



BlackBerry Enterprise Identity Integration Guide

Integrating SaaS services

Contents

- What is BlackBerry Enterprise Identity?..... 5**

- Setting up BlackBerry Enterprise Identity and the SaaS client..... 6**
 - Create a certificate and key pair.....6
 - Configure a new SAML connection in the SaaS client.....6
 - Create a SaaS service in the BlackBerry UEM console.....7
 - Create a SaaS service in the BlackBerry Enterprise Identity console.....8

- Amazon Web Services service configuration.....10**

- Box service configuration.....11**

- Citrix GoToMeeting service configuration..... 12**

- Concur service configuration..... 13**

- DocuSign service configuration.....14**

- Dropbox service configuration..... 15**

- Egencia service configuration..... 16**

- Evernote service configuration.....17**

- G Suite service configuration..... 18**

- Office 365 service configuration..... 19**
 - Set up Windows PowerShell..... 19
 - Add a new Microsoft Office 365 domain.....19
 - Update an existing Microsoft Office 365 domain..... 21

- Salesforce service configuration.....23**

ServiceNow service configuration.....	24
WebEx service configuration.....	25
WebFOCUS service configuration.....	26
Workday service configuration.....	27
Workspaces service configuration.....	28
Configuring BlackBerry Enterprise Identity to work with Workspaces.....	28
Yammer service configuration.....	30
Zendesk service configuration.....	31
Zscaler service configuration.....	32
Legal notice.....	33

What is BlackBerry Enterprise Identity?

BlackBerry Enterprise Identity provides single sign-on (SSO) to cloud services such as Microsoft Office 365, G Suite, BlackBerry Workspaces, and many others. With single sign-on, users don't have to complete multiple log ins or remember multiple passwords. Administrators can also add custom services to Enterprise Identity to give users access to internal applications. Users can access the services from any device they want to use, such as iOS, Android, or BlackBerry 10 devices and other computing platforms.

Enterprise Identity is bundled with BlackBerry UEM, BlackBerry UEM Cloud, or BES12. Administrators use the BlackBerry UEM, BlackBerry UEM Cloud, or BES12 console to add services, manage users, and add and manage additional administrators. This integration with BlackBerry EMM products makes it easy to manage users and enable them to access cloud services from their devices.

To use Enterprise Identity you must purchase user licenses for the Collaboration, Application, or Content Editions of BlackBerry Enterprise Mobility Suite, or separate BlackBerry Enterprise Identity user licenses. For more information about BlackBerry Enterprise Identity, including how to purchase Enterprise Identity, see the information on blackberry.com.

The following browsers are supported for administration: Internet Explorer 10 and 11, Google Chrome, Mozilla Firefox, and Safari. Client use is supported on all the browsers above as well as native browsers on devices running BlackBerry 10 OS version 10.2.1 or later, iOS 8 or later, and Android 4.0 or later.

Feature	Benefit
Enhance employee productivity	Employees can use one password for all cloud services, across all mobile devices (iOS, Android and BlackBerry) and traditional computing platforms (Windows and macOS). This eliminates the frustration of multiple passwords and logins.
Customize authentication	Based on your specific security scenario, BlackBerry Enterprise Identity allows you to choose the authentication method for any given service, user group, or combination of the two. You can even adapt your organization's policies to adapt to high-risk situations.
Advance your mobile strategy	Users and their identities are fundamental to enterprise mobility. BlackBerry Enterprise Identity unifies and simplifies access to cloud services like Microsoft Office 365, Salesforce, Google Apps, BlackBerry Workspaces , or most other SAML-based apps and services, supporting the productivity of your increasingly mobile workforce.
Leverage your existing EMM solution from BlackBerry	Enterprise Identity is fully integrated with BlackBerry UEM, delivering industry-leading EMM along with greater control of access to all your cloud services. This allows you to gain access to features like single-click app provisioning and SSO entitlement, BlackBerry 2FA, and Mobile Zero Sign-On (Mobile ZSO).

Setting up BlackBerry Enterprise Identity and the SaaS client

To make sure that BlackBerry Enterprise Identity and your organization's SaaS client can work together you must perform the following tasks:

- [Create a certificate and key pair](#)
- [Configure a new SAML connection in the SaaS client](#)
- [Create a SaaS service in the BlackBerry UEM console](#) or [Create a SaaS service in the BlackBerry Enterprise Identity console](#)

Create a certificate and key pair

A certificate and key pair are required for each service to function. They expire periodically and must be recreated. Your organization may have its own process for creating certificates and keys. For example, you might contract with one of the companies that sells certificates. This task describes how to create a self-signed certificate, which may not be appropriate for all organizations and is not typically the most secure. Management of the keys is important to maintain security.

1. Download OpenSSL. For Windows, use the Win32 OpenSSL light installer.
2. In a command prompt window, type:
 - `cd \OpenSSL-Win32\bin.`
 - `openssl req -newkey rsa:2048 -nodes -keyout private.key -x509 -days 730 -out certificate.pem`

When prompted by openssl, use the following values:

Country Name (2 letter code) [AU]:CA State or Province Name (full name) [Ontario]: Locality Name (eg, city) [Waterloo]: Organization Name (eg, company) [Internet Widgits Pty Ltd]: Organizational Unit Name [Marketing]: BlackBerry Identity Common Name (e.g. server FQDN or YOUR name) [example.fqdn]: ServiceName Email Address [myoffice365@email.com]:

3. Store the key file in a safe place (for example, a keystore). The key should be encrypted and password protected. The certificate is included in the service metadata and can be shared.

Configure a new SAML connection in the SaaS client

1. Log in to the SaaS service client application as an administrator.
2. Locate the SAML setup page. Some services include a search function that can make this easy. You can also refer to the documentation for your SaaS client to help you set up the connection.
3. Click the button to add an additional SAML identity provider.
4. Most services require the use of a common subset of the SAML fields. Complete the fields with the information required.
5. If you paste the IdP signing certificate manually, add `-----BEGIN-----` before and `-----END CERTIFICATE-----` after the certificate text.
6. Click the command to save the configuration page.

Create a SaaS service in the BlackBerry UEM console

Note: If you want to create two instances of the same type of service in BlackBerry UEM (for example, Box), you must provide different Service provider entity IDs for each instance.


1. In the BlackBerry UEM management console, on the menu bar, click **Settings**.
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click **+**.
4. Select the type of service that you want to create (for example Box).
5. In the **Add a BlackBerry Enterprise Identity service** screen, enter the service provider metadata. This metadata is specific to the service provider and your organization. Note that only the fields that are associated with the selected service template display.

Name	Description
Mobile zero sign-on	Select this option if you want to enable mobile zero-sign-on.
Name	Enter the SaaS provider name.
Description	The tenant description is optional.
Logo	Add a logo to associate with the service.
Service provider entity ID	Enter the URL or unique name you use to access the SaaS service.
Assertion consumer service POST URL	Enter the POST URL provided by the service provider.
IdP-initiated login support	Enter the type of login support that your organization requires.
Signing options	Enter your assertion choice.
IdP signing certificate	Enter the x509 certificate shared with the service provider.
IdP signing private key	Enter the x509 key for the corresponding signing certificate. Keep this secure.
Encryption certificate	Enter the encryption certificate
Service-specific information	Some services require additional information or information slightly different than these descriptions. Most of the time this additional information is preconfigured.
Claims - Name identifier attribute	Select the identifier attribute for your claim.

Name	Description
SAML claim attributes	<ul style="list-style-type: none"> Name - Enter a name for your SAML claim SAML attribute - Enter your SAML attribute SAML claim type <ul style="list-style-type: none"> Local - if you choose a Local claim, you have to select an option in the Attribute value list. This will map a SAML attribute to an attribute type known to BlackBerry Enterprise Identity, such as User name Static - if you choose a Static claim, you have to type an option in the Attribute value field Attribute value - select or type an attribute value. This is a defined attribute value that your SaaS service might require to set up the service for your organization's users. Attribute type - select a type for the attribute. The type is based on your SaaS service requirements. The default is anyType.

6. Click **Save**.

Create a SaaS service in the BlackBerry Enterprise Identity console

1. Log in to the BlackBerry UEM administrator console and click **Apps**.
2. Click .
3. Click the **Enterprise Identity** icon.
4. If a message appears asking you to synchronize Enterprise Identity cloud services, click **Synchronize**.
5. Click **Open Enterprise Identity console**.
6. In the left pane, click **Services**.
7. In the **Select a service type to create** list, select a service and click **+Create**.
8. Complete the fields to match your SaaS service tenant.

Name	Description
Zero Sign-On	Select this option if you want to enable zero-sign-on
Name	Enter the SaaS provider name.
Description	The tenant description is optional.
Service Provider Entity ID	Enter the URL or unique name you use to access the SaaS service.
Assertion Consumer Service POST URL	Enter the POST URL provided by the service provider.
IdP Signing Certificate	Enter the x509 certificate shared with the service provider.
IdP Signing Key	Enter the x509 key for the corresponding signing certificate. Keep this secure.

Name	Description
Service-specific information	Some services require additional information or information slightly different than these descriptions. Most of the time this additional information is preconfigured.

9. Click **Save**.

10. Click **Enable**.

11. Click the service you created.

12. Click **Download** to save the metadata document from the Enterprise Identity administrator console.

Amazon Web Services service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Amazon Web Services
Description	Amazon Web Services environment
Signing Certificate	True
Signing Key	True
SAML claim attributes	
Role	<ul style="list-style-type: none">• Attribute = https://aws.amazon.com/SAML/Attributes/Role• Value = arn:aws:iam:<your_account_id>:role/SAML_admin_user,arn:aws:iam:<your_account_id>:saml-provider/<your_provider_name>• Type = Static
Role session name	<ul style="list-style-type: none">• Attribute = https://aws.amazon.com/SAML/Attributes/RoleSessionName• Value = email address• Type = Local

For more information about setting up the AWS service configuration, see the [information from Amazon](#).

Box service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Box
Description	Box environment
Service Provider Entity ID	box.net
Signing Certificate	True
Signing Key	True

Citrix GoToMeeting service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO
Name	GoToMeeting
Description	GoToMeeting environment
Signing Certificate	True
Signing Key	True

Concur service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Concur
Description	Concur environment
Service Provider Entity ID	Retrieve from Concur metadata
Signing Certificate	True
Signing Key	True

DocuSign service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	DocuSign
Description	DocuSign environment
Signing Certificate	True
Signing Key	True

Dropbox service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Dropbox
Description	Dropbox environment
Service Provider Entity ID	Retrieve from Dropbox metadata
Signing Certificate	True
Signing Key	True

Egencia service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Egencia
Description	Egencia environment
Service Provider Entity ID	Retrieve from Egencia metadata
Signing Certificate	True
Signing Key	True

Evernote service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Evernote
Description	Evernote environment
Service Provider Entity ID	Retrieve from Evernote metadata
Assertion consumer Service (single sign-on) URL	Retrieve from Evernote metadata
Signing Options	Assertions and entire response
Signing Certificate	True
Signing Key	True

G Suite service configuration

Name	Description
Service Provider Entity ID	google.com/a/domain
Assertion Consumer Service (Single Sign On) URL	https://www.google.com/a/<email domain>/acs
Recipient	https://www.google.com/a/<email domain>/acs
Destination	https://www.google.com/a/<email domain>/acs
Signing Certificate	True
Signing Key	True

Office 365 service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Office 365
Description	Microsoft Office 365 environment
Identity Provider Entity ID	Enterprise Identity URL - vanity URL
Signing Certificate	True
Signing Key	True

Set up Windows PowerShell

Each Microsoft Office 365 tenant can support multiple email domains. Complete these steps to configure a Microsoft Office 365 domain. All Microsoft Office 365 commands are performed in Windows PowerShell.

Before you begin: Install Windows Management Framework 3.0. This includes Windows PowerShell. See <https://www.microsoft.com/en-us/download/details.aspx?id=34595> for details.

1. Download and install the Azure Active Directory module. For information, see https://docs.microsoft.com/en-us/powershell/msonline/v1/azureactivedirectory?redirectedfrom=msdn#bkmk_installmodule.
2. Install the Windows PowerShell module for Skype from <http://go.microsoft.com/fwlink/p/?LinkId=532439>.
3. Restart Windows PowerShell.
4. Setup and authenticate the following modules using your Microsoft Office 365 administrator credentials:
 - a) Type `import-module MSOnline`. Press **Enter**.
 - b) Type `$cred=Get-Credential`. Press **Enter**.
 - c) Type `Connect-MsolService -Credential $cred`. Press **Enter**.

Add a new Microsoft Office 365 domain

If you create a new email domain, you must also create a new Microsoft Office 365 domain.

Before you begin: [Set up Windows PowerShell](#)

1. Use Windows PowerShell, enter the following commands to enable ADAL for Microsoft Exchange Online:
 - a) `Set-ExecutionPolicy RemoteSigned`
 - b) `$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $cred -Authentication Basic -AllowRedirection`
 - c) `Import-PSSession $Session`
 - d) `Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true`
 - e) `Get-OrganizationConfig | ft name, *OAuth*`
2. In Windows PowerShell, enter the following commands:

- a) Import-Module SkypeOnlineConnector
 - b) \$sfboSession = New-CsOnlineSession -Credential \$cred
 - c) Import-PSSession \$sfboSession
 - d) Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed
 - e) Get-CsOAuthConfiguration
3. In Windows PowerShell, run the following commands to add a new domain. Replace text in angle brackets (< >) with the variables that fit your local environment. It can take up to an hour for changes to the settings to take effect.
 4. Type \$domain = "<email server domain>" where the email server domain is the domain of your email server. Press **Enter**
 5. Use the certificate used in the Enterprise Identity service configuration for Microsoft Office 365 and enter:\$certFile = "<cacert.pem file path>"
 6. Type \$cert = [IO.File]::ReadAllText(\$certFile). Press **Enter**.
 7. Type \$cert = \$cert.replace("-----BEGIN CERTIFICATE-----", ""). Press **Enter**.
 8. Type \$cert = \$cert.replace("-----END CERTIFICATE-----", ""). Press **Enter**.
 9. Type \$cert = \$cert.replace("`r", ""). Press **Enter**.
 10. Type \$cert = \$cert.replace("`n", ""). Press **Enter**.
 11. Type \$activeLogOnUri = "https://idp.blackberry.com/<IDP vanity URL or organization ID>/idp/profile/SAML2/SOAP/ECP/https%3A%2F%2Fidp.blackberry.com-<IDP vanity URL or organization ID>" where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
 12. Type \$brandName = "Enterprise ID". Press **Enter**.
 13. Type \$issuerUri = "https://idp.blackberry.com-<IDP vanity URL or organization ID>" where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
 14. Type \$logOffUri = "https://idp.blackberry.com/<IDP vanity URL or organization ID>/idp/profile/SAML2/Redirect/SLO/https%3A%2F%2Fidp.blackberry.com-<IDP vanity URL or organization ID>" where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
 15. Type \$passiveLogOnUri = "https://idp.blackberry.com/<IDP vanity URL or organization ID>/idp/profile/SAML2/POST/SSO/https%3A%2F%2Fidp.blackberry.com-<IDP vanity URL or organization ID>" where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
 16. Type \$protocol = "SAML" and press **Enter**.
 17. Type Set-MsolDomainAuthentication -DomainName \$domain -Authentication managed. Press **Enter**.
 18. Type Set-MsolDomainAuthentication -DomainName \$domain -Authentication federated -ActiveLogOnUri \$activeLogOnUri -FederationBrandName \$brandName - IssuerUri \$issuerUri -LogOffUri \$logOffUri -PassiveLogOnUri \$passiveLogOnUri - SigningCertificate \$cert -PreferredAuthenticationProtocol \$protocol. Press **Enter**.
 19. Use Get-MsolDomainFederationSettings -DomainName \$domain | Format-List * to check the domain settings.
 20. If the settings are correct, close Windows PowerShell. To edit the settings, run the following commands:
 21. Type Set-MsolDomainAuthentication -DomainName \$domain -Authentication managed. Press **Enter**.
 22. Make any necessary changes.
 23. Type Set-MsolDomainAuthentication -DomainName \$domain -Authentication federated -ActiveLogOnUri \$activeLogOnUri -FederationBrandName \$brandName -

```
IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -
SigningCertificate $cert -PreferredAuthenticationProtocol $protocol. Press Enter.
```

Update an existing Microsoft Office 365 domain

You can update existing domains when the email domain must be redirected to a different Enterprise Identity domain than Microsoft Office 365.

Before you begin: [Set up Windows PowerShell](#)

1. In Windows PowerShell, run the following commands to change the existing domain to point to the new domain.
2. Type `$domain = "<email server domain>"`, where the email server domain is the domain of your email server. Press **Enter**.
3. To use the certificate used in the Enterprise Identity service configuration for Microsoft Office 365, type `$certFile = "<cacert.pem file path>"`. Press **Enter**.
4. Type `$cert = [IO.File]::ReadAllText($certFile)`. Press **Enter**.
5. Type `$cert = $cert.replace("-----BEGIN CERTIFICATE-----", "")`. Press **Enter**.
6. Type `$cert = $cert.replace("-----END CERTIFICATE-----", "")`. Press **Enter**.
7. Type `$cert = $cert.replace("`r", "")`. Press **Enter**.
8. Type `$cert = $cert.replace("`n", "")`. Press **Enter**.
9. Type `$activeLogOnUri = "https://idp.blackberry.com/<IDP vanity URL or organization ID>/idp/profile/SAML2/SOAP/ECP/https%3A%2F%2Fidp.blackberry.com-<IDP vanity URL or organization ID>"`, where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
10. Type `$brandName = "Enterprise ID"`. Press **Enter**.
11. Type `$issuerUri = "https://idp.blackberry.com-<IDP vanity URL or organization ID>"`, where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
12. Type `$logOffUri = "https://idp.blackberry.com/<IDP vanity URL or organization ID>/idp/profile/SAML2/Redirect/SLO/https%3A%2F%2Fidp.blackberry.com-<IDP vanity URL or organization ID>"`, where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
13. Type `$passiveLogOnUri = "https://idp.blackberry.com/<IDP vanity URL or organization ID>/idp/profile/SAML2/POST/SSO/https%3A%2F%2Fidp.blackberry.com-<IDP vanity URL or organization ID>"`, where the *IDP vanity URL or organization ID* is the vanity URL or organization ID. Press **Enter**.
14. Type `$protocol = "SAML"`. Press **Enter**.
15. Type `Set-MsolDomainAuthentication -DomainName $domain -Authentication managed`. Press **Enter**.
16. Type `Set-MsolDomainAuthentication -DomainName $domain -Authentication federated -ActiveLogOnUri $activeLogOnUri -FederationBrandName $brandName -IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -SigningCertificate $cert -PreferredAuthenticationProtocol $protocol`. Press **Enter**.
17. Use `Get-MsolDomainFederationSettings -DomainName $domain | Format-List *` to check the domain settings.
18. If the settings are correct, close Windows PowerShell. To edit the settings, use the following commands:
19. Type `Set-MsolDomainAuthentication -DomainName $domain -Authentication managed`. Press **Enter**.

20. Make and necessary changes.

21. Type `Set-MsolDomainAuthentication -DomainName $domain -Authentication federated -ActiveLogOnUri $activeLogOnUri -FederationBrandName $brandName -IssuerUri $issuerUri -LogOffUri $logOffUri -PassiveLogOnUri $passiveLogOnUri -SigningCertificate $cert -PreferredAuthenticationProtocol $protocol`. Press **Enter**.

Salesforce service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Salesforce
Description	Salesforce environment
Service Provider Entity ID	Retrieve from Salesforce metadata
Assertion Consumer Service URL	Retrieve from Salesforce metadata
Signing Certificate	True
Signing Key	True

ServiceNow service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	ServiceNow
Description	ServiceNow environment
Service Provider Entity ID	Retrieve from ServiceNow metadata
Assertion Consumer Service POST URL	Retrieve from ServiceNow metadata
Single Logout Service URL	ServiceNow environment
Signing Certificate	True
Signing Key	True

WebEx service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	WebEx
Description	Cisco WebEx environment
Service Provider Entity ID	Retrieve from WebEx metadata
Assertion Consumer Service URL	Retrieve from WebEx metadata
Signing Certificate	True
Signing Key	True

WebFOCUS service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	WebFOCUS
Description	WebFOCUS environment
Service Provider Entity ID	Retrieve from WebFOCUS metadata
Assertion Consumer Service (Single Sign On) URL	Retrieve from WebFOCUS metadata
Service Provider-initiated Login URL	Retrieve from WebFOCUS metadata
Single Logout Service URL	Retrieve from WebFOCUS metadata
Signing Certificate	True
Signing Key	True

Workday service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Workday
Description	Workday environment
Service Provider Entity ID	Retrieve from Workday metadata
Assertion Consumer Service URL	Retrieve from Workday metadata
Signing Certificate	True
Signing Key	True

Workspaces service configuration

Single sign-on to Workspaces to work with an on-premise instance of BlackBerry UEM

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Workspaces
Description	Workspaces environment
Service Provider Entity ID	com.watchdox.saml
SP-initiated Login URL	Retrieve from Workspaces metadata
Issuer	Retrieve from Workspaces metadata
Signing Certificate	True
Signing Key	True

Configuring BlackBerry Enterprise Identity to work with Workspaces

Before you begin: You must have the following environment:

- An on-premise installation of Workspaces with vApp or Appliance-X
- A BlackBerry UEM server, or BlackBerry UEM Cloud instance enabled with Enterprise Identity

Note:

New BlackBerry UEM Cloud and Workspaces tenants are now auto-configured to allow users to sign in with Enterprise Identity, allowing application of two-factor authentication or other advanced access policies (pre-existing BlackBerry UEM Cloud tenants will gain this capability in a future release)

1. Go to `https://<your server>/saml-idp/saml/metadata`.
2. Download the metadata file.
3. [Generate a certificate key pair](#).
4. Do one of the following:
 - Use the BlackBerry UEM version 12.6.3 or earlier management console to log into the Enterprise Identity console.
 - Use the BlackBerry UEM version 12.7 or later, or the BlackBerry UEM Cloud management console to open the Enterprise Identity Services page.
5. Create a Workspaces service.
6. Map the service entity ID and the signin / signout URL from the metadata to the corresponding fields in Workspaces service.
7. Configure IDP signing certificate and private key using the key pair generated earlier.
8. Set the claims as `E-mail Address` (`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddresses`).
9. Click **Save**.

10. Download the metadata for the Workspaces service.
11. With an administrator account, log in to the Workspaces management console.
12. Click **Authentication type** and select **BlackBerry Enterprise Identity**.
13. Upload the metadata you downloaded from BlackBerry UEM for Workspaces. This creates a new IDP in Workspaces.
14. Click **Save**.
15. Log into Workspaces BlackBerry Workspaces Configuration Tool and associate the tenant with the new IDP.
16. Log into the Workspaces URL and verify that it directs to the IDP.
17. Verify that everything works by entering the username and password for a user that is entitled with BlackBerry Enterprise Identity.

Yammer service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Yammer
Description	Yammer environment
Service Provider Entity ID	Retrieve from Yammer metadata

Zendesk service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Zendesk
Description	Zendesk environment
Service Provider Entity ID	Retrieve from Zendesk metadata
Assertion Consumer Service (Single Sign On) URL	Retrieve from Zendesk metadata
Signing Certificate	True
Signing Key	True

Zscaler service configuration

Name	Description
Mobile ZSO	Select this option if you want to enable Mobile ZSO.
Name	Zscaler
Description	Zscaler environment
Service Provider Entity ID	Retrieve from Zscaler metadata
Assertion Service Consumer POST URL	Retrieve from Zscaler metadata
SP-initiated Login URL	Protected resource URL
Signing Certificate	True
Signing Key	True

Legal notice

©2018 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

Amazon Web Services is a trademark of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Android and Google Chrome are trademarks of Google Inc. Box is including without limitation, either a trademark, service mark or registered trademark of Box, Inc. Concur is a trademark of Concur Technologies, Inc. DocuSign is a trademark of DocuSign, Inc. in the United States and/or other countries. Dropbox is a trademark of Dropbox, Inc. Egencia is a trademark of Egencia LLC. Evernote is a trademark of Evernote Corporation. is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Linux is a trademark of Linus Torvalds. Mac OS and Safari are trademarks of Apple Inc. Microsoft, Active Directory and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Mozilla and Firefox are trademarks of Mozilla Foundation. OpenSSL is a trademark of the The OpenSSL Software Foundation, Inc. Oracle VM VirtualBox is a trademark of Oracle and/or its affiliates. Salesforce is a trademark of salesforce.com, inc. and is used here with permission. ServiceNow Ubuntu is a trademark of ServiceNow. is a trademark of Canonical Limited. WebFOCUS is a trademark of Information Builders, Inc. Workday is a trademark of Workday, Inc. Zendesk is a trademark of Zendesk, Inc. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO

NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION 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