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

VMware Identity Manager

OCTOBER 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 Bonusly.

Bonusly is a peer-to-peer recognition program that lets employees give micro-bonuses to their colleagues every month.

You add Bonusly to the VMware Identity Manager catalog and enable SAML authentication in Bonusly to allow users logged into the service to have single sign-on access to Bonusly.

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

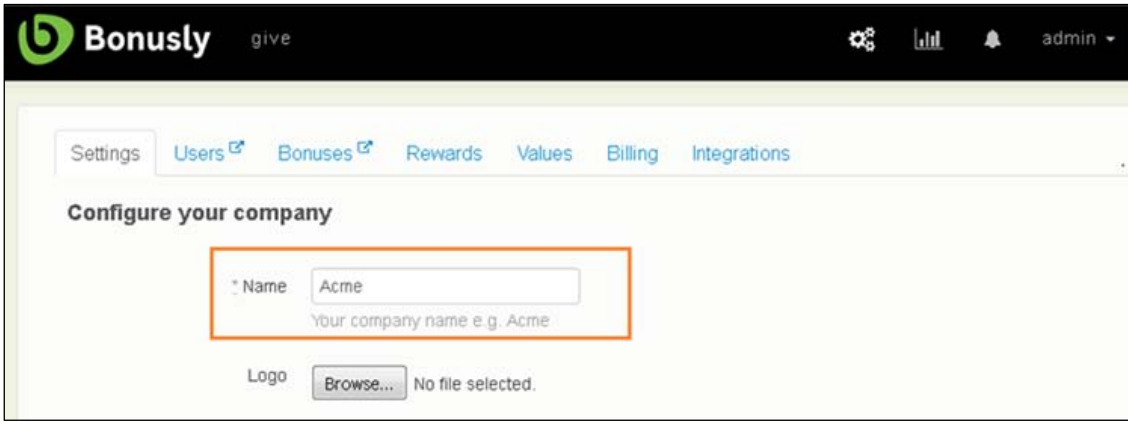
Adding Bonusly to VMware Identity Manager Catalog

To enable single sign-on to Bonusly on the service, you must configure the application in the catalog and copy the SAML- signing certificate to Bonusly.

Add Bonusly 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 **Bonusly** icon.

   The Modify application page appears.
4. Select **Configuration** in the left pane and scroll down to the **Application Parameters** section.
5. Obtain the company name from Bonusly.
   a. In another browser window, log in to the Bonusly site as administrator.
   b. Click the Settings icon  on the top-right of the page.
   c. In the **Settings** tab, from the **Configure your company** section, copy the value of the **Name** field.



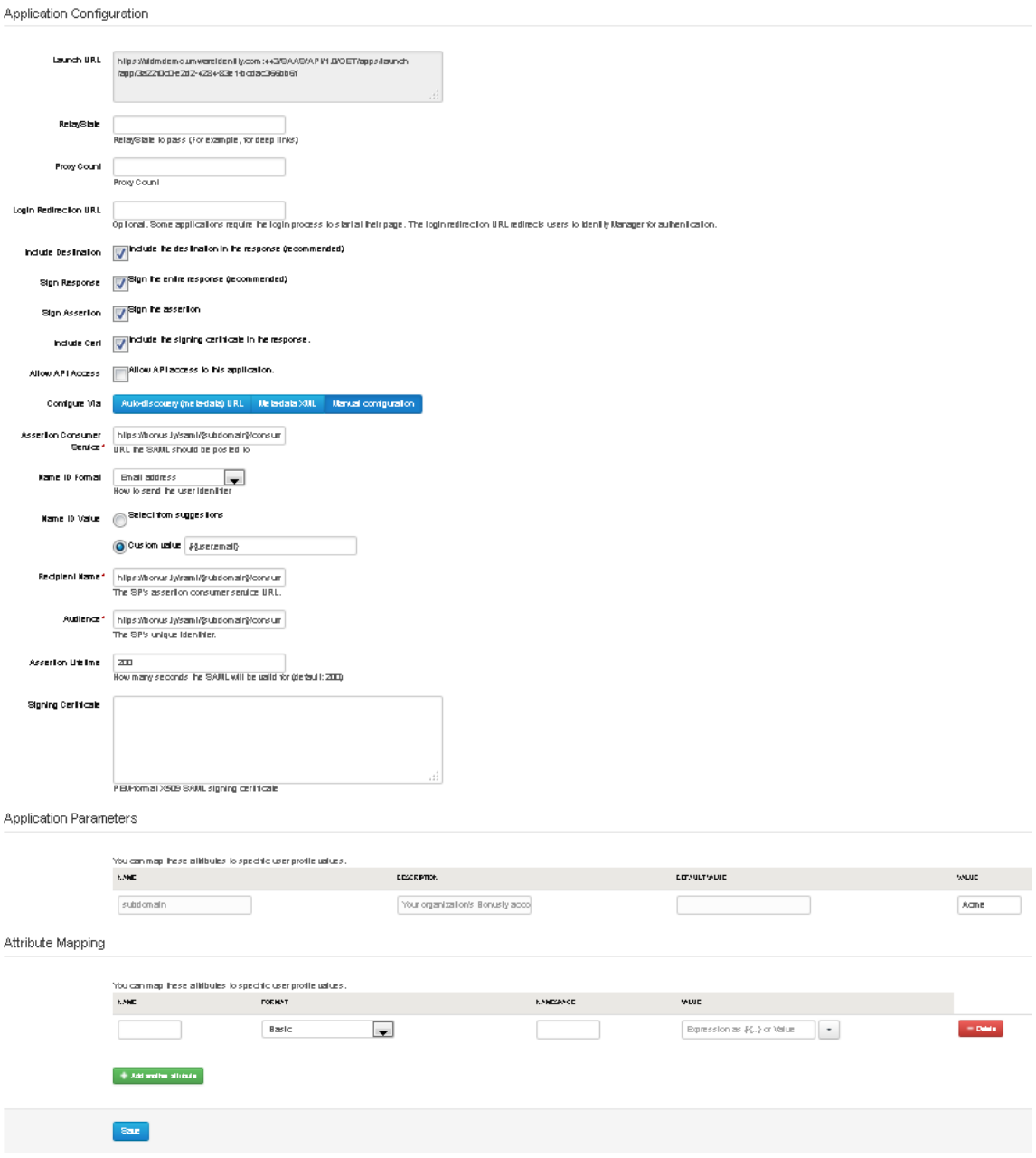
   If the **Name** field does not have a value, enter your company name, then click **Save Settings**.

6. In the VMware Identity Manager Bonusly Application Configuration page, under **Application Parameters**, set the value of the **subdomain** parameter to the name you copied from Bonusly.

   IMPORTANT: The **subdomain** value must match the value of the **Name** field in the Bonusly Settings page.
   For example:

7. Click **Save**.

   Verify that the Application Configuration page is similar to this example.

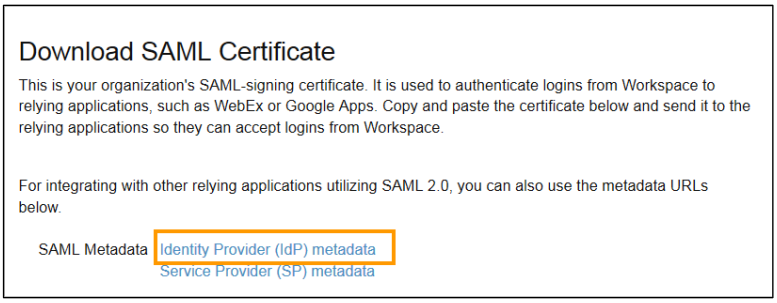


Locate Identity Provider SAML Metadata

You must have the VMware Identity Manager identity provider metadata URL to configure Bonusly.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.
2. In the **SAML Metadata** section, click the **Identity Provider (IdP) metadata** link to display the metadata content.

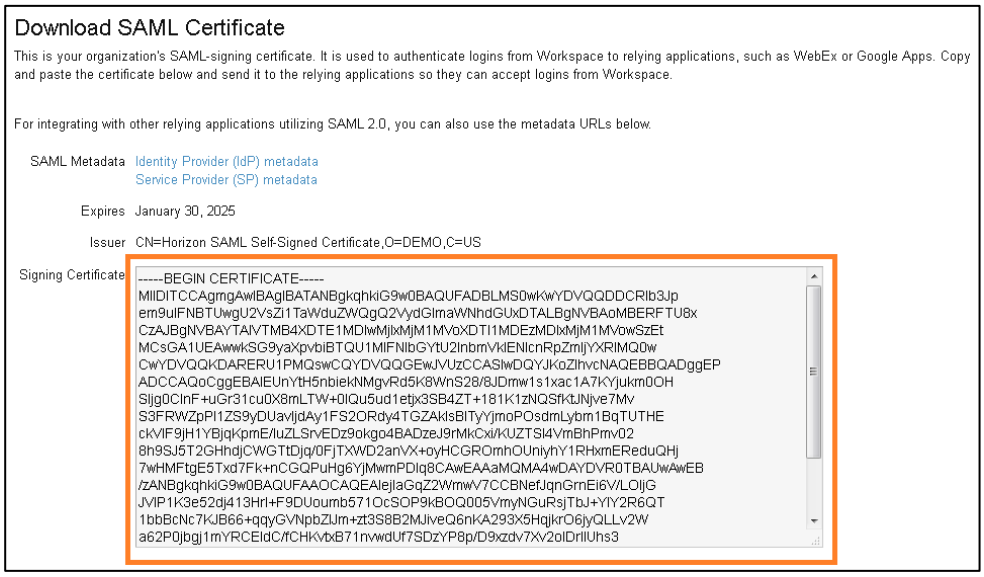
   Make a note of the URL. The URL is similar to this example.
   https://*myco.vmwareidentity.com*/SAAS/API/1.0/GET/metadata/idp.xml.



Download SAML-Signing Certificate

You must have the SAML-signing certificate from the VMware Identity Manager service for the Bonusly configuration.

1. In the **Catalog > Settings** tab, click **SAML Metadata**.
2. Copy and save the **Signing Certificate** text to a text file on your computer. Make sure that you include text from -----BEGIN CERTIFICATE---- through ---------END CERTIFICATE-----.



Setting up Bonusly

To configure Bonusly for single sign-on from the service, you set up single-sign on in Bonusly and upload the VMware Identity Manager SAML-signing certificate.

Configure Bonusly

1. Log in to Bonusly as administrator.
2. Click the Settings icon  on the top-right of the page.
3. Select the **Integrations** tab.

4. In the **Single Sign-On** section, click **SAML**.

5. In the SAML Integration page, enter the following values.

Field	Value
Idp SSO target URL	Enter the VMware Identity Manager single sign-on URL in the following format: https://myco.vmwareidentity.com/SAAS/auth/federation/sso Replace *myco.vmwareidentity.com* with your company's VMware Identity Manager service domain name.
Idp Issuer	Enter the VMware Identity Manager identity provider SAML metadata URL that you copied. For example: https://myco.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml
X.509 Cert	Paste the SAML-signing certificate you copied from the VMware Identity Manager administration console.
Disable web login	Select the checkbox **Prevent web and LinkedIn logins (SSO Only)**

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 **Bonusly**.
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 Bonusly for Testing

1. Sign in to the Bonusly site as administrator.
2. Click the Settings icon on the top-right of the page.
3. Select the **Users** tab.
4. Click the Add User icon at the top-right of the page.
5. Enter the user information and click **Save**.

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

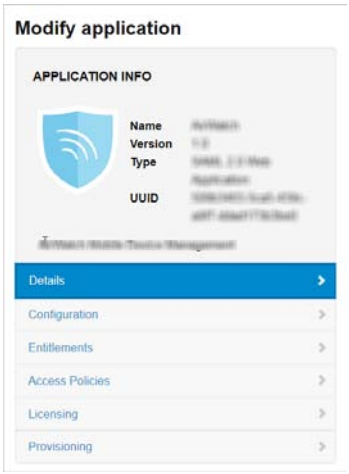
Verify Test-User can Sign into Bonusly

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

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

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 application.



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

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.

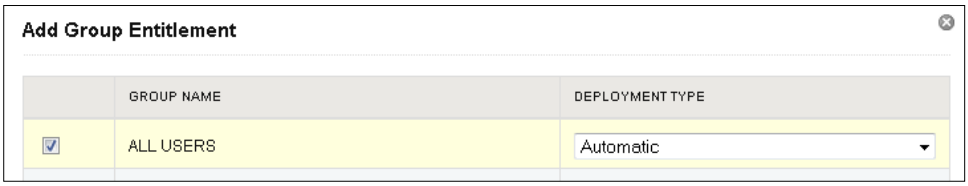
For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

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 Bonusly

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

1. Log in to the VMware Identity Manager administration console.
2. In the **Catalog** page, click **Bonusly**.
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