Configuring AirWatch Provisioning App in VMware Workspace ONE Access

FEBRUARY 2021

VMware Workspace ONE Access

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 How to Configure AirWatch Provisioning App in VMware Workspace ONE Access 4

Add AirWatch Provisioning App to the Catalog 5

Assign the AirWatch Provisioning App to Users 8

2 Troubleshooting AirWatch Provisioning Configuration 10

Provisioning Status Shows User Is Not Provisioned 10

Enrolling a Device with the Workspace ONE Intelligent Hub App Causes an Error 10

Provisioning the Mobile SSO Profile With AirWatch Provisioning Generates Error 11

How to Configure AirWatch Provisioning App in VMware Workspace ONE Access

1

This guide provides information about using the AirWatch Provisioning app to provision users and groups in Workspace ONE UEM from the VMware Workspace ONE Access service.

The AirWatch Provisioning app creates, updates, and deletes users and groups in the Workspace ONE UEM console. When users are added, the user type designated in Workspace ONE UEM is **Directory**.

Note The product name AirWatch was renamed Workspace ONE UEM. In this guide,Workspace ONE UEM service and AirWatch both refer to Workspace ONE UEM.

You use the AirWatch Provisioning app with the Workspace ONE UEM service when an LDAP server cannot be used with the VMware AirWatch Cloud Connector to synchronize users. Users who are created in the Workspace ONE Access service using either the System for Cross-domain Identity Management (SCIM) API or the just-in-time (JIT) service can be provisioning to the Workspace ONE UEM service.

To use the AirWatch Provisioning app, the following are the configuration requirements.

- Users are provisioned at the Customer Organization Group (OG) level in Workspace ONE UEM.
- An LDAP server cannot be configured at the Customer OG level in Workspace ONE UEM.
- An identity provider must be configured as the SAML provider before you configure the AirWatch Provisioning app. If you want to use Workspace ONE Access as the SAML provider, follow the instructions in the Configuring Single Sign-on from the VMware Identity Manager Service to AirWatch Applications guide.
- If you use Workspace ONE Access JIT to create users
  - You must send a valid GUID to Workspace ONE UEM as part of the SAML attribute. This GUID is required to use the Workspace ONE Intelligent Hub app to enroll user devices. The GUID is mapped to the External ID and provisioned to Workspace ONE UEM.
  - Users must use a browser the first time they log into Workspace ONE before they can use the Workspace ONE Intelligent Hub app.

Note To complete the configuration, you must have administrator privileges for both the Workspace ONE Access console and the Workspace ONE UEM console.

This chapter includes the following topics:

- Add AirWatch Provisioning App to the Catalog
- Assign the AirWatch Provisioning App to Users

Add AirWatch Provisioning App to the Catalog

You add the AirWatch Provisioning app to the catalog in the Workspace ONE Access console and assign users to the app. When users are assigned to the app, they are provisioned in Workspace ONE UEM and can access Workspace ONE.

Prerequisites

- Make sure that SAML authentication is enabled in the Workspace ONE UEM console in the **Accounts > Administrators > Administrator Settings > Directory Services** section.
- An identity provider must be configured as the SAML provider before you configure the AirWatch Provisioning app. If you want to use Workspace ONE Access as the SAML provider, follow the instructions in the Configuring Single Sign-on from the VMware Identity Manager Service to AirWatch Applications guide.
- Configure Workspace ONE UEM authentication information in the AirWatch Provisioning app.

  The recommend configuration is to enable Certificate Auth. Certificate Auth settings are configured in the Identity & Access Management > Setup > Workspace ONE UEM page. This option reduces the configuration complexity since the AirWatch Host, Admin Username, Admin Password, and AirWatch API Key fields are automatically populated in the AirWatch Provisioning settings when you select Certificate Auth.

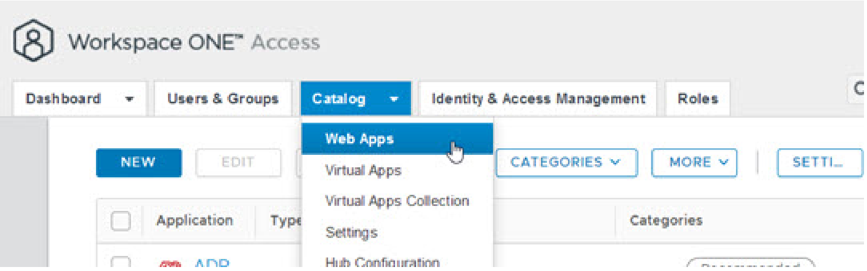
  When Certificate Auth is enabled, you avoid situations where a large number of user provisioning events reach Workspace ONE UEM API request limits causing user provisioning events to be suspended.

  Also, when you use Certificate Auth, you do not need to update the Workspace ONE UEM admin password in the AirWatch Provisioning app when the password is changed.

Procedure

1 Log in to theWorkspace ONE Access console.

2 Select the **Catalog > Web Apps** tab.



3 Click **New**.

4 Enter `AirWatch Provisioning` in the Search text box or click **or browse from catalog**, and select AirWatch Provisioning from the results.

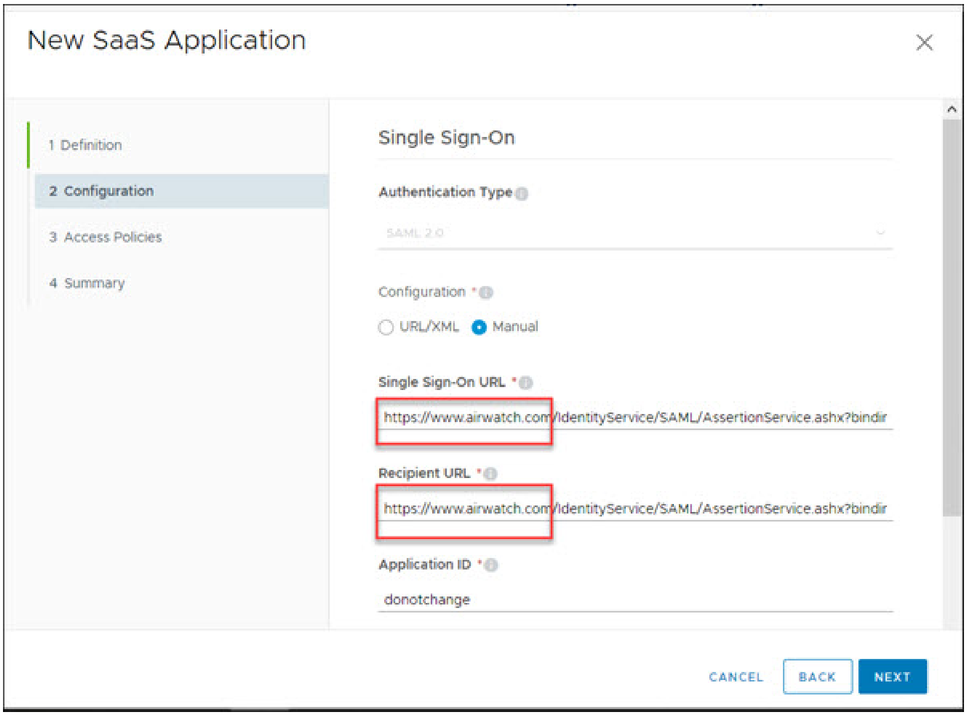
5 To proceed, click **Next**.

6 On the Single Sign-On page, configure the settings required by your organization.

Some settings are populated with default values relevant to the AirWatch Provisioning app. To learn more about a setting, click the information icon next to the setting.

Note For any setting not listed in the following table, accept the default value.

Setting	Description
Authentication Type	Populated with the SAML profile.
Configuration	Select **Manual**.
Single Sign-On URL	This field is not used for AirWatch provisioning, but cannot be empty. An empty field generates a validation error. You can leave the default address.
Recipient URL	This field is not used for AirWatch provisioning, but cannot be empty. An empty field generates a validation error. You can leave the default address.



Authentication Type: SAML 2.0

Configuration *: ○ URL/XML ● Manual

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

Recipient URL *: https://www.airwatch.com/IdentityService/SAML/AssertionService.ashx?bindir

Application ID *: donotchange

7 Click **Next**. Keep the **default_access_policy_set**.

8 Click **Save**.

The app is added to the catalog. Now you can enable provisioning.

9 Select the AirWatch Provisioning app from the catalog list and click **Edit**.

10 Select **Provisioning** and enter the following information.

Configure the Workspace ONE UEM admin account that can authenticate against the AirWatch REST API.

- (Recommended) Select **Enable Certificate Auth** to use the same values you configured in Identity & Access Management > Setup > Workspace ONE UEM to authenticate to Workspace ONE UEM.
- For **Workspace ONE UEM Group ID**, enter your top-level OG group ID.

or

- To use a basic Workspace ONE UEM admin account, enter **Workspaces ONE UEM Host URL** of your Workspace ONE UEM REST API (usually as `xxx.awmdm.com`)
- Enter the basic admin account **Admin Username** and **Admin Password**.

  Note This role for this Workspace ONE UEM admin account is configured as Console administrator.

  Important By default, the password of this administrator is changed every 30 to 90 days from the Workspace ONE UEM console. When this password is changed, you must update the password in the AirWatch Provisioning app settings in the Workspace ONE Access console.

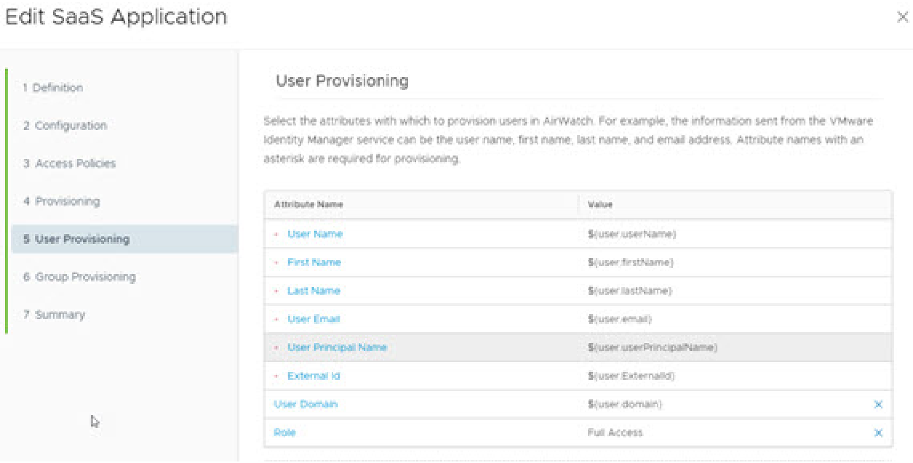
- Enter the **Workspace ONE UEM API Key**.

  Note If you do not have an API key, in the UEM console, go to **Groups & Settings > All Settings > System > Advanced > API > REST API**. Click **Override** and select **Add**. Provide a service name and the account type of **Admin**. Copy the API key to enter on this page.

- Enter the **Workspace ONE UEM Group ID**. Enter your top-level OG group ID.

11 Click **Test Connection** to validate connectivity. Click **Next**.

12 In the User Provisioning page, verify that the attributes with which to provision users in Workspace ONE UEM are listed. Attribute names with an asterisk are required for provisioning. Click **Next**.



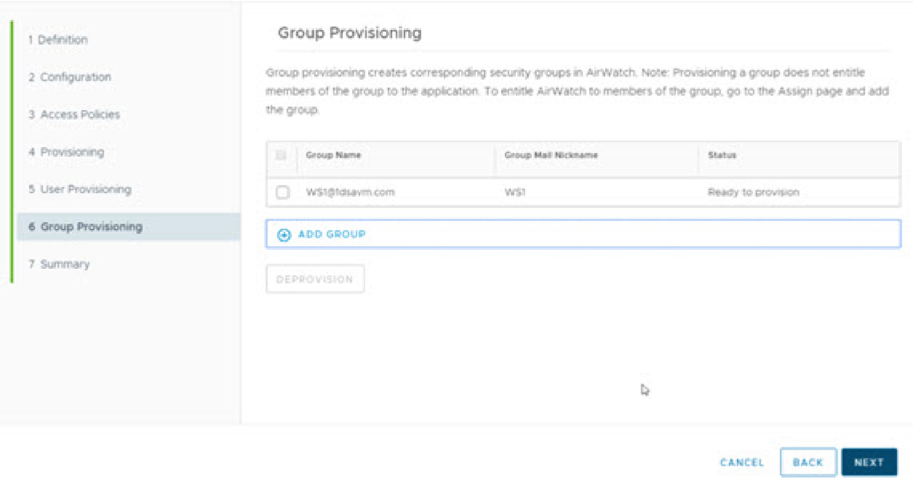
User Provisioning

Select the attributes with which to provision users in AirWatch. For example, the information sent from the VMware Identity Manager service can be the user name, first name, last name, and email address. Attribute names with an asterisk are required for provisioning.

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	×

If you are using JIT, make sure that the SAML assertion includes the User Name attribute. Also make sure that the keys in the SAML assertion match the attribute names exactly, including the case.

13 In the Group Provisioning page, add the groups that you want to provision in Workspace ONE UEM. These user groups are automatically created in Workspace ONE UEM.



Group Provisioning

Group provisioning creates corresponding security groups in AirWatch. Note: Provisioning a group does not entitle members of the group to the application. To entitle AirWatch to members of the group, go to the Assign page and add the group.

□	Group Name	Group Mail Nickname	Status
□	WS1@tdsavm.com	WS1	Ready to provision

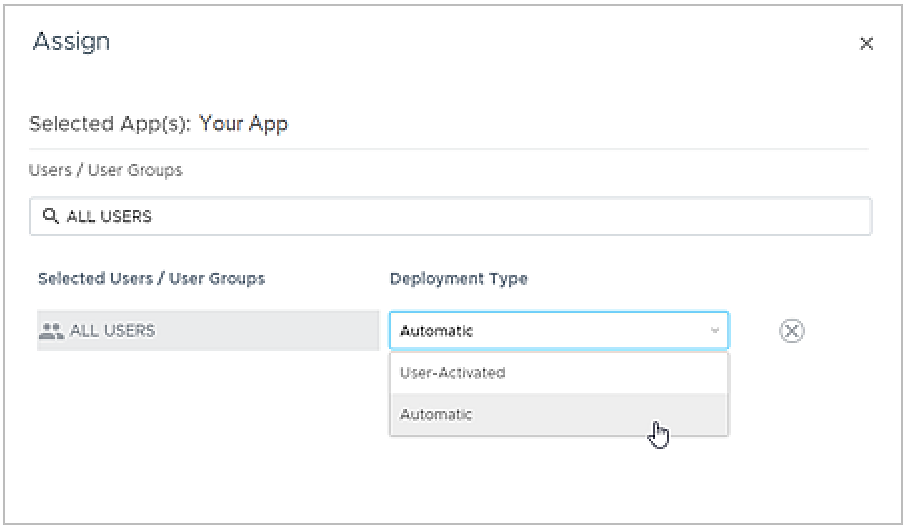
14 Click **Next** and on the Summary page, click **Save**.

Assign the AirWatch Provisioning App to Users

You can entitle individual users or you can entitle a group. When you entitle a group, the members of the group are provisioned as users, if they do no exist in Workspace ONE UEM.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select the **Catalog > Web Apps** tab.
3. Select the check box next to AirWatch Provisioning in the application list. Then click **Assign**.
4. Select users and groups by entering the name in the text box and selecting from the results. To select all users in your organization, enter `ALL USERS` in the text box.



Assign

Selected App(s): Your App

Users / User Groups: ALL USERS

Selected Users / User Groups: ALL USERS

Deployment Type: Automatic

5. Under Deployment Type, select **Automatic**.

   If you leave the default as User Activated, the user cannot be provisioned in Workspace ONE UEM.

6. Click **Save**.

   Users that are assigned to the app are provisioned in Workspace ONE UEM when they are entitled to the app.

   Group memberships are also provisioned to Workspace ONE UEM for the groups that you add in the Group Provisioning page.

Troubleshooting AirWatch Provisioning Configuration

2

The troubleshooting topics describe common problems and solutions to provisioning with the AirWatch Provisioning app.

This chapter includes the following topics:

- Provisioning Status Shows User Is Not Provisioned
- Enrolling a Device with the Workspace ONE Intelligent Hub App Causes an Error
- Provisioning the Mobile SSO Profile With AirWatch Provisioning Generates Error

Provisioning Status Shows User Is Not Provisioned

After you configured the AirWatch Provisioning app and assigned users to the app, users are not provisioned in Workspace ONE UEM.

Problem

When you are provisioning users, and you receive the error `Error not provisioned` in the assignment screen, when you point to the error, you see this message, `Failed to validate attributes while trying to provision users`.

Cause

The value of the attribute names you mapped in the User Provisioning page is missing.

Solution

- Make sure that the users created in Workspace ONE Access include all the attributes required to create the user account in Workspace ONE UEM. When using JIT, make sure that the GUID sent as part of the SAML attributes is valid. This GUID is mapped to the External ID and provisioned to Workspace ONE UEM.

Enrolling a Device with the Workspace ONE Intelligent Hub App Causes an Error

You cannot enroll your device with the Intelligent Hub app.

Problem

When users try to enroll a device using the Intelligent Hub app, they receive a generic error, `An Error has occurred`

Cause

The GUID sent as part of the SAML attribute for JIT might not be mapped to the External ID.

Solution

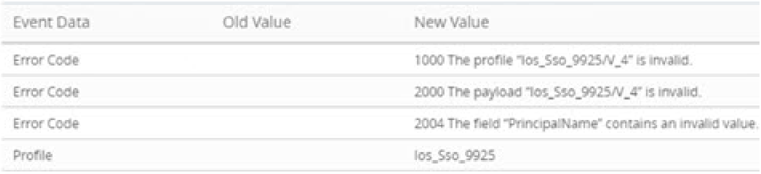
- Make sure that the attribute named External Id is correctly mapped and the provisioned to Workspace ONE UEM.

Provisioning the Mobile SSO Profile With AirWatch Provisioning Generates Error

When admins try to provision the Mobile SSO profile with the AirWatch Provisioning app, they receive an error that the PrincipalName contains an invalid value.

Problem

You see the following error codes.



Event Data	Old Value	New Value
Error Code		1000 The profile "Ios_Sso_9925/V_4" is invalid.
Error Code		2000 The payload "Ios_Sso_9925/V_4" is invalid.
Error Code		2004 The field "PrincipalName" contains an invalid value.
Profile		Ios_Sso_9925

Cause

The Workspace ONE UEM account might be configured to use an email address as the User Name attribute value.

When the Mobile SSO certificate payload is created, the payload uses the user name attribute value as the principal name on the certificate. You cannot use the @ character in the principle name.

Two ways to resolve this issue are described.

Solution

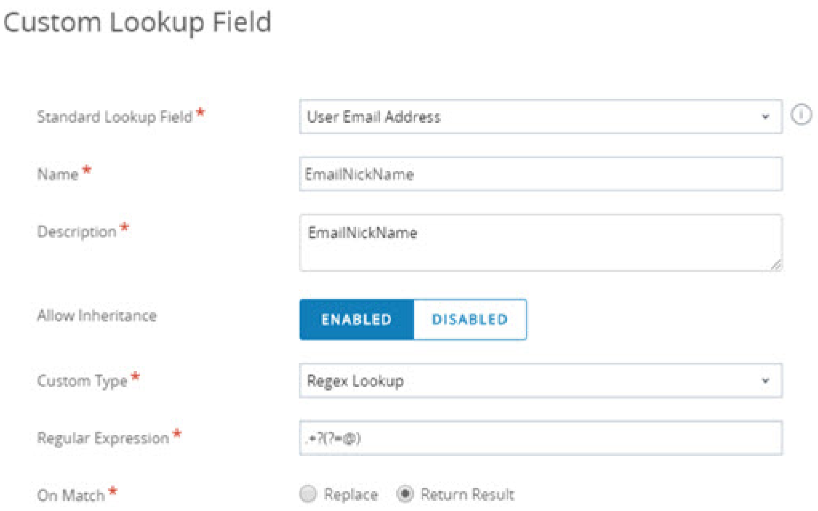
1 In the User Provisioning page of the AirWatch Provisioning app, select another attribute that does not include the @ sign to represent the user name. You might need to edit the value that is imported into . Make sure that the user name and the prefix of the UPN remain the same.

2 Configure a custom lookup field in the Workspace ONE UEM console to parse the prefix of the email address. Use that custom setting in the certificate payload.

   a In the Workspace ONE UEM console, go to **Group & Settings > All Settings > Devices & Users > General > Lookup Fields**.

   b Select **Add Custom Field**.

   c Create a name. For example, `EmailNickName` and create a regex such as `".+?(?=@)"`.



Custom Lookup Field

Standard Lookup Field* User Email Address

Name* EmailNickName

Description* EmailNickName

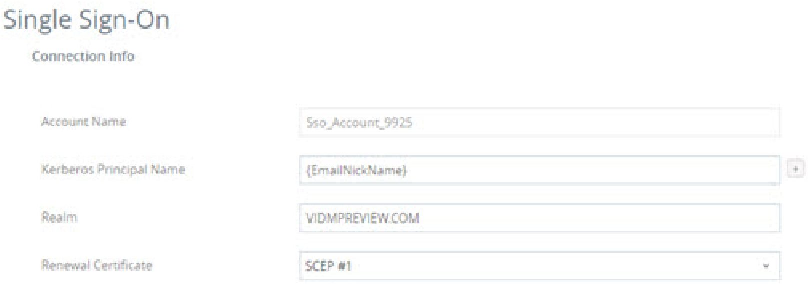
Allow Inheritance ENABLED DISABLED

Custom Type* Regex Lookup

Regular Expression* .+?(?=@)

On Match* ○ Replace ● Return Result

3 You can then use the name you created in the Certificate Payload.



Single Sign-On

Connection Info

Account Name Sso_Account_9925

Kerberos Principal Name {EmailNickName}

Realm VIDMPREVIEW.COM

Renewal Certificate SCEP #1