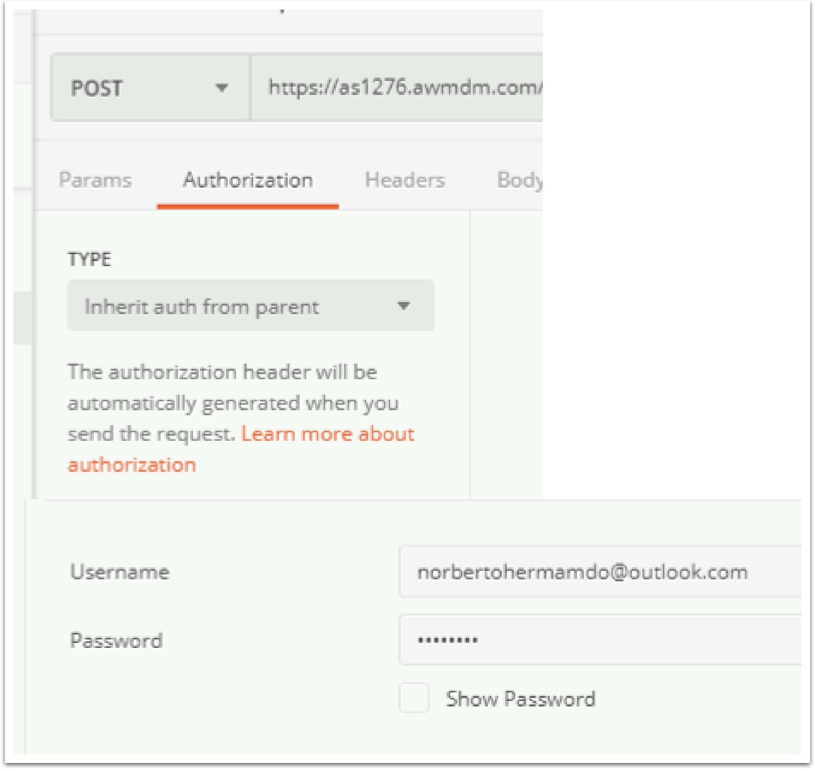
Livefire Collection + Create Folder

Create Smart Group

POST https://as1276.awmdm.com/API/mdm/smartgroups

3.

- Next to **Params** select the **Authorization** tab
  1. Under **TYPE** change **Inherit auth from parent** to **Basic Auth**
  2. Next to **Username** and **Password** ensure that your **Workspace ONE UEM** credentials have auto-filled



POST https://as1276.awmdm.com/

TYPE: Inherit auth from parent

The authorization header will be automatically generated when you send the request. Learn more about authorization

Username: norbertohermamdo@outlook.com

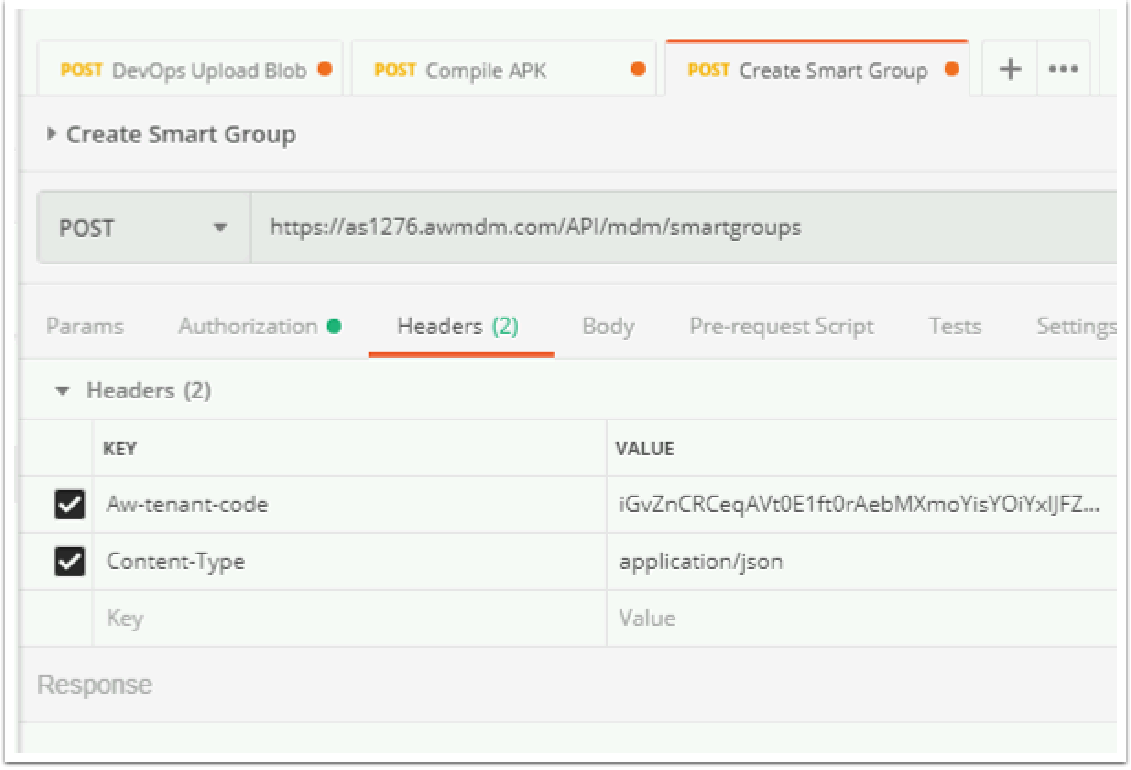
Password: ••••••••

□ Show Password

4.

- Switch to the next TAB **Headers**,
  - Enter the **KEY** and **VALUE** configuration in the below table.

KEY	VALUE
Aw-tenant-code	*YOUR API ADMIN KEY*
Content-Type	application/json



POST https://as1276.awmdm.com/API/mdm/smartgroups

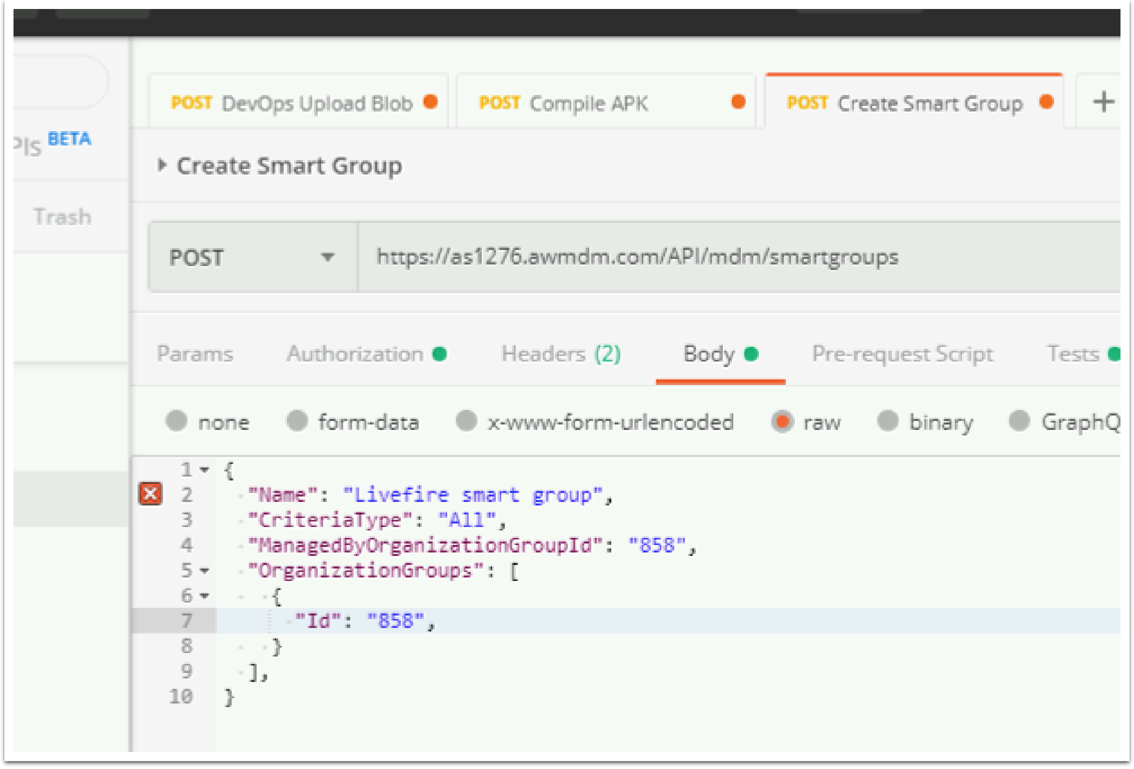
	KEY	VALUE
☑	Aw-tenant-code	iGvZnCRCeqAVt0E1ft0rAebMXmoYisYOiYxlJFZ...
☑	Content-Type	application/json
	Key	Value

5.

- Next to **Headers**, switch to the **Body** Tab
  1. Select the **raw** radio button
  2. **Copy** and **Paste** the below script,
  3. Next to the "**ManagedByOrganisationGroupId**" and **"Id"** replace the **"722**" sample code with **YOUR "ID"**

NOTE: A Customer would use the SmartGroupEditModel and replace values with their own required parameters. For simplicity, below is an example where we create a smart group, 'Livefire smart group' managed at OG with LGID 722.

```
{
  "Name": "Livefire smart group",
  "CriteriaType": "All",
  "ManagedByOrganizationGroupId": "722",
  "OrganizationGroups": [
    {
      "Id": "722",
    }
  ],
}
```



POST https://as1276.awmdm.com/API/mdm/smartgroups

```
{
  "Name": "Livefire smart group",
  "CriteriaType": "All",
  "ManagedByOrganizationGroupId": "858",
  "OrganizationGroups": [
    {
      "Id": "858",
    }
  ],
}
```

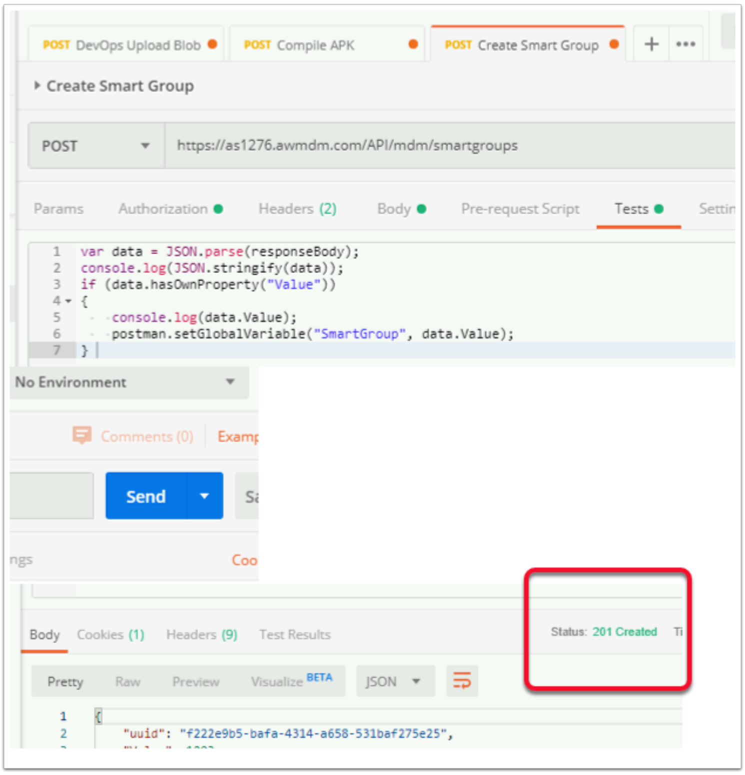
6 .

- Select the **Tests** tab
  - copy the below JSON script. In this script, we are passing the response from create smart group API call to our next call.

```
var data = JSON.parse(responseBody);
console.log(JSON.stringify(data));
if (data.hasOwnProperty("Value"))
{
    console.log(data.Value);
    postman.setGlobalVariable("SmartGroup", data.Value);
}
```

- Click **SEND**. Confirm the response **Status** is **201 Created** is displayed.

Make sure the **Variable** "SmartGroup" is created in the Settings of Postman.



POST https://as1276.awmdm.com/API/mdm/smartgroups

```
var data = JSON.parse(responseBody);
console.log(JSON.stringify(data));
if (data.hasOwnProperty("Value"))
{
    console.log(data.Value);
    postman.setGlobalVariable("SmartGroup", data.Value);
}
```

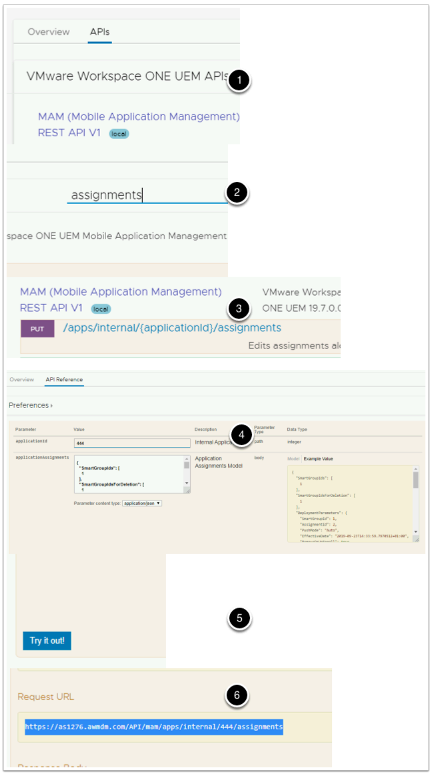
Status: 201 Created

```
{
    "uuid": "f222e9b5-bafa-4314-a658-531baf275e25",
```

Part 6: Assign and Publish.

1.

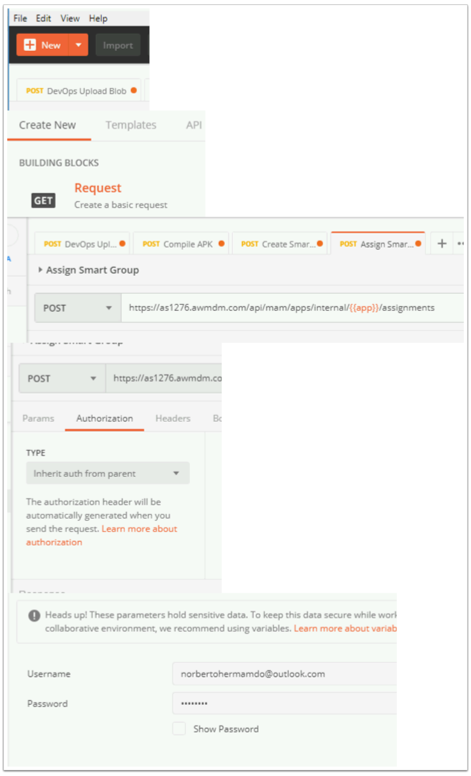
- Navigate back to your Workspace ONE UEM API console, **cn-livefire.awmdm.com/api/help.**
  1. Select the **APIs** tab,
  2. In the **Search APIs/Methods** area type **assignments**.
  3. Click on **PUT /apps/internal/{applicationId}/assignments**
  4. **Scroll down** to **Parameters**, to the right, next to **Parament Type**,
     - Under the **Data Type** header you will see a yellow box. **Click on the Yellow box**. This populates the **applicationAssignments** field to the right
     - Under **Parameter** next to **applicationId** enter **any number value** eg. 444
  5. **Scroll down**, Click **Try it Out!**
  6. **Scroll down**, to the **Request URL** area. **Copy** and **save** the **Request URL.**
- Note, the application id will be replaced by Global Variable "app" that was created in the second API call by Tests JSON script.



```
https://as1276.awmdm.com/API/mam/apps/internal/444/assignments
```

2.

- Revert back to **Postman.**
  1. Create a new Tab by selecting **+NEW**
  2. On the **Create New** page next to **GET** select **Request**
  3. On the **SAVE REQUEST** page under **Request name** type **Assign Smart Group**. Select **Save to Livefire Collection**
  4. Change the **Request type** to PUT or **POST.**
  5. Copy the Request URL. https://as1276.awmdm.com/api/mam/apps/internal/{{app}}/assignments.
  6. Under **POST** select the **Authorization** tab
  7. On the **Authorization** tab under **TYPE** change **inherit auth from parent** to **Basic Auth**
  8. Verify that your **Username** and **Password** fields have automatically been filled in with your Workspace ONE UEM credentials



Assign Smart Group

POST https://as1276.awmdm.com/api/mam/apps/internal/{{app}}/assignments

POST https://as1276.awmdm.co

TYPE

Inherit auth from parent

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while work collaborative environment, we recommend using variables. Learn more about variab

Username norbertohermamdo@outlook.com

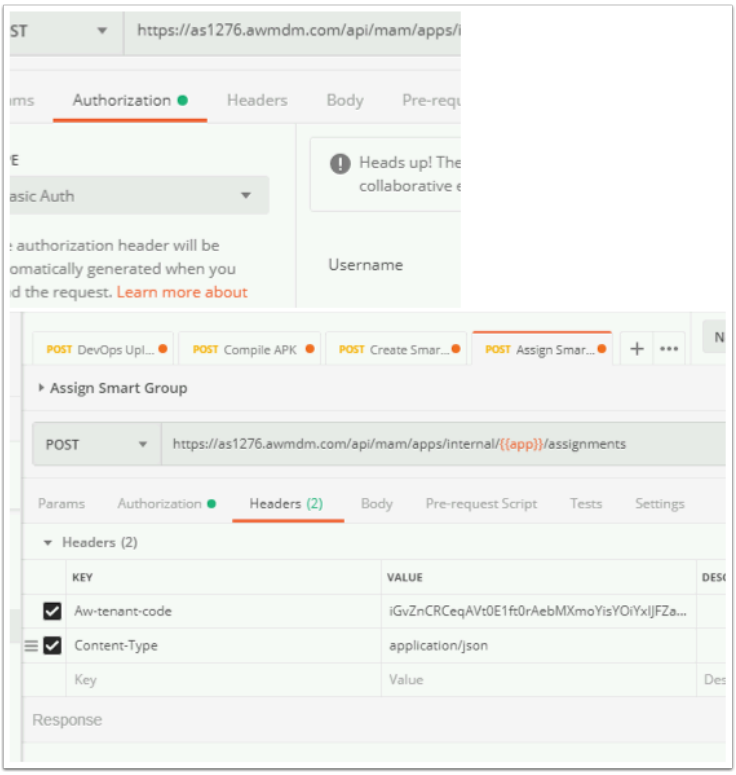
Password ••••••••

□ Show Password

3.

- From the **Authorization** tab, switch to the **Headers** tab
  - In **Headers** populate the respective, **KEY** and **VALUE** areas

KEY	**VALUE**
Aw-tenant-code	*YOUR API ADMIN KEY*
Content-Type	application/json



https://as1276.awmdm.com/api/mam/apps/i

: authorization header will be omatically generated when you d the request. Learn more about

https://as1276.awmdm.com/api/mam/apps/internal/{{app}}/assignments

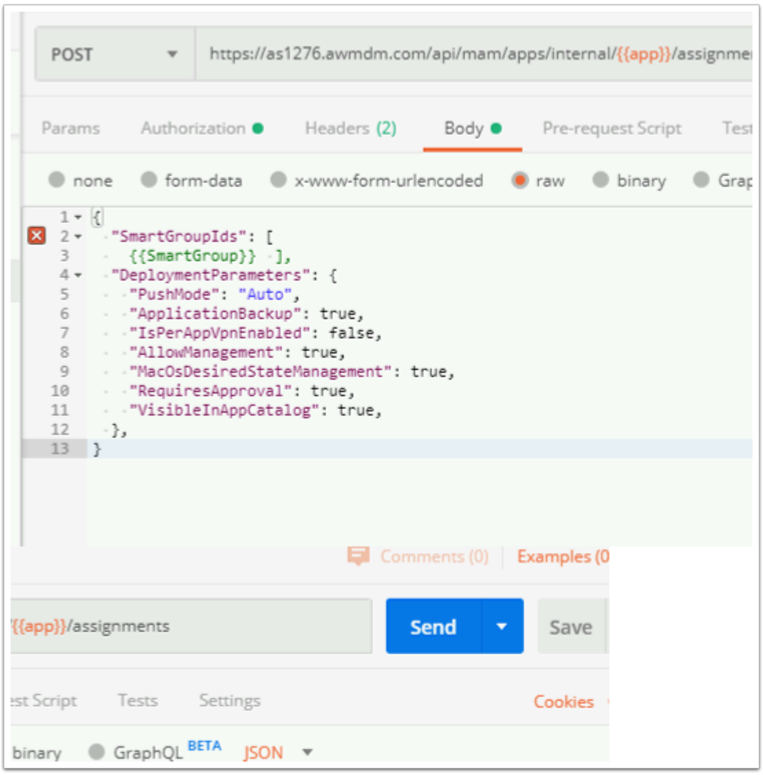
	KEY	VALUE	DESC
☑	Aw-tenant-code	iGvZnCRCeqAVt0E1ft0rAebMXmoYisYOiYxlJFZa...	
☑	Content-Type	application/json	
	Key	Value	Des

4.

- Next switch from the **Headers** tab and select the **Body** tab
  - Select the **raw** radio button. You can **copy** and **paste** the body from the API portal. For simplicity, paste the below body.
  - Click **Send**. Check for **201 Created** response.

```
{
  "SmartGroupIds": [
    {{SmartGroup}}  ],
  "DeploymentParameters": {
    "PushMode": "Auto",
    "ApplicationBackup": true,
    "IsPerAppVpnEnabled": false,
    "AllowManagement": true,
    "MacOsDesiredStateManagement": true,
    "RequiresApproval": true,
    "VisibleInAppCatalog": true,
  },
}
```

Note: We are passing the **'SmartGroup'** Global variable from the previous API call.



```
https://as1276.awmdm.com/api/mam/apps/internal/{{app}}/assignme
```

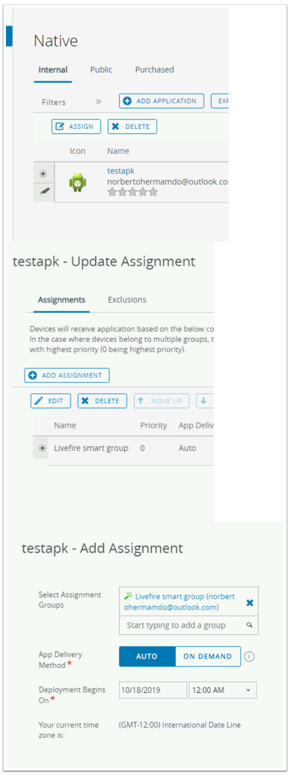
```
{
  "SmartGroupIds": [
    {{SmartGroup}} ],
  "DeploymentParameters": {
    "PushMode": "Auto",
    "ApplicationBackup": true,
    "IsPerAppVpnEnabled": false,
    "AllowManagement": true,
    "MacOsDesiredStateManagement": true,
    "RequiresApproval": true,
    "VisibleInAppCatalog": true,
  },
}
```

```
{{app}}/assignments
```

Part 7: Validation

- Navigate to the **Workspace ONE UEM** console.

1. Under **Apps&Books** > Native. Under the **Internal** tab Check your **APK** is added successfully
2. We will now validate the assignment of the APK. Select the **radio button** next to your APK icon and click **ASSIGN**.
3. On the **testapk - Update Assignment** window, below **+ADD ASSIGNMENT,** notice the Livefire smart group has already been assigned.
4. Select the **radio button** next **Livefire smart group** click **EDIT.**
5. Next to **Select Assignment Groups** is ***Livefire smart group*** and next to **App Delivery Method** the configuration is set to **AUTO.**
6. Next to **Select Assignment Groups** click on ***Livefire smart group*** In the criteria confirm your OG is selected under Organization Group.
7. Cancel all the windows. This confirms all the APIs successfully Executed.



Devices will receive application based on the below co
In the case where devices belong to multiple groups, t
with highest priority (0 being highest priority).

Select Assignment Groups: Livefire smart group (norbert ohermamdo@outlook.com) ✖ Start typing to add a group

App Delivery Method*: AUTO

Deployment Begins On*: 10/18/2019 12:00 AM

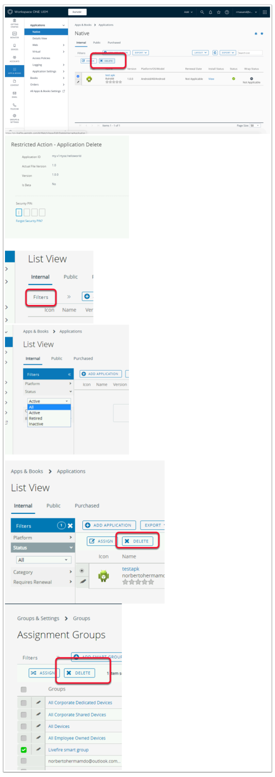
Your current time zone is: (GMT-12:00) International Date Line

Part 8: Automation

This Section will add all the above 4 API calls in one collection and execute them together to demonstrate automation. Before you begin, delete the APK and Smart Group you just created in the previous section from the workspace ONE UEM console.

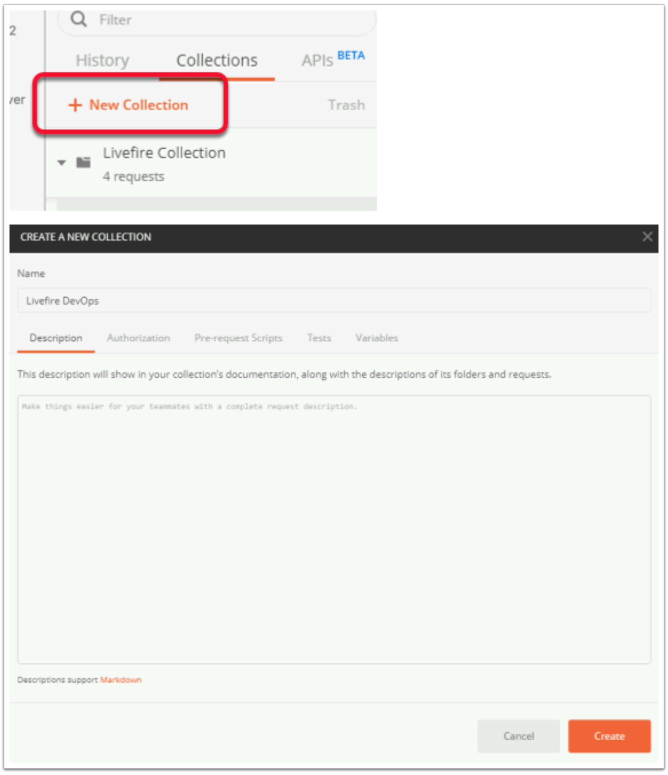
1.

- In the **Workspace ONE UEM** console,
  1. Navigate to **Apps & Books** > **Native**. Select the **APK you uploaded** and click **DELETE**. On the **Restricted Action - Application Delete** window enter your **Security PIN**
  2. Click on **Filters** on the same screen. Expand Status, select **All**. You will observe the app was not deleted but deactivated from the console. Select the **radio button** next to the **APK** click **DELETE**.
     - Note: This is a safety net in console to ensure Admin do not delete critical production application that have an active assignment.
  3. Navigate to **Groups & Settings** > **Groups** > **Assignment Groups**. Select the **check box** next to your smart group and click **DELETE**.


Restricted Action - Application Delete
List View
Internal
Public
Purchased
Filters
Apps & Books > Applications
ADD APPLICATION
EXPORT
ASSIGN
DELETE
Platform
Status
Category
Requires Renewal
Groups & Settings > Groups
Assignment Groups
Groups
All Corporate Dedicated Devices
All Corporate Shared Devices
All Devices
All Employee Owned Devices
Livefire smart group

2. Creating a New Collection.

- Navigate to **POSTMAN**.
  1. On the left pane, click **+ New Collection**.
  2. In the **CREATE A NEW COLLECTION** window under **Name** type **Livefire DevOps.**
  3. Click **Create**.



Name

Livefire DevOps

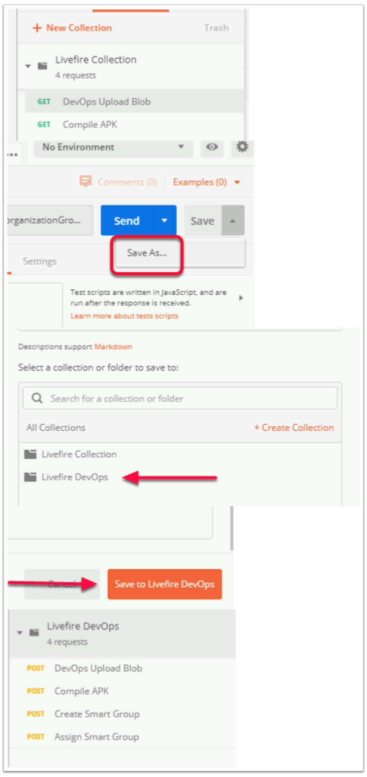
This description will show in your collection's documentation, along with the descriptions of its folders and requests.

Make things easier for your teammates with a complete request description.

Descriptions support Markdown

3 Save all 4 API calls to the new collection.

- In **POSTMAN**, from the left panel, click on **DevOPs upload blob** API call.
  1. Navigate to the right hand side of the window and look for **Save** which is to the right of **Send**. Select the **drop down arrow** next to **Save**. Click on **Save As**
  2. In the **SAVE REQUEST** window and scroll down to **All Collections** and select **Livefire DevOps.** and select **Save to Livefire DevOps**
- **Repeat** this task for the remaining 3 API calls, that being
  1. Compile APK
  2. Create Smart Group
  3. Assign Smart Group
- After you have completed the remaning 3 API calls in the left pane of PostMan **expand** the **Livefire DevOps** Collection and check that you have added all 4 requests



Test scripts are written in JavaScript, and are run after the response is received.
Learn more about tests scripts

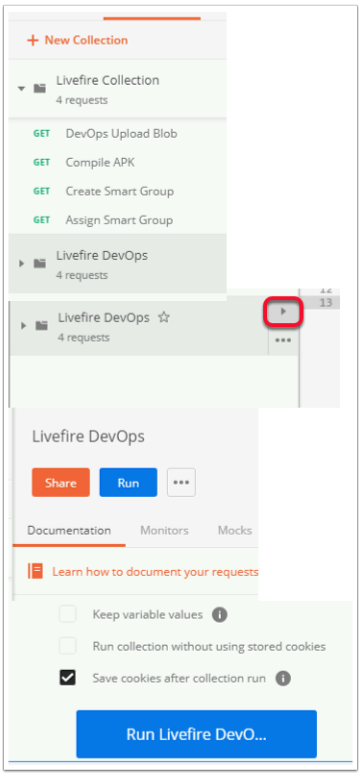
Descriptions support Markdown

Select a collection or folder to save to:

4. Run the Collection

Once the API collection is ready and console clean up is completed, you are ready to execute this automation.

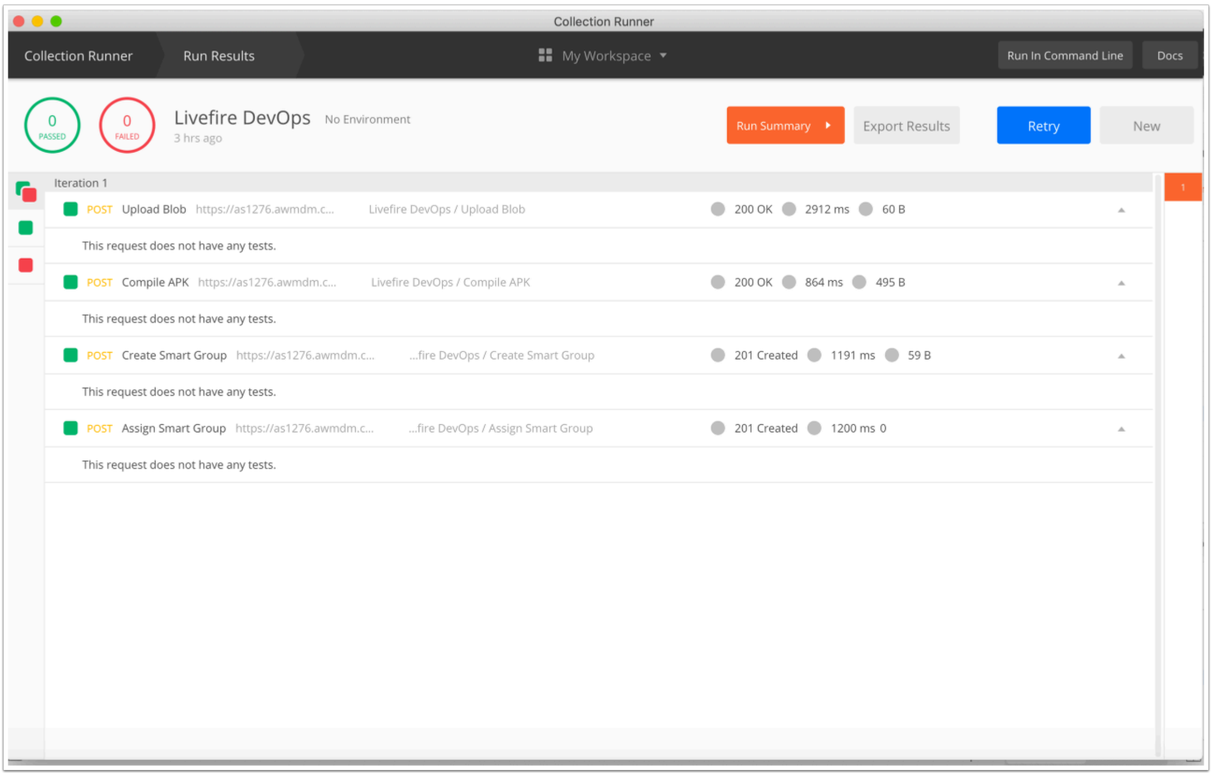
1. Select your collection in **POSTMAN.**
2. Click on the **play icon**.
3. In the expanded window view, click **RUN**.
4. This will open a new window Collection Runner, at the bottom of the window Click **Run Livefire DevOps**.
5. Go to your Workspace ONE UEM console and validate the APK is present and smart group is assigned.



□ Keep variable values

□ Run collection without using stored cookies

☑ Save cookies after collection run



Iteration 1

POST	Upload Blob	https://as1276.awmdm.c...	Livefire DevOps / Upload Blob	200 OK	2912 ms	60 B
This request does not have any tests.						
POST	Compile APK	https://as1276.awmdm.c...	Livefire DevOps / Compile APK	200 OK	864 ms	495 B
This request does not have any tests.						
POST	Create Smart Group	https://as1276.awmdm.c...	...fire DevOps / Create Smart Group	201 Created	1191 ms	59 B
This request does not have any tests.						
POST	Assign Smart Group	https://as1276.awmdm.c...	...fire DevOps / Assign Smart Group	201 Created	1200 ms	0
This request does not have any tests.						

You can export the entire collection in a json file and use tools like Newman to execute the same from Command Line. You can perform the same task sequence in Powershell leveraging the Workspace ONE UEM API Portal. This lab uses Postman to simplify and demonstrate API automation for beginners.

To export in JSON, click on the menu Icon (View More Options) next to collection. Click Export to generate a JSON script for your collection. This lab does not demonstrate Newman or Powershell.