BlackBerry Workspaces

Integration Guide

SAML SSO

Contents

Overview

This guide provides instructions for creating and testing SAML SSO Integration for BlackBerry Workspaces. **Security Assertion Markup Language (SAML)** is an XML-based, open-standard data format for exchanging authentication and authorization of data between parties, in particular, between an identity provider and a service provider.

Integrating BlackBerry Workspaces with a SAML based identity provider, enables your business to easily provide your users access utilizing their own familiar domain credentials.

BlackBerry Workspaces can be set in single or multi-mode authentication. In single mode, all users are directed to the same identity provider. Using multi-mode users are directed to the preferred identity provider based on their email domain. For example, domain users can be directed to your corporate identity provider and all others to BlackBerry Workspaces internal authentication (user/password or one time token). Changes to the authentication settings of your organization can be done through the BlackBerry Workspaces Advanced Configuration Tool.

The overall goal of this guide is to provide a good understanding of the integration requirements necessary for successful SAML SSO integration and testing and is divided into the following example workflows:

- Okta
- AD FS

Okta

Add, configure, and export the verified BlackBerry Workspaces application from the Okta directory to your Okta account.

Add BlackBerry Workspaces to your Okta account

Add the BlackBerry Workspaces app to your Okta account.

Before you begin:

- BlackBerry Workspaces has a verified application in the Okta directory called **Watchdox**.

1. On the applications tab, select **Add Application**.
2. In the Search window, enter **Watchdox** and select to **Add** the application to your account.

Configure BlackBerry Workspaces application

Follow this procedure to configure the BlackBerry Workspaces app in your Okta account.

Before you begin: Download the metadata from the BlackBerry Workspaces server at https://<*SERVER.ADDRESS*>/saml-idp/saml/metadata.

Copy the value md:SingleLogoutService Location from the downloaded xml, for example https://www.watchdox.com/saml-idp/saml/SingleLogout/alias/defaultAlias

1. From the **General Settings** screen, enter the value of md:SingleLogoutService Location you copied before as the **ACS Url**.
2. Click **Next**.
3. In the **Assign to People** screen, assign the application to the relevant users in your Okta account.
4. Click **Next**.

Export the IDP metadata XML

Export the IDP metadata XML to send to BlackBerry Workspaces to complete the integration.

In the **Application Configuration** page, navigate to the **Sign On** tab and select **Identity Provider metadata**, download and save the file to your computer.

After your successfully create and save the metadata file, finish the integration by importing the file into the BlackBerry Workspaces Advanced Configuration Tool (contact your Professional Services representative to complete this step), and complete the configuration. If your organization is hosted on the BlackBerry Workspaces cloud, contact customer support via your BlackBerry myAccount to configure your account with SAML integration. To complete the integration, the metadata pulled from your organization's identity provider is required.

Custom logout URL for cloud implementations

Add the custom logout URL to idp.xml for cloud implementations.

Okta does not offer a logout page URL in their standard idp.xml. For that reason,BlackBerry Workspaces created a custom page that your users can be redirected to after logging off from BlackBerry Workspaces. However, the page only exists on BlackBerry Workspaces cloud server and cannot be used with on-premise BlackBerry Workspaces implementations.

From the **SingleSignOnService** tag in the XML, add the following tags after the `SingleSignOnService` tag and before the `IDPSSODescriptor` tag:

- `<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="`https://www.watchdox.com/saml-idp/saml/SingleLogout/alias/defaultAlias`"/>`
- `<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="`https://www.watchdox.com/saml-idp/saml/SingleLogout/alias/defaultAlias`"/>`

AD FS

This procedure explains how to register your BlackBerry Workspaces application with AD FS. Before you can evaluate the single-sign-on (SSO) scenario, you must first install and configure AD FS on the FSWEB computer. After completing this step, the FSWEB computer will be set up in the federation server role and you can create an application profile for BlackBerry Workspaces.

Register BlackBerry Workspaces application

Before you begin: Download the metadata from the BlackBerry Workspaces server at https://<*SERVER.ADDRESS*>/saml-idp/saml/metadata.

1. From the **Start** menu, open the **ADFS Manager** application.
2. Start the Relying Party Trust wizard.
   a) Expand **Trust Relationships** and right-click **Relying Party Trusts**
   b) Select **Add Relying Party Trust...**.
3. Complete the Add Relying Party Trust wizard.
   a) On the Welcome screen, click **Start**.
   b) On the Select Data Source page, select **Import data about the relying party from a file**.
   c) Click **Browse**, and select the BlackBerry Workspaces metadata file that you downloaded.
   d) Click **Next**, and when the ADFS Management dialog appears, click **OK**.
4. If you are prompted to perform additional configurations, determine with the ADFS IT team the appropriate configuration for your organization.
   - Configure Multi-factor Authentication (ADFS 3.0+)
   - Permit all users or Deny all users
5. When the trust configuration summary dialog appears, click **Next**.
6. Select the **Open the Edit Claim Rules** check box, and click **Close**.

Configuring the BlackBerry Workspaces Settings

After you register the BlackBerry Workspaces application, you must set Claim Rules for BlackBerry Workspaces and configure BlackBerry Workspaces property settings.

- Set Issuance Tranform rules, see: Set the issuance transform rules
  - Send LDAP Attributes as Claims
  - Transform an Incoming Claim
- Set Issuance Authorization rules, see: Set the issuance authorization rules
  - Send LDAP Attributes as Claims
  - Permit All Users (optional)
- Set Delegation Authorization rule, see: Set the delegation authorization rule
  - Send LDAP Attributes as Claims
- Configure BlackBerry Workspaces property settings, see: Configure BlackBerry Workspaces properties settings

Set the issuance transform rules

On the **Issuance Transform Rules** tab, configure the Send LDAP Attributes as Claims rule and the Transform as an Incoming Claim rule.

1. Access the Edit Claim Rules application.
   a) Click **Relying Party Trust**.
   b) Right-click the new BlackBerry Workspaces Party Trust and select **Edit Claim Rules**.
2. Click the **Issuance Transform Rules** tab.
3. Click **Add rule...** > **Send LDAP Attributes as Claims** > **Next** .
4. Assign values to the rule parameters.

Rule parameter	Value
Claim Rule Name	Get LDAP Attributes
Attribute Store	Active Directory

5. Configure the LDAP attributes, and click **OK**.

LDAP attribute	Outgoing claim type
Email-Addresses	Email address
Display-Name	Given name
User-Principal-Name	UPN

6. Click **Add rule...** > **Transform an Incoming Claim** > **Next** .
7. Assign values to the rule parameters.

Rule parameter	Value
Claim Rule Name	Email to Name ID
Incoming Claim Type	Email address
Outgoing Claim Type	Name ID Do not select Name.
Outgoing Name ID Format	Email

8. Click **Pass through all claim values**.

Set the issuance authorization rules

On the **Issuance Authorization Rules** tab you configure the send LDAP attributes as claims rule and the permit all users rule. The permit all users rule is optional. Consult your AD FS IT team to determine if this rule is required for your organization.

1. Access the Edit Claim Rules application.
   a) Click **Relying Party Trust**.
   b) Right-click the new BlackBerry Workspaces Party Trust and select **Edit Claim Rules**.
2. Click the **Issuance Transform Rules** tab.
3. Click **Add rule...** > **Send LDAP Attributes as Claims** > **Next** .

4. Assign values to the rule parameters.

Rule parameter	Value
Claim Rule Name	Get LDAP Attributes
Attribute Store	Active Directory

5. Configure the LDAP attribute, and click **OK**.

LDAP attribute	Outgoing claim type
Email-Addresses	Email address

6. Optional: Click **Add rule...** > **Permit All Users** > **Next** > **Finish** .

Set the delegation authorization rule

On the **Delegation Authorization Rules** tab, configure the send LDAP attributes as claims rule.

1. Access the Edit Claim Rules application.
   a) Click **Relying Party Trust**.
   b) Right-click the new BlackBerry Workspaces Party Trust and select **Edit Claim Rules**.
2. Click the **Delegation Authorization Rules** tab.
3. Click **Add rule...** > **Send LDAP Attributes as Claims** > **Next** .
4. Assign values to the rule parameters.

Rule parameter	Value
Claim Rule Name	Email address
Attribute Store	Active Directory

5. Configure the LDAP attribute, and click **OK**.

LDAP attribute	Outgoing claim type
Email-Addresses	Email address

Configure BlackBerry Workspaces properties settings

After you set the AD FS rules, configure the BlackBerry Workspaces property settings.

1. Right-click the BlackBerry Workspaces party trust and select **Properties**.
2. Configure properties on the **Advanced** tab.
   a) Click the **Advanced** tab.
   b) Set the Secure has algorithm value to `SHA-1`.
3. Remove the endpoints from SAML Logout Endpoint.
   a) Click the **Endpoints** tab.
   b) Select each of the endpoints under SAML Logout Endpoint, and click **Remove**.
4. Add and configure endpoints for SAML.

Endpoint type	SAML Logout

Binding	POST
Trusted URL	`https://<ADFS.SERVER.ADDRESS>/adfs/ls/?wa=wsignout1.0` The *ADFS.SERVER.ADDRESS* is configured in AD FS. To verify your configuration, navigate to AD FS Management and right-click **AD FS**. Select **Edit Federation Service Properties..**. The AD FS address is listed as Federation Service name.
Response URL	`https://<WDX.SERVER.ADDRESS>/saml-idp/saml/SingleLogout/alia/defaultAlias` The *WDX.SERVER.ADDRESS* is the URL of your BlackBerry Workspaces server. You can verify the full URL by searching for SingleLogoutService in BlackBerry Workspaces metadata. The URL is listed as Location.

5. Click **OK**.

Configuring the BlackBerry Workspaces Settings for AD FS 4.0

After you register the BlackBerry Workspaces application, you must set Claim Rules for BlackBerry Workspaces and configure BlackBerry Workspaces property settings.

See Set the issuance transform rules for AD FS 4.0 and Configure BlackBerry Workspaces properties settings for AD FS 4.0.

Set the issuance transform rules for AD FS 4.0

1. On the Active Directory Federation Services server, download the Workspaces SAML metadata from https://<workspaces.server.address>/saml-idp/saml/metadata.
2. Click **Start > AD FS Manager**.
3. In the left-hand menu, click **Relying Party Trust**.
4. In the Relying Party Trust Wizard, click **Add Relying Party Trust**.
5. Select the **Claims Aware** option.
6. In the Select Data Source section, select the **Import data about the relying party from a file** option.
7. Click **Browse** and navigate to the metadata.xml from step 1.
8. Click **Next**.
9. Type a Display name, such as BlackBerry Workspaces, and click **Next**.
10. In the Choose Access Control Policy section, select **I do not want to configure access policies at this time. No user will be permitted access for this application** or adjust to match your organization's policy and click **Next**.
11. Leave the options in the Ready to Add Trust section at the default values and click **Next**.
12. In the Finish section, select the **Configure claims issuance policy for this application** option and click **Close**.
13. In the Edit Claim Issuance Policy dialog box, click **Add Rule**.
14. In the **Claim rule template** list, select **Send LDAP Attribute as Claims**.
15. In the **Claim Rule Name** field, type `Get LDAP Attributes`.

16. In the **Mapping of LDAP attributes to outgoing claim types** table, configure the following LDAP attributes.
    - User-Principal-Name = Name ID
    - Display-Name = Given Name
17. Click **OK**.

After you finish: Configure BlackBerry Workspaces properties settings for AD FS 4.0

Configure BlackBerry Workspaces properties settings for AD FS 4.0

After you set the AD FS rules, you must configure the BlackBerry Workspaces property settings.

1. In the AD FS Manager application, right-click on the Relying Party Trust that you created, and select **Properties**.
2. On the **Advanced** tab, in the **Signature Algorithm** drop-down list, select `SHA-1`.
3. Use the information in the following table to add and configure endpoints for SAML.

Endpoint type	SAML Logout
Binding	POST
Trusted URL	`https://<adfs.server.address>/adfs/ls/?wa=wsignout1.0` The adfs.server.address is configured in AD FS. To verify your configuration, navigate to AD FS Management and right-click **AD FS**. Select **Edit Federation Service Properties**. The AD FS address is listed as Federation Service name.
Response URL	`https://<workspaces.server.address>/saml-idp/saml/SingleLogout/alias/defaultAlias` The workspaces.server.address is the URL of your BlackBerry Workspaces server. You can verify the full URL by searching for SingleLogoutService in the BlackBerry Workspaces metadata. The URL is listed as Location.

4. Click **OK**.

After you finish: Create the AD FS identity provider on the BlackBerry Workspaces server

Create the AD FS identity provider on the BlackBerry Workspaces server

1. Download the AD FS metadata XML file from https://<*ADFS.SERVER.ADDRESS*>/FederationMetadata/2007-06/FederationMetadata.xml

   If you use Internet Explorer to download the metadata file the file data might display as plain text, and not like a traditional XML file. If this occurs, you must either enable Internet Explorer Compatibility View or download the file using a different web browser.
2. Save the XML file locally by selecting **File** > **Save As**.

Make sure to remove all XML elements related to `<ds:Signature> </ds:Signature>` in the metadata file before using the file with the BlackBerry Workspaces Advanced Configuration Tool. In addition, do not copy and paste the data of the XML file into a text file.

After successful creation of the metadata file, complete the integration by importing the file into tthe BlackBerry Workspaces Advanced Configuration Tool (contact your Professional Services representative to complete this step), to complete the configuration. If your organization is hosted on the BlackBerry Workspaces cloud, contact customer support via your BlackBerry myAccount to configure your account with SAML integration. To complete the integration, the metadata pulled from your organization's identity provider is required.

Legal notice

THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

The terms of use of any BlackBerry product or service are set out in a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY BLACKBERRY FOR PORTIONS OF ANY BLACKBERRY PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada