BlackBerry AtHoc

Single Sign-On Administrator Guide

7.12

Contents

Enable single sign-on

Single sign-on is not enabled by default. A system administrator must enable SSO in the Feature Enablement settings in the BlackBerry AtHoc management system. For more information, see "Enable and disable features" in the *BlackBerry AtHoc System Administrator Configuration Guide*.

When SSO is enabled for your organization, if your users are already authenticated and signed in using your identity provider (IDP), they can access the BlackBerry AtHoc management system or Self Service without the need to sign in again.

If a user is not signed in, when they attempt to sign in, they are redirected to their organization's customer IDP login. This IDP is managed by your organization or by a third party vendor that provides IDP services. The IDP authenticates the user. The user is then redirected to BlackBerry AtHoc. If the user is already signed in to the IDP they are automatically redirected to the BlackBerry AtHoc management system or Self Service with an active session.

You must have organization administrator, enterprise administrator, or system administrator permissions to enable single sign-on.

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Enabled Authentication Methods** section, select the Single Sign-On (SSO) **Enable** check box.
5. Click **Save**.

Enable single sign-on for Self Service

1. Log in to the BlackBerry AtHoc management system as an administrator.
2. In the navigation bar, click .
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, in the **Self Service** section, select **Single Sign-On** from the **Authentication Method** list. The Sign In URL field is auto populated with a URL in the following format: <*server*>/selfservice/*organization-code*. This URL is used when users attempt to access Self Service using SSO authentication.
5. Optionally, if you selected **Single Sign-On** as the authentication method, select **Username and Password** from the **Alternative Authentication Method** list to enable both SSO and Username/Password user authentication.

   Note: When an alternative authentication method is added, the Self Service sign-in URL is appended with /sso for single sign-on authentication. For example, <*server*>/selfservice/*organization-code*/sso.
6. Click **Configuration**.
7. On the **Self Service SSO configuration** window, configure Identity Provider and Service Provider settings.

   Note: You can also Export SP and IDP settings.
8. Click **Apply**.
9. Click **Save**.

Enable single sign-on for the BlackBerry AtHoc management system

1. Log in to the BlackBerry AtHoc management system as an administrator.

2. In the navigation bar, click ⚙.
3. In the **Users** section, click **User Authentication**.
4. On the **User Authentication** window, in the **Assign Authentication Methods to Applications** section, in the **Management System** section, select **Single Sign-On** from the **Authentication Method** list. The Sign In URL field is auto populated with a URL in the following format: <*server*>/client/*organization-code*. This URL is used when a user attempts to access the BlackBerry AtHoc management system using SSO authentication.
5. Click **Configuration**.
6. On the **Management system SSO configuration** window, configure Identity Provider and Service Provider settings.

   Note: You can also Export SP and IDP settings.
7. Click **Apply**.
8. Click **Save**.

Configure SSO certificates on the application server

If you are installing a new SSO configuration, you must install and configure the SSO certificates on each application server.

1. Open **mmc** as an administrator.
2. For **Computer Account**, add the certificates snap-in.
3. On the **mmc console** window, in the left pane, expand **Certificates (Local Computer)**.
4. Right-click **Personal** and select **All Tasks** > **Import...**.
5. On the **Certificate Import Wizard**, click **Next**.
6. On the **File to import** window, click **Browse** and navigate to select the certificate file on your local computer.
7. Click **Next**.
8. On the **Certificate Store** window, select **Place all certificates in the following store**.
9. In the **Certificate store:** field, click **Browse...** and select **Personal**.
10. Click **Next**.
11. Click **Finish**.
12. In the **mmc console**, right-click the installed certificate file and select **All Tasks** > **Manage Private Keys...**.
13. On the **Permissions** dialog, on the **Security** tab, select the **IUSR** and **IIS_IUSRS** users.
14. Click **OK**.
15. Restart the **IIS**.

Configure Identity Provider settings

The Identity Provider (IDP) provides authentication for users. The Service Provider (SP), in this case BlackBerry AtHoc or Self Service, requests authentication from the IDP.

When SSO is enabled for access to the BlackBerry AtHoc management system or Self Service, when a user logs in, they are redirected to their organization's IDP for authentication. If the user is already logged in to the Identity Provider, the authentication request is processed and sent to the Service Provider, and the user is granted access without the need to log in again.

If you are configuring a new SSO installation, complete the Configure SSO certificates on the application server before you configure the IDP settings.

1. On the **Management system SSO configuration** or **Self Service SSO configuration** window, configure the following **General Settings**:
   a. **Identity Provider Name**: Each SAML configuration is identified by a unique identity provider name. This name is internal to the configuration and is not exposed to partner providers. This field is required only when there are multiple SAML configurations. Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
   b. **Self Service Assertion Consumer Service URL** or **Management Assertion Consumer Service URL**: Enter the URL of the location of the identity provider's ACS where SAML responses are sent as part of SSO. Append the URL with */orgcode*.
   c. **Sign On Service URL**: Enter the URL of the location of the identity provider's SSO service where SAML authentication requests are sent as part of a service provider initiated single sign on.
   d. **Sign On Service Binding**: Optionally, select **Redirect** or **POST** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default setting is **Redirect**.
   e. **Logout Service URL**: The URL of the local service provider's single log out service where SAML logout messages are received. If single logout is not required, leave this field blank. For more information, see SSO logout service.
   f. **Logout Service Binding**: Optionally, select **Redirect** or **POST** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default setting is **Redirect**.
   g. **Artifact Resolution Service URL**: Optionally, enter an artifact resolution service URL. The service provider uses the Artifact Resolution Protocol to exchange an artifact for the actual SAML message referenced by the artifact.
   h. **Artifact Resolution Service Binding**: Optionally, select **SOAP**, **POST**, **REDIRECT** or **ARTIFACT** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner identity provider. The default is **SOAP**.
   i. **Name ID Format**: Optionally, select **Email Address**, **Persistent**, or **Transient** as the format to be used by the SP and IDP to identify a subject name identifier.
   j. **User Mapping Attribute**: Optionally, select the attribute that identifies the user. This attribute is retrieved from the SAML assertion metadata. The default is **Subject Name**.
   k. **Attribute Name**: Enter the name of the attribute used to identify the user.
2. Configure the following **Security Settings**:
   a. **SAML Response Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML authentication requests received from the partner service provider must be signed. Receiving signed authentication requests is highly recommended but optional.
   b. **Assertion Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML assertions sent to the partner service provider must be signed.

      Note: You must select **Signed** for either **SAML Response Signature** or **Assertion Signature** or both.

Note: You must have a valid certificate installed for your organization.

c. Select a **Signature Algorithm**. The default is **RSA-SHA256**.
d. **Assertion Encryption**: Select **Encrypted** or **Unencrypted**. When **Encrypted** is selected, SAML assertions sent to the partner service provider must be encrypted.
e. If **Assertion Encryption** is set to **Encrypted**, select an **Assertion Algorithm**. The default setting is **AES128**.
f. In the **Certificate*** field, click **Browse** to navigate to and select a certificate file. Only .cer and .crt files are supported.

3. Optionally, add the following **Additional information**:

a. **Company Name**: Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
b. **Company Display Name**: Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
c. **Company URL**
d. **Contact Person Name**
e. **Role or Department**
f. **Email Address**
g. **Telephone Number**

4. Click **Apply**.
5. Click **Save**.

Configure Service Provider settings

1. In the **Management system SSO configuration** or **Self Service SSO configuration** window, configure the following **General Settings**:
   a. **Service Provider Name**: Enter the name of the service provider that sends the SAML authentication request. Enter a name that is a minimum of three characters and a maximum of 512 characters. The following special characters are not allowed: `!?"<>!$%&^()={},;\:?"<>
   b. **Self Service Assertion Consumer Service URL** or **Management Assertion Consumer Service URL**: This field is pre-populated with the service provider's endpoint URL that receives the SAML from the identity provider. The assertion consumer service URL is appended with the organization code. For example:
      - Self Service URL: `https://domain/SelfService/Account/NewSSO/`*`organization-code`*
      - BlackBerry AtHoc management system: `https://domain/Client/`*`organization-code`*
   c. **Logout Service URL**: This field is pre-populated with the URL of the service provider's endpoint that receives SAML log out messages. For more information, see SSO logout service.
   d. **Custom Logout URL**: Optionally, enter a custom URL to redirect users to at logout.
   e. **Logout Service Binding**: Optionally, select **POST** or **Redirect** as the transport mechanism (SAML binding) to use when sending SAML authentication requests to the partner IDP. The default setting is **POST**.
2. Configure the following **Security Settings**:
   a. **SAML Response Signature**: Select **Signed** or **Unsigned**. When **Signed** is selected, SAML authentication requests received from the partner IDP must be signed. Receiving signed authentication requests is optional but highly recommended.

      Note: You must have a valid certificate installed for your organization.
   b. If **SAML Request Signature** is set to **Signed**, select a **Signature Algorithm**. The default setting is **RSA-SHA256**.
   c. In the **Certificate*** section, click **Import Certificate**.
      1. On the **Import Certificate** window, enter a password.
      2. lick **Browse** to navigate to and select a certificate file. Only .pfx and .p12 files are supported.
      3. Click **Import**.
3. Click **Apply**.
4. Click **Save**.

SSO logout service

If the logout URL is configured in the identity provider settings, the following steps terminate the active user session:

1. The end user initiates a logout request at a service provider.
2. The service provider forwards the logout request to an identity provider.
3. The identity provider validates the logout request.
4. The identity provider sends a logout request for the user to all other service providers that the identity provider is aware of that the user has an active security session with.
5. The identity provider terminates the user's sessions and sends a response to the original service provider.
6. The original service provider informs the user that they have been logged out.

If the logout URL is displayed in the Service Provider settings, the following steps terminate the active user session:

1. The end user initiates a logout request at a service provider.
2. The service provider terminates any of the user's active sessions that are handled by a third-party service.
3. The service provider forwards the logout request to the logout URL.

If the logout URL is not configured for either for identity provider or the service provider, when a user requests a logout, the service provider terminates the user's active session and displays the login page (for the BlackBerry AtHoc management system) or the sign out page (for Self Service.)

The following table describes the log out flows for the BlackBerry AtHoc management system:

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out or session timeout	SP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to their organization's SSO login URL. The IDP logout URL is used.
Sign out or session timeout	SP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to their organization's SSO login URL. The IDP logout URL is used.
Sign out or session timeout	SP	No	Yes	The end user is signed off locally and redirected to the custom logout URL.

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out or session timeout	SP	No	No	The end user is signed off locally and redirected to the organization's SSO login URL.
Session timeout	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Session timeout	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Sign out or session timeout	IDP	No	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the custom logout URL.
Session timeout	IDP	No	No	The end user is signed off locally and redirected to the manual login page with a Session Timeout message.
Sign out	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page.

Log out type	Initiator	IDP logout URL included	Custom logout URL available	Log out behavior
Sign out	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the manual login page.
Sign out	IDP	No	No	The end user is signed off locally and redirected to the manual login page.

The following table describes the log out flows for Self Service:

Log out type	Initiator	IDP logout URL included	Custom logout URL included	Log out behavior
Sign out or session timeout	SP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page.
Sign out or session timeout	SP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page.
Sign out or session timeout	SP	No	Yes	The end user is signed off locally and redirected to the custom URL.
Sign out or session timeout	SP	No	No	The end user is signed off locally and redirected to the sign out page.

Log out type	Initiator	IDP logout URL included	Custom logout URL included	Log out behavior
Sign out or session timeout	IDP	Yes	Yes	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page. The **Go To Login** button is not visible.
Sign out or session timeout	IDP	Yes	No	The IDP session is terminated. The end user is signed off locally and redirected to the sign out page. The **Go To Login** button is not visible.
Sign out or session timeout	IDP	No	Yes	The end user is signed off locally and redirected to the custom URL.
Sign out or session timeout	IDP	No	No	The end user is signed off locally and redirected to the sign out page.

Export SP and IDP settings

When you configure single sign-on, you can export settings data from the IDP and SP instead of manually entering this information.

1. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, in the **General Settings** section, click **Export**. The IDP settings are downloaded to an .xml file. Browse to select a location on your local computer to save the file.
2. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Service Provider**, section, in the **General Settings** section, click **Export**

   Note: Password and private key information is excluded from Service Provider metadata exports.

   The SP settings are downloaded to an .xml file. Browse to select a location on your local computer to save the file.
3. Click **Save**.

Import IDP settings

When configuring SSO, you can export and then import settings data from the IDP instead of manually entering this information.

1. On the **Management System SSO configuration** or **Self Service SSO configuration** window, in the **Identity Provider** section, in the **General Settings** section, click **Import**.
2. On the **Import Identity Provider Configuration** window, click **Browse** to select the .xml file that contains your IDP configuration.
3. Click **Open**.
4. Click **Import**. The fields in the Identity Provider section are populated with the data from the imported .xml file. If any fields were filled in before the import, they are over-written. If the .xml file contains any invalid fields, an error is displayed and no settings are imported.
5. Click **Apply**.

Import an existing IDP configuration

If you have an existing database-driven implementation of SSO and want to migrate to the improved user-interface based SSO solution, you can migrate the settings configuration from your IDP and import it into the BlackBerry AtHoc management system.

Contact your account representative or BlackBerry AtHoc customer support to obtain a copy of the `Utilities.zip` file needed to perform an SSO migration.

Note: Only IDP configurations can be imported. The SP configuration must be entered manually in the BlackBerry AtHoc management system. See Configure Service Provider settings.

1. Open a Windows command prompt and navigate to the following folder:

   ```
   <installed-directory>\AtHocENS\ServerObjects\Tools\SSO\EasyConnect
   ```

2. Run the following command to create and export a SAML metadata XML file:

   ```
   ExportMetadata.exe –partner <name> [-config <directoryName] [-baseurl <url>] [-file <filename>]
   ```

   where:

   - partner <*name* >: The name of the partner IDP configured in the `idp-partner.config` file or the partner SP configured in the `sp-partner.config` file.
     - If you specify a partner IDP, the corresponding local SP metadata is generated for the partner IDP.
     - If you specify a partner SP, the corresponding local IDP metadata is generated for the partner SP.
   - [-baseurl <*url*>]: Specify the directory that contains the EasyConnect configuration files. If you do not specify this directory, the export defaults to C:\EasyConnect\EasyConnectServer.
   - [-file <*filename* >]: Optionally, specify the name of the generated SAML metadata file. By default, the export uses the file name metadata.xml. Examples:

   Examples:

   - ExportMetadata.exe –partner ExampleIdentityProvider
   - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory"**
   - ExportMetadata.exe –partner ExampleIdentityProvider -config "specify SSO config directory" - baseurl "HTTPS://www.showcase.com"*
   - ExportMetadata.exe –partner ExampleIdentityProvider config "specify SSO config directory" - baseurl "HTTPS://www.showcase.com" -file "<File path>"**

3. Log in to the BlackBerry AtHoc management system and use the SSO IDP import feature to import the IDP metadata. See Export SP and IDP settings and Import IDP settings.

Enable SSO certificate revocation list checking

When single sign-on is enabled for your organization, a CRL is maintained. A CRL is a list of digital certificates that have been revoked and should not be trusted. If CRL checking is enabled, BlackBerry AtHoc checks the CRL before initiating a SAML authentication request to an identity provider or after receiving an SAML response from the IDP.

1. In the navigation bar, click .
2. In the **System Setup** section, click **Security Policy**.
3. In the **SSO CRL (Certificate Revocation List) Settings** section, select the **Enable CRL Checking** option.

   Note: If the **SSO CRL (Certificate Revocation List) Settings** section is not visible, single sign-on is not enabled. See Enable single sign-on for Self Service and Enable single sign-on for the BlackBerry AtHoc management system.
4. In the **CRL Timeout Interval** field, enter the number of seconds to allow for certificate validation information to be retrieved from the CA. The minimum is 1 and the maximum is 60 seconds. The default is 20 seconds.
5. Optionally, select the **Ignore Verification Errors** option. If this option is selected, a certificate that fails verification will continue to be used and an error is logged. If this option is not selected, any certificate that fails verification is not used.
6. Click **Save**.

BlackBerry AtHoc Customer Support Portal

BlackBerry AtHoc customers can obtain more information about BlackBerry AtHoc products or get answers to questions about their BlackBerry AtHoc systems through the Customer Support Portal:

https://support.athoc.com

The BlackBerry AtHoc Customer Support Portal also provides support via computer-based training, operator checklists, best practice resources, reference manuals, and user guides.

Legal notice

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
Ground Floor, The Pearce Building, West Street,
Maidenhead, Berkshire SL6 1RL
United Kingdom

Published in Canada