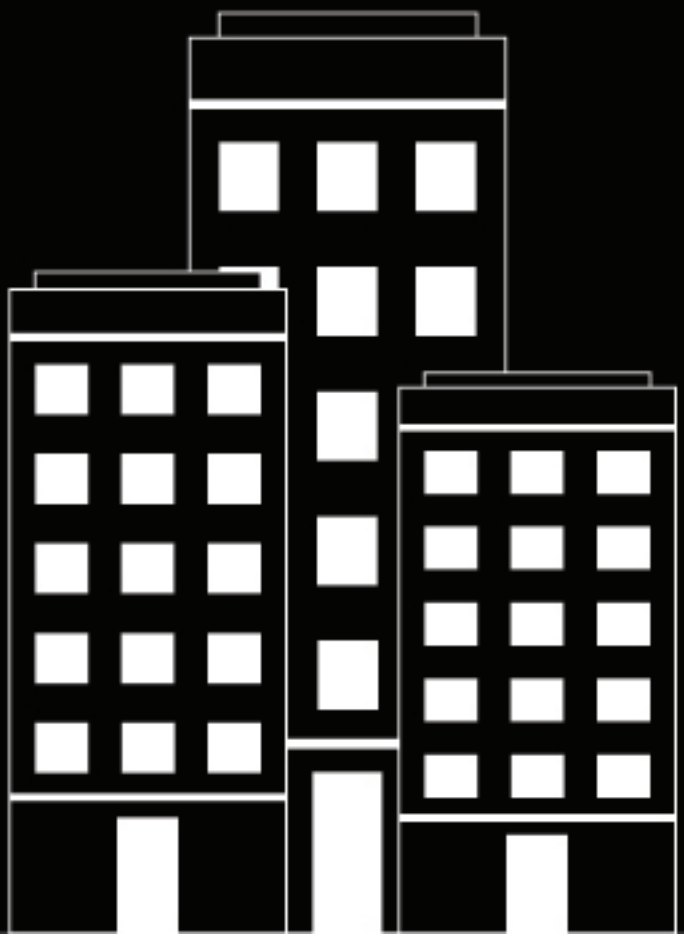

BlackBerry Intelligent Security

Administration Guide

Contents

Software requirements

Requirement	Description
BlackBerry UEM	BlackBerry Intelligent Security is supported in: • BlackBerry UEM Cloud • BlackBerry UEM version 12.11.1 Cumulative Quick Fix (QF). Upgrading to this version is mandatory to support BlackBerry Intelligent Security features. Contact your BlackBerry support representative to request this software. You must purchase BlackBerry Intelligent Security licenses to enable the service for users in your organization's UEM domain. Contact your BlackBerry representative or complete a contact form for more information. After BlackBerry applies the licenses, see Enable BlackBerry Intelligent Security in your UEM domain. For more information about configuring and managing UEM, see the BlackBerry UEM documentation or the BlackBerry UEM Cloud documentation.
BlackBerry Intelligent Security entitlement	After BlackBerry Intelligent Security licenses are added for your organization, you will receive a BlackBerry Intelligent Security entitlement. The entitlement information that you will see in the management console is: • App name: BlackBerry Intelligent Security entitlement • BlackBerry Dynamics entitlement ID: com.blackberry.entitlement.geoanalytics You must assign this entitlement to BlackBerry Dynamics app users so that BlackBerry Intelligent Security can receive and process behavioral and geolocation data from the apps. You can assign the entitlement to all users, specific user groups, or specific user accounts based on your organization's needs. After assigning the entitlement, it may take up to 24 hours for the accounts and data to be ready.
Enforcing BlackBerry 2FA authentication	If you want to use BlackBerry Enterprise Identity authentication profiles to enforce BlackBerry 2FA authentication, you must enable BlackBerry 2FA for users' devices. For more information, see Steps to manage BlackBerry 2FA in BlackBerry UEM in the BlackBerry 2FA Administration content.

Requirement	Description
BlackBerry Dynamics apps with the BlackBerry Analytics SDK	BlackBerry Intelligent Security collects data from BlackBerry Dynamics apps that use the BlackBerry Analytics SDK version 2.1.0 or later. By default, this SDK is already integrated with the BlackBerry Dynamics apps produced and distributed by BlackBerry. Use the following versions of BlackBerry Dynamics apps to ensure that the apps have the required versions of the BlackBerry Dynamics SDK and the BlackBerry Analytics SDK: • BlackBerry Work version 2.18 or later • BlackBerry Tasks version 2.18 or later • BlackBerry Notes version 2.18 or later • BlackBerry Connect version 2.9 or later • BlackBerry Access version 2.12 or later • BlackBerry UEM Client for iOS version 12.x or later For more information about adding and distributing BlackBerry Dynamics apps in a UEM domain, see Managing BlackBerry Dynamics apps in the UEM Administration content. **Note:** Within the settings of each BlackBerry Dynamics app, users can enable or disable BlackBerry Intelligent Security (by default, it is enabled). If it is disabled, BlackBerry Intelligent Security cannot collect data and events from the app. Encourage users to keep this setting enabled to ensure that BlackBerry Intelligent Security can build and use an accurate risk model.

Steps to configure and use BlackBerry Intelligent Security

The tasks in this section must be completed by a UEM administrator with the Security Administrator role.

Step	Action
1	Enable BlackBerry Intelligent Security in your UEM domain.
2	Assign the BlackBerry Intelligent Security administrator role to an administrator.
3	(Optional) Change the risk score range for behavioral risk levels.
4	Create UEM user groups that you will associate with risk levels.
5	Create a BlackBerry Intelligent Security policy.
6	Assign the BlackBerry Intelligent Security policy to a user account or to multiple user accounts.
7	Create a BlackBerry Enterprise Identity authentication policy to set the authentication requirements for different risk levels. Assign the policy to user groups.
8	Change the BlackBerry Intelligent Security operating mode.
9	Use the BlackBerry Intelligent Security Analytics Portal to view user and event statistics.

Enable BlackBerry Intelligent Security in your UEM domain

Before you begin:

- Contact your BlackBerry representative to purchase BlackBerry Intelligent Security licenses. After BlackBerry adds the licenses for your organization, complete the steps below.
- If you decide to use BlackBerry Intelligent Security in trial mode before you purchase licenses, follow the instructions provided by BlackBerry to enable the feature in a new or existing UEM or UEM Cloud instance. If you set up a new UEM instance, see the UEM documentation or UEM Cloud documention for installation and configuration instructions. After your trial period ends, you can purchase and add BlackBerry Intelligent Security licenses to the UEM domain.

1. In the management console, on the menu bar, click **Settings > Services**.
2. Locate the BlackBerry Intelligent Security service in the table and click **Enable**.
3. When prompted, click **Enable** again.
4. On the menu bar, click **Settings > External integration > Cloud directory service**.
5. Click **Enable**.

After you finish:

- Log out of the management console and log in again with the same administration account.
- Assign the BlackBerry Intelligent Security administrator role to an administrator.

Assign the BlackBerry Intelligent Security administrator role to an administrator

You must assign a BlackBerry Intelligent Security administrator role to administrator accounts that will be responsible for managing BlackBerry Intelligent Security. This task must be performed by a user with the Security Administrator role or a custom role with equivalent permissions.

Before you begin: Enable BlackBerry Intelligent Security in your UEM domain.

1. In the management console, on the menu bar, click **BlackBerry Intelligent Security > Administrators**.
2. Click  .
3. Search for and select the user account that you want to make a BlackBerry Intelligent Security administrator. The account must already have a UEM administrator role (for example, Enterprise Administrator).
4. In the **Role** drop-down list, do one of the following:
   - If you want to give the user access to BlackBerry Intelligent Security settings in the management console and to the BlackBerry Intelligent Security Analytics Portal, click **BlackBerry Intelligent Security Administrator**.
   - If you want give the user access to the BlackBerry Intelligent Security Analytics Portal only, click **BlackBerry Intelligent Security Analytics Administrator**.
5. Click **Save**.

After you finish:

- UEM sends an email notifying the user that they have been given administrator access. The email provides a link to the BlackBerry Intelligent Security Analytics Portal.
- Optional: Change the risk score range for behavioral risk levels.
- Create user groups to define security standards for different risk levels.

Change the risk score range for behavioral risk levels

You can change the risk score range that BlackBerry Intelligent Security uses to determine each user's behavioral risk level. The default risk score ranges for the risk levels are:

- Low: 0% to 30%
- Medium: 30% to 60%
- High: 60% to 80%
- Critical: 80% to 100%

Before you begin: Assign the BlackBerry Intelligent Security administrator role to an administrator.

1. In the management console, on the menu bar, click **BlackBerry Intelligent Security > Settings**.
2. Click the appropriate risk score field (**Low**, **Medium**, **High**, or **Critical**) and type the number for the upper limit of that risk score range. For example, if you want to change the **Low** risk range to be 0%-40%, in the **Low** field type `40`.
   - Update the other risk score ranges as necessary so that none of the ranges overlap.
   - If you leave a field blank, BlackBerry Intelligent Security uses the default upper limit as specified above (30 for low, 60 for medium, and so on).
   - You must specify at least two risk score ranges.
   - The ranges that you specify must account for all values from 0 to 100.
3. Click **Save**.

After you finish: Create user groups to define security standards for different risk levels.

Create user groups to define security standards for different risk levels

You must create and configure local UEM user groups that will determine security standards and device behaviors for the different BlackBerry Intelligent Security risk levels or for specific geozones that you define. In the next task, Create a BlackBerry Intelligent Security policy, you will associate each group with one (or more) of the different behavioral risk levels, geozone risk levels, or defined geozones. Configure each group with a combination of UEM policies, profiles, app assignments, and roles that reflect your organization's security standards for that level of risk or for that specific geozone. For example, you can create and configure a group for users with a high behavioral risk level. This group includes policies and profiles that are more restrictive and have greater security requirements than the group that is intended for low-risk users.

Repeat the following task for each group that you want to associate with one or more risk levels or defined geozones. Depending on how you want to configure your environment, you can create a different group for each risk level, you can use the same group for multiple risk levels, or you can choose to not require any action by UEM for certain risk levels or risk types (for example, you can choose to take action for geozone risk levels only and not take any action for behavioral risk).

Before you begin:

- Optional: Change the risk score range for behavioral risk levels.
- Create and configure all of the roles, policies, profiles, and app assignments that you want to assign to the local user groups that you will create. For more information about the full range of management options available in UEM, see the BlackBerry UEM Administration content or the BlackBerry UEM Cloud Administration content.

1. In the management console, on the menu bar, click **Groups**.
2. Click  .
3. Type a name and description for the group.
4. In the appropriate sections, click + to assign user roles, IT policies and profiles, and apps that meet the security standards and requirements for the behavioral or geozone risk level that this group is intended for.

   Note: You must assign the BlackBerry Intelligent Security entitlement to each group. For more information, see Software requirements.
5. Click **Add**.

After you finish:

- Create a BlackBerry Intelligent Security policy.

- Depending on how you choose to configure your UEM environment and manage the automatic assignment of policies, profiles, roles, and apps using BlackBerry Intelligent Security, there may be conflicting assignments that UEM must resolve. See Resolving conflicting assignments and precedence rules.

Create a BlackBerry Intelligent Security policy

You configure a BlackBerry Intelligent Security policy to determine which groups UEM will automatically assign to a user based on the user's current behavioral risk level and geozone risk level.

You can select a different UEM group for each risk level, the same group for multiple risk levels, or you can choose to not take any action for a risk level. For more information about how UEM resolves any conflicting policy, profile, role, or app assignments, see Resolving conflicting assignments and precedence rules.

You can customize the policy to suit your organization's needs. For example, you can choose to take actions for geozone risk levels only and disable actions for behavioral risk levels, or you can disable learned geozones and configure actions based on whether the user currently occupies a defined geozone (for example, an office location that you have specified).

Before you begin:

- Create user groups to define security standards for different risk levels.
- To define specific geozones (for example, a specific office location) that you want to set actions for in the policy, see Define geozones.

1. In the management console, on the menu bar, click **BlackBerry Intelligent Security > Policies**.
2. Click +.
3. Type a name and description for the policy.
4. If you don't want UEM to take action for behavioral risk levels, in the **Behavioral risk levels and actions** section, clear the **Enable behavioral risk actions** check box. Skip to step 8.
5. In the **Behavioral risk levels and actions** section, click a risk level. Do the following:
   a) In the **Assign to group** drop-down list, click the appropriate group.
   b) Critical risk level only: If you want to prevent BlackBerry Dynamics apps from running on a user's device, select the **Assign device action** check box.
   c) Click **Save**.
6. Repeat step 5 for each remaining behavioral risk level.
7. To allow users to reduce their behavioral risk level to low by completing a BlackBerry 2FA authentication prompt, do the following:
   a) Click **Edit automatic risk reduction**.
   b) In the drop-down list, click the risk levels that should allow automatic risk reduction.
   c) Click **Save**.
8. Choose one of the following methods for managing geozone risk levels and actions:

Method	Steps
• Use learned geozones • Take special action for defined geozones that you add to the policy	**a.** In the **Geozone risk levels and actions** section, verify that **Enable learned geozones** is selected. To change the geozone ranges, click **Edit dynamic geozone risk factors**. Specify the upper limit of the low-risk range from learned locations and the upper limit of the medium-risk range from learned locations. Click **Save**. **b.** Click a geozone risk level. Do the following: **1.** In the **Assign to group** drop-down list, click the appropriate group. **2.** High risk level only: If you want to prevent BlackBerry Dynamics apps from running on a user's device, select the **Assign device action** check box. **3.** Click **Save**. **c.** Repeat the previous step for each remaining geozone risk level. **d.** If you defined one or more specific geozones in the BlackBerry Intelligent Security Analytics Portal (see Define geozones) and you want those geozone settings to override what you configured in steps 2-3, in the **Overridden actions for specific geozones** section, click +. Do the following: **1.** In the **Geozone** drop-down list, click the desired geozone. **2.** In the **Assign to group** drop-down list, click the appropriate group. **3.** If you want to prevent BlackBerry Dynamics apps from running on a user's device while they are in this geozone, select the **Assign device action** check box. **4.** Click **Save**. **e.** Repeat the previous step to add additional defined geozones.
• Do not use learned geozones • Take action for defined geozones that you add to the policy • Take one default action for users that are not in the geozones that you added to the policy	**a.** In the **Geozone risk levels and actions** section, clear the **Enable learned geozones** check box. **b.** In the **Overridden actions for specific geozones** section, click +. Do the following: **1.** In the **Geozone** drop-down list, click the desired geozone. **2.** In the **Assign to group** drop-down list, click the appropriate group. **3.** If you want to prevent BlackBerry Dynamics apps from running on a user's device while they are in this geozone, select the **Assign device action** check box. **4.** Click **Save**. **c.** Repeat the previous step to add additional defined geozones. **d.** In the **Overridden actions for specific geozones** section, click +. Do the following: **1.** In the **Geozone** drop-down list, click **Not in a specified geozone**. **2.** In the **Assign to group** drop-down list, click the appropriate group. **3.** If you want to prevent BlackBerry Dynamics apps from running on a user's device while they are not in any of the geozones that you added, select the **Assign device action** check box. **4.** Click **Save**.

Method	Steps
• Do not use learned geozones • Take action for defined geozones that you add to the policy • For all other defined geozones that you don't add to the policy, use the default risk actions that you set for each risk level • Take no geozone risk action when a user is not in a defined geozone	To use this mode, you must add at least one defined geozone to the policy. **a.** In the **Geozone risk levels and actions** section, clear the **Enable learned geozones** check box. **b.** In the **Overridden actions for specific geozones** section, click +. Do the following: **1.** In the **Geozone** drop-down list, click the desired geozone. **2.** In the **Assign to group** drop-down list, click the appropriate group. **3.** If you want to prevent BlackBerry Dynamics apps from running on a user's device while they are in this geozone, select the **Assign device action** check box. **4.** Click **Save**. **c.** Repeat the previous step to add additional defined geozones. **d.** To set the default actions to take when the user is in a defined geozone that you did not add to the policy, click a geozone risk level and do the following: **1.** In the **Assign to group** drop-down list, click the appropriate group. **2.** High risk level only: If you want to prevent BlackBerry Dynamics apps from running on a user's device, select the **Assign device action** check box. **3.** Click **Save**. **e.** Repeat the previous step for each remaining geozone risk level.
• Do not take action for geozone risk levels	Configure no actions in the **Geozone risk levels and actions** section.

9. Click **Save**.

After you finish:

- Assign a BlackBerry Intelligent Security policy to a user account or Assign a BlackBerry Intelligent Security policy to multiple users.
- If you enabled automatic risk reduction, when you view user and event statistics in the BlackBerry Intelligent Security Analytics Portal you can see the status of risk reductions.

Resolving conflicting assignments and precedence rules

A BlackBerry Intelligent Security policy can only execute group assignments based on the groups that are set for behavioral risk levels, geozone risk level, or defined geozones in the policy. UEM administrators can create and assign groups, policies, profiles, and apps using the standard management console features. These assignments are not impacted by the BlackBerry Intelligent Security policy, but the group assignments carried out by the policy may result in conflicting assignments that UEM must resolve. For more information, see How BlackBerry UEM chooses which profiles to assign in the UEM Administration content.

To ensure that conflicts are resolved properly, verify that the appropriate ranking is set for each resource in the management console. For more information about how to set the ranking for policies, profiles, roles, and apps, see the BlackBerry UEM Administration content or the BlackBerry UEM Cloud Administration content.

BlackBerry Intelligent Security uses the following precedence rules to determine the actions to take when both behavioral risk and geozone risk actions are enabled.

If behavioral risk is critical or high:

- And the user is in a high-risk defined geozone, the defined geozone actions take precedence
- And the user is not in a high-risk defined geozone, the high risk geozone actions (learned or default) take precedence
- The user is not in a high-risk defined geozone, and high-risk geozone actions (learned or default) are not configured, behavioral risk actions are applied
- Learned geozones are disabled, and the policy is configured with one or more defined geozones and "Not in a defined geozone", behavioral risk actions take precedence over the risk actions configured for "Not in a defined geozone"

If behavioral risk is medium or low:

- And the user is in a defined geozone, the defined geozone risk actions take precedence
- The user is not in a defined geozone, and the user's geozone risk level is high, the high-risk geozone actions take precedence
- The user is not in a defined geozone, and the user's geozone risk level is medium or low, the corresponding behavioral and geozone risk actions are applied and UEM uses ranking to resolve conflicts
- The user is not in a defined geozone, and geozone risk actions are not configured, the corresponding behavioral risk actions are applied
- Learned geozones are disabled, and the policy is configured with one or more defined geozones and "Not in a defined geozone", the risk actions for "Not in a defined geozone" take precedence over behavioral risk actions

Assign a BlackBerry Intelligent Security policy to a user account

Before you begin: Create a BlackBerry Intelligent Security policy.

1. In the management console, on the menu bar, click **Users > All users**.
2. Search for and click a user account.
3. Above the Summary tab, click **BlackBerry Intelligent Security**.
4. In the **BlackBerry Intelligent Security policy** drop-down list, click a BlackBerry Intelligent Security policy.
5. Click **Assign**.

After you finish:

- Notify users that they will receive a prompt from BlackBerry Dynamics apps asking whether they want to provide geolocation data. Encourage users to allow BlackBerry Dynamics apps to provide this data. If a user does not, BlackBerry Intelligent Security cannot factor the data into the user's risk model.
- To change the BlackBerry Intelligent Security policy that is assigned to a user, navigate to the user details, click **BlackBerry Intelligent Security** and click +. In the **BlackBerry Intelligent Security policy** drop-down list, click the new policy and click **Replace**.
- To remove a user's BlackBerry Intelligent Security policy, navigate to the user details and click **BlackBerry Intelligent Security** above the user summary information. Click the × to the far right of the assigned policy, then click **Remove**.
- Within the settings of each BlackBerry Dynamics app, users can enable or disable BlackBerry Intelligent Security (by default, it is enabled). If it is disabled, BlackBerry Intelligent Security cannot collect data and events from the app. Encourage users to keep this setting enabled to ensure that BlackBerry Intelligent Security can build and use an accurate risk model.
- Create a BlackBerry Enterprise Identity authentication policy.
- Change the BlackBerry Intelligent Security operating mode.

Assign a BlackBerry Intelligent Security policy to multiple users

Before you begin: Create a BlackBerry Intelligent Security policy.

1. In the management console, on the menu bar, click **Users > All users**.
2. Search for and select multiple user accounts. You can use the BlackBerry Intelligent Security filter to display the users that are not currently assigned a BlackBerry Intelligent Security policy.
3. Click .
4. In the **Enable service** drop-down list, click **BlackBerry Intelligent Security**.
5. Click **Enable**.
6. In the **BlackBerry Intelligent Security policy** drop-down list, click a BlackBerry Intelligent Security policy.
7. Click **Assign**.

After you finish:

- Notify users that they will receive a prompt from BlackBerry Dynamics apps asking whether they want to provide geolocation data. Encourage users to allow BlackBerry Dynamics apps to provide this data. If a user does not, BlackBerry Intelligent Security cannot factor the data into the user's risk model.
- To change the BlackBerry Intelligent Security policy that is assigned to multiple users, repeat the steps above and select a different policy.
- To remove a user's BlackBerry Intelligent Security policy, navigate to the user details and click **BlackBerry Intelligent Security** above the user summary information. Click the ✕ to the far right of the assigned policy, then click **Remove**.
- Within the settings of each BlackBerry Dynamics app, users can enable or disable BlackBerry Intelligent Security (by default, it is enabled). If it is disabled, BlackBerry Intelligent Security cannot collect data and events from the app. Encourage users to keep this setting enabled to ensure that BlackBerry Intelligent Security can build and use an accurate risk model.
- Create a BlackBerry Enterprise Identity authentication policy.
- Change the BlackBerry Intelligent Security operating mode.

Create a BlackBerry Enterprise Identity authentication policy

BlackBerry Intelligent Security adds a new optional feature to BlackBerry Enterprise Identity authentication policies. You can now incorporate a user's behavioral and/or geozone risk level into the factors that determine the authentication requirements for work apps and services. For example, you can configure the policy so that if a user's geozone risk level is high, the user must enter both a password and use BlackBerry 2FA to access work apps.

For more information about how to enable and manage BlackBerry Enterprise Identity, see the BlackBerry Enterprise Identity docs.

Before you begin: If you want to use BlackBerry Enterprise Identity authentication profiles to enforce BlackBerry 2FA authentication, you must enable BlackBerry 2FA for users' devices. For more information, see Steps to manage BlackBerry 2FA in BlackBerry UEM in the *BlackBerry 2FA Administration Guide*.

1. In the management console, on the menu bar, click **Policies and profiles > BlackBerry Enterprise Identity**.
2. Click **Add a policy**.
3. Type a name and description.
4. In the **Minimum authentication level** level drop-down list, click the desired authentication level. For more information, see Managing authentication levels in the *BlackBerry Enterprise Identity Administration Guide*.

5. In the **Risk scenarios** table, click +.
6. Type a name and description for the risk scenario.
7. In the **Minimum authentication level** drop-down list, select the desired authentication level that is required when the risk factors are met.
8. In the **Risk factor combination** drop-down list, select the desired option.
9. If you want UEM to consider a BlackBerry Intelligent Security risk level or a defined geozone to be a risk factor, select the **BlackBerry Intelligent Security** check box. Do any of the following:
   - If you want a behavioral risk level to be a risk factor, in the **Behavioral risk level** drop-down list, click the desired risk level.
   - If you want a geozone risk level to be a risk factor, in the **Geozone risk level** drop-down list, click the desired risk level.
   - If you want a defined geozone to be a risk factor, in the **Administrator-defined geozone** drop-down list, click the desired geozone. The geozone that you select will automatically set the **Geozone risk level** based on the configuration of the defined geozone.
10. Click **Save**.
11. If necessary, repeat steps 5 to 10 to add additional risk scenarios.
12. Click **Save**.

After you finish:

- Assign a BlackBerry Enterprise Identity authentication policy to a user group.
- Notify users that they will receive prompts asking whether they want to allow BlackBerry Enterprise Identity to provide geolocation data and whether BlackBerry Enterprise Identity can trust the browser. Encourage users to accept both prompts. If a user does not, BlackBerry Intelligent Security cannot factor the data into the user's risk model. Note that if a user logs in to the BlackBerry Enterprise Identity service for the first time using Incognito mode, BlackBerry Enterprise Identity cannot send location data. Location data will be sent in a subsequent login.
- Change the BlackBerry Intelligent Security operating mode.

Change the BlackBerry Intelligent Security operating mode

BlackBerry Intelligent Security has two operating modes:

- Passive: A training mode where the BlackBerry Intelligent Security services monitor behavioral data and geozone data and build a risk model for each user, but the actions that are configured in BlackBerry Intelligent Security policies are not executed. The risk factors specified in a BlackBerry Enterprise Identity authentication policy are not active.
- Active: The BlackBerry Intelligent Security services monitor behavioral data and geozone data and build a risk data model for each user. The actions that are configured for that risk level in BlackBerry Intelligent Security policies are executed based on each user's current behavioral and geozone risk levels. The risk factors specified in a BlackBerry Enterprise Identity authentication policy are active.

By default, BlackBerry Intelligent Security operates in passive mode. After you configure and assign BlackBerry Intelligent Security policies to user accounts, BlackBerry recommends using passive mode until regular user activity generates enough events to build an accurate behavioral risk model and learned geozones for each user.

See Guidelines for developing risk models for suggested actions to help develop accurate risk models and to learn how to verify whether your environment is ready for active mode.

Before you begin:

- Assign a BlackBerry Intelligent Security policy to a user account.

- Assign a BlackBerry Intelligent Security policy to multiple users.
- Optional: Create a BlackBerry Enterprise Identity authentication policy and assign it to user groups.

1. In the management console, on the menu bar, click **BlackBerry Intelligent Security > Settings**.
2. In the **Operating mode** drop-down list, click the desired operating mode.
3. Click **Save**.

Guidelines for developing risk models

After you assign a BlackBerry Intelligent Security policy to users, follow these guidelines to help the BlackBerry Intelligent Security services develop accurate risk models for users:

- Instruct users to accept the prompts from BlackBerry Dynamics apps and BlackBerry Enterprise Identity connected apps to send geolocation data and, if applicable, to allow BlackBerry Enterprise Identity to trust the browser.
- For the first 6 hours, encourage users to open and log in to a BlackBerry Dynamics app (for example, BlackBerry Work) and a BlackBerry Enterprise Identity connected app at least 10 times each from the same geographical location.
  - If the user has to be in multiple locations, request that they repeat the same activity from each location.
- After the initial 6-hour window, encourage users to open and log in to the same apps at least once per hour during the work day for at least 2 days. This activity will generate a regular set of events and data upload cycles.

To determine whether your environment is ready to use active mode, log in to the BlackBerry Intelligent Security Analytics Portal and view the Events page. If the BlackBerry Intelligent Security services are performing risk assessments, you will see risk scores associated with the events. When you see this behavior consistently, you can enable active mode. The amount of time required will vary based on the level of user activity and how frequently events are generated by users.

Using the BlackBerry Intelligent Security Analytics Portal

You can access the BlackBerry Intelligent Security Analytics Portal to view user and event statistics and to define specific geozones that can override standard geozone risk actions in BlackBerry Intelligent Security policies. If you enabled automatic risk reduction, when you view user and event statistics you can see the status of risk reductions.

By default, privacy mode is enabled to mask exact information about user geolocations from BlackBerry Intelligent Security administrators. While enabled, the portal displays general location information for users and events instead of precise information such as a street address. Similarly, map views are zoomed out to provide accurate but non-intrusive location information.

An administrator with the BlackBerry Intelligent Security Administrator role can disable (or re-enable) privacy mode in Settings > Privacy (this action is written to the log file). Administrators with the BlackBerry Intelligent Security Analytics Administrator role cannot change the privacy mode setting.

View user and event statistics

Before you begin: In the management console, in **Settings > External integration > Cloud directory service**, verify that the status is **Enabled**.

1. To log in to the BlackBerry Intelligent Security Analytics Portal, do one of the following:
   - Visit **https://bisanalytics.blackberry.com/**<*Organization_SRP_ID*>. Log in with your BlackBerry Intelligent Security administrator account.
   - In the management console, on the menu bar, click **BlackBerry Intelligent Security > Analytics**.
2. To modify the dashboard view, perform any of the following tasks:
   - Click to modify the time frame for the information displayed in the dashboard.
   - Click to rearrange the dashboard components.
3. To view user statistics, on the menu bar, click **Users**. Users will display if they have at least one event logged with BlackBerry Intelligent Security in the specified time frame. You can search for specific user accounts, filter results by risk type and risk level, and click a user account to view more details.
   - Click to modify the time frame of the data.
   - Click to select the type of information to display.
   - Click to export a .csv file with the displayed results.
   - In the Map view you can click the Show/Hide Map Types arrow in the bottom right of the map pane to select the risk indicators that you want to view (behavioral, geozone, or both), as well as other map display options.
   - In the Map view you can click a pin on the map or drag and drop the Pegman icon in the bottom right of the map pane to switch to the Google Maps street view. To exit the street view, click the back arrow icon in the top left corner of the map pane.
4. To view event statistics, on the menu bar, click **Events**. You can search for specific events, filter results by risk type and risk level, and click an event to view more details.
   - Click to modify the time frame of the data.
   - Click to select the type of information to display.
   - Click to export a .csv file with the displayed results.

- In the Map view you can click the Show/Hide Map Types arrow in the bottom right of the map pane to select the risk indicators that you want to view (behavioral, geozone, or both), as well as other map display options.
- In the Map view you can click a pin on the map or drag and drop the Pegman icon in the bottom right of the map pane to switch to the Google Maps street view. To exit the street view, click the back arrow icon in the top left corner of the map pane.

Define geozones

When you define a geozone, you assign it a risk level to it (low, medium, or high). When you configure a BlackBerry Intelligent Security policy, you can add a defined geozone that will take precedence over the regular geozone risk actions in the policy (see Create a BlackBerry Intelligent Security policy). For example, you can define a geozone for a specific office location with a low risk level. If a user is in that geozone, their risk level will be low regardless of how far it is from their learned geozones. Note that the overall assessment of the user's geozone risk level is also impacted by the user's current behavioral risk assessment.

You can choose whether you want BlackBerry Intelligent Security to use learned geozones when it determines a user's geozone risk level. For example, you can disable learned geozones and configure the service to take action based on whether the user is in one of several defined geozones. You can set a default action for users that are not in a defined geozone.

1. To log in to the BlackBerry Intelligent Security Analytics Portal, do one of the following:
   - Visit **https://bisanalytics.blackberry.com/**<*Organization_SRP_ID*>. Log in with your BlackBerry Intelligent Security administrator account.
   - In the management console, on the menu bar, click **BlackBerry Intelligent Security > Analytics**.
2. On the menu bar, click **Settings > Geozones**.
3. On the map pane, in the **Add a geozone** field, type a location (for example, a city). As you type, suggested locations will display. Click a suggested location to narrow the map view to that location.

   If a pin appears on the map, you can click it to see the options to draw a geozone (see step 5).
4. Use your mouse or the zoom in and zoom out buttons in the lower-right corner to scope your map view to the desired location.

   To switch to the Google Street View, drag and drop the Pegman icon at the bottom right corner of the map pane to the desired location. If it's a valid location, blue lines will display on the streets while you drag the icon.

   To exit the view, click the back arrow icon in the top left corner of the map pane. Note that the Google Street View is for information purposes only and cannot be used to define a geozone (see step 5).
5. Do one of the following:
   - Click ⊙. Click a point on the map and drag to expand the circle until it covers the desired area. Click again. Type a geozone name, select a risk level, and specify a radius in kilometers or miles.
   - Click ⌑. Click a point on the map and drag to draw a line, then click again to set a new point. Repeat until you draw a polygon shape over the desired area. Close the shape by clicking the starting point again. Type a geozone name and select a risk level.
6. Click **Add**.

After you finish:

- To add a defined geozone to a BlackBerry Intelligent Security policy, see Create a BlackBerry Intelligent Security policy.
- To export a .csv file with the displayed geozones, click ➔.

Developing apps that leverage BlackBerry Intelligent Security

Enterprise developers can use the SDKs provided by BlackBerry to create custom BlackBerry Dynamics apps that can interact with the BlackBerry Intelligent Security services.

Developers can create BlackBerry Dynamics apps using the BlackBerry Dynamics SDK and integrate the BlackBerry Analytics SDK to enable the app to send events and geolocation data to the BlackBerry Intelligent Security services.

For more information about using the BlackBerry Dynamics SDK, see the BlackBerry Dynamics SDK Development Guide for your desired OS platform. For more information about integrating the BlackBerry Analytics SDK, see the BlackBerry Analytics SDK Development Guide.

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