



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

VMware Identity Manager

APRIL 2016 V 1

**Table of Contents**

Overview ..... 1

Adding Black Line to VMware Identity Manager Catalog..... 1

    Add Black Line to the Catalog..... 1

    Download SAML-Signing Certificate ..... 2

Setting up Black Line ..... 3

Testing Single Sign-on Configuration ..... 3

    Set up User in VMware Identity Manager for Testing..... 3

    Set up User in Black Line for Testing ..... 3

    Verify Test-User can Sign into Black Line ..... 3

Completing the Configuration in the Catalog ..... 4

Entitle Users to Black Line ..... 4

## 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: <code>https://myCo.example.com:443/SAAS/API/1.0/GET/apps/launch/app/a59f9455-b744-4529-bac5-543bd8e89918</code>
RelayState	
Proxy Count	
Login Redirection URL	
Include Destination	
Sign Response	
Sign Assertion	Enabled
Include Cert	

<b>Allow API Access</b>	
<b>Configure Via</b>	<b>Manual Configuration</b> selected
<b>Assertion Consumer Service*</b>	Automatically populated with the URL the SAML should be posted to: <b>https://sso.blacklineondemand.com/adfs/ls/</b>
<b>Name ID Format</b>	<b>Email address</b>
<b>Name ID Value</b>	<b>Custom value</b> selected with the value left blank.
<b>Recipient Name*</b>	Automatically populated with the SP's assertion consumer service URL: <b>https://sso.blacklineondemand.com/adfs/ls/</b>
<b>Audience*</b>	The SP's unique identifier: <b>urn:federation:sso.blacklineondemand.com</b>
<b>Assertion Lifetime</b>	<b>200</b>
<b>Signing Certificate</b>	
<b>Attribute Mapping</b>	The following attribute is set by default: <ul style="list-style-type: none"> <li><b>name</b> with a format of <b>Basic</b> and value of <b>\$(email)</b></li> </ul>

## 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-----.

**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 January 30, 2025

Issuer CN=Horizon SAML Self-Signed Certificate,O=DEMO,C=US

Signing Certificate

```
-----BEGIN CERTIFICATE-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQUFADBLS0wkwYDVQDDCRib3Jp
em9uIFNBTUwgU2VsZi1TaWduZWQgQ2VydGlnaWNhdGxudDIALBgnVBAoMBERF
TU8x
CzAJBgNVBAYTAiVTMB4XDTE1MDIwMjI1MDEzMDEzMDEzMDEzMDEzMDEzMDE
MCsGA1UEAwkzSG9yaXpvbiBTQU1MIFNlbG9yYU2lbnRmVklEbnRmRmRmRmRm
CwYDVQQKIDRERERU1PMQswCQYDVQQGEwJlbnRmRmRmRmRmRmRmRmRmRmRm
ADCCAQoCggEBAIEUnYH5nbiekNMgyRd5k8WnS28/8Jdmmw1s1xac1A7KYJukm0OH
Sjg0ClnF+uGr31cu0X8mLTW+0lQu5ud1etj3SB4ZT+181K1zNQSfKJNjve7Mv
S3FRWZpP11ZS9yDUavjIdAy1FS2ORdy4TGZAKsBITyYjmoPOsdmLybm1BqTUTHE
ckVf9JH1YBjqkpmE/luZLsrVEDz9okgo4BADzeJ9rMkcxikUzTS4VmBhPmv02
8h9Sj6T2GHhdjCwGTIDjg0FJTxD2anVX+oyHCGR0mhOUnihy11RHxmEReduQHJ
7wHMFtgE5Txd7Fk+nCGQPuHg6YJMwmPDlq8CAwEAAMQMA4wDAYDR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAEjlaGgZ2WmmwV7CCBNefJqngmEi6V/LOjg
JVIP1K3e52dj413Hr1+9DUoumb571OcSOP9kBOQ005VmyNGuRsjTbj+YIY2R6QT
1bbBcNc7KjB66+qayGVNpbZUm+zt3S8B2MjiveQ6nkA293x5HqjkrO6jyQLLv2W
a62P0jbj1mYRCeIldC/CHKvxb71nwwdUf7SDzYP8p/D9xzdV7Vx2olDrIUhs3
-----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:

Add User Entitlement		
Type to select a user		or browse...
User, Demo (demo)	Automatic	Remove

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

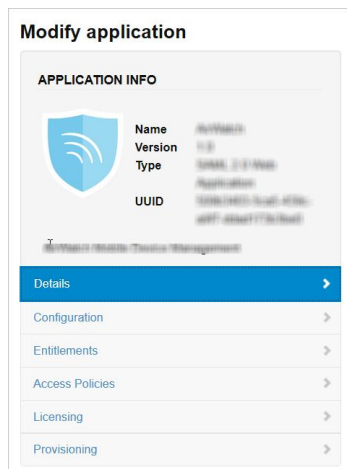
Make sure the test user you set up in VMware Identity Manager is configured in Black Line too.

### 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**.

**Add Group Entitlement** ✕

	GROUP NAME	DEPLOYMENT TYPE
<input checked="" type="checkbox"/>	ALL USERS	Automatic <span>▼</span>

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](http://www.vmware.com)

Copyright © 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.