



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

VMware Identity Manager

FEBRUARY 2016 V1

Table of Contents

Overview..... 1

Adding QuickBase to VMware Identity Manager Catalog 1

 Add QuickBase to the Catalog..... 1

 Download SAML-Signing Certificate..... 2

Setting up Identity Manager in QuickBase 3

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

 Set up User in Identity Manager for Testing 3

 Set up a User in QuickBase for Testing..... 4

 Verify Test-User can Sign into QuickBase..... 4

Completing the Configuration in the Catalog 4

 Entitle Users to QuickBase 5

Overview

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

Intuit QuickBase is a cloud platform that allows you to create custom databases.

When QuickBase is configured in the VMware Identity Manager catalog, users can sign on to QuickBase from their VMware Identity Manager apps portal.

You must have an administrator account for the VMware Identity Manager service to configure QuickBase. You work with your QuickBase customer support or sales engineer to configure Identity Manager in QuickBase.

Adding QuickBase to VMware Identity Manager Catalog

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

Add QuickBase 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 **QuickBase** icon.
4. Click **Configuration**. The Configuration page is preconfigured as follows.

FIELD	CONFIGURED VALUE
Launch URL	Automatically populated with your launch URL.
RelayState	
Proxy Count	
Login Redirection URL	
Include Destination	Enabled
Sign Response	Enabled
Sign Assertion	
Include Cert	Enabled
Allow API Access	
Configure Via	

Assertion Consumer Service*	Automatically populated with the URL the SAML is posted to. https://{subdomain}.quickbase.com/saml/SSOAssert.aspx
Name ID Format	Email address
Name ID Value <ul style="list-style-type: none"> Select from suggestions Custom value 	Custom value populated with \${user.email}
Recipient Name*	The SP's assertion consumer service URL populated as https://{subdomain}.quickbase.com/saml/SSOAssert.aspx
Audience*	The SP's unique identified populated with {subdomain}.quickbase.com
Assertion Lifetime	Populated with a value of 200 seconds
Signing Certificate	
Application Parameters	See step 5.
Attribute Mapping	See step 6.

- In the **Applications Parameter** section, in the **Value** column enter the subdomain name created for your organization in QuickBase. For example, if your QuickBase URL is *myco.quickbase.com*, set the value to *myco*.

Application Parameters

You can map these attributes to specific user profile values.

NAME	DESCRIPTION	DEFAULT VALUE	VALUE
subdomain	Your org's QuickBase subdomain		myco

- In the **Attribute Mapping** section, map the following attribute names to the user profile values. The **FORMAT** field value is Basic.

NAME	CONFIGURED VALUE
EmailAddress	\${user.email}
FirstName	\${user.firstName}
LastName	\${user.lastName}

- Click **Save**.

Download SAML-Signing Certificate

You must have a copy of the signed certificate from the VMware Identity Manager service for the QuickBase configuration.

- In the **Catalog > Settings** tab, click **SAML Metadata**.

- 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-----
MIIDITCCAgmgAwIBAgIBATANBgkqhkiG9w0BAQUFADBLMS0wkwYDVQDDCRib3Jp
em9uIFNB TUwgU2VsZi1TaWduZWQgQ2VydGlmaWNhdGUxDTALBgNVBAoMBERF
TU8x
CzAJBgNVBAYTAiVUM4XDTE1MDIwMjM1MjM1MVoXDTE1MDEzMjM1MjM1MVo
MCsGA1UEAwkzSG9yaXpvbiBTQUU1MIFNlbG9tYU2lnbWVkiElicnRpZmlyYXRIMQDw
CwYDVQQKDARERU1PMQswCQYDVQQGEWJlUzCCASlWdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAIEUnYtH5nbiekNMgvRd5k8WnS28/8JDrmw1s1xac1A7KYJukm0OH
Sjg0CinF+uGr31cu0X8mLTW+0lQu5ud1etj3SB4ZT+181K1zNQStkUNjve7Mv
S3FRWZpP11ZS9yDUavjdAy1FS2ORdy4TGZAkSBITyYjmoPOsdmLybm1EqTUTHE
ckVIF9JH1YBjgkpmE/luZLsrVEDz9okgo4BADzeJ9rMkCxI/KUZTSI4VmbPmrv02
8h9SJ5T2GHhdjCWGTIDJq/0fjTXWD2anVX+oyHCGROmhoUnlyhY1RHxmEReduQHj
7wHMFtgE5Txd7Fk+nCGQPuHg6YjMwmPDlg8CAwEAAMQMA4wDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAlejjaGgZ2WmwV7CCBNefJqnGmEi6V/LOlJC
JVIP1K3e52dj413Hri+F9DUoumb571OcSDP9kBOQ005VmyNGuRsjTbJ+YIY2R6QT
1bbBcNc7KjB66+qqyGVNpbZJm+zt3S8B2MjveQ6nKA293x5HqjkrO6jyQLLV2W
a62P0bjj1mYRCEldC/fCHKvxb71nwwdUf7SDzYP8p/D9xzdV7Xv2oIDrliUhs3
-----END CERTIFICATE-----
```

Setting up Identity Manager in QuickBase

Contact QuickBase to set up single sign-on for VMware Identity Manager. Provide them with the following information.

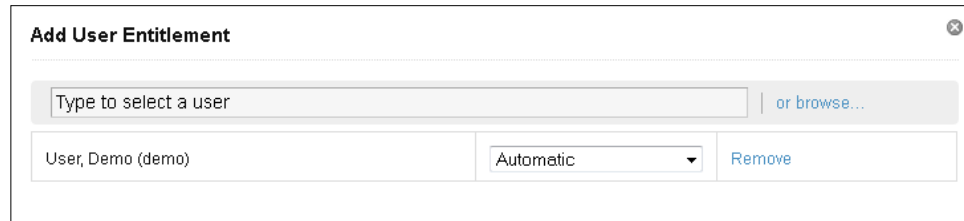
- Your identity manager domain name.
- The VMware Identity Manager SAML signing certificate you saved previously.

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 Identity Manager for Testing

- Log in to the VMware Identity Manager administration console.
- In the **Users & Groups** page, click **Users** and ensure that the user you are testing is in the list of users.
- In the **Catalog** page, click on the **QuickBase** application.
- Click **Entitlements**.
- Click **+Add user entitlement**.
- 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 a User in QuickBase for Testing

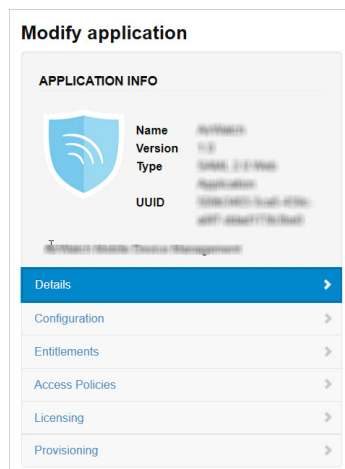
Make sure the test user you set up in VMware Identity Manager is configured in QuickBase.

Verify Test-User can Sign into QuickBase

1. Sign in to the user portal as the test user.
2. Click the **QuickBase** icon on the My Apps page.
You should now have single sign-on access to QuickBase.

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

In some applications, licensing can be used to require users to request license approval before they can access the application. In addition, 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 QuickBase

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

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

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

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.