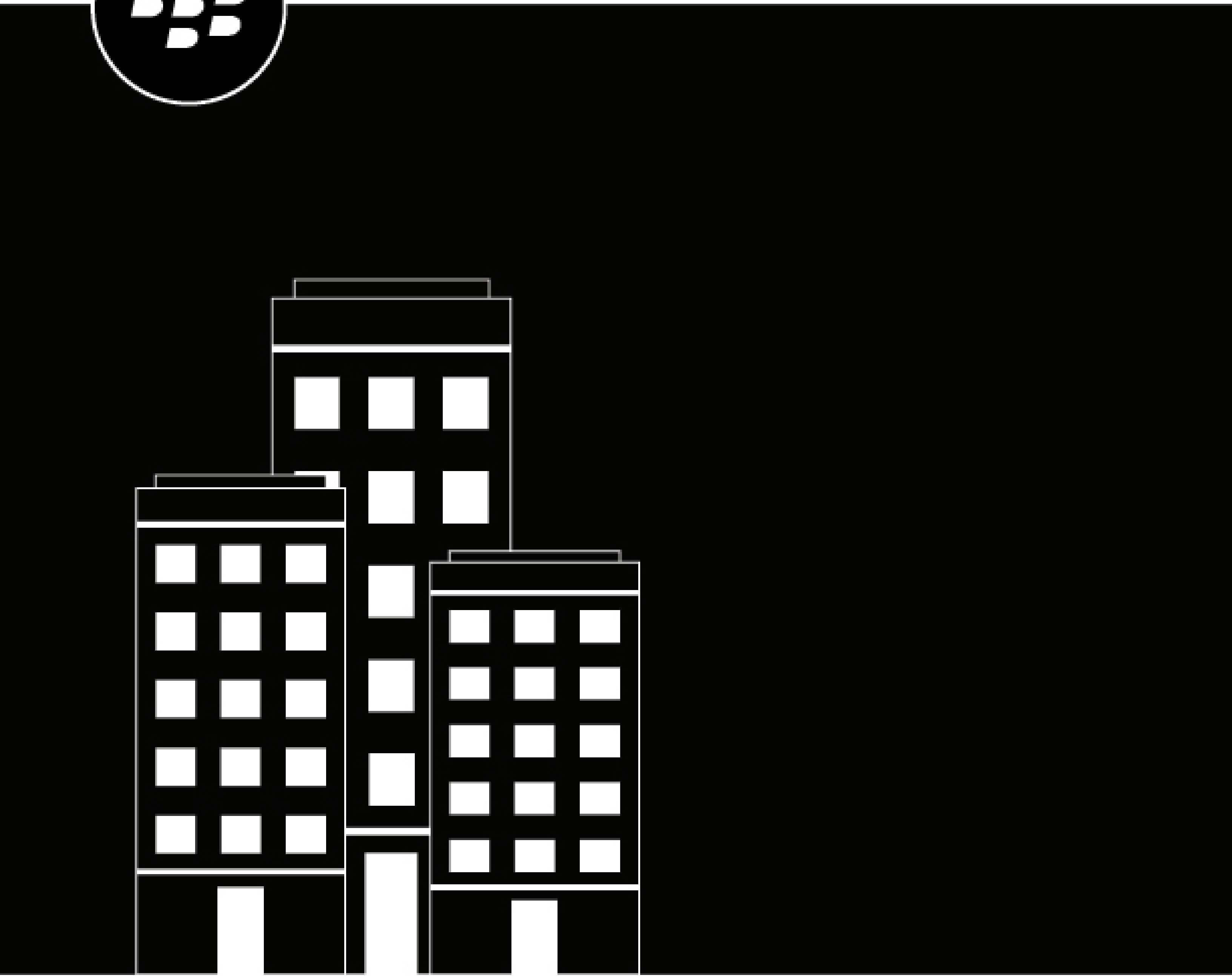

BlackBerry Enterprise Identity

Administration Guide

Contents

What is BlackBerry Enterprise Identity?

BlackBerry Enterprise Identity provides authentication to some BlackBerry web apps such as the BlackBerry UEM Cloud management console and CylancePERSONA Mobile. BlackBerry Enterprise Identity also provides single sign-on (SSO) to cloud services such as Microsoft 365, Google Workspace, 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, or Android devices and other computing platforms.

Enterprise Identity is bundled with BlackBerry UEM, and BlackBerry UEM Cloud. Administrators use the BlackBerry UEM, or BlackBerry UEM Cloud 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.

The following browsers are supported for administration: Internet Explorer 11, Google Chrome, Mozilla Firefox, and Safari. Client use is supported on all the browsers above as well as native browsers on devices running iOS and Android.

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 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).

Using Enterprise Identity for the first time

BlackBerry UEM, and BlackBerry UEM Cloud contain the BlackBerry Enterprise Identity software. In BlackBerry UEM version 12.7 MR1 and later, you do not need to enable Enterprise Identity. If your organization has the appropriate licensing, Enterprise Identity is automatically enabled.

Understanding services, entitlements, and groups

Services are applications, often located in the cloud, that users need to access. For example, Microsoft 365, BlackBerry Workspaces, or WebEx. By configuring a service in BlackBerry UEM, BlackBerry UEM Cloud, or BlackBerry Enterprise Identity, you set up a secure interface between Enterprise Identity and your instance, or tenant, of that service. After you use BlackBerry UEM or BlackBerry UEM Cloud to add a service, you use the BlackBerry UEM management console to manage the service and deploy entitlements for the service to users.

The most efficient way to entitle users is with app groups. An app group can bind together both the SSO entitlement for a service and the client applications needed on devices to interact with the service. You can assign app groups to users or user groups, giving them everything they need to access the service.

User groups give administrators flexibility to entitle large numbers of users at the same time instead of maintaining the entitlement manually as users are added or removed from the group. When a user is added to the group, the entitlement is assigned to them automatically, allowing them to sign into the service from any device using the same credentials. If a user is removed from the group, they automatically lose access to that service. Service entitlements can also be assigned to individual users if required.

Term	Description
Service	Services include Workspaces, Box, Workday, WebEx, Salesforce and others, including custom services.
Entitlement	An entitlement is a service assignment made using BlackBerry UEM that tells Enterprise Identity to provide single sign-on access to a service for a given user or group.
App group	An app group is a collection of apps that can include the single sign-on entitlement and the associated binaries for mobile devices.
User	A user is a BlackBerry UEM user.
User group	A user group is a collection of BlackBerry UEM users.

Managing services

If you are using BlackBerry UEM 12.7 or later or BlackBerry UEM Cloud, use the BlackBerry UEM management console to manage your organization’s services.

Managing services in the BlackBerry UEM management console

Before you can configure SaaS or other services in the BlackBerry UEM management console, your system administrator must add the service. For more information, see the Integrating SaaS Services content.

After your organization purchases the correct licenses for BlackBerry Enterprise Identity (for more information, see the BlackBerry UEM Licensing Guide), you can use the BlackBerry UEM console to manage the services and the features of those services. Adding services requires setting security and other parameters specific to your organization.

After you add a service, in the BlackBerry UEM management console you can entitle users to use the service on a per user or basis or through a group. You can change the configuration of the service in the BlackBerry UEM management console.

View a list of service templates in the BlackBerry UEM console

1. In the BlackBerry UEM management console, on the menu bar click **Settings**.
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click +.

The list of available service templates displays.

View a list of the custom services that you have created in the BlackBerry UEM console

1. In the BlackBerry UEM management console, on the menu bar click **Settings**.
2. Click **BlackBerry Enterprise Identity** > **Services**.

The list of custom services display.

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	Description
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.
SAML claim attributes	• Name - Enter a name for your SAML claim • SAML attribute - Enter your SAML attribute • SAML claim type • 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 • Directory - if you choose Directory, you can type the name of an Active Directory attribute. Values that match the text that you type are suggested automatically. • 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. • Optionally, if you want the attribute to be required, select the **Required** checkbox.

6. Click **Save**.

Add an AD FS Claims Provider service

If your organization has apps that use Active Directory Federation Services (AD FS) forms-based authentication, you can add an AD FS Claims Provider service so that Enterprise Identity can authenticate the AD FS apps using the forms authentication type.

Enterprise Identity supports AD FS 2019 and later

Before you begin:

- Verify that the AD FS role has been added to the Active Directory server.
- Verify that UEM is connected to the Active Directory server that has the AD FS role.

1. In the UEMmanagement console, click **Settings** > **BlackBerry Enterprise Identity** > **Services**.
2. In the **SAML Services** table, click +.
3. Click **ADFS Claims Provider**.
4. If you want to enable ZSO for users, select the **Allow Mobile ZSO when specified by authentication policy** and **Allow Kerberos Desktop ZSO when specified by authentication policy** check boxes.
5. Type a name and description for the service.
6. In the **Service provider entity ID** field, enter `http://<adfs_host>/adfs/services/trust`, where *adfs_endpoint* is the name of the Active Directory server that has the ADFS role.
7. In the **Assertion consumer service POST URL** field, enter `http://<adfs_host>/adfs/services/ls`, where *adfs_endpoint* is the name of the Active Directory server that has the ADFS role.
8. In the **Single logout service URL** field, enter `http://<adfs_host>/adfs/services/ls`, where *adfs_endpoint* is the name of the Active Directory server that has the ADFS role.
9. Click **Save**.

After you finish: Assign the service to users.

Configure the Claims Provider in AD FS

Before you begin: Configure the Claims Provider in AD FS

1. In the UEM management console, click **Settings** > **BlackBerry Enterprise Identity** > **Services**.
2. In the **SAML Services** table, click the AD FS Claims Provider service.
3. In the **SAML service metadata** section, click the link to download the SAML service metadata. Copy the file to the Windows server that runs AD FS.
4. Open the AD FS manager.
5. In the left pane, click **Claims Provider Trusts**.
6. In the right pane, click **Add Claims Provider**.
7. In the **Claims Provider Trusts Wizard**, click **Start** > **Next**.
8. Select **Import data about the claims provider from file** and open the metadata file that you downloaded in step 3. Click **Next**.
9. Enter a name and description for the Claims Provider Trust. Click **Next** until the Save button appears.
10. Click **Save**.

If you want to test your ADFS configuraton, you can create a test app using Claims X-Ray. For more information, see https://adfshelp.microsoft.com/ClaimsXray/TokenRequest

Use Enterprise Identity as the default claims provider

To use Enterprise Identity as the default claims provider, you can run the following command in Windows PowerShell. When Enterprise Identity is the default claims provider, users are not prompted to authenticate when they access a service.

In Windows PowerShell, run the following command:

```
Set-AdfsRelyingPartyTrust -TargetName <relying_party_name> -ClaimsProviderName
 @("<claims_provider_display_name>")
```

Example: Configure claims mapping for Office 365

The following steps provide an example of how to configure basic claims mapping for Microsoft 365. Your organization may have different claims mapping requirements.

Before you begin: Use Enterprise Identity as the default claims provider.

1. In the AD FS manager, click **Edit Claim Rules** for the Enterprise Identity claims provider that you have configured.
2. Click **Add rule** > **Send claims using a custom role**.
3. In the **Select Rule** template window, in the **Claim Rule Template** drop-down list, select **Send Claims Using a Custom Rule**. Click **Next**.
4. In the **Configure Rule** window, in the **Claim rule name** field, type `Pass all claims`.
5. In the **Custom rule** pane, enter the following:

   ```
   c:[]
                => issue(claim = c);
   ```
6. Click **Finish**.
7. In the **Configure Rule** window, in the **Claim rule name** field, type `Transform UPN`.
8. In the **Custom rule** pane, enter the following:

   ```
   c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
    => issue(Type = "http://schemas.xmlsoap.org/claims/UPN", Issuer =
    c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = regexreplace(c.Value,
    "^(?<user>.*)$", "${user}<domain_suffix_for_your_users>"), ValueType =
    c.ValueType);
   ```

   Where the domain suffix is the email domain for users (for example "${user}@example.com").
9. Click **Finish**.
10. In the UEM management console, click to **Settings** > **BlackBerry Enterprise Identity** > **Services**.
11. In the **SAML Service** table, click the ADFS service that you created.
12. Under **Claims**, in the **Name identifier attribute** drop-down list, select **Immutable ID**.
13. In the SAML claim attributes table, click +. Do the following:
    a) In the Name field, type `Username`.
    b) Under SAML attribute, select http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name.
    c) Set the SAML claim type to Local.
    d) Set the attribute value to the name that you entered for the claim attribute (for example, Username).
    e) Set the attribute value to anyType.
    f) Click **Save**.

14. In the SAML claim attributes table, click +. Do the following:
    a) In the Name field, type `UPN`.
    b) Under SAML attribute, select http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn.
    c) Set the SAML claim type to Local.
    d) Set the attribute value to the name that you entered for the claim attribute (for example, UPN).
    e) Set the attribute value to anyType.
    f) Click **Save**.
15. In the SAML claim attributes table, click +. Do the following:
    a) In the Name field, type `ImmutableID`.
    b) Under SAML attribute, select http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID.
    c) Set the SAML claim type to Local.
    d) Set the attribute value to the name that you entered for the claim attribute (for example, ImmutableID).
    e) Set the attribute value to anyType.
16. Click **Save**.

Add a custom service in the BlackBerry UEM console

BlackBerry provides a growing selection of predefined service templates. As an administrator, you may also want to add custom services to BlackBerry Enterprise Identity. Most services that use the SAML 2.0 protocols can be integrated. SAML services that you integrate may be customized and specific to your organization, or you might choose to integrate a service from a SaaS provider that is in broader use.

When a service is enabled, users that you entitle can use the service. When a service is disabled, all entitled users lose access until it is enabled again.

For detailed information about the available service templates, see Integrating SaaS services.

1. In the BlackBerry UEM management console, on the menu bar click **Settings**.
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click +.
4. Select **Custom Service**.
5. Complete the fields to configure the custom service.
    - When you add a SAML claim, if you choose a Local claim, you then 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.
    - When you add a SAML claim, if you choose a Static claim, you have to type an option in the Attribute value field.
6. Click **Save**.

Change an active service in the BlackBerry UEM console

1. In the BlackBerry UEM management console, on the menu bar, click **Settings**.
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click the service that you want to change.
4. To change the service configuration for an editable service or feature, in the **Service Configuration** section, complete the fields. Some services might not allow edits.
5. Click **Save**.

Remove a service in the BlackBerry UEM console

Before you remove a service, you must remove all user entitlements from that service in the BlackBerry UEM management console.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings.**
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click the X beside the service that you want to delete.
4. Click **Remove.**

View SAML configuration settings in the BlackBerry UEM console

1. In the BlackBerry UEM management console, on the menu bar, click **Settings.**
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click the SaaS service configuration to view the SAML settings.

Export SAML service metadata in the BlackBerry UEM console

You might need the SAML service metadata to set up the secure interface between BlackBerry Enterprise Identity and your instance, or tenant, of the service that you are configuring (for example, Box).

1. In the BlackBerry UEM management console, on the menu bar, click **Settings.**
2. Click **BlackBerry Enterprise Identity > Services**.
3. Click the SaaS service configuration to view the SAML metadata header.
4. Click the hyperlink to download the XML file.

Add an OpenID Connect app

You can add OpenID Connect apps that have been made a available to your organization or UEM tenant. OpenID Connect apps are made available by an administrator or the app developer.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings**.
2. Click **BlackBerry Enterprise Identity** > **Services**.
3. In the **OpenID Connect apps** table, click +.

   A list of the OpenID Connect apps that are available is displayed.
4. Select an app.
5. In the **Add a BlackBerry Enterprise Identity service** screen, do any of the following:
   - Select **Allow Mobile ZSO when specified by an authentication policy**
   - Select **Allow Kerberos Desktop ZSO when specified by authentication policy**
6. Review the scopes for the app. Click **Save**.

To edit the app, click the app name in the OpenID Connect apps table.

Update consent for an OpenID Connect app

If the required scopes for an OpenID Connect app change, you must update consent for the app. When the required scopes change, a notification is displayed in the OpenID Connect section of the BlackBerry Enterprise Identity Services page.

1. In the BlackBerry UEM management console, on the menu bar, click **Settings**.
2. Click **BlackBerry Enterprise Identity** > **Services**.
3. In the **OpenID Connect** apps table, in the **Consent required** section, click the notification for an app.
4. In the **Update app** dialog box, review the scopes or clients that were added or removed. Click **Save**.

Remove an OpenID Connect app

1. In the BlackBerry UEM management console, on the menu bar, click **Settings**.
2. Click **BlackBerry Enterprise Identity** > **Services**.
3. In the **OpenID Connect apps** table, click ✕ beside the app that you want to remove.
4. In the **Remove consent** dialog box, click **Remove**.

Log in to the BlackBerry Enterprise Identity console

You might need to log in to the BlackBerry Enterprise Identity console to perform some tasks such as looking at system logs.

Before you begin: Enable pop-ups in your browser.

1. In the BlackBerry UEM management console, on the menu bar, click **Apps**.
2. Click **Add an app**.
3. Click **Enterprise Identity**.
4. Click **Open Enterprise Identity console**. The administrator console opens in a new browser tab. If the console does not open, ensure that you have enabled pop-ups in your browser.
5. When you are done, close the browser tab.

Managing authentication levels

Three authentication types are available in Enterprise Identity. The ranking of these authenticators can be changed in the BlackBerry UEM console, on the **Settings** page. For more information on ranking, see Change Enterprise Identity settings.

Authenticator type	Description
Enterprise password	This security method requires a password before users can access a service. It is the default method. The password is one currently associated with a user account in Active Directory, an LDAP directory, or BlackBerry UEM.
Enterprise password and BlackBerry 2FA	This security method leverages BlackBerry 2FA and requires both a password and an acknowledgment on a user's mobile device before they can access a service.
Mobile ZSO	This security method, available on mobile devices, allows a user to access a service without having to explicitly authenticate. Instead, it leverages the user's authentication with the device or secure container as proof of identity.
Ping password	This security method, available to PingFederate users, requires users to enter their Ping Identity password before they can access a service. For additional security, you can also require users to acknowledge a prompt, or enter their PingID.

You can assign these authentication levels to the user or group for each service by defining an authentication policy. For more information on policies, see Managing authentication policies.

Enable two-factor authentication

Enabling two-factor authentication means enabling BlackBerry 2FA, deciding its authenticator ranking, and assigning an authentication policy that requires its authentication level.

Before you begin:

- Enable BlackBerry 2FA in BlackBerry UEM and apply the BlackBerry 2FA profile to the user or group.
- Ensure any users that need to use BlackBerry 2FA have their mobile devices and that they are activated. For more information about activating devices, see the BlackBerry 2FA content.

1. Assign BlackBerry 2FA to an authentication level. For more information, see Managing authentication levels.
2. Configure an authentication policy that specifies BlackBerry 2FA as the authentication level to be used by a particular group of users or specific service. For more information, see Managing authentication policies.

Enabling Mobile ZSO

When you enable Mobile Zero Sign-On (Mobile ZSO), you enable it for the services you want to use it, specify its authenticator ranking, and assign an authentication policy that requires its authentication level.

Turning on Mobile ZSO for a service makes it possible for that service to authenticate with the certificate on a user's managed device without using a username and password.

Enable Mobile ZSO in BlackBerry UEM

Before you begin:

- Users must have an Android Enterprise activated device, a Samsung Knox device, or an iOS device enrolled with UEM.
- Users must have BlackBerry Secure Connect Plus on their devices.

1. Log in to BlackBerry UEM as an administrator.
2. On the menu bar, click **Settings > BlackBerry Enterprise Identity > Services.**
3. Click the service that you want to enable Mobile ZSO for.
4. Select the **Allow Mobile ZSO when specified by authentication policy** option.
5. Click **Save**.
6. Assign Mobile ZSO to an authentication level. For more information, see Managing authentication levels.
7. Configure an authentication policy that specifies Mobile ZSO as the authentication level to be used by a particular group of users or specific service. For more information, see Managing authentication policies.

Turning on Mobile Zero Sign-On (Mobile ZSO) for a service allows that service to authenticate using Mobile ZSO. The overall authentication policy assigned in BlackBerry UEM must permit Mobile ZSO.

If you set up a service for Mobile ZSO without a fallback authenticator, it will only be accessible from managed mobile devices. However, if a password fallback authenticator is configured, Mobile ZSO will be used on managed mobile devices, and the user will be permitted to use the password on other devices.

Managing risk factors

Risk factors are optional features in authentication policies that provide a way to balance the level of authentication based on risk. When a user is in a trusted browser or network, they can experience easier access to the services they need, but you can apply a more stringent authentication policy in other circumstances.

Risk factor	Description
Browser detection	This risk factor asks users to establish a reference of trust between the browser and Enterprise Identity the first time that they open a browser. After the trust is established, subsequent logins can use a simpler authentication level. Users can view and remove trusted browser entries in BlackBerry UEM Self-Service.
Network detection	This risk factor assesses whether a user's app or browser is connected to the same network as the BlackBerry UEM server. If it's not, a higher authentication level can be applied. This risk factor can allow users to sign in more easily to certain services when they are on the work network. For more information about configuring this risk factor, see Configure the network detection risk factor. If you want to disable network detection globally, you can log in to the Enterprise Identity console and turn off Work Network Detection in the UEM tenants list. **Note:** You can't enable the network detection risk factor in BlackBerry UEM Cloud.

Configure the network detection risk factor

Before you begin: You cannot enable the network detection risk factor in BlackBerry UEM Cloud.

1. In the BlackBerry UEM management console, click **Settings > BlackBerry Enterprise Identity > Settings.**
2. Enter the work network host name of the BlackBerry UEM server that your work computers and devices use. Alternatively, enter the DNS pool name that resolves to multiple BlackBerry UEM server IP addresses.
3. Confirm that your work computers and devices can connect to the host name via the port number listed. The risk factor will not work if the port is blocked by a firewall.
4. Click **Save**.
5. Click **Settings** > **Infrastructure** > **Server certificates** > **SSL certificate for BlackBerry Web Services**.

   The work computer browsers and devices must trust the certificate when they connect to the work network host name, and the default certificate is self-signed and untrusted. You can upload a trusted BlackBerry Web Services certificate in BlackBerry UEM.

After you finish: An externally trusted certificate might be required by some web browsers. If it is, a new BlackBerry Web Services certificate can be uploaded in BlackBerry UEM. Click **Settings** > **Infrastructure** > **Server certificates** > **SSL certificate for BlackBerry Web Services**.

After you finish: When you create or edit an Enterprise Identity authentication policy, click the **Network detection** checkbox to add the risk factor. For more information about creating authentication policies, see Create an Enterprise Identity authentication policy.

Managing authentication policies

You use the BlackBerry UEM management console to create, manage, and rank authentication policies. Policies can be overridden on a per-service basis. For general information on polices and profiles, see IT policies in the BlackBerry UEM administration content.

Create an Enterprise Identity authentication policy

Complete the following task to create an Enterprise Identity policy for user groups.

1. In the BlackBerry UEM console, on the menu bar, click **Policies and Profiles** > **BlackBerry Enterprise Identity**.
2. Click the + beside **Authentication policies**.
3. Enter a name and description for the profile.
4. In the **Minimum authentication level** drop-down list, specify an authentication level. For more information, see Managing authentication levels.
5. In the **Risk scenarios** table, click +.
6. Enter a name, and description.
7. In the **Minimum authentication level** drop-down list, select the desired authentication level that you want to be applied when the risk factors are met.
8. In the **Risk factor combination** list, choose one of the following options:
    - If you want to apply all selected risk factors to the scenario, select **All selected factors are present**
    - If you want to have any of the selected risk factors apply to the scenario, select **Any of the selected factors is present**
9. If you want to assess whether a user's app or browser is connected to the same network as the BlackBerry UEM server, select the **Network detection** option, and in the **Configuration** drop-down list, select the desired option. Note that you cannot enable the network detection risk factor in BlackBerry UEM Cloud.
10. If you want to establish a reference of trust between the browser and Enterprise Identity the first time that they open a browser, select the **Browser detection** option, and in the **Configuration** drop-down list, select the desired option.
11. If you want to use CylancePERSONA Mobile risk levels and geozones as risk factors, choose the **BlackBerry Persona** option and select from the following options:
    - **Behavioral risk level**: CylancePERSONA cloud services in the BlackBerry Infrastructure gather and process app data and use it to calculate a risk level for each user.
    - **Admin-defined geozone**: Choose a geozone that your organization's BlackBerry UEM administrator created.

      Note: For more information about risk levels and geozones, refer to the CylancePERSONA Mobile content.
    - **Geozone risk level**: Choose from High, Medium, or Low. This setting specifies a level of risk that can be attributed to a user by comparing the user's physical location to the region contained within an Admin-defined geozone or a learned geozone.
12. Click **Save**.
13. If you want to create an exception for any of your organization's services, click **Manage service exceptions**, select the service from the list, and set up any necessary risk scenarios for the service.
14. If necessary, repeat steps 5 to 11 to add additional risk scenarios. Note that each risk scenario must use a unique set of risk factors.
15. Click **Save**.

Assign an Enterprise Identity policy to a user group

Before you begin: Create an Enterprise Identity authentication policy.

1. In the BlackBerry UEM management console, on the menu bar, click **Groups** > **User**.
2. Either create a new group or click the name of the group you want to edit.
3. Click the **BlackBerry Enterprise Identity** tab.
4. Click **+**.
5. Choose an authentication policy from the drop-down.
6. Click **Assign**.

Delete an Enterprise Identity policy

Before you begin: Create an Enterprise Identity authentication policy.

1. In the BlackBerry UEM management console, on the menu bar, click **Policies and profiles** > **BlackBerry Enterprise Identity**.
2. Click the name of the profile that you want to delete.
3. Click 🗑.
4. Click **OK**.

Using authenticator level ranking and authentication policies to manage security

You can use authenticator level ranking and BlackBerry Enterprise Identity authentication policies to specify the types of authentication that users must perform when the sign in to a service. The authenticator rankings are security methods that define what type of user authentication is required on service log in. You use risk scenarios and risk factors in authentication policies to specify the settings that apply to users and groups when they access Enterprise Identity services.

Requiring additional authentication when users are connected to an external network

Complete the following tasks to require users to enter their password and respond a BlackBerry 2FA prompt when they try to connect to a service using an external network. You can also allow users to authenticate using only their password from any network. **Note:** You can't enable the network detection risk factor in BlackBerry UEM Cloud.

Set authenticator ranking

1. On the menu bar, click **Settings > BlackBerry Enterprise Identity > Settings**.
2. In the **Authenticator level ranking** section, set **Enterprise password** to Level 1 and **Enterprise password + BlackBerry 2FA** to Level 3. For more information about setting up BlackBerry 2FA, see Enable two-factor authentication.
3. Click **Save**.

Add an authentication policy for external networks

1. On the menu bar, click **Policies and profiles**. Click **BlackBerry Enterprise Identity** below Managed devices.
2. In the **Authentication policies** pane, click **Add a policy**.
3. Enter a name and description for the authentication policy.
4. In the **Minimum authentication level** drop-down list, select Level 1.

   This level corresponds to the Enterprise password authenticator ranking that you set in the previous task. If you save this policy without adding a risk scenario and assign it to users, they will be required to enter only their enterprise password when they log into a service. If you want to require additional authentication based on the type of network that they are connected to, complete the following steps to add a risk scenario.
5. In the **Risk scenarios** table, click +.
6. Enter a name and description for the scenario.
7. In the **Minimum authentication level** drop-down list, select Level 3. This level corresponds to the Enterprise password + BlackBerry 2FA authenticator ranking that you set in the previous task.
8. Click **Network detection**.
9. In the **Configuration** drop-down list, select **Not on a work network**.

   If you configure this option, when one of your organization’s users is not on a work network and they try to log into a service, they will be required to enter their enterprise password and respond to a BlackBerry 2FA prompt on their device.
10. Click **Save**.
11. Click **Save**.

After you finish: Assign the authentication policy to users or groups.

Requiring additional authentication when users use a browser for the first time

Complete the following tasks to require your users to enter their password and respond to a BlackBerry 2FA prompt when they try to connect to a service using a browser for the first time. After the trust is established, subsequent logins can use a simpler authentication level.

Set authenticator ranking

1. On the menu bar, click **Settings > BlackBerry Enterprise Identity > Settings**.
2. In the **Authenticator level ranking** section, set **Enterprise password** to Level 1 and **Enterprise password + BlackBerry 2FA** to Level 3. For more information about setting up BlackBerry 2FA, see Enable two-factor authentication.
3. Click **Save**.

Add an authentication policy for the first time users use a browser

1. On the menu bar, click **Policies and profiles**. Click **BlackBerry Enterprise Identity** below Managed devices.
2. In the **Authentication policies** pane, click **Add a policy**.
3. Enter a name and description for the authentication policy.
4. In the **Minimum authentication level** drop-down list, select Level 1.

   This level corresponds to the Enterprise password authenticator ranking that you set in the previous task. If you save this policy without adding a risk scenario and assign it to users, they will be required to enter only their enterprise password when they log into a service. If you want to require additional authentication if they are using the browser for the first time, complete the following steps to add a risk scenario.
5. In the **Risk scenarios** table, click +.
6. Enter a nameand description for the scenario.
7. In the **Minimum authentication leve**l drop-down list, select Level 3. This level corresponds to the Enterprise password + BlackBerry 2FA authenticator ranking that you set in the previous task.
8. Click **Network detection**.
9. In the **Configuration** drop-down list, select **Browser detected for the first time**.

   If you configure this option, when one of your organization's users is using a browser for the first time and they try to log into a service, they will be required to enter their enterprise password and respond to a BlackBerry 2FA prompt on their device.
10. Click **Save**.
11. Click **Save**.

After you finish:

- Assign the authentication policy to users or groups.

Allowing users to authenticate with PingFederate

BlackBerry Enterprise Identity can redirect user authentication to PingFederate, which provides existing Ping Identity users with a familiar user interface. You can also use BlackBerry Enterprise Identity or BlackBerry

Intelligent Security policies to allow Ping Identity's authentication to adapt to both risk and context, including extension by PingID, or BlackBerry 2FA multifactor authentication.

Before BlackBerry Enterprise Identity and PingFederate can communicate, you must create a Ping Identity client on your organization's PingFederate server, and a corresponding identity provider in BlackBerry UEM.

Before you create a Ping Identity client, ensure that your organization's PingFederate authentication policy has the OBJECTGUID attribute set to Hex. For more information, refer to the documentation from Ping Identity.

Note: You must have the latest version of BlackBerry UEM 12.11 installed in your environment.

Create a Ping Identity client on a PingFederate server

Before your BlackBerry Enterprise Identity users can authenticate with PingFederate, you must set up a Ping Identity client on your organization's PingFederate server.

1. Log in to the PingFederate administration console.
2. Click **OAuth Server**.
3. Under the Clients column, click **Create New**.
4. In the **Client ID** field, type a unique ID for the client. Note that you will use this same ID when you set up the Identity provider in BlackBerry UEM.
5. Type a name and description for the client.
6. In the Client Authentication section, click **Private Key JWT**.
7. Select the **Require Signed Requests** option.
8. To generate a JSON Web Key Set, go to https://mkjwk.org/.
9. Click the **Elliptic curve** tab.
10. In the **Curve** drop-down list, select **P-256**.
11. In the **Algorithm** drop-down list, select **ES256**.
12. Click **New Key**.
13. Copy the key from the **Keypair set** field. Note that you will use this same key in the Configure an Identity provider in BlackBerry UEM task.
14. Paste the key into the **JWKS** field in the PingFederate site.
15. In the **Redirect URI** field, add the URI of your organization's PingFederate server, and click **Add**.
16. In the **Allowed grants** section, select the **Authorization Code** option.
17. In the **ID Token Signing Algorithm** drop-down list, select any of the **ECDSA** options. Note that you use same option in the Configure an Identity provider in BlackBerry UEM task.
18. Click **Save**.

After you finish: Configure an Identity provider in BlackBerry UEM

Configure an identity provider in BlackBerry UEM

After you create a Ping Identity client, you must create a corresponding identity provider in the BlackBerry UEM management console.

Before you begin: Create a Ping Identity client on a PingFederate server

1. In the BlackBerry UEM management console click **Settings > BlackBerry Enterprise Identity > Identity providers**.
2. Click **+** and select **PingFederate**.
3. In the **Name** field, type a name for the identity provider.
4. In the **OIDC discovery document URL** field, type the location of your organization's PingFederate server.

5. In the **Client ID** field, enter the same ID that you used in the Create a Ping Identity client on a PingFederate server topic.
6. In the **Private key JWKS** field, enter the same key that you used in the Create a Ping Identity client on a PingFederate server topic.
7. In the **ID token signing algorithm** drop-down list, select the same option that you selected in the Create a Ping Identity client on a PingFederate server topic.
8. In the **Available services** list, select the services that you want to assign to the Ping Identity client and click the right arrow to move the service to the **Selected service** list. Note that you can assign only one Ping Identity client for each service.
9. Click **Save**.

Create a BlackBerry Enterprise Identity policy for PingFederate users

1. In the BlackBerry UEM console, on the menu bar, click **Policies and Profiles > BlackBerry Enterprise Identity > Add a policy**.
2. Enter a name and description for the policy.
3. In the **Minimum authenticator** level drop-down, select the number that corresponds to the authentication level for one of the Authentication levels for Ping Identity on the **Settings > BlackBerry Enterprise Identity > Settings** screen. You can choose a level that corresponds to the following options: Ping password, Ping password + BlackBerry 2FA, or Ping password + PingID.
4. Optionally, you can add a Risk scenario which provides additional security if certain conditions exist, such as if a user is not on an internal network. In the **Risk scenarios** table, click **+**.
5. Enter a name and description for the risk scenario.
6. Select a Minimum authentication level that corresponds to one of the Authenticator levels for Ping on the Settings > BlackBerry Enterprise Identity > Settings screen. You can choose to allow your users to enter only their password or respond to a BlackBerry 2FA prompt or enter their PingID if any of the risk factors are present when the user logs into the service. Choose from the following Risk factors:
    - **Network detection**: If you want to assess whether a user's app or browser is connected to the same network as BlackBerry UEM, select the Network detection option, and in the Configuration drop-down list, select the desired option.
    - **Browser detection**: If you want to establish a reference of trust between the browser and Enterprise Identity the first time that the user opens a browser, select the Browser detection option, and in the Configuration drop-down list, select the desired option.
    - **BlackBerry Persona**: If you want to use CylancePERSONA Mobile risk levels and geozones as risk factors, choose the CylancePERSONA option
7. Click **Save**.
8. Click **Save**.

After you finish: Assign the policy to your organization’s PingFederate users. If you have your users configured in a group, you can follow the Assign an Enterprise Identity policy to a user group topic to easily assign the policy to all the users at once.

Allowing users to authenticate with Okta

BlackBerry Enterprise Identity can redirect user authentication to Okta, which provides existing Okta users with a familiar user interface. You can also use BlackBerry Enterprise Identity or CylancePERSONA policies to allow Okta’s authentication to adapt to both risk and context, including BlackBerry 2FA multifactor authentication.

Before BlackBerry Enterprise Identity and PingFederate can communicate, you must create a Ping Identity client on your organization’s PingFederate server, and a corresponding identity provider in BlackBerry UEM.

Before you create a Ping Identity client, ensure that your organization's PingFederate authentication policy has the OBJECTGUID attribute set to Hex. For more information, refer to the documentation from Ping Identity.

Note: You must have the latest version of BlackBerry UEM 12.11 installed in your environment.

Create an Okta app

Before you begin:

Your Okta instance must have a connection to Microsoft Active Directory, and your users must be imported into Okta. For instructions see, https://help.okta.com/en/prod/Content/Topics/Directory/ad-agent-main.htm

1. Log in to the Okta administration console.
2. Create a security token.
    a) Click **Security** > **API** > **Tokens**.
    b) Click **Create Token**.
    c) Copy the token.
3. Generate JWKS keys.
    a) Go to https://mkjwk.org.
    b) Click the **EC** tab.
    c) In the **Curve** drop-down list, select **P-521**.
    d) In the **Algorithm** drop-down list, select **ES512: ECDSA using P-521 and SHA-512**.
    e) In the **Key ID** drop-down list, select **SHA-256**.
    f) Copy the Public and Private Keypair, Keypair Set, and Public Key.

    Note: In the Public and Private Keypair Set, you must remove the **"d":** attribute because it is a private key.
4. In a command prompt, use a CURL request to register an OIDC app with Okta and update the following fields in the JSON. Creating this type of app is not currently supported in the Okta console.

    - Verify that the Authorization SSWS value is the token that you created in step 2.
    - Replace the jwks keys with the keys from step 3.
    - Verify that the "d;" attribute has been removed.

    Your entry should be similar to the following.

```
curl --request POST 'https://<oktaDomain>.okta.com/api/v1/apps/' \
--header 'Authorization: SSWS <token>' \
--header 'Content-Type: application/json' \
--data-raw '{
    "name": "oidc_client",
    "label": "BlackBerry Enterprise ID Client",
    "signOnMode": "OPENID_CONNECT",
    "credentials": {
        "oauthClient": {
            "token_endpoint_auth_method": "private_key_jwt"
        }
    },
    "settings": {
        "oauthClient": {
            "redirect_uris": [
                "https://idp.blackberry.com/idp/externalIdpCb"
            ],
            "response_types": [
                "code"
            ],
            "grant_types": [
                "authorization_code"
            ],
            "application_type": "native",
            "jwks": {
                "keys": [
                    {
                        "kty": "EC",
                        "crv": "P-521",
                        "kid": "OJE1cjnUBHGXHtOiHc64gSO1xxNzhoe9sRorb2CCKgU",
                        "x": "AV4Ljfyl2eCoP1oyO_U3047BTprKxuwlUm57p7FsQJFMtW
                         1Xks7j8IQe4H0S8tNpd21Q_2NcKiJg5gjWKs0H3Oh6",
                        "y": "AIWYPJ-c1UWEWQXO4Zkl3TKCPxCiAqv7ju_vJsO0Jye7zC
                         1SzqAFbfIzCRRq_MJJJfmw2ZbfgtvHmG28avR1O287",
                        "alg": "ES512"
                    }
                ]
            }
        }
    }
}'
```

For information about the JSON specification, see https://developer.okta.com/docs/reference/api/apps/.

5. View your app in the Okta console and copy the **Client ID**.
6. Assign the app to users. For instructions, see https://help.okta.com/en/prod/Content/Topics/Provisioning/lcm/lcm-user-app-assign.htm.
7. To set up Okta ID claims, go to **Security** > **API** > **Authorization server** and select your authorization server.
8. On the **Claims** tab, click **Add claims** and add a claim with the following values:
   a) **Name**: object_guid
   b) **Include in token type**: ID Token, Always
   c) **Value type**: Expression
   d) **Value**: findDirectoryUser().externalId
9. Click **Create**.

Configure Okta as an identity provider in BlackBerry UEM

After you create an Okta client, you must create a corresponding identity provider in the BlackBerry UEM management console.

Before you begin: Create an Okta app

1. In the BlackBerry UEM management console click **Settings > BlackBerry Enterprise Identity > External Identity providers**.
2. Click **+** and select **Okta**.
3. In the **Name** field, type a name for the identity provider.
4. In the **OIDC discovery document URL** field, type the location of your organization's Okta server. For example, `https://<oktaDomain>.okta.com/oauth2/<authorizationServerName>/.well-known/oauth-authorization`, where authorizationServerName is the name of the authorization server in step 7 of Create an Okta app.
5. In the **Client ID** field, enter the same ID that you created in the Create an Okta app task.
6. In the **Private key JWKS** field, enter the Private key that you used in the Create an Okta app task.

   Your entry should be similar to the following.

```
{
  "keys": [
            {
              "kty": "EC",
              "crv": "P-521",
              "kid": "OJE1cjnUBHGXHtOiHc64gSO1xxNzhoe9sRorb2CCKgU",
              "x": "AV4Ljfyl2eCoP1oyO_U3047BTprKxuwlUm57p7FsQJFMtW
              1Xks7j8IQe4H0S8tNpd21Q_2NcKiJg5gjWKs0H3Oh6",
              "y": "AIWYPJ-c1UWEWQXO4Zkl3TKCPxCiAqv7ju_vJsO0Jye7zC
              1SzqAFbfIzCRRq_MJJJfmw2ZbfgtvHmG28avR1O287",
              "alg": "ES521"
            }
          ]
 }
```

7. In the **Available services** list, select the services that you want to assign to the Okta client and click the right arrow to move the service to the **Selected service** list. Note that you can assign only one Okta client for each service.
8. Click **Save**.

After you finish: Create an Enterprise Identity authentication policy and assign it to users or groups. In the policy, add your service in Manage service exceptions and set the minimum authentication level to Level 4.

Managing app groups

You can use app groups to create a collection of apps in BlackBerry UEM and assign them to users, user groups, or device groups. Grouping apps helps to increase efficiency and consistency when you manage apps. For example, you can use app groups to group the same app for multiple device types, or to group apps for users with the same role in your organization. With BlackBerry Enterprise Identity, an app group can also contain the single sign-on entitlement in addition to the mobile app source files for a specific service. This allows you to give users everything they need to access that service in a single action.

You use the BlackBerry UEM management console to manage app groups. For more information, see Managing app groups in the BlackBerry UEM administration content.

Assign entitlements to users or groups

Before you begin: You must add users and services in BlackBerry UEM before you can entitle users to services. For information on adding services, see the guide Integrating SaaS Services. After Enterprise Identity services are synchronized with BlackBerry UEM, the services are available in the management console as apps. You assign an app to a user to entitle them to that service.

1. In the BlackBerry UEM management console, select the user or group that you want to assign the entitlements to. Perform one of the following actions:
   - To assign entitlements to a user, on the menu bar, click **Users** and select their name.
   - To assign entitlements to a group, on the menu bar, click **Groups** and select the group. Click the **Settings** tab.
2. Select the app or app group to assign.
3. Click the checkbox beside the service that you want to assign.
4. Click **Assign**.
5. If you are asked to assign licenses, click **Yes**.

Change Enterprise Identity settings

Some BlackBerry Enterprise Identity settings are adjustable within the BlackBerry UEM management console. You can change the display name of credentials in the Enterprise Identity login page. You may also adjust the ranking of authenticators. The authentication process for services starts with the highest-ranked authenticator and works down.

1. On the menu bar, click **Settings** > **BlackBerry Enterprise Identity**.
2. You can enter or change the user-friendly name for your BlackBerry UEM credentials in the Name text box.
3. To change the rank of authenticators, click the up or down arrows in the **Ranking** column. Mobile ZSO is not supported by all services so if that authenticator is placed at the top, some services will not be available.
4. Click **Save**.

Customize your organization's user sign in page

You can customize your organization’s BlackBerry Enterprise Identity user sign in page. For example, you can add your organization’s logo.

1. In the BlackBerry UEM management console, on the menu bar, click **Apps**.
2. Click **Add an app**.
3. Click **Enterprise Identity**.
4. Click **Open Enterprise Identity console**. The administrator console opens in a new browser tab. If the console does not open, ensure that you have enabled pop-ups in your browser.
5. On the **Settings** page, click **Sign In Page**.
6. In the **Login security text** field, type any additional information that you want your users to be aware of. This text will display below the Password field on the sign in page.
7. In the **Login title** field, type the text that will display at the top of your organization’s BlackBerry Enterprise Identity sign in page. You can use the **Insert token** drop-down list to format the login title text.
8. In the **Username description** field, type the text that will display above the username text field on your organization’s BlackBerry Enterprise Identity sign in page. You can use the **Insert token** drop-down list to format the username description text.
9. In the **Password description** field, type the text that will display above the password text field on your organization’s BlackBerry Enterprise Identity sign in page. You can use the **Insert token** drop-down list to format the password description text.
10. In the **Logo** field, click **Choose File** to navigate to and add a logo to your organization’s BlackBerry Enterprise Identity sign in page.
11. Choose options for the **Logo style**, **Text color option**, and **Background** fields.
12. Click **Save**.

SAML ECP support for Microsoft 365

Some mobile email clients, including some versions of BlackBerry Hub and BlackBerry Work, do not support Microsoft's ADAL interface when used with Microsoft 365, which prevents BlackBerry Enterprise Identity from displaying its normal login UI. To enable these mobile email clients, you can turn on Enterprise Identity's ECP (Enhanced Client or Proxy Profile) support for Office 365, which allows authentication with text-based credentials, such as username and password. These credentials are typically gathered from the email client's own user interface. Note that when ECP is used for Office 365, Enterprise Identity authentication policies are not applied to ECP-based logins.

Enable ECP support for Office 365

1. In the BlackBerry UEM management console, on the menu bar, click **Apps**.
2. Click **Add an app**.
3. Click **Enterprise Identity**.
4. Click **Open Enterprise Identity console**. The administrator console opens in a new browser tab. If the console does not open, ensure that you have enabled pop-ups in your browser.
5. On the **Settings** page, click **ECP Support**.
6. Turn on **ECP Support for Microsoft Office 365**.
7. Click **Save**.

Prevent users from being locked out of their accounts

You can configure BlackBerry Enterprise Identity to prevent users, such as Active Directory users, from being locked out of their account because of too many failed BlackBerry Enterprise Identity sign-in attempts. This feature is disabled by default.

Note: If you set the BlackBerry Enterprise Identity lock out threshold lower (for example, one less) than the Active Directory lockout threshold, your organization's users will be locked out of BlackBerry Enterprise Identity before being locked out of Active Directory.

1. In the BlackBerry UEM management console, on the menu bar, click **Apps**.
2. Click **Add an app**.
3. Click **Enterprise Identity**.
4. Click **Open Enterprise Identity console**. The administrator console opens in a new browser tab. If the console does not open, ensure that you have enabled pop-ups in your browser.
5. On the **Settings** page, click **Lockout**.
6. Turn on **Enable account lockout**.
7. Set the following options:
   - **Login attempt threshold**: Sets the number of failed attempts before the account is temporarily locked out.
   - **Login duration (minutes**): Sets the number of minutes that an account will be locked out for. When this timer has been exceeded, the account should be unlocked for the next sign in attempt.
   - **Reset duration (minutes)**: Sets the number of minutes that must elapse after a failed log in attempt before the failed log in attempt counter is reset to 0.
8. Click **Save**.

Tenant and domain selection

Most users login to Enterprise Identity with a username and password and specify whether to trust the browser. If a username exists in more than one tenant or domain, the first time that the user logs in, they must select the tenant from a drop-down list or enter the domain. The selections are saved for subsequent logins.

Managing BlackBerry UEM tenants in the BlackBerry Enterprise Identity console

You can use the UEM Tenants page in the Enterprise Identity console to manage your organization's BlackBerry UEM tenants. You can edit the properties of the tenants or you can disable the tenants. Note that if you disable a tenant, your organization's users will not be able to authenticate with any of the Enterprise Identity services that you enabled in BlackBerry UEM.

You can edit the following properties of BlackBerry UEM tenants.

Item	Description
Display Name	Change the display name of the tenant. This name displays in the UEM tenant picker on the log in screen when a user exists in more than one UEM tenant.
Authenticator Types - AD	Toggle the associated Microsoft Active Directory instance on or off and change the display name of the Active Directory instance.
Authenticator Types - LDAP	Toggle the associated LDAP directory on or off and change the display name of the LDAP directory.
Work Network Detection	Toggle network detection on or off. This risk factor assesses whether a user's app or browser is connected to the same network as the BlackBerry UEM server.

Managing administrators and users

You can add or remove administrators and users or change their entitlements in the BlackBerry UEM management console. For more information about managing administrators and users, see the BlackBerry UEM administration content.

If you need to redeploy BlackBerry UEM for any reason, you must first remove all users that have Enterprise Identity entitlements from BlackBerry UEM. If users are not removed before BlackBerry UEM is redeployed, they may still have services assigned to them but be unable to access them.

Create a custom Enterprise Identity administrator

You can use administrator roles to delegate specific BlackBerry Enterprise Identity administrative tasks to users. The Security Administrator role in BlackBerry UEM has full permissions to the management console, including creating and managing roles and administrators. At least one administrator must be a Security Administrator. BlackBerry UEM includes preconfigured roles in addition to the Security Administrator role. You can edit or delete all roles except the Security Administrator role. You can also create custom roles.

Note: Any new custom BlackBerry Enterprise Identity administrators that you create do not have the ability to assign BlackBerry Enterprise Identity entitlements or to assign apps and app groups to users or user groups. For more information, see Assign entitlements to users or groups and Managing app groups.

Before you begin: You must be a Security Administrator to create a custom role.

1. In the left menu click **Settings > Administrators > Roles**.
2. Click .
3. Type a name and description for the role.
4. In the **Polices and Profiles** section, select the Enterprise Identity policy options. The choices are:
    - **View Enterprise Identity Authentication Policy**
    - **Create/Edit Authentication policy, Delete Authentication policy**
    - **Assign Authentication policy to users and groups**: This setting requires view permissions for users and groups to display the Users and Devices tab and the Groups tab, respectively. For example, if you want the role to assign policies to users, you must enable the "View users and activated devices." If you want the role to assign policies to groups, you must enable the "View group settings."
5. In the **Settings** section, select the Enterprise Identity options. The choices are: **View Enterprise Identity Enterprise Settings, Edit Enterprise Identity Enterprise Settings, View Enterprise Identity Services**, and **Edit Enterprise Identity Services**.
6. Click **Save**.
7. Add the role to a user account or user group.

After you finish:

For more information about roles, see the BlackBerry UEM Administration content.

View and filter the audit events in BlackBerry Enterprise Identity

If you have BlackBerry UEM Cloud, UEM Cloud keeps user and audit events in log files that you can use to investigate any administrator and user actions (for example, user log in failure and authentication success) for the enterprise. UEM Cloud records all actions that users perform in the management console. You can filter the list of actions to display only the actions that are relevant to your investigation. For further analysis or reporting purposes, you can export the filtered list to a .csv file.

Security audit events include user actions such as authentication, modify data that is associated with a user, and creating a new user account. To view the audit logs, complete the following:

1. In the UEM Cloud management console, on the menu bar, click **Apps**.
2. Click **Add an app**.
3. Click **Enterprise Identity**.
4. Click **Open Enterprise Identity console**.
5. On the **User Logs** page, all of the user events have been logs are displayed. You can enter a search term to filter the events that are displayed.
6. On the **User Logs** page, all of the user events are displayed by default. Optionally, enter a search term to only display the logged events for the search criteria.

After you finish: To export all security audit events from the last 30 days to a .csv file, in the Enterprise Identity console, click **Export last 30 days to CSV**.

Legal notice

Android and Google Workspace are trademarks of Google Inc. Box is including without limitation, either a trademark, service mark or registered trademark of Box, Inc. iOS 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. Microsoft, Active Directory, and Office 365 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Salesforce is a trademark of salesforce.com, inc. and is used here with permission. WebEx is a trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.Workday is a trademark of Workday, 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, MERCHANTABLE QUALITY, 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 Ground Floor, The Pearce Building, West Street, Maidenhead, Berkshire SL6 1RL United Kingdom Publis