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

VMware Identity Manager

APRIL 2016 V1

vmware®

Table of Contents

Overview

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

Black Line provides enterprise-class software designed to automate and control the entire financial close process.

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

You must have an administrator account for the VMware Identity Manager service as well as an administrator account for Black Line. You work with your Black Line representative to configure Black Line.

Adding Black Line to VMware Identity Manager Catalog

To enable single sign-on to Black Line on the service, you must configure the application in the catalog.

Add Black Line 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 **Black Line** icon.

   The Modify application page appears.
4. Select **Configuration** in the left pane.

   The Configuration page is preconfigured as follows.

   IMPORTANT: Do not change any of the preconfigured values, unless specified below.

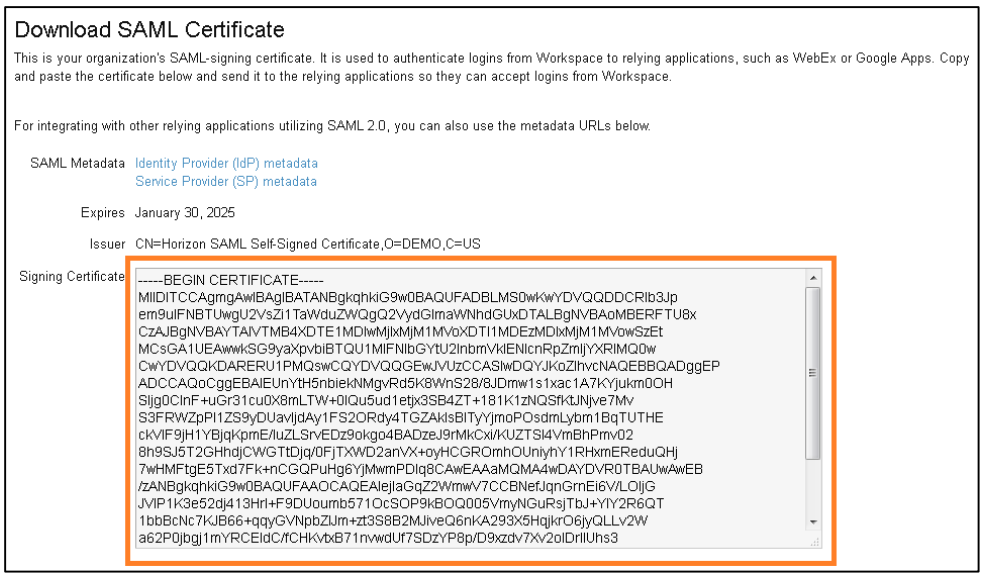
FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL. For example: **https://myCo.example.com:443/SAAS/API/1.0/GET/apps/launch/app/a59f9455-b744-4529-bac5-543bd8e89918**
RelayState	
Proxy Count	
Login Redirection URL	
Include Destination	
Sign Response	
Sign Assertion	Enabled
Include Cert	

Allow API Access	
Configure Via	**Manual Configuration** selected
Assertion Consumer Service*	Automatically populated with the URL the SAML should be posted to: **https://sso.blacklineondemand.com/adfs/ls/**
Name ID Format	**Email address**
Name ID Value	**Custom value** selected with the value left blank.
Recipient Name*	Automatically populated with the SP's assertion consumer service URL: **https://sso.blacklineondemand.com/adfs/ls/**
Audience*	The SPs unique identifier: **urn:federation:sso.blacklineondemand.com**
Assertion Lifetime	**200**
Signing Certificate	
Attribute Mapping	The following attribute is set by default: • **name** with a format of **Basic** and value of **${email}**

Download SAML-Signing Certificate

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

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



Setting up Black Line

Contact Black Line to complete the VMware Identity Manager configuration in Black Line. You may need the following information:

- Your VMware Identity Manager domain name
- The VMware Identity Manager SAML signing certificate you saved previously

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 **Black Line**.
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 Black Line for Testing

Make sure the test user you set up in VMware Identity Manager is configured in Black Line too.

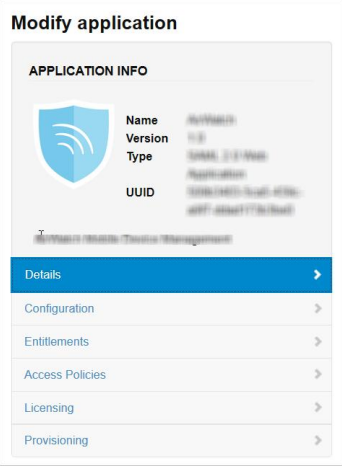
Verify Test-User can Sign into Black Line

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

   You should now have single sign-on access to Black Line.

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.

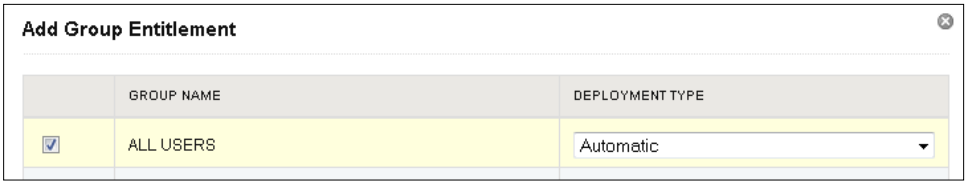
For example, you can create a stricter policy than the default, with rules that specify which IP addresses have access to the application, using which authentication methods, and for how long until reauthentication is required. See the VMware Identity Manager documentation at http://pubs.vmware.com.

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.

Entitle Users to Black Line

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

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