



BlackBerry Guard

User Guide

Contents

- Overview..... 4**
 - Product requirements.....5
 - Supported third-party integrations..... 6
 - System requirements..... 6
 - Configuration and firewall settings for Guard syslog mirroring..... 7
 - Email address whitelist.....8
 - Onboarding and configuration.....9
 - About this guide..... 9

- Log in to the portal..... 10**

- Profile..... 11**
 - Reconfigure multi-factor authentication.....11
 - Change your password..... 12

- Dashboard..... 13**

- Contacts..... 14**
 - Create a user..... 14
 - Export a list of users..... 15

- Escalations..... 16**
 - Set the priority of an alert..... 16
 - Assign alerts..... 16
 - Add comments..... 17
 - Close alerts..... 17

- Reports..... 18**
 - Export a report..... 18

- Legal notice..... 19**

Overview

BlackBerry Guard is a subscription-based, 24x7-managed extended detection and response (XDR) service that provides actionable intelligence for customers to prevent threats quickly, while minimizing alert fatigue without requiring additional resources. This service is fully integrated with BlackBerry Protect, BlackBerry Optics, BlackBerry Persona, BlackBerry Gateway, and third-party vendors to provide holistic and unified telemetry across all endpoints and enable highly skilled BlackBerry analysts to threat-hunt through customer environments to find and contain threats, prevent major breaches, and allow organizations to mature their security posture. BlackBerry has the strategy, expertise, and technology to protect an organization by analyzing, preventing, and containing threats as well as large-scale breaches.

BlackBerry Guard requires BlackBerry Protect and BlackBerry Optics, which are a part of the BlackBerry Spark Suite and Cyber Suite. The suites also include BlackBerry Persona and BlackBerry Gateway, which are applicable to BlackBerry Guard Advanced subscriptions. For more information, see the [Product requirements](#).

What's included in the subscription

The following table highlights the features that are included in BlackBerry Guard Advanced and BlackBerry Guard Essentials subscriptions.

The BlackBerry Guard Advanced subscription includes closed-loop communications and access to a Guard analyst to help navigate incidents and provide regular updates and ongoing review of the overall threat prevention status. Optionally, Advanced customers are also eligible to secure services for third-party applications, such as for integrating and managing telemetry data from SIEM.

Feature	BlackBerry Guard Advanced	BlackBerry Guard Essentials
Customized product configuration, optimization, and assurance (including BlackBerry product onboarding)	✓	✓
Email, portal, and mobile alert escalation management	✓	✓
24x7x365 monitoring	✓	✓
Automated and proactive threat hunting (Alert, intelligence, and methodology hunting)	✓	✓
Defined service levels	✓	✓
Outreach for critical alerts	✓	✓
Access to BlackBerry Guard analysts for incident response, guidance, and strategy	✓	
Monthly reports on activity and threat landscape	✓	

Feature	BlackBerry Guard Advanced	BlackBerry Guard Essentials
Quarterly reports and ongoing prevention review with BlackBerry experts	√	
Support for third-party solution integration	√ ¹	

¹ You must obtain a third-party solution (for example, for SIEM integration). For more information, see [Supported third-party integrations](#).

Feature descriptions

- **Customized product configuration, optimization, and assurance:** Leverage the expertise of BlackBerry UES ThreatZero experts for a personalized, white-glove service to optimize the BlackBerry Guard solution.
- **Email alerts and escalation management:** Receive email notifications.
- **24x7x365 monitoring:** BlackBerry Guard analysts are monitoring all day and night on all 365 days of the year to follow up on triggering events.
- **Automated and proactive threat hunting (Alert, intelligence, and methodology hunting):** This includes ongoing collection of artifacts and information to facilitate hunting of potential security threats. Threat hunting occurs using various different methods, including alert-based, intelligence, and methodology hunting, leveraging proven methods that identify potential attacks, data exfiltration, unauthorized access, or other potential vectors of compromise in the environment.
- **Defined service levels:** Service levels for security event investigation, median incident resolution time, and BlackBerry Guard monthly reports are defined.
- **Outreach for critical alerts:** When there is a critical alert, BlackBerry Guard analysts reach out to make sure the customer is aware of the situation.
- **Access to BlackBerry Guard analysts for incident response guidance and strategy:** When a threat has been identified, consult BlackBerry Guard analysts to guide you through your incident response plan. For example, you can engage the BlackBerry Security Services Incident Response team, who will work together with an analyst to guide you to a resolution as quickly as possible.
- **Monthly reports on activity and threat landscape:** Receive monthly reports on activity and the threat landscape.
- **Quarterly reports and ongoing prevention reviews:** BlackBerry experts provide insight and knowledge to help obtain and maintain a state of prevention.
- **Support for third-party solution integration:** Integrate BlackBerry Guard with third-party solutions for managed XDR services in a single unified console to improve visibility and control of security incidents.

Product requirements

Some products such as BlackBerry Protect and Optics are required when you want to subscribe to BlackBerry Guard. The following table lists the products and solutions that BlackBerry Guard supports and highlights which are required, optional, and not applicable for BlackBerry Guard Advanced or BlackBerry Guard Essentials subscriptions.

For example, your organization must have BlackBerry Protect and Optics if you want to subscribe to BlackBerry Guard Advanced. BlackBerry Persona, Gateway, and third-party solution integrations are not available if you want to subscribe to BlackBerry Guard Essentials.

BlackBerry Protect, Optics, Persona, and Gateway are included in the BlackBerry Spark Suite and Cyber Suite.

Product	BlackBerry Guard Advanced	BlackBerry Guard Essentials
BlackBerry Protect	Required	Required
BlackBerry Optics	Required	Required
BlackBerry Persona	Optional ¹	N/A
BlackBerry Gateway	Optional ¹	N/A
Third-party solution integration (for example, for SIEM integration)	Optional ¹	N/A
Incident response retainer (for example, BlackBerry Security Services)	Optional ¹	Optional ¹

¹ If you want to integrate these features, an additional purchase may be required.

Supported third-party integrations

When you integrate BlackBerry Guard with third-party vendors for managed XDR services, you unify endpoint detection and response (EDR) with other security and business tools for improved visibility and control of security incidents across the business in a single unified console. Related telemetry data from various tools across the environment are automatically associated with a single incident, reducing the manual effort and unnecessary context switching. Based on the efficacy, correlation, and actions of incidents from the various telemetry sources, BlackBerry Guard can be optimized to automatically take action against security incidents in real-time.

A BlackBerry Guard Advanced subscription is required to support third-party integrations.

The following table lists the supported third-party solutions that can be integrated with BlackBerry Guard.

Solution	Supported third-party integrations
Security Incident and Event Management (SIEM) technology supports threat detection, compliance, and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources.	<ul style="list-style-type: none"> Exabeam

System requirements

BlackBerry Guard requires the following:

- BlackBerry Protect Desktop agent, BlackBerry Protect app, and Optics agent installed on the endpoints.
- BlackBerry Persona and Gateway agents installed on the endpoints (for BlackBerry Guard Advanced subscriptions)

- The latest Google Authenticator app is required to log in to the Guard console using multi-factor authentication (MFA).

Requirement	Description
Agent versions	<ul style="list-style-type: none"> • Windows and Linux: BlackBerry Protect Desktop agent 1580 or later • macOS: BlackBerry Protect Desktop 1584 or later • Android and iOS: BlackBerry Protect app 2.0 or later • BlackBerry Optics 2.5 or later • BlackBerry Persona Desktop 1.2 or later • BlackBerry Gateway (desktop agent) 1.4 or later
Operating system versions	<ul style="list-style-type: none"> • Windows 7 or later • Windows Server 2008 or later • macOS 11 (Big Sur) or later • Linux (for details, see the BlackBerry Protect Desktop Administration Guide) • Android 9 or later • iOS 13 or later
Data storage and collection	BlackBerry Guard collects data that is natively collected by BlackBerry Protect and BlackBerry Optics. Potential forensic data sets may be collected in the case of an incident. Data collection includes information contained in both BlackBerry Protect and BlackBerry Optics alerts as well as data captured through the Package Deploy (Refract) and InstaQuery. Package Deploy has the ability to pull forensic artifacts from the file system at almost any level, while InstaQuery returns filesystem, registry, process, and network information from the customer environment.

Configuration and firewall settings for Guard syslog mirroring

To allow communication between BlackBerry syslog mirroring servers and your organization's syslog servers, you need to configure your organization's firewall and provide a signed certificate to BlackBerry. The following table lists the IP addresses that you should allow based on the your assigned region for the BlackBerry UES management console, as well as information about the signed certificate.

Item	Description
Source IP address (from BlackBerry)	<p>Based on your assigned region, allow the appropriate IP address from BlackBerry:</p> <ul style="list-style-type: none"> • US: 52.202.215.1 • EU: 52.29.124.76 • JP: 35.73.65.169 • AU: 54.206.75.195 • SA: 54.232.154.173

Item	Description
Destination IP address	The IP address of your organization's syslog server. This IP address typically matches the configuration in the BlackBerry UES management console.
Port	The port for your organization's syslog server. This port typically matches the configuration in the UES management console.
Protocol	<ul style="list-style-type: none"> TCP
Signed certificate	<p>A signed certificate is required to encrypt traffic and establish a trusted connection using mTLS authentication.</p> <ul style="list-style-type: none"> BlackBerry provides a certificate signing request (.csr) to your organization. Verify that TLS Web Server Authentication, TLS Web Client Authentication are present when signing the certificate. When signing the certificate, use the same certificate authority as your organization's syslog server. <pre>#example command to sign a certificate openssl x509 -req -CA rootCA.crt - CAkey rootCA.key -in blackberry.csr -out blackberry.crt -days 3650</pre>

Email address whitelist

You can expect to receive email messages from BlackBerry Guard and analysts. To prevent the email messages from being blocked or marked as spam, it is recommended that your email software is configured to allow messages from the certain addresses and domains. The following table lists the email addresses and domains that you should whitelist:

Email address or domain	Description
admin@portal.cylance.io	This email address is used for email notifications from the BlackBerry UES management console, such as invitations and escalations for BlackBerry Protect and BlackBerry Optics.
noreply@blackberry.com	This email address is used for email notifications from BlackBerry Guard, such as invitations and onboarding email messages.
*.blackberry.com	You may receive email messages, such as reports, from analysts that have an email address in this domain.

Email address or domain	Description
*.service-now.com	You may receive automated email messages, such as incident escalation notifications, from BlackBerry Guard that have an email address in this domain.

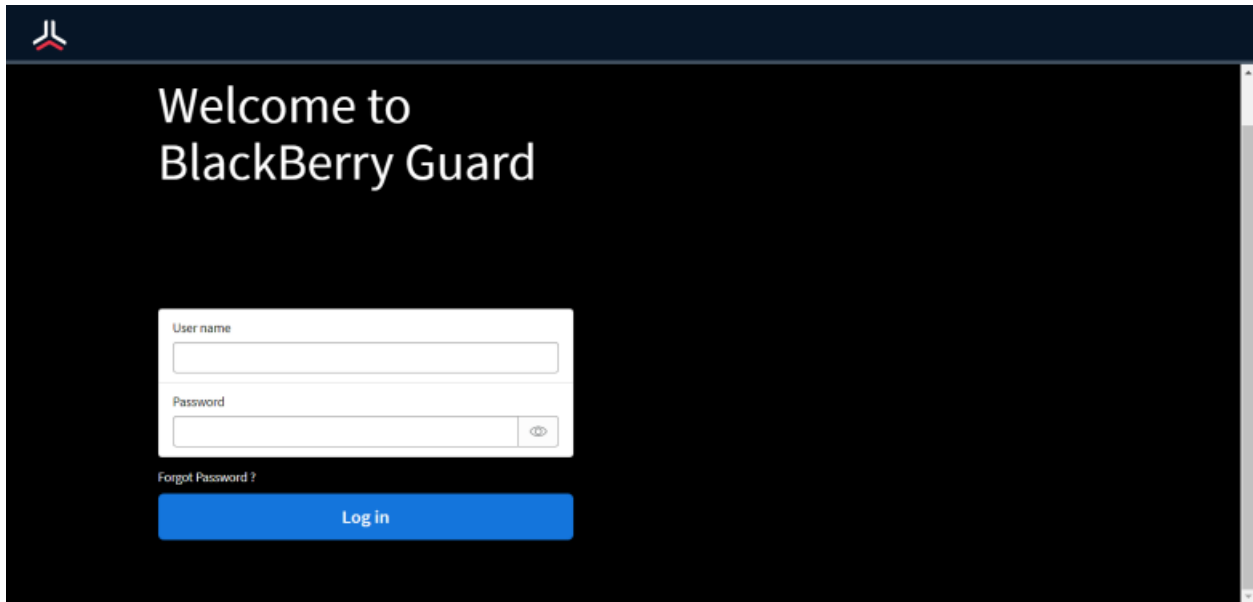
Onboarding and configuration

BlackBerry Guard is deployed through a proven onboarding process led by a ThreatZero expert while leveraging BlackBerry Protect, Optics, Persona, and Gateway agent technology. When the deployment process is complete, you are granted access to a transparent web portal where you can manage threats to the environment.

About this guide

This guide helps users become familiar with the Guard portal that they can use to engage with Guard analysts and their 24x7 managed detection and response offerings. BlackBerry recommends that BlackBerry Guard users become familiar with the capabilities of BlackBerry UES while leveraging the product. For more information about BlackBerry UES and its components, see the [BlackBerry UES overview content](#).

Log in to the portal



When you are invited to use the BlackBerry Guard portal, you receive an email with login information. Click the link in the email and follow the instructions on the screen to set a new password and set up multi-factor authentication using the Google Authenticator app to complete the registration process. The authenticator app is used to generate a multi-factor code that is required each time you log in to the BlackBerry Guard portal.

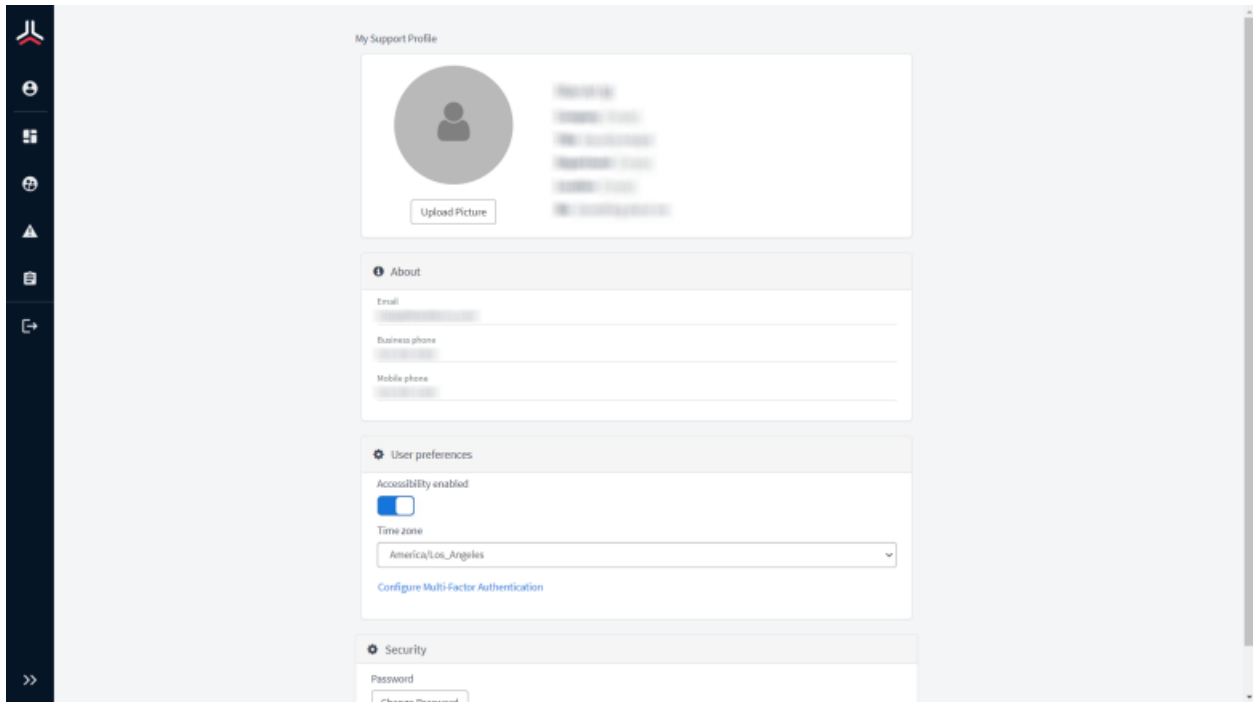
Before any of your organization's users can access the BlackBerry Guard portal, an administrator in your organization must log in and accept the relevant end user license agreements: the BlackBerry Solution License Agreement and the Professional Services Agreement.

Before you begin: You must download and install an authenticator app, such as Google Authenticator, on your mobile device.

1. Click the portal link in the email invitation.
2. Enter your username and password.
3. If prompted, change and confirm your password.
4. Enter the six-digit code displayed in the authenticator app. If you're logging in for the first time, follow the instructions on the screen to set up multi-factor authentication.
 - a) On your mobile device, open the Google Authenticator app.
 - b) Tap **+ > Scan a QR code** to scan the QR code that is displayed on the screen.
 - c) On your computer, in the **6-digit code** field, enter the code that the authenticator app generated.
 - d) Tap **Pair device and login**.
5. If it is displayed, read the **BlackBerry Solution License Agreement** and the **Professional Services Agreement** and select the checkbox to agree to them.

The portal dashboard opens. You are logged in.

Profile



On the Profile screen, you can fill in your user profile to add information about yourself, including contact information. You can do the following:

- Set your location
- Fill in your bio
- Add contact information such as email and phone numbers
- Enable accessibility
- Set your time zone
- Reconfigure multi-factor authentication
- Change your password

Reconfigure multi-factor authentication

When you reconfigure multi-factor authentication, you can generate new codes and invalidate codes that are generated on previously-configured devices (for example, if your device was lost or stolen), or you can add other devices that will generate the same code.

If you are trying to log in and you have lost access to your device that you already configured with multi-factor authentication, click the **Click here to receive a one time code via email** option at the top of the **2-Factor Authentication** screen. After you log in, you can follow these steps to reconfigure it.

Before you begin: You must download and install an authenticator app, such as Google Authenticator, on your mobile device.

1. On the menu, click **Profiles**.
2. In the **User preferences** section, click **Configure Multi-Factor Authentication**.
A dialog with a QR Code appears.

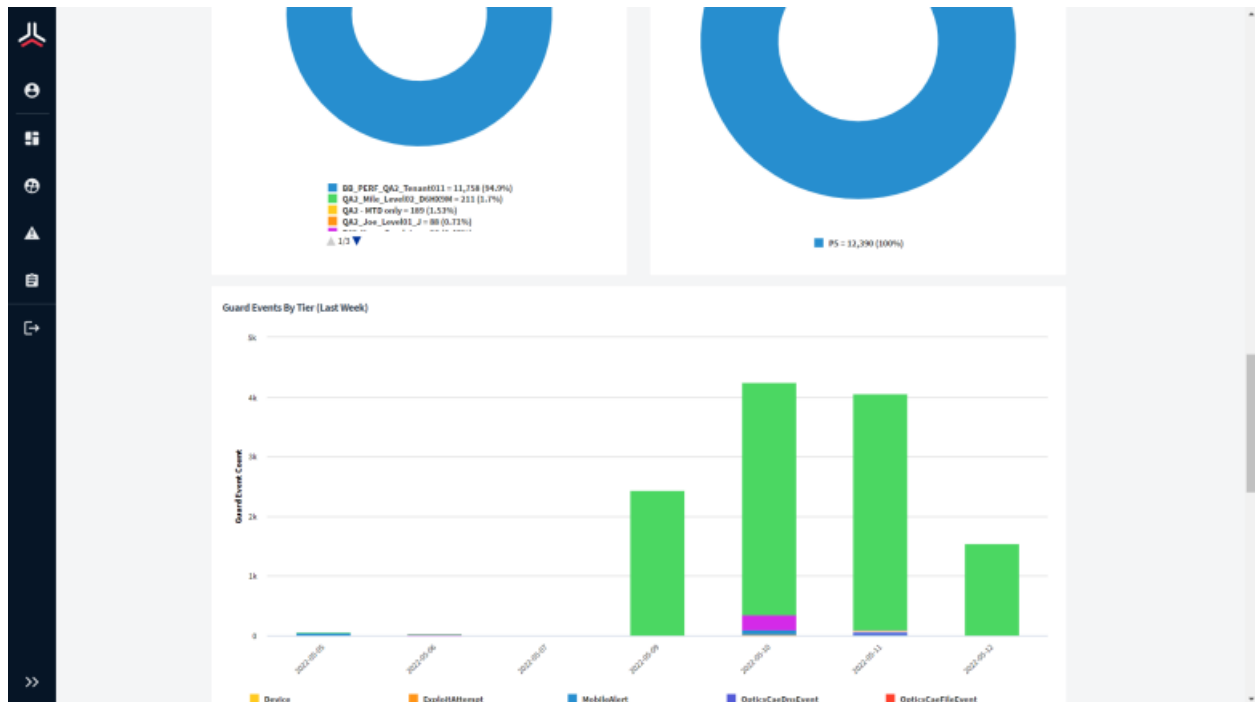
3. Do one of the following:
 - If you want to generate new codes and invalidate codes that are generated on previously configured devices (for example, if your device was lost or stolen), click **Generate a new code** and **OK** to confirm.
 - If you want to keep codes generated on previously-configured devices valid and add another device that will generate the same code, skip this step.
4. Follow the instructions on the screen to configure multi-factor authentication:
 - a) On your mobile device, open the Google Authenticator app.
 - b) Tap **+ > Scan a QR code** to scan the QR Code that is displayed on the screen.
 - c) If you chose to generate new codes, enter the new code and tap **Pair device**.

At the top of the dialog box, a **Multi-factor authentication has been successfully configured** message displays in green.

Change your password

1. On the menu, click **Profiles**.
2. In the **Security** section, click **Change Password**.
3. In the **Current Password** field, enter your current password.
4. In the **New password** field, enter your new password.
5. In the **Confirm password** field, confirm your new password.
6. Click **Change**.

Dashboard

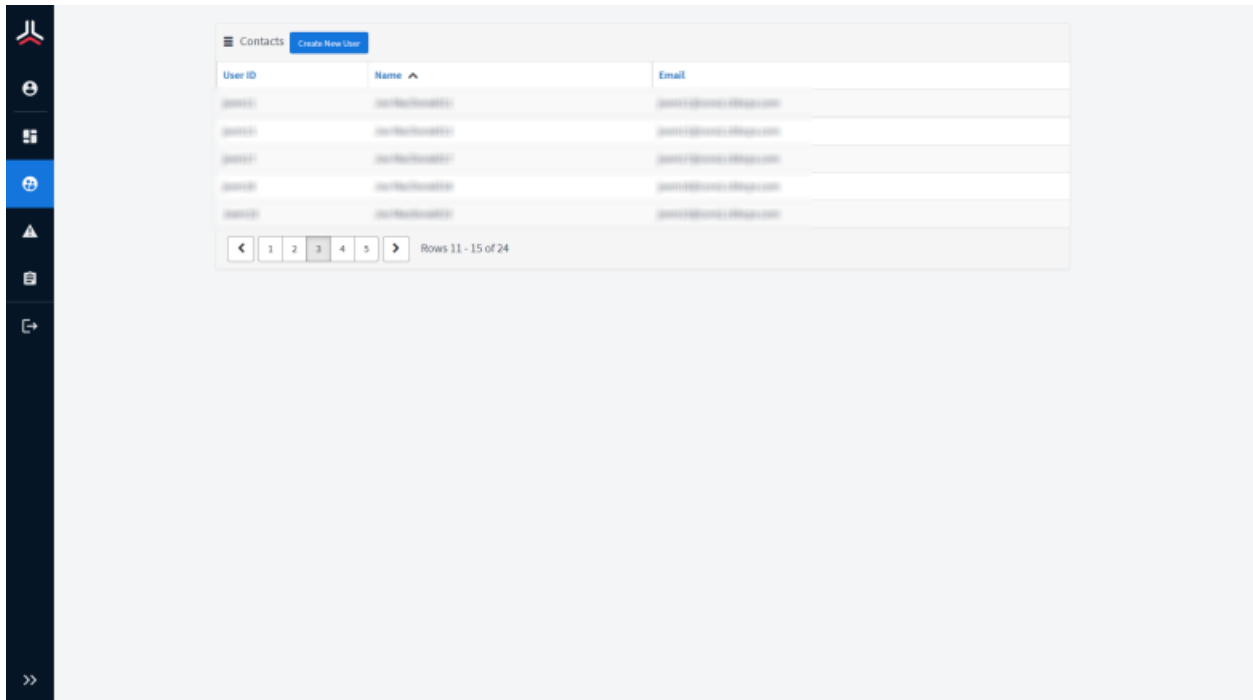


The BlackBerry Guard Dashboard page displays a high-level view of various alert metrics for your organization. You can adjust the timeframe of the metrics to the last 24 hours, the last week, or the last month.

The following are some examples of metrics that are displayed in the dashboard:

- Number of open alerts for your organization
- Number of closed alerts for your organization
- Number of alerts that were escalated for your organization
- Mean time to detect
- Mean time to respond
- Number of threat detections that missed the service levels
- Number of threat responses that missed the service levels
- Number of events by tier (trigger event, observation, whitelist, discard)
- Number of events by category
- Number of alerts by organization
- Number of alerts by priority
- Number of closed alerts by priority
- Number of closed alerts by category

Contacts



On the Contacts page, administrators in an organization can add and manage their BlackBerry Guard users. They can also export a list of users in PDF, CSV, and Excel format.

Create a user

If you are an administrator of an organization, you can add users so that they can use the BlackBerry Guard portal. If you manage multiple organization accounts in BlackBerry Guard, you can select the organization that the user can access (if you select a parent organization, they can also access its child organizations).


If you want to create an administrator, you must contact BlackBerry Support.

1. On the menu, click **Contacts**.
2. Click **Create New User**.
3. Enter the following required information:
 - User ID
 - Account
 - First Name
 - Last Name
 - Email address
4. Optionally, enter the following information.
 - Business Phone
 - Mobile Phone
 - Title
 - Language

5. Click **Submit**.

After you finish: The user receives an email invitation to access the BlackBerry Guard portal. They must follow the instructions in the email message to complete the registration.

Export a list of users

1. On the menu, click **Contacts**.
2. Click  and do one of the following:
 - Click **Export as PDF**.
 - Click **Export as Excel**.
 - Click **Export as CSV**.
3. Save the file to your computer.

Escalations

Escalations

1 Total alerts 29 Total Escalated 7 Open Escalations


Search for escalations

Case Number	Artifact of interest	Host/ Device name	Priority	Severity	Trigger Product	Assigned to	Timestamp	Status
CS0001085	ProtectMobileAlert	10.10.10.10	P5	High	Protect Mobile		2022-05-11 10:29:02	New
CS0001084	threat_found	10.10.10.10	P5	High	Protect		2022-05-09 21:17:45	New
CS0001083	threat_found	10.10.10.10	P5	High	Protect		2022-05-09 21:11:59	New
CS0001082	threat_found	10.10.10.10	P5	High	Protect		2022-05-09 21:05:05	New
CS0001081	threat_found	10.10.10.10	P5	High	Protect		2022-04-26 09:02:56	Closed


< 1 2 3 4 5 6 7 > Rows 1 - 5 of 31

An alert is a collection of events that are correlated into a single incident. The Escalations page provides users detail and access to the triggering events captured from BlackBerry Protect and BlackBerry Optics. When an analyst identifies a threat, they escalate the alert so that designated groups in your organization are notified about them and view them on the Escalations page. Each alert that was escalated displays as a separate escalation on this page and can be assigned to you or another group member. You can add comments to escalations to communicate with BlackBerry Guard analysts about the threat.

On the Escalations page, you can do the following:

- Click an alert or escalation to view its details.
- Enter keywords in the search field to filter the alerts list.
- To refresh the list of escalations, click .

Set the priority of an alert

1. Open the details view of an alert.
2. Beside **Priority**, click .
3. Select the priority that you want to set for the alert.
4. Click **Save**.

Assign alerts

From the Alerts page, you can assign all alerts to yourself, or just individual incidents.

1. To assign all alerts in the search to yourself, select the Alerts checkbox. This selects all alerts.

2. Click **Assign to Me**.
3. To assign an individual alert to yourself, locate the alert on the page, then click **Assign to Me**. If an alert is assigned to you, a strikethrough displays over the Assign To Me link.

Add comments

You can add comments when you view the details of an alert. Use comments to share useful information and note the actions that need to be taken to resolve the threat. Comments in the conversation are shown in reverse chronological order. When you add comments, BlackBerry Guard sends email notifications.

1. On the menu, click **Escalations**.
2. Click the alert that you want to add a comment to.
3. On the right pane, in the **Activity** tab, type your comment in the **Comments** box.
4. If you want to attach a file, click **Add attachments** and select the file that you want to add.
5. Click **Send**.
The comment is added to the conversation and the text box is cleared.

Close alerts

1. Do one of the following:
 - To close an individual alert, at the bottom of the alert, click **Close**.
 - To close all alerts, in the top right of the page beside Bulk Actions, click **Close**. The Close Alert dialog displays.
2. Select whether the alert was Resolved or Unresolved.
3. In the Resolution Description box, enter a reason for closing the alert.
4. Select a priority for this alert from the drop-down list.
5. Select a category for this alert from the drop-down list.
6. Click on **Close Alert**.

Reports

The screenshot shows a dashboard with a dark sidebar on the left containing navigation icons. The main content area is divided into two sections. The top section, titled 'Closed Alerts by Trigger Event Type', displays a table with columns for 'Event Type' and 'Closed'. The bottom section, titled 'Escalated Alerts Detail Report', displays a table with columns for 'Case Number', 'Alert ID', 'Host/ Device name', 'Artifact of Interest', 'Timestamp', 'Priority', 'Category', and 'Status'.

Event Type ↑	Closed
Device	2022-05-10 11:59:40
Device	2022-05-10 11:59:49
ExploitAttempt	2022-05-10 11:59:41
ExploitAttempt	2022-05-10 11:59:41
ExploitAttempt	2022-05-10 11:59:42

Rows 1 - 5 of 426


Case Number ↑	Alert ID	Host/ Device name	Artifact of Interest	Timestamp	Priority	Category	St
CS0001078	CS0001078	Host: [REDACTED]	threat_found	2022-04-26 08:29:43	Low	Issue	Ne
CS0001082	CS0001082	Host: [REDACTED]	threat_found	2022-05-09 21:05:05	Low	Issue	Ne
CS0001083	CS0001083	Host: [REDACTED]	threat_found	2022-05-09 21:11:59	Low	Issue	Ne
CS0001084	CS0001084	Host: [REDACTED]	threat_found	2022-05-09 21:17:45	Low	Issue	Ne
CS0001085	CS0001085	Host: [REDACTED]	ProtectMobileAlert	2022-05-11	Low	Issue	Ne

The BlackBerry Guard Reports page displays more detailed alert metrics for your organization. Beside each alert metric, you can choose to export a report in XLS, CSV, or PDF format.

The following are some examples of reports that are displayed on this dashboard:

- Closed alerts by event trigger type
- Escalated alerts detail
- User last login

Export a report

1. On the menu, click **Reports**.
2. Beside the report that you want to export, click  and do one of the following:
 - Click **Export as PDF**.
 - Click **Export as Excel**.
 - Click **Export as CSV**.
3. Save the file to your computer.

Legal notice

©2022 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, CYLANCE and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners.

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.

Use of this BlackBerry product and/or service is governed by a separate license or other agreement with BlackBerry applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY SUCH WRITTEN AGREEMENTS OR OTHER WARRANTIES PROVIDED BY BLACKBERRY.

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