Configuring Single Sign-on from the VMware Identity Manager Service to Mingle

VMware Identity Manager

NOVEMBER 2015 V1

vmware®

Table of Contents

Overview

This document provides information about configuring SAML-based single sign-on from the VMware Identity Manager service to Mingle.

Mingle is a ThoughtWorks Studios project management software that enables companies to implement and scale agile practices.

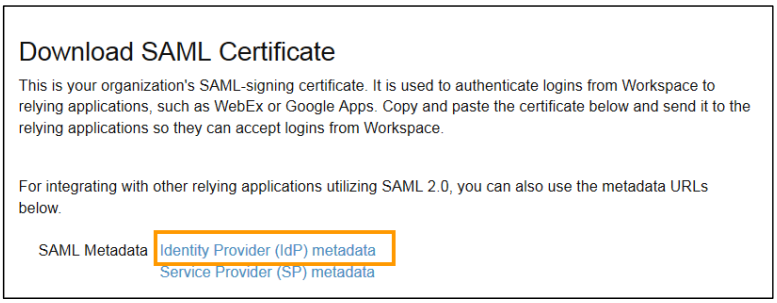
When Mingle is configured in the VMware Identity Manager catalog, users can sign into Mingle from their apps portal or if they sign in to their Mingle account directly, they are redirected to the VMware Identity Manager sign in page to enter their sign-in credentials

You must have an administrator account for the VMware Identity Manager service, as well as an administrator account for Mingle.

Save the Identity Provider SAML Metadata

You must have the VMware Identity Provider identity provider metadata xml file to configure Mingle.

1. In the Catalog > Settings tab, click **SAML Metadata**.
2. In the SAML Metadata section, right-click **Identity Provider (IdP) metadata** and safe the **idp.xml** file.



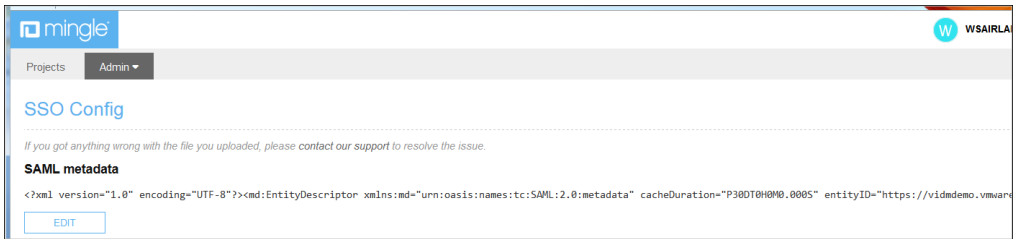
You upload this file in the Mingle administration console.

Setting up Mingle

To set up Mingle for single sign-on from the service, you add the SAML metadata file to the Mingle SSO page on the administration console.

Configure Mingle

1. Sign in to the Mingle admin console as the admin user and navigate to the **Admin > SSO Config** page.
2. Click **Edit**.
3. Upload the VMware Identity Provider SAML metadata XML file you saved previously.
4. Click **Save changes**.



Adding Mingle to VMware Identity Manager Catalog

To enable single sign-on to Mingle on the service, you must configure the app in the catalog.

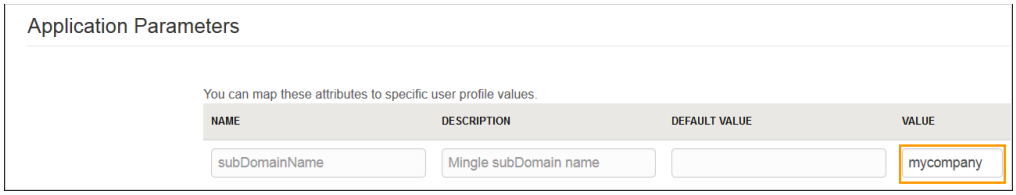
Add Mingle to the Catalog

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Add Application > ...from the cloud application catalog**.
3. Click the **Mingle** icon.
4. Click **Configuration**. The Configuration page displays, preconfigured as follows.

FIELD	CONFIGURATION CHANGES REQUIRED Y/N DESCRIPTION
Launch URL	Automatically populated with your launch URL.
RelayState	https://{subDomainName}.mingle.thoughtworks.com
Proxy Count	
Login Redirection URL	https://{subDomainName}.mingle.thoughtworks.com/
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	Enabled
Include Cert	Enabled
Allow API Access	
Configure Via	
Assertion Consumer Service*	Automatically populated with the URL the SAML should be posted to. **https://profile.thoughtworks.com/saml/consume**
Name ID Format	**Unspecified (username)**

Name ID Value • **Select from suggestions** • **Custom value**	Custom value populated with **${user.email}**
Recipient Name*	The SP's assertion consumer service URL populated as **https://profile.thoughtworks.com/saml/consume**
Audience*	The SP's unique identified populated with **https://profile.thoughtworks.com**
Assertion Lifetime	Populated with a value of **200** seconds
Signing Certificate	
Application Parameters	Must be configured. See step 5.
Attribute Mapping	

5. In the **Application Parameters** section, enter your company domain name in the **Value** field.



6. Click **Save**.

Testing Single Sign-on Configuration

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 Testing

1. Log in to the VMware Identity Manager administration 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** page, click on the **Mingle** application.
4. Click **Entitlements**.
5. Click +**Add user entitlement**.
6. Select the test user and change the **DEPLOYMENT** field value for the user to **Automatic**. For example:

7. Click **Save**, then click **Done**.
8. In the top-right corner of the page, click your user name and select **Logout**.

Set up User in Mingle for Testing

1. Sign in to the Mingle admin console as the admin user and navigate to the **Admin > Manage Users** page.
2. On the Manage Users page, click **New User**.
3. Enter the sign-in name, display name, and email addresses for the test user.

Next, verify that the test user can sign in to the My Apps portal.

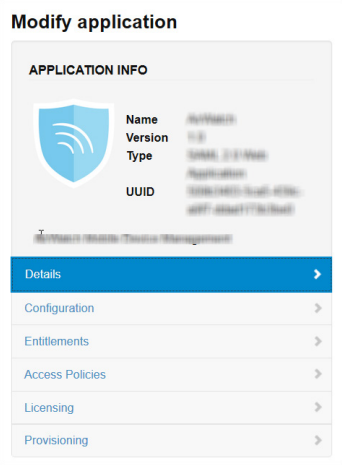
Verify Test-User can Sign into Mingle

1. Sign in to the user portal as the test user.
2. Click the **Mingle** icon on the My Apps page.

   You should now have single sign-on access to Mingle.

Completing the Configuration in the Catalog

In addition to configuring the Web application for single sign-on to the service, you can configure additional settings to add an access policy, set up app licensing requirements, and entitle users and groups to the app.



Entitlements After you configure a Web application, you can add group entitlements and entitle individual users to the Web app.

Access Policies The VMware Identity Manager service includes a default policy that is automatically assigned to the Web app when you add the app to the Catalog. If you do not want to use the default access policy, create a new access policy and in the Access Policies link, select the access policy to use for this Web application.

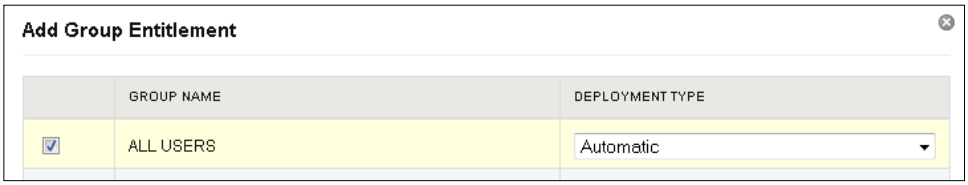
For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

Licensing	Licensing can be used to require users to request license approval before they can access the application. You can add additional information, including pricing, license type, cost per license and the number of licenses. You can run the Resource Usage report to see the licensing information for the application.
Provisioning	Provisioning provides automatic application user-management from a single location. Provisioning adapters allow the Web application to retrieve specific information from VMware Identity Manager, as required. The provisioning adapters that can be selected are either Google Apps, Mozy, or Vchs. If you configure these applications, you can select the appropriate provisioning adapter.

Entitle Users to Mingle

You can activate single sign-on for all users. Before you do so, ensure that all the user accounts are provisioned in Mingle.

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Mingle**.
3. In the **Modify application** page, click **Entitlements**.
4. Click +**Add group entitlement**.
5. Select **ALL USERS** and change the **DEPLOYMENT TYPE** field value to **Automatic**.



6. Click **Save,** then click **Done**.

.

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