

Authentication Method - Android SSO

Configure Single-Sign-on for Android Device from the Workspace ONE UEM Admin Console

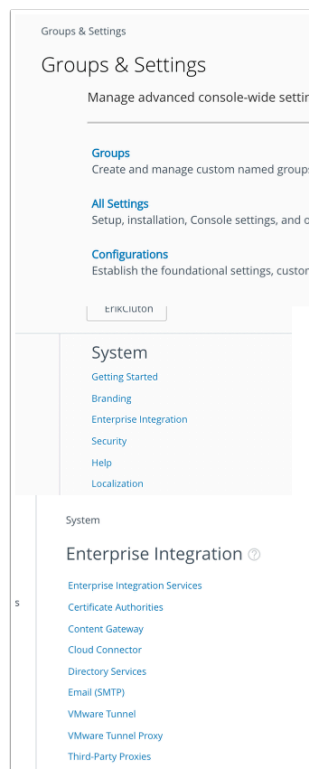
Pre-requisites to this lab

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

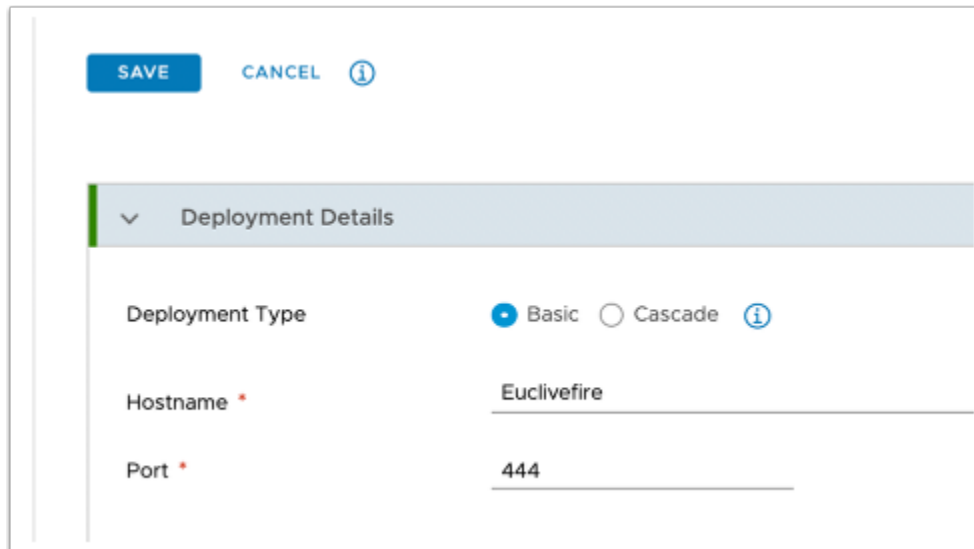
1.1 In this section we will download a certificate from WorkspaceONE UEM and use to configure Android Mobile SSO in Workspace ONE Access. After we will round all the remaining Workspace ONE Access configurations.

- 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

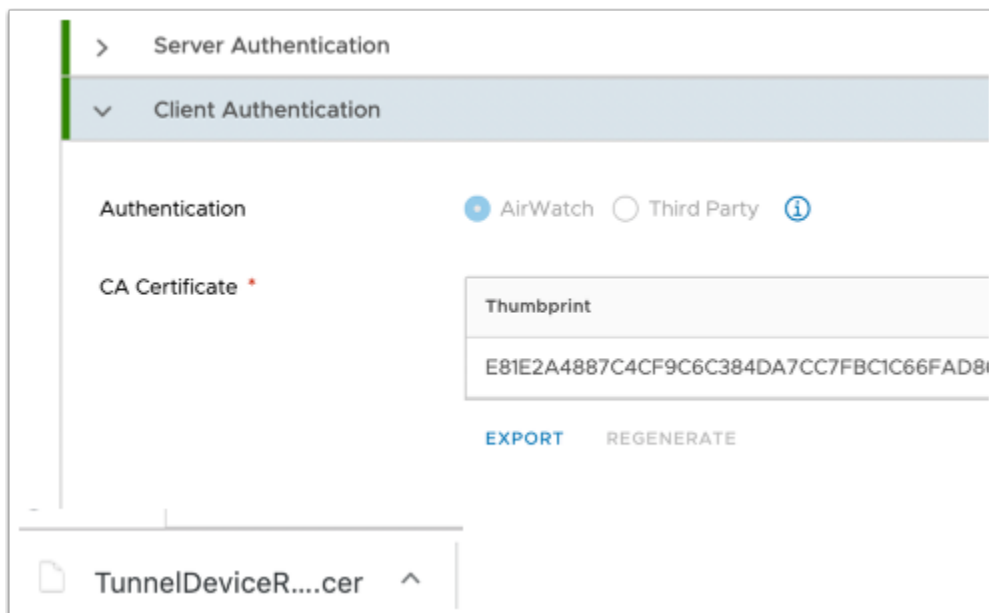
- Next to **Hostname:** **EUClivefire** (this can be anything)
- **Port:** **444** (this can be anything)
- At the top of the page select **SAVE**



The screenshot shows the 'Tunnel Configuration' page. At the top, there are buttons for 'SAVE' (in blue), 'CANCEL', and an information icon. Below this is a section titled 'Deployment Details' with a dropdown arrow. Under 'Deployment Details', there are three fields: 'Deployment Type' with radio buttons for 'Basic' (selected) and 'Cascade', and an information icon; 'Hostname' with a red asterisk and the value 'Euclivefire'; and 'Port' with a red asterisk and the value '444'.

1.3 Expand **Client Authentication**

- Below **Thumbprint** select **EXPORT**
- Note the name of the certificate is **TunnelDeviceRootCertificate.cer**

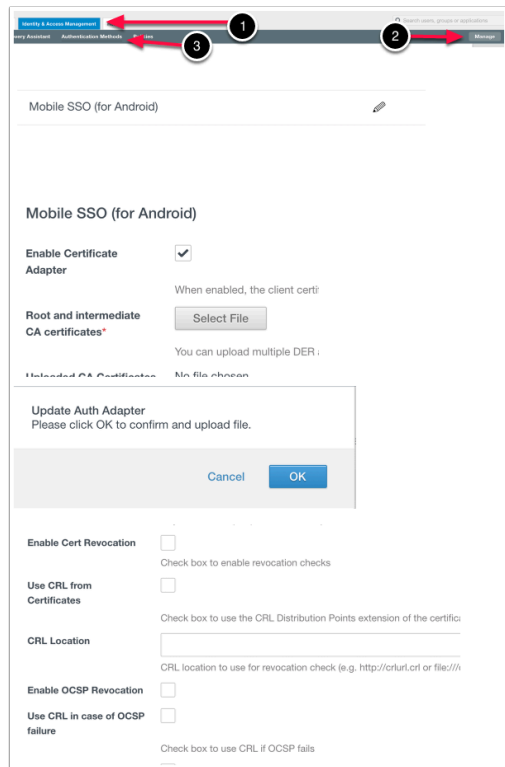


The screenshot shows the 'Client Authentication' section, which is expanded. It contains two radio buttons: 'AirWatch' (selected) and 'Third Party', with an information icon. Below this is a 'CA Certificate' field with a red asterisk. To the right of this field is a 'Thumbprint' box containing the value 'E81E2A4887C4CF9C6C384DA7CC7FBC1C66FAD81'. Below the thumbprint box are two buttons: 'EXPORT' (in blue) and 'REGENERATE'. At the bottom of the page, there is a file icon and the text 'TunnelDeviceR....cer' with an upward arrow.

1.4 Login to your SaaS instance of Workspace ONE Access

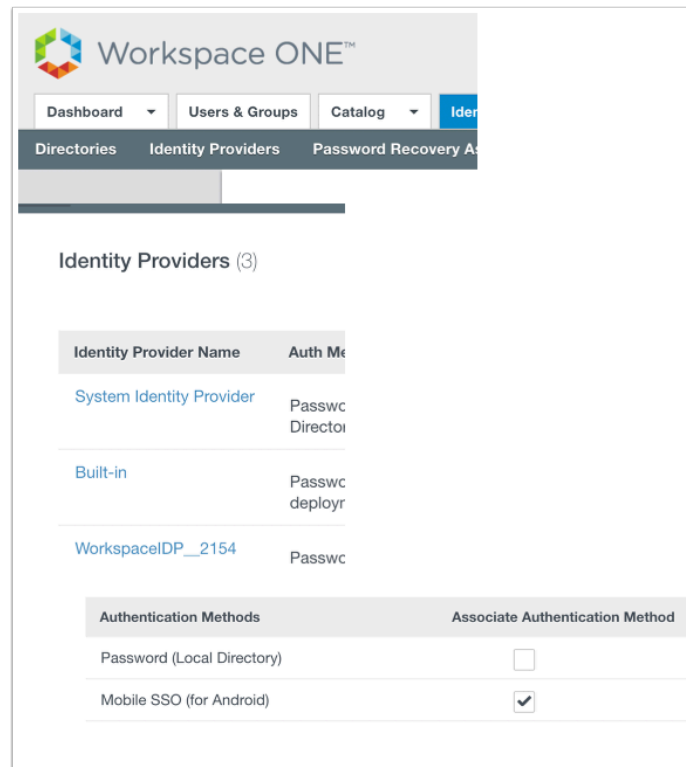
1. Select the **Identity & Access Management** tab select **Manage** and then select **Authentication Methods**
2. Under **Authentication methods** select the **Pencil Icon** next to **Mobile SSO (for Android)**
3. On the **Mobile SSO (for Android)** window select the following: Next to

- **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**



1.5 On the **Identity & Access Management** tab > **Manage ...**

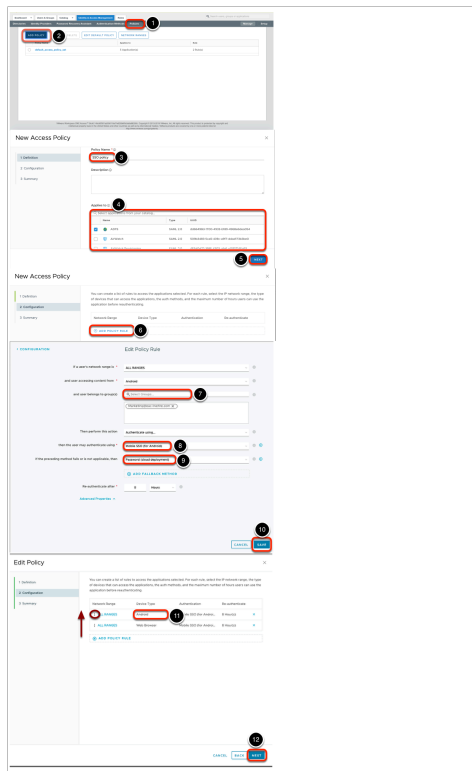
- , select **Identity Providers**
 1. On the **Identity Providers** window, select **Built-in**
 2. Under the **Authentication Methods** area select **Mobile SSO (for Android)** **checkbox**
 3. Select **Save**



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**



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 to **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-livewire.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**

ADD POLICY EDIT DELETE EDIT DEF

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 SSO	8 H

ADD POLICY RULE

and user belongs to group(s) Select Groups...

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)

ADD FALLBACK METHOD

Re-authenticate after * 8 Hour

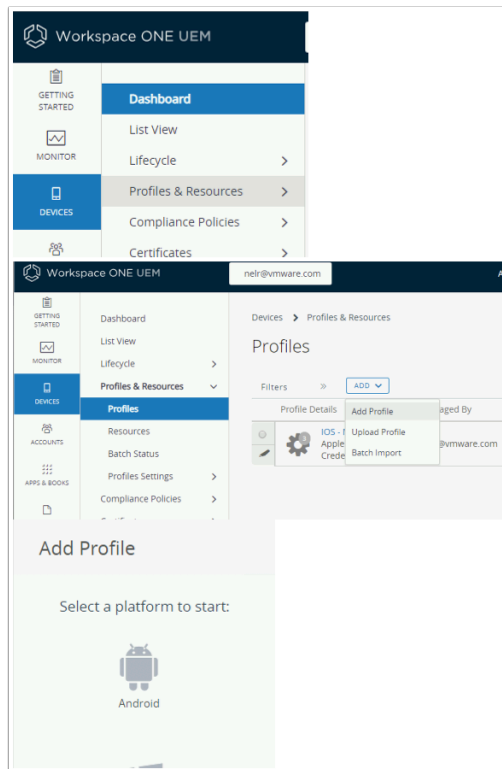
CANCEL SAVE

Network R.	Device Ty.	Authentic.	Re-auth.
ALL R.	Android	Mobile S.	8 Hour(0)
ALL R.	iOS	Mobile S.	8 Hour(0)
ALL R.	Web Bro.	Certificat...	8 Hour(0)

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)

Add a New Android Profile

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)

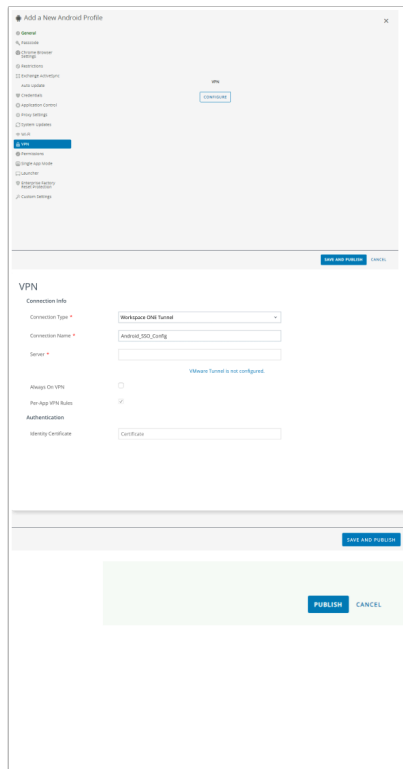
Exclusions: All Corporate Shared Devices (neir@vmware.com), All Devices (neir@vmware.com), All Employee Owned Devices (neir@vmware.com)

Additional Assignment Criteria: **CREATE SMART GROUP**

SAVE AND PUBLISH **CANCEL**

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**

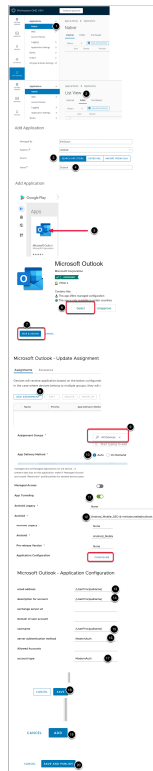


Part 3: Configuring an Android Native applications for a Per App VPN Profile in WorkspaceONE UEM for SSO

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 **Add 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** ,

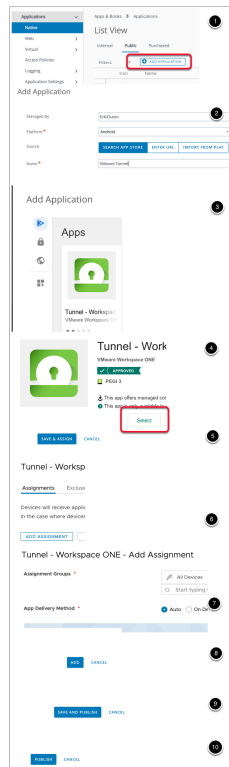
11. Next to **App Delivery Method** select the AUTO **radio button**
12. Next to **App Tunneling** select **ENABLED**. Next to **Android*** select your **Android_Mobile_SSO@*** profile
13. Next **Application Configuration** select **Configure**
 - Next to the following add the respective configuration 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



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**

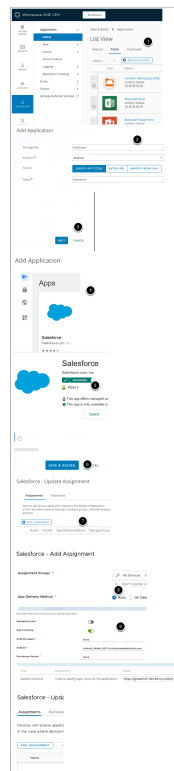


3.4 Configuring Sales Force for native Android Single Sign-On

- 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

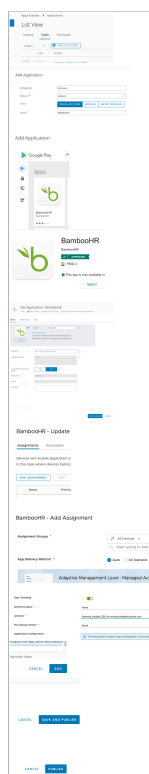
- Next to **Application Configuration** select **Configure**. You will notice a whole range of additional configurations now become available
- Next to the Title **AppServiceHosts**
 - Under the middle area type in your **custom Salesforce domain**
 - e.g. **sanjose35-dev-ed.my.salesforce.com**
 - At the bottom of the **Salesforce - Application Configuration** page select **SAVE**
 - At the bottom of the **Salesforce - Add Assignment** window select **ADD**
- On the **Salesforce - Update Assignment** window select **SAVE AND PUBLISH**
- On the **Preview Assigned Devices** window select **PUBLISH**



3.5 Configuring BAMBOOHR for native Android Single Sign-On

- In the **WorkspaceONE UEM** console, select **APPS & BOOKS > Applications > Native**
 - Under the Pubic select **+ADD APPLICATION**
- In **Add Application** window, select the following, next to:-
 - **Platform*:** **Android**
 - **Name*:** **BAMBOOHR**
 - Select **NEXT**
- In the **Add Application** window under **Apps** select **BambooHR**
- In the **Add Application** window under **BambooHR** click **Select**
- On the **Edit Application - BambooHR** window, select **SAVE & ASSIGN**
- On the **BambooHR - Update Assignment** window select **ADD ASSIGNMENT**
- 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...**
- At the bottom of the **BambooHR - Add Assignment** window select **ADD**
 - On the **BambooHR - Update Assignment** window select **SAVE AND PUBLISH**
 - 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



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
- In the **APPS & BOOKS > Applications > Native > Public** tab continued..
 - Select **+ADD APPLICATION**
 - In the **Add Application** window next to: Select
 - **Platform* :** **Android**
 - **Name*:** **Chrome**
 1. select **NEXT**
 - In the top of the **Add Application** window select **Google Chrome Fast & Secure**
 - 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**

The screenshot displays the 'Add Assignment' configuration window for Google Chrome. At the top, the 'Add Application' section shows 'Google Chrome' selected from a list of apps. Below this, the 'Assignments' section for 'Google Chrome: Fast & Secure' is shown. It includes an 'Add Assignment' button and a list of assignment groups. The 'All Devices' group is selected. Under 'App Delivery Method', the 'Auto' radio button is selected. The 'App Tunneling' section is expanded, showing 'Enabled' status. Below this, the 'Android*' section is visible, showing 'Android_Mobile_SSO' as the selected assignment group. At the bottom, the 'Application Configuration' section is visible, showing 'Completed' status.

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.

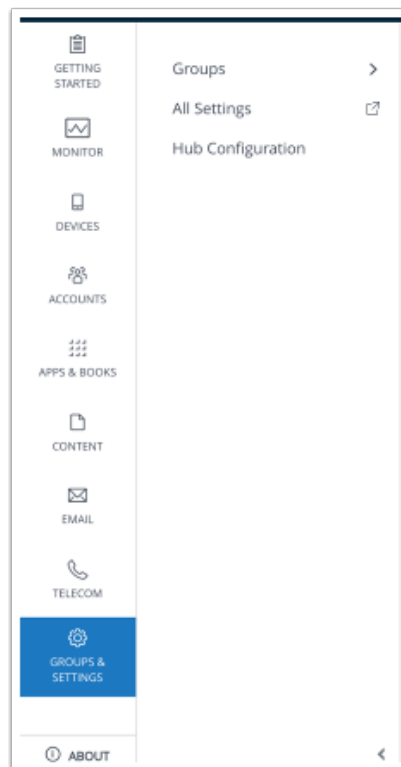
About this task

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**

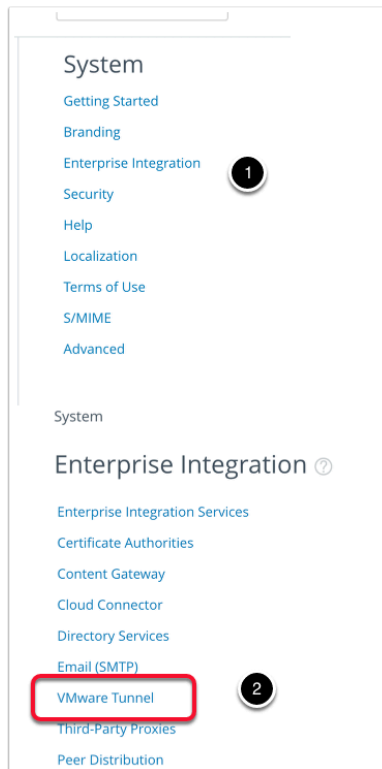
1. Ensure you launch your on your Control center desktop and launch your browser to enter <https://cn-livewire.awmdm.com>
2. Log into your **Workspace ONE UEM** admin console with your Admin credentials.
3. In the **Workspace ONE UEM** admin console, select **GROUPS & SETTINGS**, select **All Settings**



4.2 Configuring Single-Sign-on for Android.... continued

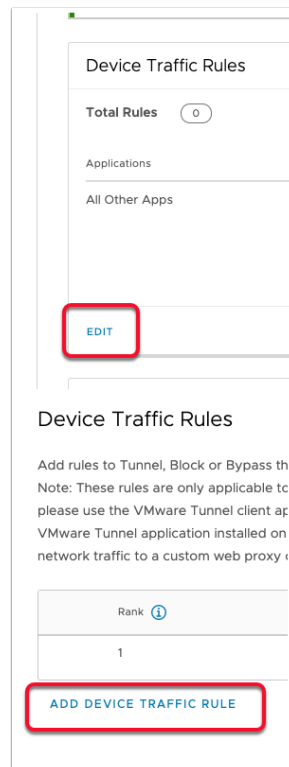
- **Configuring VMware Tunnel Component...**

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 select **EDIT**
 - To the left of the **Device Traffic Rules** window select **ADD DEVICE TRAFFIC RULE**



4.4 Configuring Single-Sign-on for Android.... continued

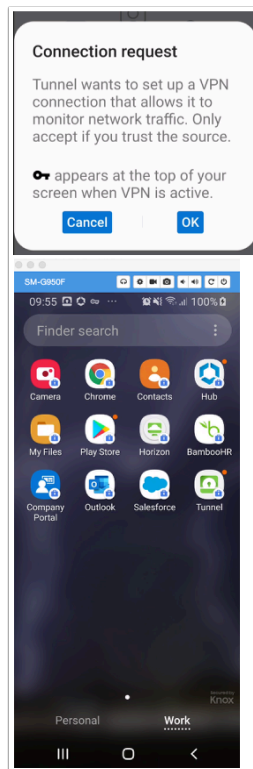
- **Configuring VMware Tunnel Component...**

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**

The screenshot displays the VMware Tunnel configuration window. It features a table with two rows representing different ranks. Rank 1 is configured with a list of applications (BambooHR, Google Chrome, Intune Company Portal, Microsoft Outlook, Salesforce, Android workspace, AirWatch Secure Browser) and the action set to PROXY with a specific web proxy and destination. Rank 2 is set to BYPASS for all other apps. The interface includes 'CANCEL', 'SAVE', and 'SAVE AND PUBLISH' buttons. A confirmation dialog is shown at the bottom asking 'Are you sure you want to continue?' with 'CANCEL' and 'OK' options.

4.4

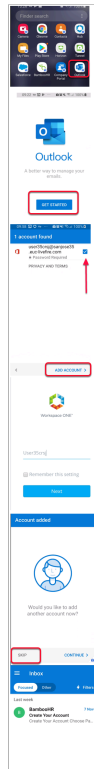
- On your Mobile Device, wait until all your apps have been deployed. That being **Microsoft Outlook; BambooHR; Salesforce, Intune Company Portal, Android Workspace, Airwatch Secure Browser** and **Chrome** and **VMware Tunnel**
- Look to be prompted for the following message : **Connection request. Tunnel wants to set up a VPN connection....** You have the option to select **Cancel** and **OK**. Select **OK**



Part 5: Testing Mobile SSO for Android

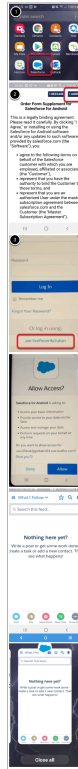
5.1 We will test Mobile SSO using the Microsoft OUTLOOK Application

- 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.



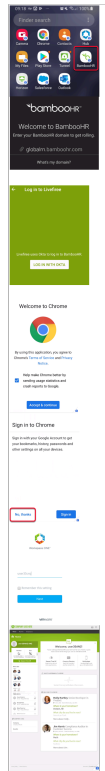
5.2. Testing Mobile SSO for Salesforce

- On your Android device, choose your **Work** profile
 - Select the **Salesforce icon**
 - On the terms and conditions select **I AGREE**
 - On your login notice you have the option at the bottom **OR Log in using: your custom domain**. Select **your custom domain**
 - In the **Salesforce for Android** window select **Allow**
 - Notice you are now in your Salesforce application for the first time. Close the application and 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



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