VMware Identity Manager Integration with Office 365

VMware Identity Manager

APRIL 2019 V10

Table of Contents

Overview

This document provides information about configuring the VMware Identity Manager integration with Office 365 for the following services.

- Single sign-on from the VMware Identity Manager service to Office 365 applications
- Create client access policies for Office 365 username/password clients
- Configure outbound provisioning of users and groups to the Office 365 tenant
- Configure reverse proxy when using Office 365 legacy authentication with mobile devices
- Prepare a non-routable domain with Office 365 and Active Directory

Configuring Single Sign-on to Office 365

For single sign-on, VMware Identity Manager is the identity provider and allows Office 365 to trust the VMware Identity Manager service for authentication to Office 365 apps. To use single sign-on to access these Office 365 applications, the Office 365 domain must be changed from managed to federated, and the Office 365 domain parameters settings changed to authenticate through the service.

The Office 365 application must be configured to synchronize with the local Active Directory to create the Office 365 user accounts When you add Office 365 to the catalog through VMware Identity Manager, you identify the source anchor from Active Directory during the set up. This is configured because the sourceAnchor attribute acts as a unique identifier for each object which lets you change other properties such as UPN and replicate them to the proper matching object in Office 365.

For many Office 365 app deployments, Microsoft recommended the objectGUID attribute to be used as the source anchor. The VMware Identity Manager configuration supports using the objectGUID attribute as the anchor by default.

Microsoft recommends that deployments of Azure AD Connect use the ms-DS-ConsistencyGuid as the sourceAnchor attribute. Beginning with VMware Identity Manager 19.03, VMware Identity Manager created a sourceAnchor attribute that can be mapped to the attribute you identify as the source anchor to use as the unique identifier, including ms-DS-ConsistencyGuid.

Before you grant Office 365 entitlements to your organization’s users and groups, work with your Office 365 account administrator to configure your account to use SAML-based federated authentication with the service.

To set up single-sign-on between Office 365 and the service, you perform the following actions.

- Update user attributes mapping in the VMware Identity Manager directory to include user attributes
  - userPrincipalName and objectGUID mapped to Active Directory attributes.
  - If you use an attribute other than objectGUID as the source anchor, map the sourceAnchor attribute in VMware Identity Manager to the anchor you use as the unique identifier in Active Directory.
- Synchronize Active Directory to the VMware Identity Manager directory if you are not using provisioning.
- Add the Office 365 applications to the Catalog and configure the Office 365 settings.
- Change the values in the Office 365 domain authentication settings to the VMware Identity Manager settings for single sign-on.

Authentication Profiles Options for Single Sign-on

Two authentication profiles for single sign-on to Office 365 are available in the VMware Identity Manager service, modern authentication and the legacy authentication flow.

The modern authentication flow supports single sign-on to Office 365 web applications and native applications using a web browser interface. Users who launch Office 365 applications are directed to VMware Identity Manager to sign in according to polices set in the VMware Identity Manager service.

The legacy authentication flow supports single sign-on to the legacy Office applications, such as older version of Outlook. The legacy authentication flow is also commonly used by third party office clients such as Android native email apps or Thunderbird. Users who launch these applications provide their credentials directly into the application interface. Office 365 proxies the request to VMware Identity Manager on behalf of the client.

Configure Multiple Domains to Access Office 365 App

You can configure multiple domains in your deployment to access a single Office 365 app in the VMware Identity Manager catalog. This configuration gives you the ability to manage SSO federation information, entitlements from one Office 365 app in the VMware Identity Manager catalog.

The Office 365 domains can be domains from a single directory or can belong to different directories in VMware Identity Manager.

You must convert each Office 365 managed domain created through the Office 365 admin console to a federated domain for single sign-on to the Office 365 app. The Office 365 account settings must be configured to the service settings.

When you configure the Office 365 application parameters in the catalog, you configure the Office 365 Tenant Domain and the Office 365 Tenant Issuer for each domain.

Note: Provisioning users is not available when multiple domains are configured to access the Office 365 app.

Adding Office 365 App to VMware Identity Manager Catalog

To enable single sign-on to Office 365 applications in the VMware Identity Manager service, you must update the user attribute map, and configure the apps in the catalog.

Map User Attributes

The VMware Identity Manager directory syncs the Active Directory user attributes that you configure. You specify on the User Attributes page which default attributes you want to map to Active Directory attributes.

If you enable the provisioning feature, map the same attributes and values for provisioning users as you configure for single sign-on.

When you add attributes, the attribute name you enter is case-sensitive. For example, objectGUID, ObjectGUID, ObjectGuid are different attributes.

Procedure

1. In the VMware Identity Manager admin console, Identity & Access Management tab, click **Setup > User Attributes**.
2. In the **Default Attributes** section, verify that **userPrincipalName (UPN)** is a mapped attribute.
3. Map other attributes as required for your organization.
4. In the **Add other attributes to use** section, click **+**.
5. In the text box, enter **objectGUID**.

   If configuring Azure AD Connect, V11.524 or later, and the source anchor in Active Directory is not objectGUID, you can select **sourceAnchor** as the attribute that as required.
6. Click **Save**.
7. Next, go to the **Manage > Directories** page and select the directory to use.
8. Click **Sync Settings > Mapped Attributes**.
9. In the **Attribute Name in Active Directory** column, select the Active Directory attributes to map to the VMware Identity Manager attributes selected in the User Attributes page.

   Usually, the userPrincipalName is mapped in an email address format.
10. Click **Save**.

The directory is updated the next time the directory syncs to the Active Directory. When you configure Office 365 in the catalog, these attributes are automatically added to the Office 365 Configuration page.

Add Office 365 Application to the Catalog

Add the Office 365 with Provisioning web application to the Workspace ONE catalog and create the access policy.

All the Office 365 apps can be accessed through the Office 365 portal with single sign-on. When users sign in, they can select the Office 365 app to use.

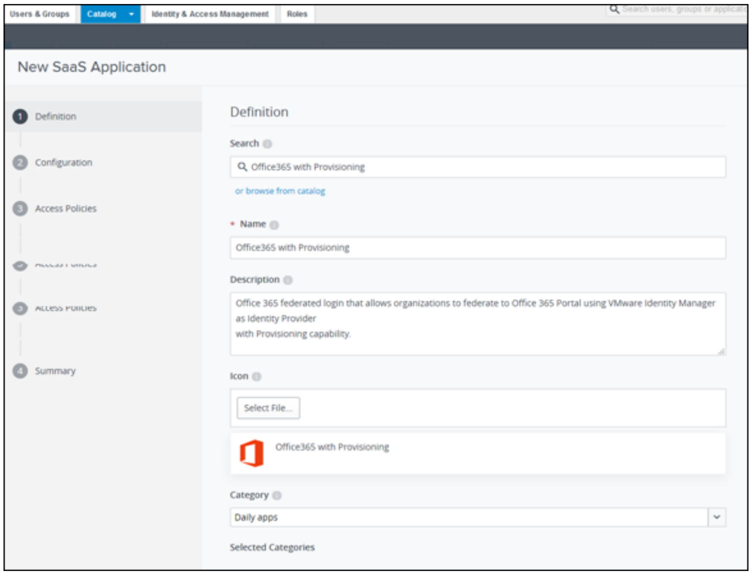
Procedure

1. Log in to the VMware Identity Manager admin console.
2. In the Catalog > **Web Apps** page, click **New**.
3. In the Definition page, **Search** text box, enter **Office365** and select the Office 365 with Provisioning application to add to the catalog.

   The page is updated with the Office 365 Provisioning name, description and icon to display.

   You can add a category to apply to this application

   Click **Next**.



New SaaS Application

Definition

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

Category: Daily apps

Selected Categories

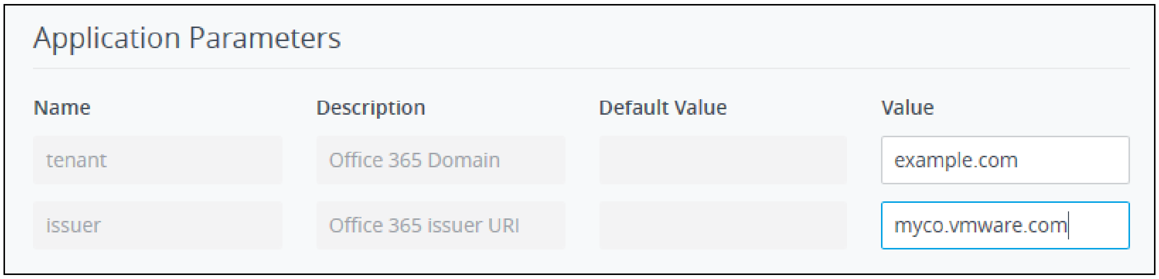
4. Click **Configuration**. Some of the fields are automatically populated. Modify the application configuration as required.

FIELD	**CONFIGURED VALUE**
Target URL	Populated with the URL to go to after the SAML is accepted.
Single Sign-On URL	Enter the Office 365 sign in page URL. This is also known as the Assertion Consumer Services URL .**https://login.microsoftonline.com/login.srf**

Username Format	This value is how the user identifier is sent. In most cases, select **Unspecified (username)**. If your configuration requires a format other than username, select the format from the drop-down menu.
Username Value	Custom value ${user.userName}
Application ID	Enter the Office 365 service provider unique identifier **urn:federation:MicrosoftOnline**
Assertion Time	The number of seconds the SAML assertion is valid. The assertion issued by the service is valid for 200 seconds by default. You can change this.
Credential Verification	Active Directory password is the default authentication method used for credential verification to sign in to the Office applications. Per-App password requires users to configure a password for their Office 365 applications in their portal. This per-app password must also be configured in the Office 365 native client.
Signature Algorithm	SHA1 with RSA
Digest Algorithm	SHA1

5. In the **Application Parameters** section, configure the value for Office 365 Tenant Domain and for Office 365 Tenant Issuer.

- **Outlook Tenant Domain**, enter the Office 365 domain which is configured as a Federated Domain within the Office 365 Active Directory admin console.
- **Outlook Tenant issuer**, enter the Office 365 application tenant issuer URL. This value must be a globally unique identifier across all of Microsoft Office 365 Active Directory environments. Because the VMware Identity Manager tenant name space is a globally unique name, you can enter this same value here. For example, myco.vmwareidentity.com.



Application Parameters

Name	Description	Default Value	Value
tenant	Office 365 Domain		example.com
issuer	Office 365 issuer URI		myco.vmware.com

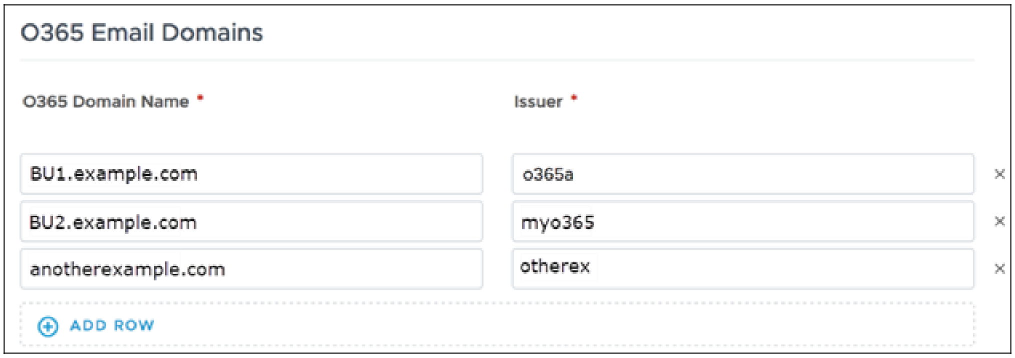
To configure multiple domains to use the Office 365 app

a. Click **Advanced Properties** and switch Enable Multiple O365 Email Domains to **Yes**.

b. Click **ADD ROW**.

c. Enter the Office 365 domain name and the issuer value.

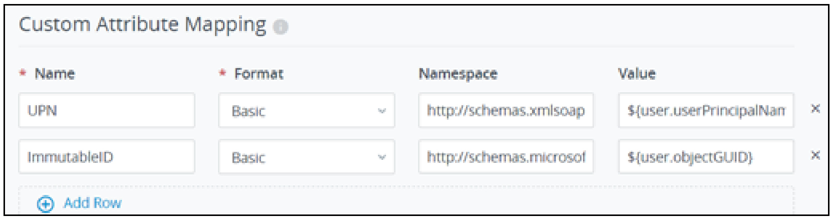
To enter another domain, click **Add Row**.



O365 Email Domains

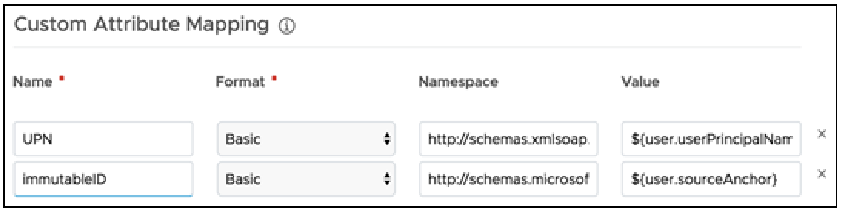
O365 Domain Name *	Issuer *
BU1.example.com	o365a
BU2.example.com	myo365
anotherexample.com	otherex

6. The values in the **Custom Attribute Mapping** section are the userPrincipalName and objectGUID or the sourceAnchor attributes mapped in the directory.



Custom Attribute Mapping

* Name	* Format	Namespace	Value
UPN	Basic	http://schemas.xmlsoap	${user.userPrincipalNam
ImmutableID	Basic	http://schemas.microsof	${user.objectGUID}



Custom Attribute Mapping

Name *	Format *	Namespace	Value
UPN	Basic	http://schemas.xmlsoap.	${user.userPrincipalNam
immutableID	Basic	http://schemas.microsof	${user.sourceAnchor}

7. Click **Next**.

   Create the access policy for Office 365.

   See Conditional Access Policies for Legacy Authentication Office 365 Clients to learn more about creating access policies.

Adding Multiple Copies of Office 365 Applications to the Catalog

You can configure multiple copies of the Office 365 application in the catalog to manage different sets of users. When your organization manages multiple Office 365 tenants, you can include all the tenants in a single instance of VMware Identity Manager. This enables you to manage single sign-on and access to all the tenants from one location.

When users log into Workspace ONE and click the Office 365 application to which they are entitled, the correct app is launched. When users log into the service provider directly, the service provider redirects to VMware Identity Manager for authentication and VMware Identity Manager authenticates the users and launches the correct app based on user entitlements.

You can add multiple copies of the application from the catalog and configure each application separately. Or, you can configure the first application and then make copies of the application. The UUID is automatically changed in the copied application, but the values configured in the Details and Configuration, pages are not changed. In copied applications, the only values you must change are the application name, the tenant domain, and the tenant issuer value. You configure user entitlements for each copy of the app and set the access policies.

Add a Copy of the Application.

1. In the Catalog page, select the Office 365 application to copy.
2. In the Details page, click **Copy**.
3. Select the copied application from the Catalog page and edit the application details as follows
   a. In the Details page, change the name to identify the Office 365 tenant.
   b. In the Configuration page, Application Parameters section, change the **Outlook Tenant Domain** and **Outlook Tenant Issuer** name to the domain and tenant issuer URL for this tenant.
   c. Click **Save**.
   d. Click **Entitlements** and add user and group entitlements.
   e. Click **Access Policies** to select the access policy set and to create client access policies for username/password clients.
   f. Click **Save**.

Preparing to Set Up Single Sign-on to Office 365

Work with your Microsoft service provider to make sure that your managed Office 365 environment is correctly set up before you configure the Office 365 application in the VMware Identity Manager service for single sign-on.

Office 365 Prerequisites

- Microsoft Office 365 Business Premium account
- Access and credentials for the Microsoft Office 365 Tenant Admin Portal
- Attributes userPrincipalName and object GUID or sourceAnchor enabled
- PowerShell must be installed on the Windows server

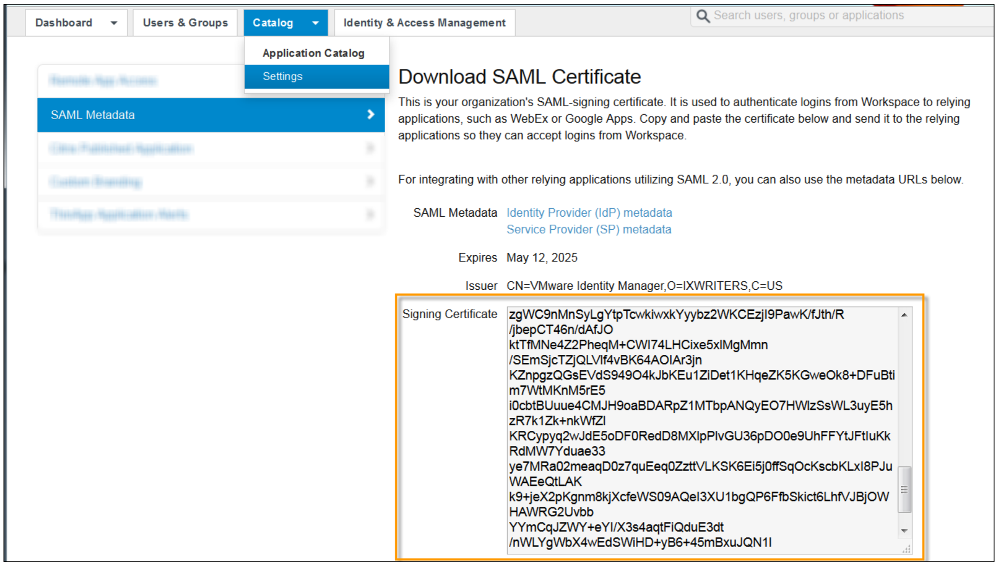
Download Identity Provider Signing Certificate from VMware Identity Manger

When you configure single sign-on to Office 365 applications, you must copy the VMware Identity Manager service's signing certificate and send it to the relying Office 365 application's service.

1. In the VMware Identity Manager admin console **Catalog** tab, click **Setup > SAML Metadata.**
2. Copy and save the **Signing Certificate** text to a .txt or .crt file.

   To use this with Office 365 admin domain federation configurations, you must make the certificate value a single line item. Remove the beginning and ending certificate brackets ("------BEGIN CERTIFICATE------" and "------END CERTIFICATE------) and all carriage returns.

   You add the signing certificate text when you configure Office 365.



Download SAML Certificate

This is your organization's SAML-signing certificate. It is used to authenticate logins from Workspace 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 Workspace.

For integrating with other relying applications utilizing SAML 2.0, you can also use the metadata URLs below.

SAML Metadata: Identity Provider (IdP) metadata
Service Provider (SP) metadata

Expires: May 12, 2025

Issuer: CN=VMware Identity Manager,O=IXWRITERS,C=US

Signing Certificate:

```
zgWC9nMnSyLgYtpTcwkiwxkYyybz2WKCEzjI9PawK/fJth/R
/jbepCT46n/dAfJO
ktTfMNe4Z2PheqM+CWI74LHCixe5xlMgMmn
/SEmSjcTZjQLVIf4vBK64AOIAr3jn
KZnpgzQGsEVdS949O4kJbKEu1ZiDet1KHqeZK5KGweOk8+DFuBti
m7WtMKnM5rE5
i0cbtBUuue4CMJH9oaBDARpZ1MTbpANQyEO7HWlzSsWL3uyE5h
zR7k1Zk+nkWfZI
KRCypyq2wJdE5oDF0RedD8MXlpPlvGU36pDO0e9UhFFYtJFtIuKk
RdMW7Yduae33
ye7MRa02meaqD0z7quEeq0ZzttVLKSK6Ei5j0ffSqOcKscbKLxI8PJu
WAEeQtLAK
k9+jeX2pKgnm8kjXcfeWS09AQeI3XU1bgQP6FfbSkict6LhfVJBjOW
HAWRG2Uvbb
YYmCqJZWY+eYI/X3s4aqtFiQduE3dt
/nWLYgWbX4wEdSWiHD+yB6+45mBxuJQN1I
```

Configure Office 365 as a Federated Domain for Single Sign-on

You must convert your Office 365 managed domain to a federated domain for single sign-on and update the Office 365 account settings to the service settings.

If you are configuring multiple tenants to use the Office 365 app from the catalog, convert each managed domain to a federated domain and update the Office 365 account settings to the service settings for each domain.

Prerequisite

- Windows PowerShell installed

You use Windows PowerShell and run the **Set-MsolDomainAuthentication** cmdlet to change the domain authentication settings to the VMware Identity Manager settings for single-sign-on.

1. In the PowerShell, enter **Connect-MsolService** to connect to the Office 365 tenant.
2. List the domains. Enter **Get-MsolDomain**.
3. Convert the domain that was created through the Office 365 admin console. Run the **Set-MsolDomainAuthentication** cmdlet to change the following variables to the service's settings.

LINE OF CMDLET	CMDLET VARIABLE OR VARIABLES	REPLACE WITH
–DomainName	*domain_name*	The fully qualified domain name of the VMware Identity Manager service domain that is registered with Microsoft. *example.mycompanydomain_name.com*.
–IssuerUri	*horizon_org_name*	The Outlook tenancy issuer. The unique identifier of the domain in the Office 365 identity platform used in the service, such as *example*.
-FederationBrandName	*Federation_server_name*	This is the company brand name, such as *Mycompany Inc*.
-PassiveLogOnUri	*host* and *port*	The URL that Web-based clients are directed to when signing in, such as https:// *myco.vmwareidentity.com:443/SAAS/API/1.0/POST/sso*. When configuring multiple domains, enter the domain ID for the specific domains. *myco.vmwareidentity.com:443/SAAS/API/1.0/POST/sso?domainid=BU1.example.com*
-ActiveLogOnUri	*host* and port	The URL that specifies the end point used by active clients when authenticating with domain set up for single sign-on, such as https:// *myco.vmwareidentity.com:443/SAAS/auth/wsfed/active/logon.* When configuring multiple domains, enter the domain ID for the specific domains. https:// *myco.vmwareidentity.com:443*/SAAS/auth/wsfed/*active/logon?domainid=BU1.example.com*
-LogOffUri	*host* and *port*	The URL clients are redirected to when they sign out, such as *https://login.microsoftonline.com/logout.srf*.
-MetadataExchangeUri	*host* and *port*	The URL that specifies the metadata exchange end point used for authentication, such as https:// *myco.vmwareidentity.com:443*/SAAS/auth/wsfed/*services/mex*. When configuring multiple domains, enter the domain ID for the specific domains. *https:// myco.vmwareidentity.com:443/SAAS/auth/wsfed/services/mex?domainid=BU1.example.com*
-SigningCertificate	*SAML signing cert from Application Manager*	This is the current certificate used to sign tokens passed to the service. Paste the VMware Identity Manager Signing Certificate here. Before you paste the certificate, exclude the text "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE---

	--" from the certificate content. **Important**. Make sure you do not include additional spaces or extra line returns when you paste the certificate, or it will not work.

4. After the changes are made, verify the federation changes are correct. To do this, type
   `Get-MsolDomainFederationSettings -DomainName <YOUR DOMAIN>`

The following is an example of the output from the PowerShell cmdlet.

```
Get-MsolDomainAuthentication
-DomainName myco.vmwareidentity.com
-Authentication Federated
-IssuerUri example
-FederationBrandName Mycompany, Inc.
-PassiveLogOnUri https://host:port/SAAS/API/1.0/POST/sso
-LogOffUri https://login.microsoftonline.com/logout.srf
-ActiveLogOnUri https://host:port/SAAS/auth/wsfed/active/logon
-MetadataExchangeUri https://myco.vmwareidentity.com/SAAS/auth/wsfed/services/mex
-SigningCertificate
MIICKDCCAZGgAwIBAgIBATANBgkqhkiG9w0BAQUFADBRMS0wKwYDVQQDEy1cejoyyM2otqFmfiQ
jsinm/40TFSj2L7UyRIb3Jpem9uIFNBTUwgU2VsZi1TaWduZWQgQ2VydGlmaWNhdGUxEzARBgNV
BAoT
UklaT043MzAxCzAJBgNVBAYTAlVTMB4XDTEyMDkyMDE4MzIzOFoXDTIyMDkxODE4MzIzOFowUTE
tMCsGA1UEAxMkSG9yaXpvbiBTQU1MIFNlbGYtU2lnbmVkIENl
cnRpZmljYXRlMRMwEQYDVQpIT1JJWk9ONzMwMQswCQYDVQQGEwJVUzCBnzANBgkqhkiG9w0BAQE
FAAOBjQAwgYkCgYEAoYCFzs3pjWke0LhkztflPRv8mhji
fjbsQ9WlFqbFMKkeS8PA47Dwr7lUHqGSAOcfny55m8LLlL554llelrgCHjENi9w6AMFizvALI7q
4kEikTX38IHgAsrg30f4S+Qbr3wj6VmS1wPNFOKqHoqsUbFzI
MzAl2BevuFySvZKWx/cCAwEAAaMQMA4wDAYDVUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQCHdlsh
W//UzL
```

Testing Single Sign-on Configuration

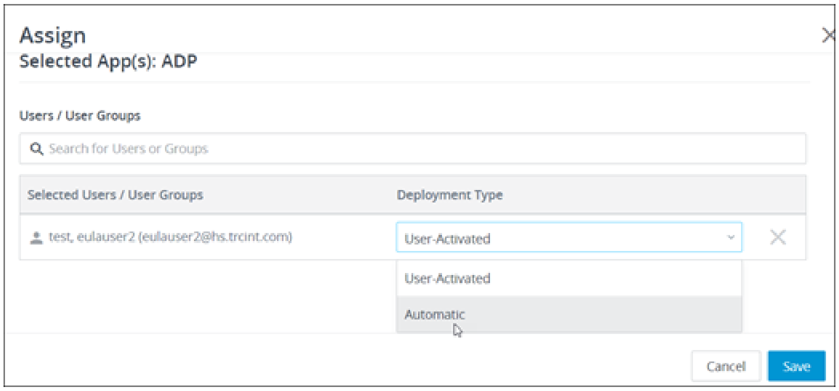
You should test your single sign-on configuration with a small number of users before deploying the application across your organization.

Set up User in VMware Identity Manager for Test

Configure the user ID and email address for testing.

Entitle the test user to an Office 365 application.

1. Log in to the VMware Identity Manager admin console.
2. In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
3. In the Catalog Web Apps page, click on the Office 365 application to be tested.
4. Click **Assign**.
5. In the Users/Users Groups search box, search for the user to add.
6. Select the test user and in the Deployment Type column drop-down menu, select **Automatic**.



Assign

Selected App(s): ADP

Selected Users / User Groups	Deployment Type
test, eulauser2 (eulauser2@hs.trcint.com)	User-Activated

7. Click **Save**.
8. Log out of the administration console. In the header by your name, click the arrow and select **Logout**.

Set Up User in Office 365 for Test

You provision a user in Office 365 application to test single sign-on through the VMware Identity Manager service.

1. Log in to the Office 365 portal as the administrator.
2. Navigate to the **users and groups Add new users** page.
3. In the page that appears, in the **Display name** and a **User name** text box, enter the test user name. The User name is the name used to sign in to Office 365.
4. If you have more than one domain, select the correct domain for this user from the drop-down menu.
5. Click **Create** to create the test account.

Verify Test-User Can Sign in to an Office 365 Web Application

Now that a user is entitled in the service and set up in Office 365, test that the user can sign in to the Office 365 Web application from the apps portal.

1. In the browser, enter the URL to the user’s apps portal sign-in page and sign in with the test user name and password.

2. In the apps portal page, click the Office 365 application.

You should successfully sign in to Office 365.

Verify Test-User Can Sign in to an Office 365 Native Application

1. Launch the Office 365 native application installed on the test user's computer.
2. Click the login link for the application and enter the email address and password.
    a. If the Per App Password is configured, enter the password that was set through the apps portal page.
    b. If Active Directory password is configured, enter the test user's Active Directory password.

You should successfully sign in to Office 365.

Entitle Users to Office 365

After Office 365 is configured and tested, you can entitle users to the application. Users see the application and can launch the app from their app portal. If you remove the entitlement, users cannot see or launch the application.

You can select how the entitled resource is activated.

- **Automatic** displays the application by default in an entitled user's list of Web applications the next time that user signs in using the VMware Identity Manager Desktop application.
- **User-Activated** requires that an entitled user must add the Web Identity Manager Desktop application before the user can use the Web application.

1. Log in to the VMware Identity Manager admin console.
2. In the Catalog page, click on the Office 365 application.
3. Click **Assign**.
4. In the Users/Users Groups search box, search for the user to add.
5. In the Deployment Type column drop-down menu, select how to activate the application, either **Automatic** or **User Activated**.
6. Click **Save**.

Conditional Access Policies for Legacy Authentication Office 365 Clients

When you add the Office 365 with Provisioning application to the Workspace ONE catalog, you can configure client access policies that control user access to Office 365 services that use the legacy authentication flow.

Office 365 clients that collect credentials such as user name and password in their own user interface are using the legacy authentication flow for authentication. For example, the 2007 and 2010 versions of Office require users to enter credentials directly into the client application user interface.

Note: If the client redirects users in a browser or a web view to an identity provider, you are using modern authentication. You can control access to modern authentication clients using the VMware Identity Manager conditional access policies. See Configuring Access Policy Settings in the VMware Identity Manager Administration guide.

Configuring Access Controls

By default, older versions of Office and mobile email client applications use legacy username and password authentication flow to log in to the Office 365, where they can access valuable business data such as emails, OneDrive files, and SharePoint documents. These older client versions only support user name and password for authentication. To add an additional level of access control, admins can configure access policies to control access or block access to Office 365 applications in the Workspace ONE Catalog pages.

Important. Applications that use legacy username/password authentication rely on headers provided by the client app to make access decisions. When you configure access policies for Office 365 services, VMware Identity Manager reads the HTTP headers such as the x-ms-client-user-agent header to derive information about clients and users. The clients are responsible for the accuracy of the header information. Attackers can spoof headers from username/password clients.

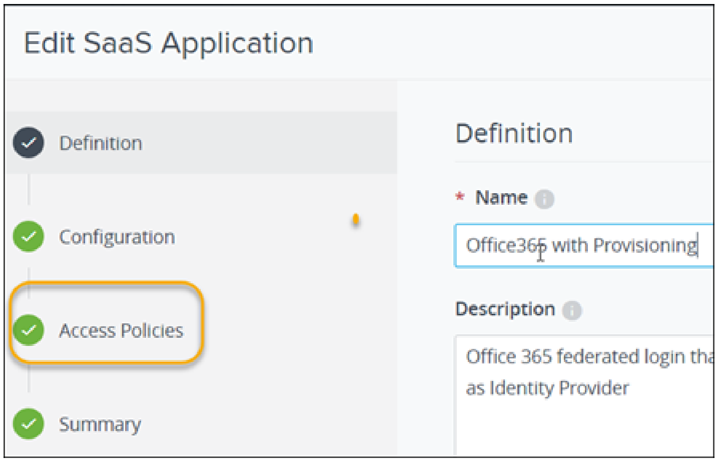
Configure Client Access Policies

In the VMware Identity Manager admin console, client access policies can be configured to manage access or deny access to Office 365 services based on location, group membership, device type, email protocol, and client type.

Procedure

You configure the client access policies in the Office 365 Provisioning application in the Workspace ONE catalog.

1. Log in to the VMware Identity Manager admin console.
2. In the Catalog page, select the **Office365 with Provisioning** application.
3. Click **Edit. > Access Policies**



Edit SaaS Application

Definition

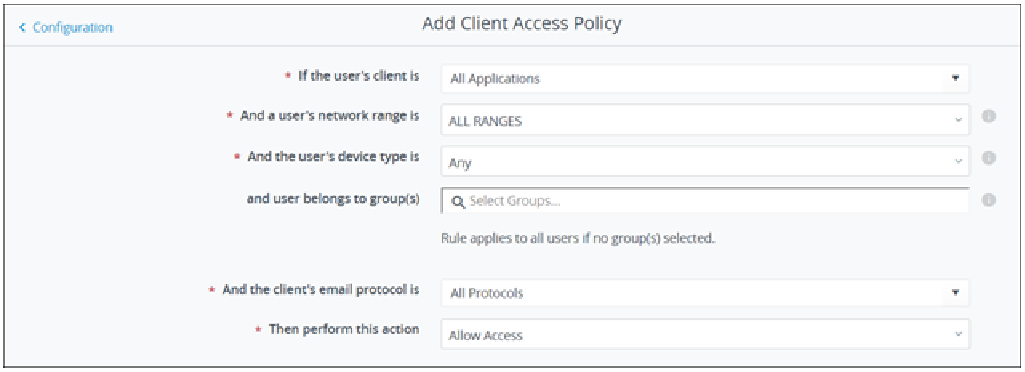
* Name

Office365 with Provisioning

Description

Office 365 federated login tha
as Identity Provider

4. In the Client Access Policies for Username/Password Clients section, click **Add Policy Rule** to add a new client access policy.



< Configuration

Add Client Access Policy

* If the user's client is: All Applications

* And a user's network range is: ALL RANGES

* And the user's device type is: Any

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

Rule applies to all users if no group(s) selected.

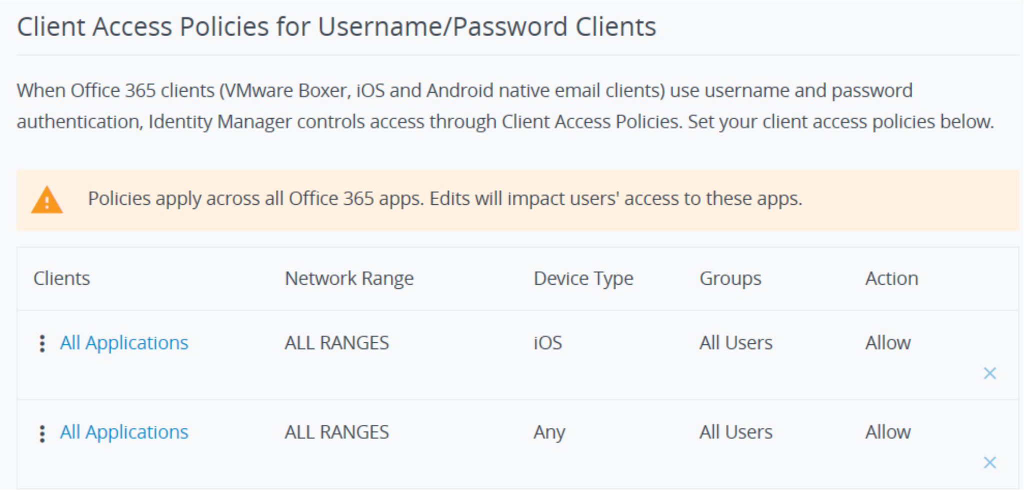
* And the client's email protocol is: All Protocols

* Then perform this action: Allow Access

5. Select the conditions to apply to the client access policy.

Option	Description
If the use's client is	Select the user client that this policy is used with. • The user clients that are preconfigured are VMware Boxer and Microsoft Outlook. • You can select All Application to use this policy for all clients that use username/password to access Office 365.
User's network range is	Select the network range for this policy. The network range defines the IP addresses for which users can log in.
User's device type is	Select the type of device that the policy manages. The types available are Android, iOS, macOS, or Windows 10. You can select All Device Types to apply this policy to all of these devices.
User belongs to groups	Select the groups that this access rule applies to. If you do not select a group, the access policy applies to all users.
User's client email protocol is	Select the email protocol. The email protocols are Microsoft Exchange Active Sync, POP, All Protocols.

6. In the Then perform this action drop-down menu, select whether to **allow access** or to **deny access** based on the conditions you applied.
7. Click **Save** to create a client access policy to Office 365.
8. Create additional client access policies as required.
9. Drag the policies to arrange the policies in the order in which they are applied.
10. Click **Save**.



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.

Policies apply across all Office 365 apps. Edits will impact users' access to these apps.

Clients	Network Range	Device Type	Groups	Action
All Applications	ALL RANGES	iOS	All Users	Allow
All Applications	ALL RANGES	Any	All Users	Allow

It is important to arrange the Client Access Policies in order as the policies are enforced from the first policy in the list to the last policy. The first policy that applies to a client is used to either authenticate for access or to deny access. For example, if you create a policy denying access to any device type and drag it above a policy allowing access for iOS devices, the deny policy on top is enforced for all devices, including iOS devices, that attempt username/password authentication. The policy to allow access for iOS devices is not enforced as users are denied access before the Allow Access policy can be applied.

Client Access Policy Use Cases

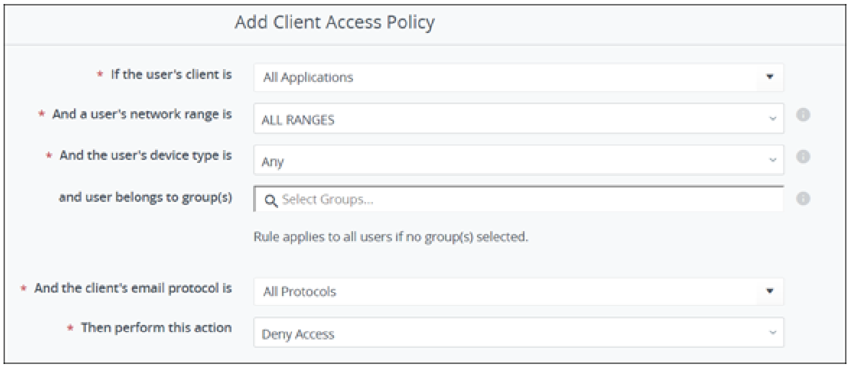
The following are samples of common use cases where client access policies can be applied.

Allow legacy username/password access to Office 365 for mobile email only

In this approach, an organization can block legacy username/password access to Office 365 apps and data for all apps. Then add an exception for native mobile email clients that use Exchange ActiveSync. This approach works well with the Mobile Email Management features in Workspace ONE. Many organizations choose this path because Exchange ActiveSync clients do not download the user’s entire mailbox, reducing the risk of data loss. Your organization can also choose to limit mobile email access to the extra-secure VMware Boxer app.

To learn more about Mobile Email Management, see the Managing and Protecting Mobile Email white paper.

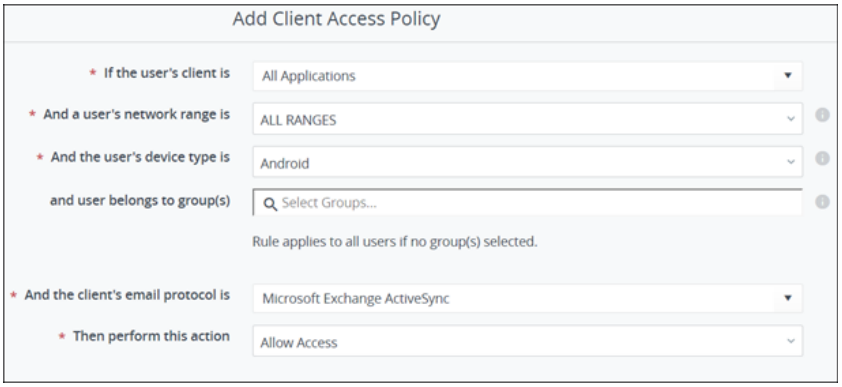
1. Create a policy that denies access to all clients.



Add Client Access Policy

* If the user's client is	All Applications
* And a user's network range is	ALL RANGES
* And the user's device type is	Any
and user belongs to group(s)	Select Groups...
	Rule applies to all users if no group(s) selected.
* And the client's email protocol is	All Protocols
* Then perform this action	Deny Access

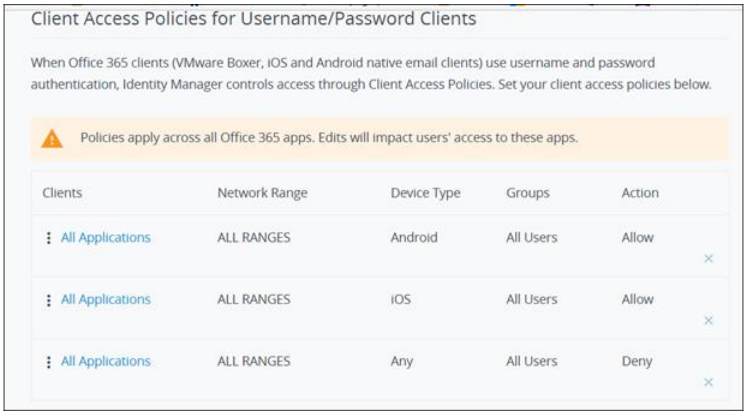
2. Create a policy that allows all clients to access Exchange ActiveSync on Android.



Add Client Access Policy

* If the user's client is	All Applications
* And a user's network range is	ALL RANGES
* And the user's device type is	Android
and user belongs to group(s)	Select Groups...
	Rule applies to all users if no group(s) selected.
* And the client's email protocol is	Microsoft Exchange ActiveSync
* Then perform this action	Allow Access

3. Create a policy that allows all clients to access Exchange ActiveSync on iOS.
4. Arrange the policies so that the policy to deny access to all devices is the last in the list.
5. Save your changes.



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.

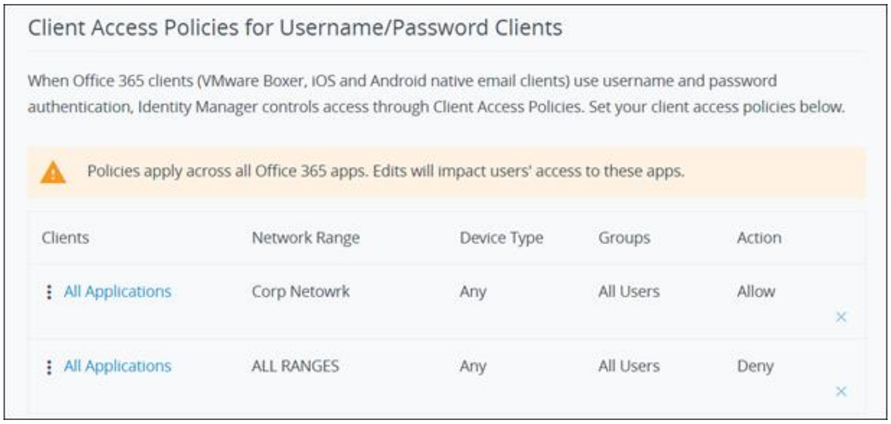
Policies apply across all Office 365 apps. Edits will impact users' access to these apps.

Clients	Network Range	Device Type	Groups	Action
All Applications	ALL RANGES	Android	All Users	Allow
All Applications	ALL RANGES	iOS	All Users	Allow
All Applications	ALL RANGES	Any	All Users	Deny

Allow legacy username/password access to Office 365 under more secure conditions

Because legacy username/password clients such as the Thunderbird app or older versions of Office do not support multifactor authentication (MFA), some organizations want to limit these clients to only connect to Office 365 under more secure circumstances. For example, you might only allow Thunderbird on your corporate network to ensure users are not downloading their mailboxes on multiple computers. This approach can reduce the risk of data loss.

1. Create a policy that denies access to all clients.
2. Create a policy that allows all clients to access only the internal corporate network IP ranges.
3. Arrange the policies so that the policy to access to the internal corporate network is listed first.
4. Save your changes.



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.

⚠ Policies apply across all Office 365 apps. Edits will impact users' access to these apps.

Clients	Network Range	Device Type	Groups	Action
All Applications	Corp Netowrk	Any	All Users	Allow
All Applications	ALL RANGES	Any	All Users	Deny

Allow legacy username/password access only for specific users or groups

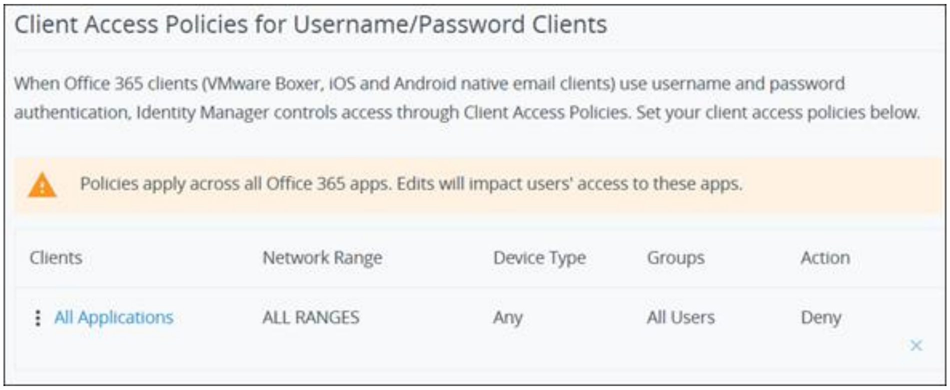
Organizations might want to limit which users can connect to Office 365. For example, a policy could be created to block retail employees from accessing mobile email while they are not on site.

1. Create a policy that denies access to all retail employees from all device types.
2. Create a policy that allows retail employees to access only the internal corporate network IP ranges from all device types.
3. Arrange the policies so that the policy to access to the internal corporate network is listed first.
4. Save your changes.

Block All Access to Office 365 for Username/Password Clients

Some organizations want to ensure all users access Office 365 using multifactor authentication, Mobile SSO, or other secure methods. Because modern authentication supports these methods, but legacy username/password authentication does not, these organizations must block username/password client apps. Users can still access Office 365 through Office 2016 apps (or Office 2013 apps, if they are configured correctly).

1. Create a policy that denies access to all clients.
2. Save your change.



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.

⚠ Policies apply across all Office 365 apps. Edits will impact users' access to these apps.

Clients	Network Range	Device Type	Groups	Action
All Applications	ALL RANGES	Any	All Users	Deny

Provisioning Users from the Service

You can use the Provisioning Adapter for Office 365 to automatically provision users and groups in the Office 365 tenant from the VMware Identity Manager service. Whenever you entitle users and groups to an Office 365 application in the Catalog, the users and members of the group are provisioned in the Office 365 tenant, if they are not already a member. The actual group is not provisioned.

When you enable automatic user provisioning, you can specify what type of user account information to send from the VMware Identity Manager service. For example, the information sent can be the user name, first name, and last name, and email address.

When you edit and disable users and groups, from the VMware Identity Manager service, the records in the Office 365 instance are updated accordingly. When users are no longer entitled to the application, the Office 365 account is disabled.

In the cloud application catalog, you select the Office 365 with Provisioning application to configure provisioning

Create a Service Principal with PowerShell

You must create a Service Principal as a user account administrator role in the Office 365 tenant. You assign specific permissions so that the VMware Identity Manager service can access the Active Directory to provision and update, users and groups.

You add and configure the service principal user from the PowerShell cmdlets.

1. Open the PowerShell on your computer
2. In the PowerShell, run **Connect-MsolService** to connect to the Office 365 tenant.

   The credentials dialog box appears. Enter the Office 365 credentials when prompted.

   The credentials object provides an encrypted way to pass your user name and password to Windows PowerShell.

3. Create a new service principal user. Run **New-MSOLServicePrincipal –DisplayName '<*serviceprincipalName*>' –Type password – Value '<*strongpassword*>'**

   Replace ***serviceprincipalName*** with the name of the service principal account and create a password for this account. Note the following objects that are created.

   - The **AppPrincipalId GUID** is created. This is the application identifier of the service principal.
   - The **ObjectId** is created. This is the unique identifier of the service principal.

   Save the AppPrincipalId value; the ObjectId value, and the password you created. You need this information to configure the provisioning adapter.

4. Assign a role to the ServPrinc1 user. *Run* **Add-MsolRoleMember -RoleMemberType ServicePrincipalName -RoleName 'User Account Administrator' -RoleMemberObjectId <YOUR_OBJECT_ID>**

   Replace <YOUR_OBJECT_ID> with the object ID you saved previously.

Your Active Directory application is added to the 'User Account Administrator' role, granting Active Directory permissions to delete both users and groups created with the Office 365 provisioning adapter.

Configuring the Provisioning Adapter for Office 365

Make sure that no other account provisioning tool is enabled when you set up the Office 365 provisioning adapter. If users are provisioned in Office 365 with another provisioning tool, VMware Identity Manager service cannot be used to manage those users.

The Azure Active Directory Connect sync must be disabled when provisioning users with VMware Identity Manager.

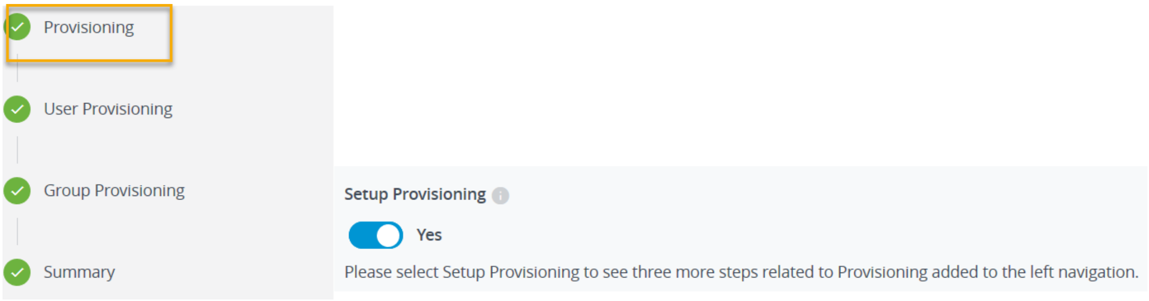
Prerequisite

- Office 365 tenant set up and configured correctly.
- Service Principal with permission to access the Office 365 tenant created. VMware Identity Manager uses the service principal to provision users and groups in Office 365. See Create a Service Principal.

Enable Provisioning in the VMware Identity Manager Service

1. Log in to the VMware Identity Manager admin console.
2. In the **Catalog** page, select the Office 365 with Provisioning application.
3. Select **Edit > Configuration** and click **Advanced Properties**.
4. Scroll to **Setup Provisioning** and click the radio button to change No to **Yes**.

   The page refreshes and four additional provisioning options are listed.



Setup Provisioning

Yes

Please select Setup Provisioning to see three more steps related to Provisioning added to the left navigation.

.

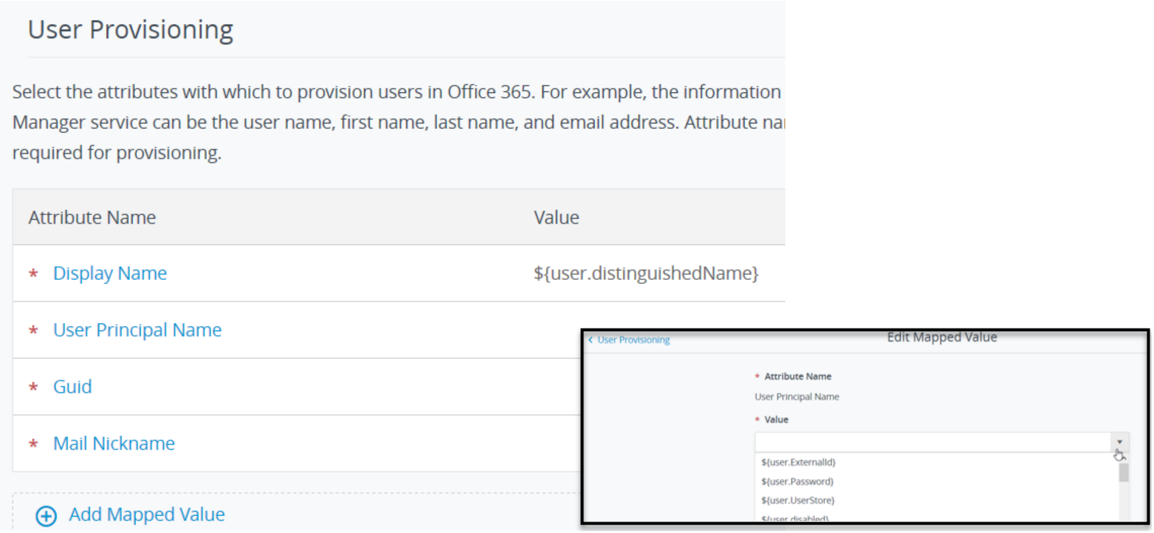
5. Select **Provisioning**, enter the following information.

FIELD	DESCRIPTION
Office 365 Domain	Enter the Office 365 domain name. For example, **example.com.** Users are provisioned under this domain.
Client ID	Enter the AppPrincipalId obtained when creating the service principal user.
Client Secret	Enter the password created for the service principal user.

6. If you also want to provision users with a license, click the **Provision with License** radio button to change No to **Yes**.

   The SKU ID is required if licensing is enabled. The SKU ID will be supplied when you purchase the license. Alternatively, you can use the PowerShell command, `GetMsolAccountSku` to find the SKU ID.

7. Click **Next**.
8. Select the attributes with which to provision users in Office 365 and select the value from the drop-down menu. Attribute names with an asterisk are required for provisioning.



User Provisioning

Select the attributes with which to provision users in Office 365. For example, the information Manager service can be the user name, first name, last name, and email address. Attribute nai required for provisioning.

Attribute Name	Value
* Display Name	${user.distinguishedName}
* User Principal Name	
* Guid	
* Mail Nickname	

Edit Mapped Value

* Attribute Name
User Principal Name

* Value

${user.ExternalId}
${user.Password}
${user.UserStore}
${user.disabled}

Make sure that the following required Active Directory attributes are configured to one of the required attribute names in the User Attributes page.

- The Mail Nickname attribute must be unique within the directory and cannot contain any special characters. Map the Mail Nickname attribute to ${user.userName}. Once mapped, do not change the Mail Nickname.
- Map the GUID value to ${user.objectGUID}. For AirWatch users, the attribute name is EXTERNAL ID.

Note: The userPrincipalName (UPN) is constructed automatically. You do not see the mapped value. The provisioning adapter appends the Office 365 domain to the mailNickname attribute value (user.userName) to create the UPN. This is appended as, userName +@+ O365_domainname. For example, jdow@office365example.com

9. Click **Save**.

The Office 365 provisioning adapter is configured, and provisioning is enabled. When you entitle users to the Office 365 application, if users do not exist in Office 365, the users are created.

If the provisioning type is set to automatic, users that are entitled to the application are provisioned in Office 365 when they are entitled to the app. If the provisioning type is user-activated, users are provisioned when users add Office 365 to the Launcher page in their Workspace ONE portal.

Group Provisioning

When a group is provisioned in Office 365, the group is provisioned as a security group. The members of the group are provisioned as users, if they do not exist in the Office 365 tenant.

The group is not entitled to resources when provisioned. If you want to entitle the group to resources, create the group and then entitle resources to that group.

Prerequisite

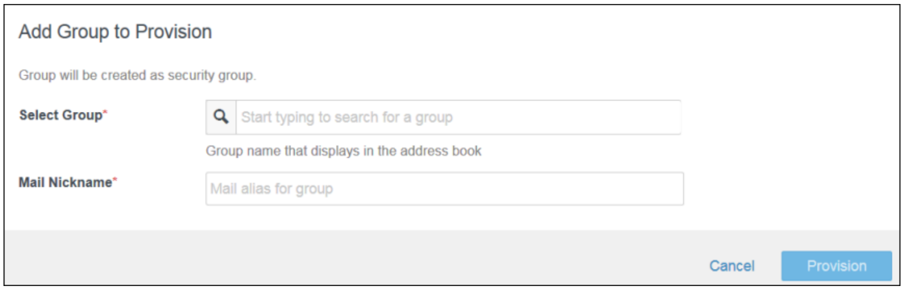
- Entitle the group to resource.

Procedure

1. Select **Group Provisioning**.
2. Click **Add Group**
   a. In the **Group Name** text box, search for the group to be provisioned in Office 365

b. In the **Nickname** text box, enter a name for this group. The nickname is used as an alias: Special characters are not allowed in the nickname.

c. Click **Save**.



Add Group to Provision

Group will be created as security group.

Group name that displays in the address book

Deprovision Groups

You can deprovision a group in the Office 365 application. The security group is removed from the Office 365 tenant. Users in the group are not deleted.

1. Log in to the VMware Identity Manager admin console.
2. In the **Catalog** page, select the Office 365 application with the group to deprovision.
3. In the Modify application page, click **Provisioning > Group Provisioning**.
4. Check the box for the group to deprovision and click **Deprovision**.

Testing Provisioning Configuration

Test that provisioning is configured correctly.

1. Create a test user in Active Directory.
2. Sync that test user to the VMware Identity Manager directory. Make sure the test user has all the required properties, including UPN and GUID/EXTERNALID.
3. Configure and map all the necessary attributes in the User Provisioning page.
4. Entitle the test user to the Office 365 application. Entitling a user triggers provisioning.
5. Validate whether the user is provisioned successfully. The status in the Entitlement page changes to provisioned.
6. Sign in to the apps portal as the newly provisioned test user.
7. The test user should be able to see the Office 365 application he is entitled to.
8. Launch the Office 365 application. The test user should be successfully signed in to the Office 365 portal.
9. Test the active flow/thick client. Sign in from Outlook or OneNote where it prompts to enter both the user ID and password. Verify the test user can sign in as well.

Configuring Reverse Proxy when Using Office 365 Legacy Authentication Flow with Mobile Devices

Some mobile native applications, such as Microsoft Outlook, iOS Mail, and VMware Boxer, use the Office 365 legacy authentication flow for single sign-on. When the legacy authentication flow is used, the VMware Identity Manager Connector must be externally reachable through port 443. A reverse proxy server can be used to achieve this.

Prerequisite

- The reverse proxy must have a well-known CA signed SSL.
- The SSL can be terminated at the reverse proxy or can be set up to pass through.
- The reverse proxy must have a DNS entry that is resolvable publicly.

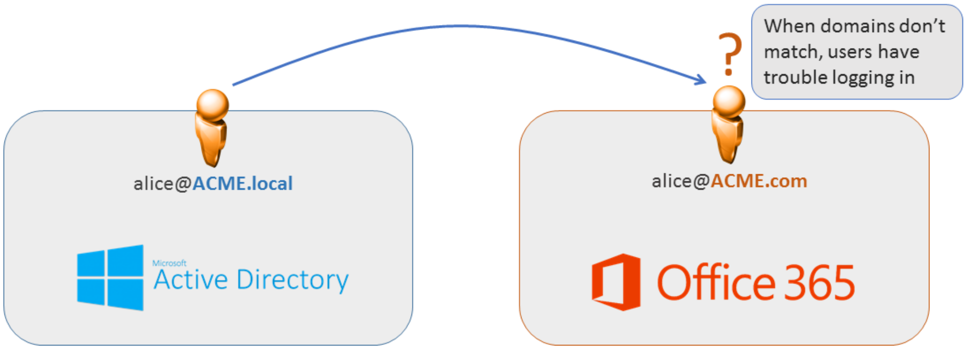
Procedure

1. Log in to the VMware Identity Manager admin console.
2. In the Identity & Access Management tab, go to **Manage > Identity Providers**.
3. Select the identity provider that is configured with the connector that can be reached from the reverse proxy server.
4. Scroll down to the **IdP Hostname** section. Enter the value of the IdP Hostname to point to the FQDN of your reverse proxy.

Prepare a Non-routable Domain with Office 365 and Active Directory

When your organization buys Office 365 licenses, you must verify a valid Internet domain with Microsoft, for example, ACME.com. Office 365 uses that verified domain as the domain for all users, for example, johndoe@ACME.com.

Organizations can have multiple domains or non-routable domains in their User Principle Names (UPN) in their on-premises Active Directory. For example, ACME.local. Office 365 cannot sync users with non-routable domains. You can configure VMware Identity Manager to take care of mismatched domains.


When domains don't match, users have trouble logging in
?
alice@ACME.local
Microsoft Active Directory
alice@ACME.com
Office 365

This problem can affect your transition to Office 365 if any of the following conditions apply.

- You have a non-routable domain that does not end in .com, .org, .net, .us, or another valid domain (for example, alice@ACME.local).
- You have multiple domains in your on-premises Active Directory UPNs (for example, bob@ACMEcorp.com and charlie@ACMEmanufacturing.com).
- You verified a different domain with Microsoft than you use in Active Directory UPNs (for example, you verified ACMEcorp.com but your internal UPNs use the domain ACME.com).

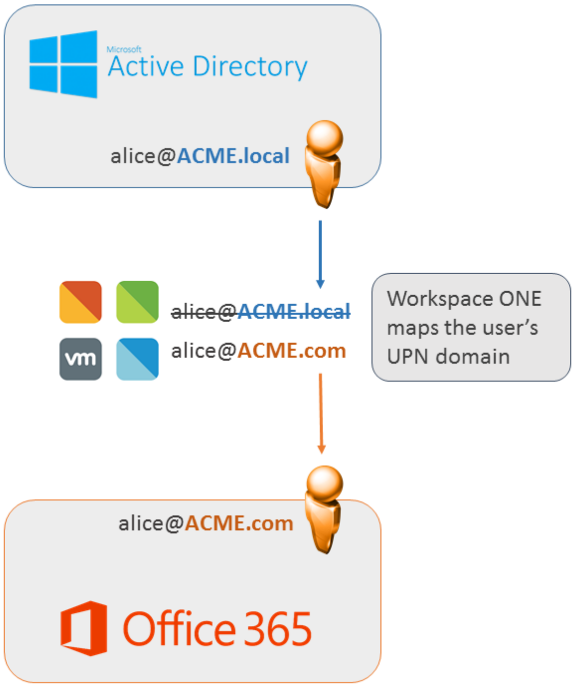
In general, any mismatch between Office 365 domains and the domains in your on-premises Active Directory requires remediation.

Fixing Mismatched Domains in VMware Identity Manager

To sync all Active Directory users to Office 365, you must follow the basic principle that the users you sync to Office 365 must have UPNs that match your Office 365 domain.

Without making changes to your on-premises Active Directory UPN, you can configure VMware Identity Manager to provision your Active Directory users in to Office 365. The VMware Identity Manager service updates the user's UPNs so that the UPN matches the domain that Office 365 expects.

For example, the Office 365's valid domain is Acme.com and a user in Active Directory is named alice@ACME.local. VMware Identity Manager syncs alice@ACME.local to Office 365 as alice@ACME.com. When Alice tries to log in to Office 365, VMware Identity Manager sends the UPN alice@ACME.com to Office 365. When Alice tries to log in to other apps that rely on her non-routable UPN (alice@ACME.local), VMware Identity Manager sends the correct UPN.

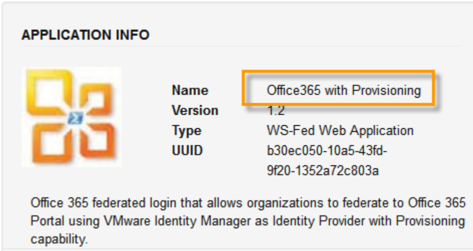


Two options can be configured in the VMware Identity Manager service to resolve the non-routable UPN issue.

- Use VMware Identity Manager to provision users into Office 365.
- Use the Microsoft Azure AD Connect tool to sync users to Office 365 and then set up VMware Identity Manager to use your Office 365 domain.

Use Provisioning to Update the UPN Attributes in VMware Identity Manager

To configure VMware Identity Manager to automatically fix mismatched domains as users are synced to Office 365, configure the Office 365 with Provisioning application in the Catalog page.



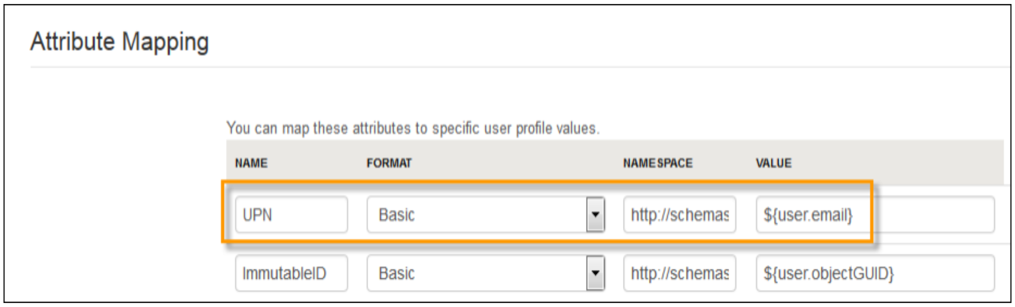
APPLICATION INFO

Name	Office365 with Provisioning
Version	1.2
Type	WS-Fed Web Application
UUID	b30ec050-10a5-43fd-9f20-1352a72c803a

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

1. Log into the VMware Identity Manager admin console.
2. Click the **Catalog** tab.
3. Click **Add Application** > …**from the cloud application catalog**.
4. Select the **Office365 with Provisioning** application.
5. To set up the application for single sign-on, see Add Office 365 Applications to the Catalog.
6. To configure the application provisioning feature, see Provisioning Users from the Service.

7. In the Configuration tab, scroll down to the Attribute Mapping section.
    a. Choose **UPN** in the Name field.
    b. Leave the Format field as **Basic**.
    c. Leave the Namespace field as **http://schemas.xmlsoap.org/claims**.
    d. In the Value field, enter **${user.email}.**



Attribute Mapping

You can map these attributes to specific user profile values.

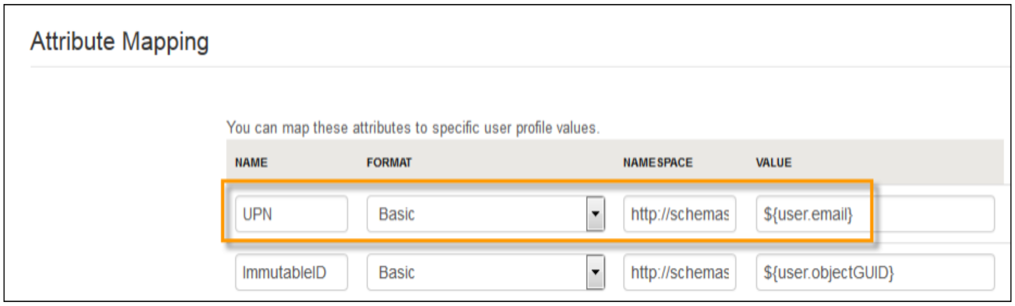
NAME	FORMAT	NAMESPACE	VALUE
UPN	Basic	http://schemas	${user.email}
ImmutableID	Basic	http://schemas	${user.objectGUID}

Use the Azure Active Directory Connect Tool to Provision and Sync Users to Office 365

When you use the Azure AD connect tool to provision users in to Office 365, the Azure AD Connect tool can automatically fix the mismatched domains when it syncs users.

For instructions on using Azure AD Connect, see this article: https://blogs.msdn.microsoft.com/vilath/2016/03/02/changing-the-userprincipalsuffix-with-azure-ad-connect/

1. Log into the VMware Identity Manager admin console.
2. Click the **Catalog** tab.
3. Click **Add Application** > …**from the cloud application catalog**.
4. Select the **Office365 for Provisioning** application.
5. To set up the application for single sign-on see Add Office 365 Applications to the Catalog.
6. In the Configuration tab, scroll down to the Attribute Mapping section.
    a. Choose **UPN** in the Name field.
    b. Leave the Format field as **Basic**.
    c. Leave the Namespace field as **http://schemas.xmlsoap.org/claims**.
    d. In the Value field, enter **${user.email}.**



Attribute Mapping

You can map these attributes to specific user profile values.

NAME	FORMAT	NAMESPACE	VALUE
UPN	Basic	http://schemas	${user.email}
ImmutableID	Basic	http://schemas	${user.objectGUID}

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com