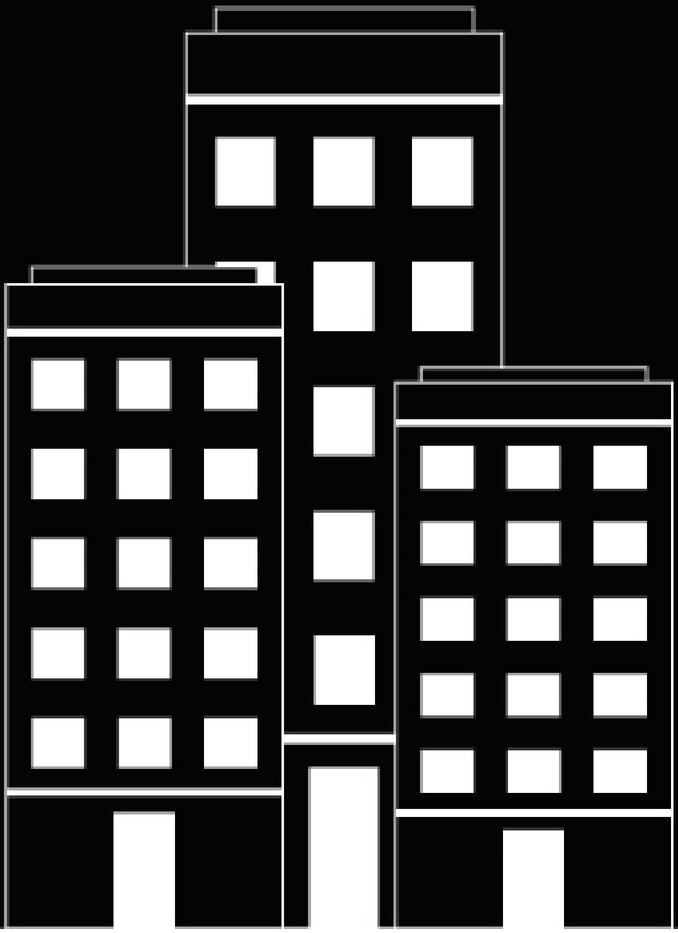

CylancePERSONA Mobile

Administration Guide

Contents

CylancePERSONA Mobile software requirements

Requirement	Description
BlackBerry UEM	CylancePERSONA Mobile is supported in: • BlackBerry UEM Cloud • BlackBerry UEM version 12.13 and later You must purchase CylancePERSONA Mobile licenses to enable the service for users. Contact your BlackBerry representative or complete a contact form for more information. After BlackBerry applies the licenses, see Enable CylancePERSONA Mobile in your UEM domain. For more information about configuring and managing UEM, see the BlackBerry UEM documentation.
CylancePERSONA Mobile entitlement	After CylancePERSONA Mobile licenses are added for your organization, you will receive a CylancePERSONA Mobile entitlement. The entitlement information that you will see in the management console is: • App name: CylancePERSONA Mobile entitlement • BlackBerry Dynamics entitlement ID: com.blackberry.entitlement.geoanalytics You must assign this entitlement to BlackBerry Dynamics app users so that CylancePERSONA Mobile can receive and process behavioral and location 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	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 3.2 or later • BlackBerry Tasks version 3.2 or later • BlackBerry Notes version 3.2 or later • BlackBerry Connect version 3.2 or later • BlackBerry Access version 3.1 or later • BlackBerry UEM Client for iOS (latest) • BlackBerry UEM Client for Android (latest) For more information about adding and distributing BlackBerry Dynamics apps in a UEM domain, see Managing BlackBerry Dynamics apps. **Note:** Within the settings of each BlackBerry Dynamics app, users can enable or disable CylancePERSONA Mobile (by default, it is enabled). If it is disabled, CylancePERSONA Mobile cannot collect data and events from the app. Encourage users to enable this setting to ensure that CylancePERSONA Mobile can build and use an accurate risk model.
Device connections to the CylancePERSONA Mobile services	For optimal performance, BlackBerry recommends permitting a direct connection between devices and the CylancePERSONA Mobile services. In the BlackBerry Dynamics connectivity profiles that are assigned to users, in the App server section, add the CylancePERSONA Mobile entitlement. Add the following app servers: • receiver.analytics.blackberry.com • discovery.bis.blackberry.com • scoring.bissanalytics.blackberry.com • service.bis.blackberry.com • actor.ca1.bis.blackberry.com For each app server, specify port 443, primary priority, and a direct connection. Alternatively, you can manage device connections to the services using other configuration options available in the BlackBerry Dynamics connectivity profile. For more information, see Create a BlackBerry Dynamics connectivity profile in the UEM Administration content.

Using the analytics portal

You configure and manage CylancePERSONA Mobile using a browser-based console known as the Persona Analytics Portal. CylancePERSONA administrators can use one of the following methods to access the portal:

- Browse to https://personaanalytics.blackberry.com/*<Organization_SRP_ID>*
- In the UEM management console, on the menu bar, click CylancePERSONA > Analytics.

You use the UEM management console to enable CylancePERSONA and to assign CylancePERSONA Mobile administrator roles to users. You perform all other configuration and management tasks in the portal.

By default, privacy mode is enabled in the portal to mask exact information about user locations from 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 CylancePERSONA administrator role can disable (or re-enable) privacy mode in Settings > General settings > Privacy mode (this action is written to the log file). Administrators with the CylancePERSONA Analytics Administrator role cannot change the privacy mode.

Steps to configure and use CylancePERSONA Mobile

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

Step	Action
1	Enable CylancePERSONA Mobile in your UEM domain.
2	Assign the CylancePERSONA Mobile administrator role to an administrator.
3	Optional customization: • Specify how long CylancePERSONA Mobile retains data • Customize the risk engines
4	Create UEM user groups that you will associate with risk levels.
5	Optional: Define geozones to enforce security standards for specific locations.
6	Create a BlackBerry Persona policy.
7	Assign a BlackBerry Persona policy to users and groups.
8	Create a BlackBerry Enterprise Identity authentication policy to set the authentication requirements for different risk levels. Assign the policy to users and groups.
9	Change the operating mode.
10	View user and event statistics.

Enable CylancePERSONA Mobile in your UEM domain

Before you begin:

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

1. In the management console, on the menu bar, click **Settings > Services**.
2. Locate the CylancePERSONA 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 CylancePERSONA Mobile administrator role to an administrator.

Assign the CylancePERSONA Mobile administrator role to an administrator

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

Note: In the UEM management console, the CylancePERSONA Mobile administrator role is displayed as BlackBerry Persona Administrator.

Before you begin: Enable CylancePERSONA Mobile in your UEM domain.

1. In the UEM management console, on the menu bar, click **BlackBerry Persona > Administrators**.
2. Click .
3. Search for and select the user account that you want to make a CylancePERSONA Mobile 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:
    - To give the user full management permissions for the Persona Analytics Portal and the ability to assign CylancePERSONA Mobile administrator roles to users, click **BlackBerry Persona Administrator**.
    - To give the user read-only access to the Persona Analytics Portal, click **BlackBerry Persona 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 portal.
- Optional: Specify how long CylancePERSONA Mobile retains data.
- Optional: Customize the risk engines.
- Create user groups to define security standards for different risk levels.

Specify how long CylancePERSONA Mobile retains data

You can specify how long you want the CylancePERSONA Mobile services to retain the data that is collected and used for risk assessments. By default, CylancePERSONA Mobile retains data for 30 days.

Before you begin: Assign the CylancePERSONA Mobile administrator role to an administrator.

1. In the Persona Analytics Portal, click **Settings > General settings**.
2. In the **Data retention** section, in the **User data retention (in days)** field, specify a value between 1 and 30.

3. Click **Save**.

Customize the risk engines

You can choose which risk engines you want CylancePERSONA Mobile to use. For example, you can choose to turn off the identity risk engines (behavioral pattern, IP address, and continuous authentication app anomaly) and have CylancePERSONA determine a user's risk level and corresponding actions using defined geozones and learned geozones only. If you disable a risk engine, the corresponding scoring and risk actions for all users are disabled, regardless of whether actions are configured for that risk engine in an individual policy. Enable the risk engines that meet your organization's security standards.

You can customize the risk score ranges for behavioral risk and learned geozone risk. The default risk ranges are:

Risk level	Behavioral risk score (%)	Learned geozone risk range (upper limit of the distance from a learned geozone)
Low	0 - 40	150 yards
Medium	40 - 80	10 miles
High	80 - 100	> 10 miles

Before you begin:

- Assign the CylancePERSONA Mobile administrator role to an administrator.
- Optional: Specify how long CylancePERSONA Mobile retains data.

1. In the Persona Analytics Portal, on the menu bar, click **Settings > Risk engines.**
2. In the **Identity risk** section, enable or disable the **Behavioral pattern risk** engine. By default, the Behavioral pattern risk is enabled.
3. If you want to change the behavioral risk score ranges, in the **Behavioral pattern risk** section, click and drag the sliders.
4. Enable or disable the **IP address** risk engine. If IP address risk factors are enabled, you must configure trusted and untrusted IP addresses in Settings. Trusted IP addresses are automatically treated as low risk, and untrusted IP addresses are treated as critical risk. You can specify the risk levels that are applied for undefined and undetected IP addresses. By default, this risk engine is disabled.
5. If you enabled IP address risk, in the drop-down lists, set the risk level that you want to apply to **Undefined** and **Undetected** IP addresses. By default, these IP addresses are treated as medium risk.
6. Enable or disable the **Continuous Authentication app anomaly** risk engine. By default this risk engine is enabled.
7. If Continuous Authentication app anomaly risk is enabled, in the **Risk factor** section, do the following:
    a) Move the slider under **Setting** to set the scoring threshold for when users' app usage should be treated as at risk.
    b) In the drop-down list under **Risk level**, specify the risk level that should be applied when users' app usage is considered at risk. You can select either Critical or High.
8. In the **Geozone risk** section, enable or disable the **Defined geozone** and **Learned geozone** risk engines. By default, these risk engines are enabled.
9. If you want to change the learned geozone risk ranges, in the **Learned geozone risk engine** section, specify the upper limit of the low-risk range and medium-risk range from learned locations.
10. 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 risk levels or for specific geozones that you define. When you create a BlackBerry Persona policy, you will associate each group with one (or more) of the behavioral risk levels, learned geozone risk levels, or defined geozones. Configure each group with the UEM policies, profiles, app assignments, and roles that reflect the desired 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 may include policies and profiles that are more restrictive and have greater security requirements than a 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 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: Customize the risk engines.
- 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.

1. In the UEM 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 for the behavioral or geozone risk level that the group is intended for.

   Note: You must assign the CylancePERSONA Mobile entitlement to each group. For more information, see CylancePERSONA Mobile software requirements.
5. Click **Add**.

After you finish:

- Optional: Define geozones.
- Create a BlackBerry Persona policy.
- Depending on how you choose to configure your UEM environment and manage the automatic assignment of policies, profiles, roles, and apps using CylancePERSONA, there may be conflicting assignments that UEM must resolve. See Resolving conflicting assignments and precedence rules.

Create a BlackBerry Dynamics override profile

You can create a override profile and apply it in a BlackBerry Persona policy. When the device is at risk, the BlackBerry Dynamics override profile is applied and supersedes the profile that is assigned in UEM.

1. In the UEM management console, on the menu bar, click **Policies and Profiles**.
2. Click **Policy > BlackBerry Persona > BlackBerry Dynamics override**.

3. Click +.
4. Type a name and description for the profile.
5. Configure the appropriate values for the profile settings. For more information about each profile setting, see BlackBerry Dynamics profile settings.
6. Click **Save**.

Add whitelisted or blacklisted IP addresses

If IP address risk factors are enabled, you must configure trusted and untrusted IP addresses. Trusted IP addresses are automatically treated as low risk, and untrusted IP addresses are treated as critical risk. You can specify the risk levels that are applied for undefined and undetected IP addresses.

You can add discrete IP addresses, IP address ranges, or use CIDR notation to include subnets.

Note: If the same IP addresses are included in a trusted and untrusted IP address configuration, the trusted configuration takes precedence automatically and they are treated as low risk.

1. In the Persona Analytics Portal, on the menu bar, click **Settings** > **IP addresses**.
2. On the **IP address configuration** page, do one of the following:
   a) To add whitelisted IP addresses, click the **Trusted IP addresses** tab.
   b) To add blacklisted IP addresses, click the **Untrusted IP addresses** tab.
3. Click +.
4. In the Trusted IP addresses or Untrusted IP addresses dialog box, in the **Name** field, type a name for the list.
5. In the IP addresses pane, enter a discrete IP address, an IP address range, or define a subnet using CIDR.
6. Click **Save**.

After you finish: Create a BlackBerry Persona policy .

Define geozones

You can define geozones if you want to enforce specific security standards while users occupy those locations. For example, you can define a geozone for a certain office location and associate it 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 (the overall assessment is also impacted by the user's current identity risk assessment). When you define a geozone, you assign it a low, medium, or high risk level. When you configure a BlackBerry Persona policy, you can add a defined geozone that will take precedence over the regular geozone risk actions in the policy (see Create a BlackBerry Persona policy).

You can choose whether you want CylancePERSONA Mobile 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.

Before you begin: Create user groups to define security standards for different risk levels.

1. In the Persona Analytics Portal, on the menu bar, click **Settings > Geozones**.
2. On the map pane, in the **Add a geozone** field, type a location (for example, a city). As you type, suggested locations are displayed. 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.

3. 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.
4. 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.
5. Click **Add**.

After you finish:

- To export a .csv file with the displayed geozones, click ➔.
- Create a BlackBerry Persona policy.

Create a BlackBerry Persona policy

You create a BlackBerry Persona policy to define which risk engines you want CylancePERSONA Mobile to use to determine user risk levels and the actions that the service should take for different types and levels of risk. How you configure the policy determines how CylancePERSONA enforces adaptive security standards that are appropriate for each user's current activity and context.

CylancePERSONA offers several actions for the different types and levels of risk, from enforcing UEM group assignments to temporarily blocking BlackBerry Dynamics apps. For more information about how CylancePERSONA resolves conflicting assignments, see Resolving conflicting assignments and precedence rules.

Before you begin:

- Create user groups to define security standards for different risk levels.
- Optional: Create a BlackBerry Dynamics override profile
- Optional: Define geozones.

1. In the Persona Analytics Portal, on the menu bar, click **Policies**.
2. Click +.
3. Type a name and description for the policy.
4. If you don't want CylancePERSONA to take action for identity risk levels, turn off **Behavioral pattern risk** , **IP address risk**, and **App anomaly risk** and skip to step 8.
5. If IP address risk is enabled, by default, all trusted and untrusted IP address configurations are applied. If you want the policy to apply to specific configurations, do the following:
   a) In the **Critical** risk row, in the **IP address** panel, click **All untrusted IP addresses** and clear the check box.
   b) Select the IP address configurations that you want the policy to apply to.
   c) In the **Low** risk row, in the **IP address** panel, click **All trusted IP addresses** and clear the check box.
   d) Select the IP address configurations that you want the policy to apply to.
6. To configure an action for a behavioral pattern or app anomaly risk, click + next to the risk level and do any of the following:

- Click **Assign to UEM group**. Select a group from the list.
- Click **BlackBerry Dynamics apps action** and do one of the following:
  - Click **Assign BlackBerry Dynamics override profile**. Select a profile from the list.
  - Click **Block all BlackBerry Dynamics apps**.
  - Click **Block the BlackBerry Dynamics app that initiated the request**.

The Block all BlackBerry Dynamics apps and Block the BlackBerry Dynamics app that initiated the action are available for the Critical and High risk levels only.

7. To allow users to reduce their behavioral risk level to low by completing a BlackBerry 2FA authentication prompt, do the following:

   a) In the **Identity risk** section, click **Automatic risk reduction**.
   b) In the drop-down list, click the risk levels that will allow automatic risk reduction.
   c) Click **Apply**.

   Note: If a user successfully authenticates to access a BlackBerry Dynamics app, the user cannot be prompted for another authentication (for example, a continuous authentication prompt or automatic risk reduction prompt) for a grace period of at least 5 minutes.

8. Choose one of the following methods to manage geozone risk levels and actions:

Method	Steps
• Use learned geozones • Do not use defined geozones	**a.** Verify that **Learned geozone risk** is turned on. **b.** Turn off **Defined geozone risk**. **c.** To configure an action for a learned geozone risk level, click + next to a risk level and do any of the following: • Click **Assign to UEM group**. Select a group from the list. • Click **BlackBerry Dynamics apps action** and do one of the following: • Click **Assign BlackBerry Dynamics override profile**. Select a profile from the list. • In the high risk level, click **Block all BlackBerry Dynamics apps**. • In the high risk level, click **Block the BlackBerry Dynamics app that initiated the request**.
• Use learned geozones • Use defined geozones • Optional: Take special actions for certain defined geozones	**a.** Verify that **Learned geozone risk** and **Defined geozone risk** are turned on. **b.** To configure the default risk actions for both learned and defined geozones, click + next to a risk level and do any of the following: • Click **Assign to UEM group**. Select a group from the list. • Click **BlackBerry Dynamics apps action** and do one of the following: • Click **Assign BlackBerry Dynamics override profile**. Select a profile from the list. • For defined geozones, click **Block all BlackBerry Dynamics apps**. • For defined geozones, click **Block the BlackBerry Dynamics app that initiated the request**. **c.** If you want to take special actions for a certain defined geozone, click + in the top-right corner of the table and click the geozone. Click + for the defined geozone and select the desired actions.

Method	Steps
• Do not use learned geozones • Use defined geozones • Optional: Take special actions for certain defined geozones • Optional: Take special actions for users that are not in defined geozones	**a.** Turn off **Learned geozone risk**. **b.** Verify that **Defined geozone risk** is turned on. **c.** To configure an action for all defined geozones set to a certain risk level, click + next to the risk level and do any of the following: • Click **Assign to UEM group**. Select a group from the list. • Click **BlackBerry Dynamics apps action** and do one of the following: ◦ Click **Assign BlackBerry Dynamics override profile**. Select a profile from the list. ◦ Click **Block all BlackBerry Dynamics apps**. ◦ Click **Block the BlackBerry Dynamics app that initiated the request**. **d.** If you want to take special actions for a certain defined geozone, click + in the top-right corner of the table and click the geozone. Click + for the defined geozone and select the desired actions. **e.** If you want to take special actions for users that are not in defined geozones, in the top-right corner of the table, click + **> Undefined geozone**. Click + for the undefined geozone and select the desired actions. **Note:**
• Do not use learned or defined geozones	Turn off **Defined geozone risk** and **Learned geozone risk**.

9. Click **Save**.

After you finish:

- Rank BlackBerry Persona policies.
- Assign a BlackBerry Persona policy to users and groups.

Rank BlackBerry Persona policies

When more than one BlackBerry Persona policy is assigned to a user account or group (through direct assignment or inheritance), the policy ranking determines which policy is assigned. Set the ranking to ensure that the correct policy is applied when a conflict occurs.

For more information about how CylancePERSONA Mobile resolves conflicting assignments, see Resolving conflicting assignments and precedence rules.

1. In the Persona Analytics Portal, on the menu bar, click **Policies**.
2. Click ↓↑.
3. Click the arrows next to the policies to set the ranking.
4. Click **Save**.

After you finish: Assign a BlackBerry Persona policy to users and groups.

Resolving conflicting assignments and precedence rules

A BlackBerry Persona policy can execute only the actions that are configured for the different types and levels of risk. 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 Persona 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 UEM management console. For more information about how to set rankings, see the BlackBerry UEM Administration content.

CylancePERSONA Mobile uses the following precedence rules to determine which risk actions to execute when both identity risk and geozone risk actions are enabled. The rules are executed in the order listed, and processing stops as soon as a rule is satisfied.

In the scenarios below where both identity risk actions and geozone risk actions are executed, all risk actions are aggregated into a pool of actions. If this results in more than one risk action of the same type (for example, more than one group assignment), only one action of that type is executed, with priority given to the identity risk action (unless otherwise noted). For example, in a scenario where identity risk is high and geozone risk is high, and both risk actions are group assignments, only the group assignment for identity risk is executed. In the same scenario, if the identity risk action is a group assignment and the geozone risk action is “Block all BlackBerry Dynamics apps”, both actions are executed.

Critical or high identity risk

- If a user's identity risk (behavioral, IP address, or app anomaly) is critical or high, and any level of geozone risk is processed (high, medium, low), the critical or high identity (whichever is higher) risk actions and the default high geozone risk actions are executed.
- If a user's identity risk (behavioral, IP address, or app anomaly) is critical or high, and the user is in a defined geozone with a custom risk action, the custom risk action for the defined geozone is not executed. Custom risk actions for defined geozones are executed only if identity risk is medium or low or if the behavioral and app anomaly risk engines are disabled.
- If a user's identity risk (behavioral, IP address, or app anomaly) is critical or high, and a risk action is configured for “Undefined geozone”, the risk action for the undefined geozone is not executed. The undefined geozone is considered a custom risk action, so the same rules apply.

Medium or low identity risk

- If a user's identity risk (behavioral or IP address) is medium or low, and the user is in a defined geozone with a custom risk action, the identity risk actions and the custom risk actions for the defined geozone are executed. The custom risk actions of the same type take precedence.
- If a user's identity risk (behavioral or IP address) is medium or low, and the user is in an “Undefined geozone” with custom risk actions, the identity risk actions and the custom risk actions for the undefined geozone are executed. The undefined geozone risk actions of the same type take precedence.
- If a user's identity risk (behavioral or IP address) is medium or low, and the user’s geozone risk (default configuration) is high, the identity risk actions and the high geozone risk actions are executed. The high geozone risk actions of the same type take precedence.
- If a user's identity risk (behavioral or IP address) is medium or low, and the user’s geozone risk (default configuration) is medium or low, the identity risk actions and geozone risk actions are executed.

Assign a BlackBerry Persona policy to users and groups

To put a BlackBerry Persona policy into effect, you must assign it to user accounts or groups.

Before you begin: Create a BlackBerry Persona policy.

1. In the Persona Analytics Portal, on the menu bar, click **Policies**.
2. Click the BlackBerry Persona policy that you want to assign.
3. On the **Applied users and groups** tab, click +.
4. Search for and select a UEM user account or group.
5. Repeat step 4 to assign the policy to additional users and groups.
6. Click **Add**.

If more than one BlackBerry Persona policy is assigned to a user account or group, the policy ranking determines which policy is applied.

After you finish:

- Notify users that they will receive a prompt from BlackBerry Dynamics apps asking whether they want to provide location data. Encourage users to allow BlackBerry Dynamics apps to provide this data. If a user does not, CylancePERSONA Mobile cannot factor the data into the user's risk model.
- BlackBerry Dynamics app users can view information about their current security status in the BlackBerry Dynamics Launcher. The user can view summary information about their current risk levels.
- In the settings of each BlackBerry Dynamics app, users can enable or disable CylancePERSONA (by default, it is enabled). If it is disabled, CylancePERSONA cannot collect data and events from the app. Encourage users to enable this setting so that CylancePERSONA can build and use an accurate risk model.
- Create a BlackBerry Enterprise Identity authentication policy.
- Change the operating mode.

Create a BlackBerry Enterprise Identity authentication policy

CylancePERSONA Mobile 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.

1. In the UEM 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 content.
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 CylancePERSONA risk level or a defined geozone to be a risk factor, select the **BlackBerry Persona** check box. Do any of the following:

- If you want a behavioral risk level to be a risk factor, in the **Identity 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 location data and whether BlackBerry Enterprise Identity can trust the browser. Encourage users to accept both prompts. If a user does not, CylancePERSONA 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 operating mode.

Change the operating mode

CylancePERSONA Mobile has two operating modes:

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

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

See Guidelines for developing risk models for suggestions for developing accurate risk models and verifying whether your environment is ready for active mode.

Before you begin:

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

1. In the Persona Analytics Portal, on the menu bar, click **Settings > General 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 CylancePERSONA policy to users, follow these guidelines to help the CylancePERSONA 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 location 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 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 Persona Analytics Portal and view the Events page. If the CylancePERSONA 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.

View user and event statistics

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

1. Log in to the BlackBerry Intelligent Security Analytics Portal.
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 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 export a .csv file with the displayed results.
   - When you view user details, click 📅 to modify the time frame of the data.
   - 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 corner 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 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 corner 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.

Developing apps that leverage CylancePERSONA Mobile

Enterprise developers can use the SDKs provided by BlackBerry to create custom BlackBerry Dynamics apps that can interact with the CylancePERSONA Mobile services, and leverage CylancePERSONA features such as continuous authentication.

Previously, CylancePERSONA functionality was included in the separate BlackBerry Analytics SDK. As of the BlackBerry Dynamics SDK version 8.0, all BlackBerry Analytics and CylancePERSONA functionality is now built into the BlackBerry Dynamics SDK.

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

Legal notice

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

Published in Canada