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.



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
 - 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.



Part 2. Establish SAML Trust

- 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
 - 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



- Navigate back to your SalesForce site where you should now be able to login with your unique registered domain *-dev-ed.lightning.force.com
 - 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.
 - 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.

- Peterporte parametera 🗙 🦾 Politica Peterporte	X (M president down real	y 🗶 🗭 My Linnen Leferburg 🕺 🌄 Shinare Biologase Life	
C Secure https://blojolivefire-dev-ec Noriess Administrat: App Volumes Marce: App Volumes Marce: App Vol	Lightning force.com, lightning (or Westsh 📰 Hericon (mp. 🖸 West	tup/OrgConain/home	
	Q. Search Setup	1	
III Setup Home Otiect Manager V			
PLATFORM TOOLS	Reality of the second of the	6/11/2005/01/11/10/06/2007 - 2016/01/2005/01/	
SETTINGS	B SETUP	•	
 Company Settings 	My Dc	2	
Business Hours	1 C 1 1 1 1 1 1 1 1	-	
> Calendar Settings	Showcase your com features require it. It		
Company Information			
Data Protection and Privacy			
Fiscal Year			
Holidays			
Language Settings			
My Domain			
✓ Identity			
Auth. Providers	Your domain name		
Identity Connect	Your domain name		
Identity Provider	To test your new do		
Identity Provider Event Log	Deploy to Users R		
Identity Verification History			
Login Flows	Authentication (
Login History			
Single Sign-On Settings	Baci Use the native br		
Single Sign-On Single Sign-On Setti Configure single sign-on in order to a	Settings ngs uthenticate users in sale	sforce.com from external environmenta. Your organization has the folic	
 Federated authentication, a s 	ingle sign-on method that	uses SAML assertions sent to a Salesforce endpoint.	
		Fill SAM Assertion Validator	
Endersted Single Sign On Using S			
SAML Enabled	N.W.L.		
 (77) (0)		6	
Single Sign-On	Settings		
Single Sign-On Setti	ngs		
	54	Ne Lance	
Federated single Sign-On Using	SAML	0	
SAML Englied		•	
		un Crassel	

- 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.
 - 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.

AML Single Sign-On Settings to SAML Single Sign-On Settings AML Single Sign-On Settings AML Single Sign-On Settings to consort file to some file	
AML Single Sign-On Settings Tex Rev from Metadata File New from Metadata URL No SAML Single Sign-On Settings AML Single Sign-On Settings AML Single Sign-On Settings AML Single Sign-On Settings AML Single Sign-On Settings AML Single Sign-On Settings	
AML Single Sign-On Settings we configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't we configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Cancel Create Cancel Metadata File Choose File idp.xml	
AML Single Sign-On Settings texters rive Coose File No file chosen Corponice Control Center > Downloads Corganice New Folder Control Center > Downloads Construction Control Center > Downloads Construction	
tete configuration using an XML fie (1 MB or smaller) containing SAML 2.0 settings from your identify provider. (Salesforce doesn't store that the image of the constraints of the const	
Image: Conset Trie Conset Trie	
Wessels File Description Image: Consent File No Bile chosen Image: Consent File Open Image: Consent File No mile chosen Image: Consent File Image: Consent File	
Image: Control Center → Downloads Organize ▼ Organize ▼ New folder Image: Control Center → Downloads	
Open Image: Imag	
Open Image: Second Se	
Image: Source Center > Downloads Image: Source Center > Downloads Organize Image: Source Center > New folder Image: Source Center > Determodified Image: Source Center > New folder Image: Source Center > Determodified Image: Source Center > Determodified Type Image: Source Center > Determodified Source > Determodified Image: Source Center > Determodified Source > Determodified Image: Source Center > Determodified Source > Determodified Image: Source Center > Determodified Image: Source > Determodified Image: Source Center > Determodified Image: Source > Determodified Image: Source > Determodified > Determodifie	
Organize New folder 3 Favorites Name Date modified Type Desktop idp.xml 8/30/2018 12:10 PM XML Doc Downloads iginingCertificate.cer 8/30/2018 12:15 PM Security (Control Center Science) Recent places socialcast.jpg 5/25/2018 3:55 AM IPEG ima AML Single Sign-On Settings Security (Create Create 4 Metadata File Choose File idp.xml 4	
Organize New folder Favorites Name Desktop Date modified Type Desktop Didpxml 8/30/2018 12:10 PM XML Doc Downloads Downloads 8/30/2018 12:10 PM XML Doc Downloads Downloads 8/30/2018 12:15 PM Security (Control of the security of the secure of the security of the secure of the secure of the	V 0 3
Favorites Name Date modified Type Desktop Downloads Downloads Downloads Socialcast.jpg	
Desktop Downloads Downloads SigningCertificate.cer S/30/2018 12:15 PM Security C Socialcast.jpg	
Bownloads Greate Create Cancel Metadata File Choose File idp.xml	ument
	Certificate
AML Single Sign-On Settings eate configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Cancel Metadata File Choose File idp.xml	ige
AML Single Sign-On Settings eate configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Cancel Metadata File Choose File idp.xml	
eate configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Cancel Metadata File Choose File idp.xml	
eate configuration using an XML file (1 MB or smaller) containing SAML 2.0 settings from your identity provider. (Salesforce doesn't Create Cancel Metadata File Choose File idp.xml	
Create Cancel Metadata File Choose File idp xml	t store this
Metadata File Choose File idp xml	
Metadata File Choose File idp xml	
Create Cancel	

- 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 Nameldentifier element of the Subject statement
 - Next to API Name: leave as default
 - Next to Entity ID: Change to <u>https://saml.salesforce.com</u>
 - Next to Identity Provider Login URL: leave 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**

	Save Save & New Cancel		
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 Nameldentifier element of the Subject statement		
Service Provider Initiated Request Binding	HTTP POST		
SAML Single Sign	On Settings		e ₁₄
Back to Single Sign-On Settings	er e e mige		
	Edit Delete Cone Download Metadata	SAT L Assertion Validator	
Name	workspaceone	API Name work	spaceone
SAML Version	2.0		
Issuer	https://workspaceone.euc- livefire.com/SAAS/API/1.0/GET/metadata/idp.xml	Entity ID https	://saml.salesforce.com
SAMLSP-00D0b00xml	▲ signingCertificate.cer ▲ 🗈 idp.xml	^	

- On the SalesForce admin console
 - 1. Navigate to **Settings** > Company Settings > My Domain
 - 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

SETTINGS	Your domain name is rbojolivefire-dev-ed.my.salesforce.com
Company Settings	Vour domain name is rearly Los in to test it out
Business Hours	To test your new domain, click tabs and links. If you've customized the UI, check for hard it
> Calendar Settings	
Company Information	Deploy to Users Roll out the new domain to your org.
Critical Updates	Authentication Configuration
Data Protection and Privacy	Addienocation Comparation
Fiscal Year	Header Logo
Holidays	Background Color Use the native browser for user
Language Settings	authentication on IOS
My Domain	authentication on Android
 Identity 	Right Frame URL Authentication Service Login Page
Auth. Providers	
Identity Connect	Edit
	2
N	avigate to this page?
Authentication Configura	ation
Authentication Configuration	Save Great Greater Datast
Login Page Type 🥹 Sta	ndard 🔁
Authentic Bon Service	Login Form
Logo File O Chr	oose file No file chosen
background Color	#64669
× Single Sign-On Settings ×	My Domain ~ Salesforc: × C VMware Work
ne/DomainName.apexp	
rkspaceOne 🗋 vSphere Client	
	-
	0

• 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

Gene	ral Informa	tion	
First	Name Us	ser33SCR	
Last	Name	R	
	Alias	ser33SC	
	Email us	er33SCR@sanjose33.eu	
User	name us	er33SCR@sanjose33.eu	
Nick	name Us	ser33SCR	
	i		
Corr			
Depar	tment		
Depan	vision		
DI	131011		
			= Require
Role	<none sp<="" td=""><td>ecified></td><td>≎ i</td></none>	ecified>	≎ i
ense	Force.com	n - Free 📀	
ofile	Force.com	n - Free User ᅌ 👔	
ctive	~		

- 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



- 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}**.
 - Select Next, on the Access Policies page, select Next, on the definition page, select Save.

hboard - Users & Gr	
	200ps Catalog - Identity & Access Management Appliance Settings
Edit	Asign Delete Djegories v More v Setting
Application	Туре
R Soles	Jurce SAML 2.0 Web Application
	5 N
t SeeS Application	
	A Report III C
Definition	The second
origination	- Application (C (D
	Nga dan daga nga nga nga nga nga nga nga nga nga
	* menune forme ()
	Ungerfiel -
· · · · ·	
	River and love
L	
	these leasts a
	Capacity Manuare Researce ()
Seas Application	
	A REAL PROPERTY OF A READ PROPERTY OF A REAL PROPER
ethologi	
orfigundos	Approxime D
	Mpc-rundum/hox com
ces Polos	Destant fund
	Unpediat -
	Decement Value 10
	New York
	Advand Papertex -
	Open in Minure Browley @
	Casa Pin Vol
SeeS Application	1990 VIII
SeeS Application	
SeeS Application	Acons Pillos
SeeS Application	Access Policies secondary de rener alerte a celle a celle quitares, Secondary and gener
SeeS Application	Laura Philos Access philos de hanne ha este a des autoritations laiser es este Constrainte de la const
SeeS Application	
SeeS Application	And have a set of the
SeeS Application	
SeeS Application atom atom atom atom atom atom atom atom	Anno halos Anno h
SeeS Application when many and the second se	Accel frage and the second and the s
SeeS Application where w	
SeeS Application where w	According to the second
SeeS Application	According to the second
I SaaS Application where antipoten antipoten anter bilan	
SeatS Application	A contract manufacture of the second contract manuf
SeaS Application atom atom atom atom atom atom atom atom	
SeaS Application	
SeaS Application atom angunan	And the And And the And
SeaS Application	
Sea5 Application t Sea5 Application	
I SeaS Application I SeaS Application	
SeaS Application	
SeaS Application	
Sea5 Application among among among to Saa5 Application among	
SeaS Application may tisses Application	Image: Control of the control of t
Seo Application mmm mpmm mpmm mpmm mpmm son that Sao S Application mpmm mpmm mpmm mpmm mpmm mpmm mpm mpm	
Ses Application man	
Ses Agalasian mar	Image: Control of the control of t
Ses Application	
Ited Application maximum maximum them them them them them them them the	
Ited Application main free free free free free free free fre	We were Beene were were were were were were were
Isab Appleador Anna Isab Anna Maria Anna Maria Anna Maria Anna Maria Anna Maria	
Isal Application maximum and	
Isal Agalashan mar ana Man Isal Agalashan Isal Agalashan Man Man Man Man Man Man Man M	Image: Control of the control of t

- 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

asnooard	1 +	Users & Gro	ups Catalog	ld -	entity & Access	Managemen	nt Appli	ance Settings	Roles
	Nev	v Edit	Assign	Delete	Categories	~ 1	More 🗸	1 ttin	gs
		Application				Туре			
	۷	Salesfo	rce			SAML 2.0	Web Appli	ication	
	н	$\leftarrow \uparrow \rightarrow$	н						
Assigi	n							2	
Selecte	ed Ap	p(s): Salesfo	rce						
Users / Us	ser Gro	ups							
Q mark	(e								
👪 Mar	rketing(@euc-livefire.com	De	ployment Ty	/pe:				

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

Í	Paint Citrix		∯ Оре	N
•	PowerPoint Website		රූ Ope	N
	Salesforce Website		Сре	N
	WordPad	All V Q Search	Salesforce	
iii Sales	Home Opportuniti	ns ∨ Learls ∨ Tasks ∖	Files V Accounts V Con	
300к — 200к —	Add the o view your	pportunities you're working on, I performance.	then come back here to	
100к 0	Aug		Sep	
Today's Eve	ents	Today	's Tasks	
PowerPo	int	♪		
PowerPo	int v	P Search		
PowerPo	v +	C Search		