BlackBerry Gateway

Overview and Administration Guide

October 2021

Contents

What is BlackBerry Gateway?

BlackBerry Gateway provides zero trust network access (ZTNA) that both gives your users access to your extended network perimeter and protects your extended network from threats. Organizations today face a challenging environment as cybersecurity threats become more sophisticated and pervasive while the numbers of connected enterprise endpoints and the amount of data sent to and stored in cloud services instead of within the traditional network perimeter grows exponentially. ZTNA modernizes network security while simultaneously enhancing and improving the network experience for end users. ZTNA trusts nothing and no one by default. Every user, endpoint, and network are assumed to be potentially hostile and no user can access anything until they prove who they are, that their access is authorized, that they're not acting maliciously, and that the local network they are connected to is not compromised.

BlackBerry Gateway protects users' Windows 10 and macOS devices by allowing you to block connections to Internet destinations that you don't want devices to reach, even when the device isn't connected to your network. BlackBerry continually maintains an ever-growing list of unsafe Internet destinations that it can block endpoints from connecting to. If your organization also wants to block users from visiting specific sites that don't meet your acceptable use standards, you can create policies to specify additional destinations that all users or specific users or groups can't access.

In addition to protecting devices, BlackBerry Gateway protects access to your organization's private network and cloud-based applications by continuously analyzing whether users' actions are expected or anomalous behavior. If BlackBerry Gateway determines that a user's recent usage pattern indicates a high-risk, it blocks connections by the user until the risk level is mitigated.

BlackBerry Gateway also supports using source IP pinning when it forwards connections to your cloud services. If your SaaS applications are configured to accept connections only from specific IP addresses, such as your organization's own IP addresses, you can add BlackBerry Gateway source IP addresses obtained by your organization to the allowed list. For users working remotely, this means you can secure access between your users and cloud-based applications using source IP pinning without requiring them to use your organization's VPN, which can reduce the traffic on your network and improve connections for users.

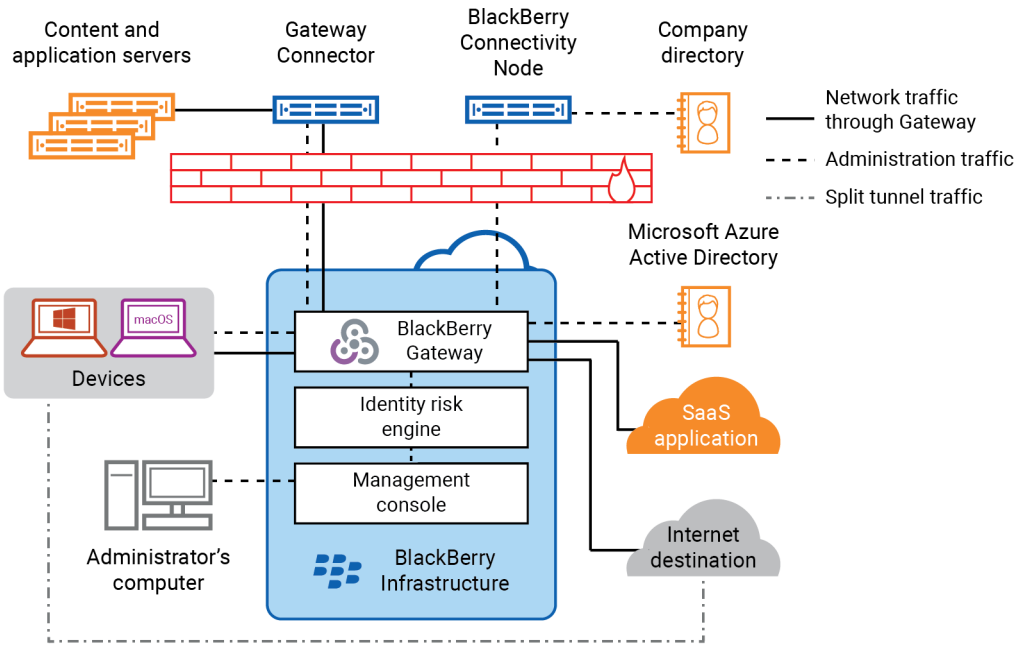
Key BlackBerry Gateway features

BlackBerry Gateway offers the following features.

Feature	Description
Continuous evaluation of Internet destinations	BlackBerry uses machine learning, IP reputation, and risk scoring to maintain an ever-evolving list of malicious Internet destinations. BlackBerry Gateway blocks devices from connecting to these destinations, saving your organization the work of manually compiling and maintaining its own list.
Continuous identity risk analysis	The identity risk engine uses machine learning to continuously evaluate user behavior. Network anomaly events are detected when a Gateway user's network usage pattern is not consistent with past behavior. When an unusual network event is detected, Gateway can dynamically override the user's network access control policy and block the connection.

Feature	Description
Segmented private network access	You can install Gateway Connectors on-premises and on private cloud networks to provide network access to remote devices without changing network topology or routing, and without opening firewall holes for incoming traffic. Access through Gateway offers strong isolation; only the parts of the network you choose are exposed to endpoints, and endpoints are not exposed to the whole private network.
Support for IP-pinned services	Most SaaS applications allow source IP pinning to limit access only to connections from a specific range of trusted IP addresses. By limiting users to connections only through trusted entry points, organizations have an additional level of verification that the user is entitled to use the service. Your organization may already use this method to limit access to a SaaS application to connections from IP address used by devices connected to your organization's network. For users working remotely without using BlackBerry Gateway, this means that all traffic between remote devices and a SaaS application must travel over VPN to your network and then to the SaaS application. BlackBerry Gateway allows you to reserve Gateway IP addresses that are dedicated to your organization. You can use these IP addresses for source IP pinning in addition to your organization's IP addresses, providing the same level of security without requiring remote users to be connected to your organization's VPN.
Split tunneling	You can allow remote users to connect to safe public Internet sites directly over the Internet without tunneling through BlackBerry Gateway.
Industry-leading tunnel technology	BlackBerry Gateway provides advanced layer 3 encryption for IP tunnels carrying TCP, UDP, and ICMP traffic.
Windows 10 and macOS support	The Gateway Agent installed on devices sends traffic through the tunnel to BlackBerry Gateway and provides users with connection statistics and status information and the ability to disable work mode and stop using Gateway for connections.
Cloud-based unified management console	You can manage policies, Gateway Connectors, users, and groups and monitor traffic using the same cloud-based management console shared by other BlackBerry Unified Endpoint Security products.
Integration with BlackBerry UES products	BlackBerry Gateway is integrated with other BlackBerry Unified Endpoint Security products. BlackBerry UES products share a management console and work together to provide an AI-powered solution for Zero Trust across the spectrum of networks, devices, apps, and people.
Monitor network access and traffic patterns	The Gateway dashboard in the management console displays multiple widgets that show connections, usage patterns, and alerts to help you monitor network traffic.

Architecture: BlackBerry Gateway



Component	Description
BlackBerry Gateway	BlackBerry Gateway is a cloud-based service that provides zero trust network access to provide your users with access to your extended network perimeter and protect devices and your extended network from threats.
Identity risk engine	The identity risk engine uses machine learning to continuously evaluate user behavior and provide adaptive response to network anomaly events.. Network anomaly events are detected when a Gateway user's network usage pattern is not consistent with past behavior. If the percentage of anomalous events exceeds a set threshold, Gateway can dynamically override the user's network access control policy to block network access and require the user to authenticate before they can continue.
Management console	The cloud-based management console allows you to set up, manage, and monitor BlackBerry Gateway and the connections made through it. The management console shared by all BlackBerry Unified Endpoint Security products.
BlackBerry Infrastructure	The BlackBerry Infrastructure is a global private data network distributed across multiple regions that enables and secures data in transit between thousands of organizations and millions of users around the world. It is designed to efficiently manage the transport of data between BlackBerry services and end-user devices. The BlackBerry Infrastructure registers user information for device activation, validates licensing information, and maintains a trusted connection with on-premises BlackBerry components installed behind the firewall and with user's devices inside and outside the firewall.

Component	Description
Gateway Connector	The Gateway Connector is an optional component that you can install behind your firewall and in and in private cloud networks to establish a secure tunnel between the BlackBerry Infrastructure and your private network. The Gateway Connector allows users to communicate with content and application servers behind your firewall using BlackBerry Gateway instead of a traditional VPN.
BlackBerry Connectivity Node	The BlackBerry Connectivity Node is an optional component that allows BlackBerry Gateway to synchronize users and groups with your on-premises Microsoft Active Directory or LDAP directory. BlackBerry Gateway can synchronize users and groups with Azure Active Directory without the BlackBerry Connectivity Node.
Devices	This version of BlackBerry Gateway supports Windows 10 and macOS devices. An agent installed on the device, sends Internet traffic through a secure tunnel to the BlackBerry Infrastructure. Users can enable and disable work mode to specify whether data traffic uses the tunnel to the BlackBerry Infrastructure.
SaaS applications	Software-as-a-Service applications provide cloud-based enterprise software, making apps and data available to users on multiple devices. Applications and data reside mostly on cloud-based servers managed by the vendor, easing deployment and reducing on-premises infrastructure costs, but requiring security measures that extend beyond firewalls and other perimeter-based security methods. BlackBerry Gateway can help secure user access to SaaS applications without requiring traffic to route through your organization's VPN.
Internet destinations	Public Internet destinations include any web site, SaaS application, or other entity with an IP address that a client app can connect to over the Internet. BlackBerry maintains an ever-growing list of destinations know to be malicious. BlackBerry Gateway can block apps on devices from connecting to destinations on the list. If you enable split tunneling, traffic between devices and safe public sites that you specify can go directly over the Internet instead of through BlackBerry Gateway.

How BlackBerry Gateway routes data

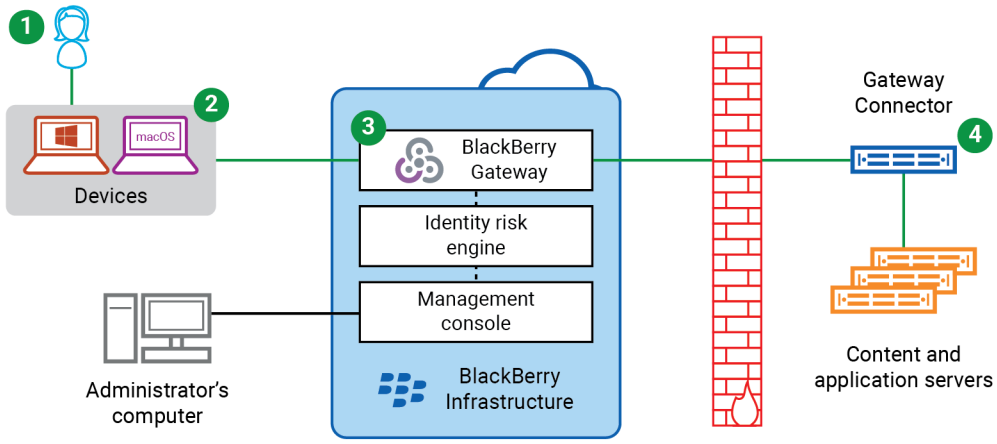
When BlackBerry Gateway is active on a device, Gateway routes network traffic in the following ways.

Destination	Action
Allowed destination on the private network	Users can access destinations on your private network only if they are explicitly allowed by the network access control policy. All data between the device and your private network is encrypted using industry-leading tunnel technology and routed through secure tunnels from the BlackBerry Protect app or Gateway Agent to the BlackBerry Infrastructure and then from the BlackBerry Infrastructure to the Gateway Connector installed behind your firewall.

Destination	Action
Allowed Internet destination	Users can connect to any public Internet destination unless it is explicitly blocked by your network access control policy or determined by BlackBerry to be a potentially malicious destination. Connections to public Internet destinations are routed through the secure tunnel between the BlackBerry Protect app or Gateway Agent and the BlackBerry Infrastructure and then BlackBerry Gateway routes the traffic to the destination. If you enable split tunneling, traffic safe Internet destinations is routed directly to the destination rather than through the tunnel to BlackBerry Gateway. For example, you can choose to reduce the traffic sent through BlackBerry Gateway by allowing traffic to safe public sites to route directly to the destination.
Allowed SaaS app	By default, connections to SaaS apps are routed in the same way as connections to other Internet destinations. If you enable source IP pinning, you can configure your SaaS app tenant to only accept connections from your organization's own IP addresses and BlackBerry Gateway.
Blocked destination on the private network	Users can access destinations on your private network only if they are explicitly allowed by the network access control policy. If the destination is not allowed, BlackBerry Gateway blocks the connection and doesn't route the data to the Gateway Connector.
Blocked Internet destination	If a destination is explicitly blocked by your network access control policy or determined by BlackBerry to be a potentially malicious destination, BlackBerry Gateway can block the connection.

Data flow: Accessing an application or content server on your private network

This data flow describes how data travels between devices and servers on your private network using BlackBerry Gateway.

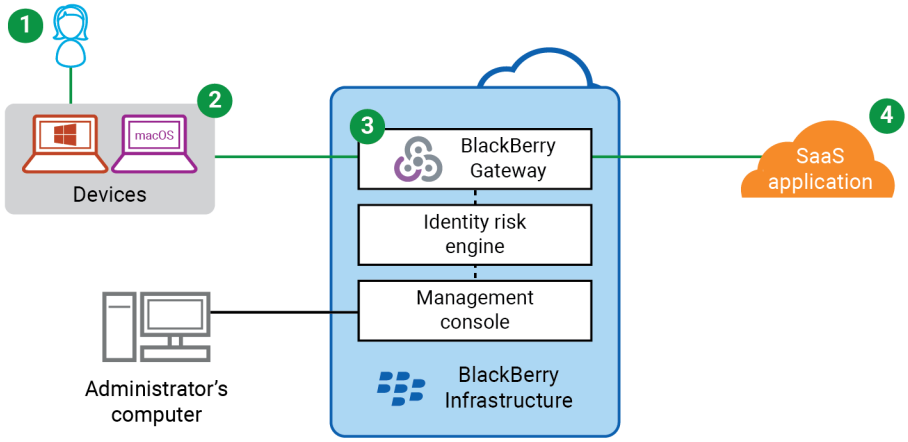


1. The user opens an app and attempts to access a resource on your private network.
2. The Gateway Agent routes the connection through a secure tunnel to BlackBerry Gateway in the BlackBerry Infrastructure.

3. BlackBerry Gateway performs the following actions:
   a. Determines, based on the Network Control policy whether the user has access to that location on the private network.
   b. If the user has access, routes the connection through a secure tunnel to Gateway Connector.
4. The Gateway Connector routes the connection to its destination on the private network.

Data flow: Accessing a cloud-based application

This data flow describes how data travels between devices and a cloud-based SaaS application using BlackBerry Gateway.



1. The user opens an app and attempts to access a cloud-based application outside of your private network.
2. The Gateway Agent sends the encrypted data through a secure tunnel to BlackBerry Gateway in the BlackBerry Infrastructure.
3. BlackBerry Gateway performs the following actions:
   a. Determines, based on the network control policy whether the user has access to that location.
   b. If the user has access, sends the encrypted data to the SaaS application.
4. If source IP pinning is enabled, the SaaS application verifies that the connection is coming from an IP address that is associated with your BlackBerry Gateway tenant before allowing access.

Sign in to BlackBerry Gateway

After BlackBerry Gateway is activated for your organization, you will receive an email message with sign-in information. The first person in your organization to sign in to the management console must do so using the account that was created for the email address that the message was sent to. After signing in, you can give administrator access to additional users.

1. Click the link in the email message to open the sign-in page or go to one of the following URLs:
   - **North America:** https://login.cylance.com
   - **Europe** https://login-euc1.cylance.com
2. Type your credentials and click **Sign in**.

   If this is the first time anyone has signed in, you must create a password.

Setting up BlackBerry Gateway

To set up BlackBerry Gateway, perform the following actions.

Steps 1 to 3 are required only if you are installing one or more Gateway Connectors. You must install at least one Gateway Connector if you want to use Gateway to control access to your private network. If you don't install a Gateway Connector, you can use Gateway only to block access to public destinations and secure access to cloud applications using source IP pinning.

Step	Action
1	Specify the addresses that are part of your private network.
2	Specify your private DNS settings and suffixes.
3	If you want to use Gateway to establish a secure tunnel between devices and your private network, Install and set up one or more Gateway connectors.
4	If you want to create user accounts by searching for and importing user data from your company directory, link Gateway to your company directory.
5	Configure network access control policies to manage which Internet and private network destinations Gateway allows and blocks access to.
6	Configure adaptive response options to manage how the identity risk engine monitors and responds to user behavior.
7	Configure enrollment policies to allow users to activate the Gateway Agent on their device.
8	Add users and user groups to Gateway.
9	Assign policies to users and groups.
10	After users have enrolled with Gateway, monitor network connection activity and update settings and users as necessary.

Setting up the BlackBerry Gateway Connector

You install the Gateway Connector using an OVA file. After you install the connector, you must configure it.

To set up the Gateway Connector, perform the following actions.

Step	Action
1	Review the prerequisites.
2	Install the BlackBerry Gateway OVA file.
3	Configure the firewall.
4	Register the connector with the BlackBerry Infrastructure.

Prerequisites: Installing the Connector

You install the Gateway Connector in a VSphere environment that meets the following minimum requirements.

Item	Description
RAM	5 GB
Disk space	2 GB
Number of CPUs	2

Install the BlackBerry Gateway OVA file

Before you begin: Make sure you have permissions to deploy an OVF template into the VSphere environment.

1. Download the BlackBerry Gateway OVA file (blackberry-gateway-connector.ova) to your computer from *myAccount*.
2. Log in to the VSphere environment.
3. Right-click on the cluster where you want to install the BlackBerry Gateway connector and select **Deploy OVF template**.
4. On the **Select an OVF template** screen, select the **Local file** button.
5. Click **Choose Files** and navigate to the blackberry-gateway-connector.ova file.
6. Click **Next**.
7. On the **Select a name and folder** screen, type a name for the virtual machine and click **Next**.
   The default name is blackberry-gateway-connector.
8. On the **Select a computer resource** screen, select a location for the virtual machine and click **Next**.
9. After the compatibility checks are complete, click **Next**.
10. On the **Review details** screen, review the setup information and click **Next**.
11. On the **License agreements** screen, review the license agreement.
12. Select the button beside **I accept all license agreements** and click **Next**.
13. On the **Select storage** screen, for **Virtual disk format**, select Thin Provision.
14. On the **Select networks** screen, configure the **Destination Network** for this BlackBerry Gateway connector.
    Set the **Source Network** to NAT.

15. Click **Next**.
16. On the **Ready to complete** screen, review the configuration settings and click **Finish**.

Configure settings for the Gateway Connector

You can log in to the Gateway Connector to configure a static IP address for the network adapter or change the default password for the connector. For more information on configuring the Gateway Connector with a static IP address, visit the support community to read article 86997.

Note: The Gateway Connector is a minimal install of the Ubuntu operating system, which can operate without a user logging in. You need to log in only if you want to update the default settings.

1. In the vSphere console, click the host name of the Gateway Connector.
2. Click **Launch Remote Console** or **Launch Web Console**.
3. At the UNIX prompt, type the administrator username and press **Enter**.
   The default username is **admin**.
4. Type the administrator password.
   The default password is **admin**.

Configure the firewall

The Gateway Connector runs inside your private network, behind your firewall, and has a private IP address. It connects to the BlackBerry Gateway cloud service with HTTPS and UDP, so you must configure the Connector to reach at least those Internet destinations (via NAT).

The Gateway Connector must be able to use DNS to resolve public BlackBerry Gateway FQDNs to Internet IP addresses. The Connector uses the DNS servers assigned to it by your private network to do this.

For more information about FQDNs, ports, IP address ranges and other firewall requirements, visit support.blackberry.com/community to read article 79017.

Register the connector with the BlackBerry Infrastructure

After you install the Gateway Connector and configure its firewall, you must connect it to the BlackBerry Infrastructure.

1. In a web browser, navigate to the IP address of your Gateway Connector.
2. Click **Advanced**.
3. Review the text about the self-signed certificate and click **Proceed to the HTTPS service**.
4. Accept the self-signed certificate.
5. Reload the HTTPS service page if necessary.
6. In the **URL** field, type the URL of the management console.
   You can find the URL in the management console under **Gateway > Settings > Gateway Connectors**.
7. Click **Register this Connector**. The management console opens.
8. Log in to the management console as an administrator for your tenant.
9. In the **Connector name** field, type a name for the Connector.
10. Review the Connector URL.
11. Click **Save**.

The Connector appears in the list of Gateway Connectors. The STATUS field shows whether or not the private network, its DNS, and health checks are functioning normally.

Check for Gateway Connector updates

You can check whether an update for the Gateway Connector or update for the virtual machine OS is available.

1. Check *my*Account to see whether a new version of the Gateway Connector software is available, and perform one of the following actions:
   - If new connector software is available, download it and reinstall the virtual machine.
   - If no new connector software update is available, check for a Linux OS update.
2. To check for a Linux OS update, click **Settings** > **Network** > **Gateway Connectors**.
3. In the list of installed connectors, look for a **Reboot required** notification.
4. For any connector showing a **Reboot required** notification, restart the virtual machine to finish installing the OS security patches update.

Linking to your company directory

You can configure BlackBerry Gateway to synchronize with your company directory to simplify adding and managing users and groups. Connecting BlackBerry Gateway to a company directory allows your organization create user accounts by searching for and importing user data from the company directory. Directory users can use their directory credentials to connect to Gateway.

You can link to a company directory in two ways.

- If you want to synchronize with Microsoft Azure Active Directory, you can configure Gateway to connect with it.
- If you want to synchronize with an on-premises Microsoft Active Directory, you must install a BlackBerry Connectivity Node to create a secure connection between Gateway and your directory.

To link Gateway to your company directory, you perform the following actions.

Step	Action
1	If you want to link to an on-premises company directory, install a BlackBerry Connectivity Node.
2	Depending on the type of directory you want to connect to, configure BlackBerry Gateway to synchronize with Azure Active Directory or connect to a Microsoft Active Directory.
3	Configure onboarding and offboarding.
4	Configure directory synchronization schedules.

Configure BlackBerry Gateway to synchronize with Azure Active Directory

To configure BlackBerry Gateway to synchronize with Azure Active Directory, you must configure both Azure and Gateway to make the connection.

1. Log in to the Azure portal.
2. Create a new app registration for Azure Active Directory and assign the appropriate settings and permissions.
   a) Add a name for the app.
   b) Specify the account types can use the application or access the API.

c) Select **Web** as the redirect URI type and set the URI as `http://localhost`.
d) Set the following application permissions:
   - Group.Read.All (Application)
   - User.Read (Delegated)
   - User.Read.All (Application)
e) Grant Admin consent to the application.

3. Record the name you assigned to the app and the Application (client) ID.
4. Create a new client secret and record the value of the secret.
5. In the Gateway management console, click **Settings > Directory Connection**.
6. Click **Add Connection**
7. Enter a **Name** for the directory connection and the **Domain** for your Azure Active Directory.
8. In the **Client ID** field, type the application ID generated by the Azure app registration.
9. In the **Client key** field, type the client secret generated by the Azure app registration.
10. Click **Add**.

Installing the BlackBerry Connectivity Node

Follow the instructions in this section to install the BlackBerry Connectivity Node.

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy.

You must install each instance on a dedicated computer.

You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Nodes, all of the directory connections must be configured identically. If one directory connection is missing or incorrectly configured, that BlackBerry Connectivity Node will appear as disabled in the management console.

If you have more than one BlackBerry Connectivity Node, you must upgrade all of them to the same software release.

Note: If you are upgrading multiple BlackBerry Connectivity Nodes, directory services are disabled after the first node is upgraded until all the nodes are upgraded to the same version.

BlackBerry Connectivity Node planning information

Before you install the BlackBerry Connectivity Node, consider the following information.

Hardware

The BlackBerry Connectivity Node must be installed on a dedicated computer that is reserved for technical purposes, instead of a computer that is used for everyday work. The computer must be able to access the Internet and your company directory.

The computer that hosts the BlackBerry Connectivity Node must meet the following hardware requirements:

- 6 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent
- 12 GB of available memory
- 64 GB of disk space

Scalability and high availability

You can install one or more instances of the BlackBerry Connectivity Node to provide redundancy. You must install each instance on a dedicated computer. Use the same company directory configuration for all instances.

Deploy more than one BlackBerry Connectivity Node in a server group to allow for high availability and load balancing.

Prerequisites: Installing the BlackBerry Connectivity Node

- Choose a directory account with read permissions for each configured directory connection that the BlackBerry Connectivity Node can use to access the company directories.
- Use a Windows account with permissions to install and configure software on the computer that will host the BlackBerry Connectivity Node.
- Verify that the following outbound ports are open in your organization's firewall so that the BlackBerry Connectivity Node components can communicate with the BlackBerry Infrastructure (<*region*>.bbsecure.com, for example na.region.com or eu.region.com):
  - 443 (HTTPS) to activate the BlackBerry Connectivity Node
  - 3101 (TCP) for all other outbound connections

Set an environment variable for the Java location

You must install a JRE 8 implementation on the server where you will install BlackBerry Connectivity Node, and you must have an environment variable that points to the Java home location. When you begin the installation, the BlackBerry Connectivity Node verifies that it can find Java. If you have installed the Oracle Java SE Runtime Environment in the default location, the BlackBerry Connectivity Node will find it and automatically set the environment variable. If the BlackBerry Connectivity Node can't find Java, the setup application will stop and you must set an environment variable for the Java location and ensure that the Java bin folder is included in the Path system variable.

Visit support.blackberry.com to read article 52117.

Before you begin: Verify that you have installed a supported JDK on the server where you will be installing the BlackBerry Connectivity Node.

1. Open the **Windows Advanced system settings** dialog box.
2. Click **Environment Variables**.
3. Under the **System variables** list, click **New**.
4. In the **Variable name** field, type `BB_JAVA_HOME`.
5. In the **Variable value** field, type the path to the Java installation folder and click **OK**.
6. In the **System variables** list, select **Path** and click **Edit**.
7. If the Path doesn't include the Java bin folder, click **New** and add `%BB_JAVA_HOME%\bin` to the Path.
8. Move the %BB_JAVA_HOME%\bin entry high enough in the list that it won't be superseded by another entry and click **OK**.

Download the installation and activation files for the BlackBerry Connectivity Node

1. In the management console, on the menu bar, click **Gateway > Settings > Connectivity Node**.
2. Click **Add Connectivity Node**.
3. On the software download page, click **Download**.
4. Click the button beside **Yes** or **No**, and then click **Download** again.
5. Extract the BlackBerry Connectivity Node installation files to the computer.

   Do not copy used installation files from another computer. You must re-extract the installation files on each computer.
6. Click **Download Activation File**.

7. Save the activation file (.txt).

   The activation file is valid for 60 minutes. If you wait longer than 60 minutes before you use the activation file, you must generate a new activation file. Only the latest activation file is valid.

Install and configure the BlackBerry Connectivity Node

1. Open the BlackBerry Connectivity Node installation file (.exe) that you downloaded from the management console.

   If a Windows message appears and requests permission to make changes to the computer, click **Yes**.
2. Choose your language. Click **OK**.
3. Click **Next**.
4. Select your country or region. Read and accept the license agreement. Click **Next**.
5. The installation program verifies that your computer meets the installation requirements. Click **Next**.
6. To change the installation file path, click **...** and navigate to the file path that you want to use. Click **Install**.
7. When the installation completes, click **Next**.

   The address of the BlackBerry Connectivity Node console is displayed (http:/localhost:8088). Click the link and save the site in your browser.
8. Select your language. Click **Next**.
9. When you activate the BlackBerry Connectivity Node, it sends data over port 443 (HTTPS) to the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com). After it is activated, the BlackBerry Connectivity Node uses port 3101 (TCP) for all other outbound connections through the BlackBerry Infrastructure. If you want to send data from the BlackBerry Connectivity Node through an existing proxy server behind your organization's firewall, click **Click here to configure the proxy settings for your organization's environment**, select the **Proxy server** option, and do any of the following:

   - To send activation data through a proxy server, in the **Enrollment proxy** fields, type the FQDN or IP address and the port number of the proxy server. The proxy server must be able to send data over port 443 to bbsecure.com (for example na.bbsecure.com or eu.bbsecure.com). Click **Save**.
   - To send other outbound connections from the components of the BlackBerry Connectivity Node through a proxy server, in the appropriate fields, type the FQDN or IP address and the port number of the proxy server. The proxy server must be able to send data over port 3101 to bbsecure.com (for example na.bbsecure.com or eu.bbsecure.com). Click **Save**.
10. In the **Friendly name** field, type a name for the BlackBerry Connectivity Node. Click **Next**.
11. Click **Browse**. Select the activation file that you downloaded from the management console.
12. Click **Activate**.

    If you want to add a BlackBerry Connectivity Node instance to an existing server group when you activate it, your organization's firewall must allow connections from that server over port 443 through the BlackBerry Infrastructure (for example na.bbsecure.com or eu.bbsecure.com) to activate the BlackBerry Connectivity Node and to the same bbsecure.com region as the main BlackBerry Connectivity Node instance.
13. Click + and select the type of company directory that you want to configure.
14. Link your directory to the BlackBerry Connectivity Node by following the appropriate task:

    - Connect to a Microsoft Active Directory
    - Connect to an LDAP directory

After you finish:

- To install a second BlackBerry Connectivity Node instance for redundancy, download another set of installation and activation files and repeat this task on a different computer. This should be done after the first instance has been activated.

- You can configure one or more directory connections, but if you have multiple BlackBerry Connectivity Nodes, all of the directory connections must be configured identically. If one directory connection is missing or incorrectly configured, that BlackBerry Connectivity Node will appear as disabled in the management console. You can make this task easier by copying directory connection configurations from one BlackBerry Connectivity Node to another.
- To change the directory settings that you configured, in the BlackBerry Connectivity Node console (http:/localhost:8088), click **General settings > Company directory**. Click ✎ for the directory connection.

Connect to a Microsoft Active Directory

1. In the **Connection name** field, type a name for this company directory connection.

   If you have a Microsoft Azure directory configured, this connection name must be different than the name of the Azure directory connection. You cannot change the name after you save the configuration.
2. In the **Username** field, type the username of the Microsoft Active Directory account.
3. In the **Domain** field, type the FQDN of the domain that hosts Microsoft Active Directory. For example, domain.example.com.
4. In the **Password** field, type the password of the Microsoft Active Directory account.
5. In the **Domain controller discovery** drop-down list, click one of the following:
   - If you want to use automatic discovery, click **Automatic**.
   - If you want to specify the domain controller computer, click **Select from list below**. Click + and type the FQDN of the computer. Repeat this step to add more computers.
6. In the **Global catalog search base** field, type the search base that you want to access (for example, OU=Users,DC=example,DC=com). To search the entire Global Catalog, leave the field blank.
7. In the **Global catalog discovery** drop-down list, click one of the following: .
   - If you want to use automatic catalog discovery, click **Automatic**.
   - If you want to specify the catalog computer, click **Select from list below**. Click + and type the FQDN of the computer. If necessary, repeat this step to specify more computers
8. If you want to enable support for linked Microsoft Exchange mailboxes, in the **Support for linked Microsoft Exchange mailboxes** drop-down list, click **Yes**. To configure the Microsoft Active Directory account for each forest that you want BlackBerry UEM Cloud to access, in the **List of account forests** section, click +. Specify the forest name, user domain name (the user can belong to any domain in the account forest), username, and password.
9. To synchronize more user details from your company directory, select the **Synchronize additional user details** check box. The additional details include company name and office phone.
10. Click **Save**.

After you finish: If you want to add a directory synchronization schedule, see Configure directory synchronization schedules.

Copy directory connection configurations

If your environment has multiple BlackBerry Connectivity Nodes, the directory connections must be configured identically on all nodes. To help make this task easier, you can export the directory connection configuration from one BlackBerry Connectivity Node and import it to another.

Note: Before you can import company directory configurations to a BlackBerry Connectivity Node, you must remove any existing company directory connections from that node.

1. On the BlackBerry Connectivity Node that you want to copy the configuration from, in the **Company directory connection** screen, click **Export the directory connections in .txt file**.

   A .txt file containing information about the company directory connections is downloaded to your computer.

2. On the BlackBerry Connectivity Node that you want to copy the configuration to, on the **Company directory connection** screen, browse to the .txt file you downloaded.
3. Click **Import connections**.

   The company directory connections are added to the BlackBerry Connectivity Node.

Configure BlackBerry Connectivity Node logging

You can set the logging level, Syslog information, and local file information for BlackBerry Connectivity Node events.

1. In the management console, on the menu bar, click **Gateway > Settings > Connectivity Node**.
2. Click **Settings**.
3. From the **Server debug levels** drop-down menu, select the level of event you want to log.
4. To send logs to SysLog, click the button beside **SysLog** and fill in the **Host** and **Port** fields.
5. To send logs to the computer that the BlackBerry Connectivity Node is installed on, click the button beside **Enable local file destination**.
6. Fill in the fields for **Maximum log file size** in MB and **Maximum server log file age** (in days).
7. To compress the logs folder, click the button beside **Enable logging folder compression**.
8. Click **Save**.

Configure onboarding and offboarding

Onboarding allows you to automatically add user accounts to BlackBerry Gateway based on user membership in a company directory group. Directory groups and user accounts are added to Gateway during the synchronization process.

If you enable onboarding, you can also choose to configure offboarding. When a user is disabled in the directory or removed from all company directory groups in the onboarding directory groups, Gateway deletes the user account and stops allowing network connections from the user's devices.

You can use offboarding protection to delay the deletion of user accounts to avoid unexpected deletions because of directory replication latency. Offboarding protection delays offboarding actions for two hours after the next synchronization cycle.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Directory Connection**, click the directory connection that you want to configure onboarding for.
3. On the **Sync settings** tab, select **Directory onboarding**.
4. In the **Sync** field, type the maximum number of changes you want to allow for each synchronization process.

   By default, there is no limit. If the number of changes to be synchronized exceeds the limit you set, the synchronization process stops. Changes include users added to groups, users removed from groups, users to be onboarded, and users to be offboarded.
5. In the **Nesting level** field, type the number of nested levels to synchronize for company directory groups. By default, there is no limit.
6. To force the synchronization of directory groups, select **Force synchronization**.

   If this option is selected, when a group is removed from your company directory, the links to that group are removed from onboarding directory groups and directory-linked groups. If not selected, if a company directory group is not found, the synchronization process is canceled.
7. To delete a user account from Gateway when a user is removed from all linked groups in the directory, select **Delete user when the user is removed from all onboarding directory groups**. The first time that a synchronization cycle occurs after a user account is removed from all linked directory groups, the user account is deleted from Gateway.

8. To prevent user accounts or device data from being deleted from Gateway unexpectedly, select **Offboarding protection**.

   Offboarding protection means that users will not be deleted from Gateway until two hours after the next synchronization cycle.
9. Click **Save**.

Configure directory synchronization schedules

You can add a schedule to automatically synchronize BlackBerry Gateway with your organization's company directory.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Directory Connection**, click the directory connection that you want to add a sync schedule for.
3. On the **Sync schedule** tab, click **Add Schedule**.
4. In the **Sync type** drop-down list, select one of the following options:
   - **All users and groups**: This is the default setting. If you choose this option and onboarding is enabled, users are onboarded and offboarded and linked to the appropriate directory linked groups during the synchronization. Users who are not onboarded or offboarded but change directory groups, and users with changes to their attributes are synchronized.
   - **Onboarding groups**: If you choose this option and onboarding is enabled, users are onboarded and offboarded and linked to the appropriate directory linked groups during the synchronization, and users with changes to their attributes are synchronized. Users who are not onboarded or offboarded but change directory groups are not synchronized.
   - **Directory linked groups**: If you choose this option, users are not onboarded and offboarded during the synchronization. Users with changes to their directory groups are linked appropriately. Users with changes to their attributes are synchronized.
   - **User attributes**: If you choose this option, users are not onboarded and offboarded during the synchronization. Users with changes to their directory groups are not synchronized. Users with changes to their attributes are synchronized.
5. In the **Recurrence** drop-down list, select one of the following options:
   - **Interval**: This is the default setting. If you choose this option, you can specify the number of minutes between synchronizations and the hours and days during which synchronization can occur.
   - **Once a day**: If you choose this option, you can specify the days of the week and the time of day when synchronization occurs.
   - **No recurrence**: If you choose this option, you can specify a day and time within the next week for one synchronization.
6. Specify appropriate day and time details for the schedule.
7. Click **Submit**.

Synchronize with your company directory

You can synchronize BlackBerry Gateway with your directory connections at any time.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Directory Connection** click ⟳ for the directory that you want to synchronize with.

Defining your private network

To use BlackBerry Gateway to control access to your private network, you need to define your private network. You can include on-premises locations and private clouds within your private network. Gateway blocks

users from connecting to any location in your private network unless the connection is allowed by the assigned network access control policy.

You define your private network using IP addresses and CIDRs. You can also specify your private DNS servers and private DNS suffixes and group addresses together into a network service to simplify setting up network access control policies.

You must also install one or more Gateway Connectors so that all destinations you want users to be able to access in your defined private network can be connected to through a Gateway Connector. Connections to your private network are routed through a secure tunnel from the device to the BlackBerry Infrastructure and then to a Gateway Connector inside your network.

Specify your private network

Before you begin: Collect the IP addresses or CIDRs for all destinations that you want to define as part of your private network.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Network Settings** click **Private Network Routing**.
3. Click **Add Address**.
4. Type one or more IP addresses, IP ranges, or CIDRs and click **Add**.
5. To edit an address, click next to the address.
6. To remove an address, click next to the address.

Specify your private DNS

You can specify settings for your private DNS to help BlackBerry Gateway route traffic in your private network. You can specify the IP addresses of your DNS servers, the domain names delegated to your DNS servers for forward lookups, and the CIDRs delegated to your DNS servers for reverse lookups.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Network Settings** click **Private Network DNS**.
3. To specify a DNS server, perform the following actions:
   a) Click **DNS Servers**.
   b) Click **Add DNS Server**.
   c) Type the IP address for a DNS server and click **Add**.
4. To specify a domain for forward lookups, perform the following actions:
   a) Click **Forward Lookup Zone**.
   b) Click **Add Forward Zone**.
   c) Type a domain name and click **Add**.
5. To specify a a CIDR for reverse lookups, perform the following actions:
   a) Click **Reverse Lookup Zone**.
   b) Click **Add Reverse Zone**.
   c) Type a CIDR and click **Add**.
6. To edit an address or domain name, click .
7. To remove an address or domain name, click .

Specify your DNS suffixes

You can specify up to three suffixes that are appended to searches performed by your private DNS. If you specify more than one suffix, you can rank them.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Network Settings** click **Client DNS**.
3. Select **DNS search domain (or suffix)**
4. Click **Add DNS Suffix**.
5. Type the DNS suffix name and click **Add**.
6. Repeat steps 4 and 5 for each suffix that you want to add.
7. To edit a suffix, click .
8. To remove a suffix, click .
9. To change the order of the list, drag for the suffix to the appropriate location in the list

Using source IP pinning

BlackBerry Gateway allows you to obtain dedicated IP addresses that you can use for source IP pinning. Many SaaS applications allow source IP pinning as a way to limit access only to connections from a specific range of trusted IP addresses. Your organization may already use this method to limit access to a SaaS application tenant to the IP address used by devices connected to your organization's network. For users working remotely, this means you can secure access between your users and cloud-based applications using source IP pinning without requiring them to use your organization's VPN, which can reduce the traffic on your network and improve connections for users.

If you have enabled source IP pinning for BlackBerry Gateway, the Source IP Pinning network settings display the IP addresses that BlackBerry has allocated for use only by your organization.

To obtain dedicated IP addresses, contact your BlackBerry representative.

To view your allocated IP addresses, on the menu bar, click **Gateway > Settings**, and under **Network Settings** select **Source IP Pinning**.

Define network services

A network service is a group of addresses (FQDNs or IP addresses) that you can use to simplify setting up network access control policies. When you create network access control policies, you can specify a network service instead of each address in the policy. BlackBerry maintains and regularly updates network services for many common SaaS applications to simplify the process for you. You can define additional network services for both public and private applications.

1. On the menu bar, click **Gateway > Settings**.
2. Under **Network Settings** click **Network Services**.
3. Click **Add**.
4. Type a name for the network service.
5. Type the FQDNs, IP addresses, IP ranges, or CIDRs for the service and click **Add**.
6. Repeat steps 3 to 5 for each network service that you want to define.
7. To edit a service, click next to the service name.
   You can't edit services that are defined by BlackBerry.
8. To remove a service, click next to the service name.
   You can't remove services that are defined by BlackBerry.

Managing users and groups

You can add user accounts to BlackBerry Gateway and create user groups to help manage users efficiently.

If you link Gateway to your company directory, you can import users and link user groups to your directory list. You can also add users who are members of your organization in *my*Account and create local groups.

Add an administrator

You can add administrators to give access to the management console. Administrators can manage all BlackBerry Unified Endpoint Security products for your organization in the management console.

1. On the menu bar, click **Settings > User Management**.
2. Perform one of the following actions.

Task	Steps
Add a new user as an administrator	**a.** In the **Add users** section, type the new administrator's email address. **b.** In the **Select role** drop-down list, select **Administrator**. **c.** Click **Add**.
Assign the Administrator role to an existing local user.	**a.** In the **User list**, search for the user that you want to make an administrator. **b.** Click the email address for the user. **c.** In the right pane, click **Administrator**. **d.** Click **Save**.

Add a user

You can add user accounts to BlackBerry Gateway. If you have linked Gateway to your company directory and enabled onboarding, users are added automatically when Gateway synchronizes with the directory. If you haven't enabled onboarding or if you want to add a new user before Gateway synchronizes with the directory, you can add directory users individually. You can also add *my*Account users manually.

Before you begin: Verify that the user who you want to add is in your linked company directory or is a member of your organization in *my*Account

1. On the menu bar, click **Gateway > Users**.
2. Click **Add users**.
3. Perform one of the following actions:

Task	Steps
To add a directory user	**a.** In the **Search** field, start typing the name or email address of the user. **b.** When the user appears in the search results, click the user. **c.** Click **Save**.

Task	Steps
To add a *my*Account user	**a.** Click in the **Search** field and select **Add a user manually**. **b.** Type the user's name and email address as they appear in *my*Account in the appropriate fields and click **Save**.

After you finish: If the user doesn't belong to a group with an assigned enrollment policy, assign an enrollment policy to the user to allow them to use Gateway.

Creating and managing user groups

A user group is a collection of related users who share common properties. Administering users as a group is more efficient than administering individual users because properties can be added, changed, or removed for all members of the group at the same time. When you assign policies to user groups, the policies apply to all members of the group.

Users can belong to more than one group. If a user belongs to two or more groups that are assigned different policies, the highest ranked of the assigned polices is applied to the user.

You can create two types of user groups:

- Directory groups link to groups in your company directory. The membership of the group in BlackBerry Gateway synchronizes with the membership list in the directory. For more information, see Configure onboarding and offboarding.
- Local groups are created and maintained in BlackBerry Gateway. You can assign any local user or directory user to a local group.

Add a directory group

If you have linked BlackBerry Gateway to one or more company directories and enabled onboarding, directory groups can be automatically added to Gateway You can also add a directory group if it has not been added through onboarding.

1. On the menu bar, click **Gateway > Groups**.
2. Click **Add Group > Directory group**.
3. Start typing the name of a group
4. Select the group name when it appears in the search results.
5. If you want the group and any nested groups to be enabled for onboarding, select **Nested directory groups**
6. To assign a policy to the group, click ⊕ and select the type of policy that you want to add.
7. Select the policy and click **Save**.

Add a local group

1. On the menu bar, click **Gateway > Groups**.
2. Click **Add Group > Local group**.
3. To assign a policy to the group, click ⊕ and select the type of policy you want to add.
4. Select the policy and click **Save**.
5. When you've finished assigning policies, click **Save**.
6. To add users to the group, click the group name, then click **Users**.
7. Click **Add user**.

8. Start typing a name to search for the user you want to add.
9. Select one or more names from the search results.
10. Click **Save**.

    You can also add and remove users from groups on the User Configuration page.

Rank policies

You can assign policies to individual users and to user groups. If you assign a policy to an individual user, it takes precedence over policies assigned to groups that the user belongs to. If no policy is assigned directly to a user and the user belongs to two or more groups that are assigned different policies, the highest ranked of the assigned polices is applied to the user.

Before you rank policies you should decide on a strategy based on your objectives and which groups you assign policies to. For example, you may want network access control policies that apply to specific departmental groups to be ranked highest and more restrictive polices to be ranked below them, or you may want your most restrictive policy to be ranked highest.

1. On the menu bar, click **Gateway > Policies**.
2. Select the policy type that you want to rank.
3. Click **Rank**.
4. To change the order of a policy in the list, drag ⠿ for the policy.
5. Click **Save**.

Manage users

You can view events, alerts, and activated devices for any user, add and remove users from local groups, and manage which policies are assigned to users from the user screen.

1. On the menu bar, click **Gateway > Users**.
2. Click the name of the user who you want to view or update.
3. To view alerts, events, or activated devices for the user, click the appropriate link.
4. To manage groups and policies for the user, click **Configuration**.
5. To add a user to one or more local groups, click **Assign User Groups**.

   Directory groups are managed in your company directory. You can't add or remove users from directory groups.
6. In the **Group name** field, start typing the name of the group.
7. When the group appears in the search results, select the group name.
8. Click **Assign**.
9. To assign a policy to a user, click **Assign User Policies**.

   You can also assign policies to many users and groups at one time in the policy settings.
10. Select the type of policy you want to assign.
11. Select the policy name and click **Assign**.

    If the user is already assigned a policy of that type, the new selection replaces the previously assigned policy.
12. To unassign a policy from a user, click 🗑 next to the policy name.

Create an enrollment policy

You create enrollment policies to define the device types that users can enroll with BlackBerry Gateway and send an email message to users that explains how to install and activate the Gateway Agent. You must assign an enrollment policy to users to allow them to activate devices with Gateway.

1. On the menu bar, click **Gateway > Policies**.
2. Select **Enrollment**.
3. Click **Add Policy**.
4. Type a name and description for the policy.
5. To limit the device types that the user can enroll, select **Allowed Platforms**.
6. Type a subject and text for an email message sent to users when they are assigned the enrollment policy. You should include instructions to download, install, and activate BlackBerry Gateway.
7. Click **Add**.

After you finish: Assign the policy to users and groups.

Create a Gateway service policy

You can use the Gateway service policy to enable split tunneling and specify device-specific options. If you enable split tunneling, connections to allowed public destinations bypass the tunnel unless you specify that connections to the destination must use the tunnel.

1. On the menu bar, click **Gateway > Policies**.
2. Click the **Gateway Service** tab.
3. Click **Add Policy**.
4. Type a name and description for the policy.
5. To allow traffic to some public destinations to bypass BlackBerry Gateway, perform the following actions:
   a) Turn on **Split tunneling**.
   b) To specify destinations that must use the tunnel, click ⊕.
   c) Type the CIDR addresses for destinations that must route through the tunnel and click **Add**.
6. Select any of the following options:

Option	Description
Windows	
Force applications to use the tunnel	Specify whether all non-loopback connections must use the tunnel. Any split tunnel routes that do not use the tunnel will not function.
Allow incoming connections	Specify whether to allow incoming TCP connections from non-tunnel, non-loopback interfaces. Gateway never routes incoming connections on its tunnel.
Allow Gateway to run only if BlackBerry Protect is also activated on the device.	Specify whether BlackBerry Protect must also be activated to use Gateway on Windows devices.

7. Click **Add**.

After you finish: Assign the policy to user and groups.

Assign a policy to users and groups

You can assign a policy to any number of groups and users, but only one of each policy type can be assigned to each user. A policy assigned to a user takes precedence over policies assigned to groups that the user belongs to. If no policy is assigned directly to a user and the user belongs to two or more groups that are assigned different policies, the highest ranked of the assigned polices is applied to the user.

1. On the menu bar, click **Gateway > Policies**.
2. Select the policy type that you want to assign.
3. Click the name of the policy that you want to assign.
4. Click **Assigned Users and Groups**.
5. Click **Add users or group**.
6. Start typing a name to search for the user or group that you want to add.
7. Select one or more names from the search results.
8. Click **Add**.

   You can also assign policies to a user on the User Configuration page and assign policies to a group on the Group Settings page.
9. To unassign the policy from a user or group, Select the user and group names that you want to unassign the policy for and click **Remove**.

Controlling network access

You define the network resources that devices enrolled with BlackBerry Gateway can connect to using a network access control policy. The network access control policy defines allowed and blocked destinations on private and public networks. You can also use the network access control policy to enable split-tunneling, which allows traffic to trusted public Internet sites to route directly rather than through BlackBerry Gateway.

When you create a network access control policy, you specify blocked and allowed network connections. For addresses that are part of your private network, all connections are blocked unless you add the address to the allowed list. For destinations that are not part of your private network, all connections are allowed unless you add the address to the blocked list or BlackBerry has determined that the destination is malicious. If you add a public destination to the allowed list, connections are always allowed, even if BlackBerry considers the destination to be unsafe.

If you enable split tunneling, traffic to public destinations can be routed directly to the destination rather than through the tunnel to BlackBerry Gateway. If you have enabled source IP pinning for BlackBerry Gateway, do not enable split tunneling for any destinations that use source IP pinning.

Create a network access control policy

Before you begin: Define your private network.

1. On the menu bar, click **Gateway > Policies**.
2. Click the **Network Access Control** tab.
3. Click **Add Policy**.
4. Type a name and description for the policy.
5. To specify public Internet destinations that you want to block access to, select **Blocked Network Connections**, then click ⊕.
6. Perform one of the following actions:

Task	Steps
To block access to a network service	**a.** Select **Network Services**. **b.** elect one or more network services from the list. **c.** Click **Add**.
To block access by IP address or CIDR	**a.** Select **IP addresses / IP ranges / CIDRs**. **b.** Type the addresses that you want to block. **c.** Click **Add**.
To block access by FQDN	**a.** Select **FQDNs**. **b.** Type the addresses that you want to block. **c.** Click **Add**.

7. To specify destinations on your private network that you want to allow access to, select **Allowed Network Connections**, then click ⊕.
8. Perform one of the following actions

Task	Steps
To allow access to a private network service	**a.** Select **Network Services**. **b.** Click **Allowed network connections** and select one or more network services from the list. **c.** Click **Add**.
To allow access by IP address or CIDR	**a.** Select **IP addresses / IP ranges / CIDRs**. **b.** Type the addresses that you want to allow access to. **c.** Click **Add**.
To allow access by FQDN	**a.** Select **FQDNs**. **b.** Type the addresses that you want to allow access to. **c.** Click **Add**.

9. Click **Add** to save the policy.

After you finish: Assign the policy to user and groups.

Configuring threat detection and response settings

You can configure how BlackBerry Gateway detects and reacts to threats in various ways.

You can configure adaptive response, which uses an identity risk engine to continuously monitor a user's network activity and build a usage model for the user. The model is used to detect unusual network events and block connections. You can set the operating mode that adaptive response runs in to control whether the risk response action is applied.

You can use intrusion protection to enable deep network threat detection using the network connection's signatures. When intrusion protection is enabled, Gateway automatically blocks connections where threats are detected. Intrusion protection is enabled by default.

Configure adaptive response settings

You can set adaptive response to one of two operating modes:

- Passive: A training mode where the identity risk engine monitors data and builds a risk model for each user. In passive mode, alerts are generated for events, but the actions that are configured in adaptive response policies are not executed.
- Active: The identity risk engine monitors data and builds a risk model for each user. When an unusual network event is detected, the actions that are configured in policies are applied.

1. On the menu bar, click **Gateway > Settings** .
2. Click the **Adaptive Response** tab.
3. In the **Operating mode** drop-down list, select the operating mode.

   Note: When the first user is added to an adaptive response policy, a training period for the adaptive response risk model is started and lasts until the following conditions are met: 1000 events are collected for the user's tenant and 14 calendar days pass. Alerts are not generated during the training period.
4. Click **Save**.

After you finish: Create adaptive response policies.

Create an adaptive response policy

You create and assign adaptive response policies to specify the risk response actions that are applied to devices. You can specify whether to override the network access control policy when a user's network usage patterns do not match past behavior.

When the first user is added to an adaptive response policy, a training period for the adaptive response risk model is started and lasts until the following conditions are met: 1000 events are collected for the user's tenant and 14 calendar days pass. Alerts are not generated during the training period.

By default, when adaptive response is running in active mode and an anomalous network event is detected, the assigned adaptive response policy overrides the network access control policy and connections are blocked. For example, if a user tries to connect to an Internet destination that is not typical for them in their day-to-day behavior, or if they try to connect to resources at a time that is not typical for them, the adaptive response policy overrides the user's network access control policy and assigns one that blocks connections to your private network or SaaS services. When the user browses to safe locations that are typical for them, the identity risk engine detects the behavior and the policy override is reverted.

1. On the menu bar, click **Gateway > Policies**.

2. Click the **Adaptive Response** tab.
3. Click **Add policy**.
4. Type a name and description for the policy.
5. Under **Response actions**, click ⊕.
6. Click **Override network access policy** and select a policy from the drop-down list.
7. Click **Save**.
8. Click **Add**.

After you finish: Assign the policy to users and groups.

Configure intrusion protection

You can use intrusion protection to enable deep network threat detection using network connection signatures. Intrusion protection is enabled by default.

When intrusion protection is enabled, Gateway records and automatically blocks connections when a threat is detected. When intrusion protection is disabled, threats are recorded as events but the connection is not blocked.

1. On the menu bar, click **Gateway > Settings**.
2. Click the **Network Settings** tab.
3. Click the **Network Protection** tab.
4. Turn on **Enable intrusion protection**.
5. Click **Save**.

Monitoring BlackBerry Gateway

You can monitor your network and connections using several tools

- The Dashboard provides a visual overview of network connections and the status of each Gateway Connector.
- Alerts show each risk events detected by the identity risk engine.
- Event logging records every connection attempt by every user.

Using the Dashboard

The dashboard in the management console includes several widgets that give you a visual overview of the status of BlackBerry Gateway. Information about public and private network connections, users, network access control policies, and installed Gateway Connectors displays on a single page to give you up-to-the-moment status information.

Some widgets allow you to adjust the time range and others allow you to click to jump to additional information.

To view the dashboard, on the menu bar, click **Gateway > Dashboard**.

Viewing alerts

BlackBerry Gateway logs all network connection alerts. The alert log records the user, device model and OS, destination, date and time, and other details about each attempted connection alert.

To view the alert log, on the menu bar, click **Gateway > Alerts**. If adaptive response is running in passive mode, a warning is displayed to indicate that risk response actions aren't applied when alerts are generated.

To filter any column, click at the top of the column. By default, all alerts are labelled as network anomaly alerts and treated as high risk.

You can click on a row to view details about the alert, including when the alert was detected, the analyzed events that caused the alert, the user and device that are affected and the policy changes that were applied.

Viewing events

BlackBerry Gateway logs all network connection events. The event log records the user, device model and OS, destination, date and time, and other details about each attempted connection event.

If a connection is identified as a potential threat, the **Anomaly** column specifies the type of threat detected.

- **Behavioral risk** anomalies are potential threats based on unusual user behavior.
- **Reputation** anomalies are potential threats from addresses on the BlackBerry list of unsafe Internet destinations.
- **Signature detection** anomalies refer to potential threats detected by intrusion protection.

To view the event log, on the menu bar, click **Gateway > Events**.

To filter any column, click at the top of the column.

To change which columns are displayed, click at the right side of the column headings.

Using BlackBerry Gateway on a device

After you add users to BlackBerry Gateway and assign an enrollment policy and network access control policy, users can install and activate the Gateway Agent on Windows 10 and macOS devices.

The BlackBerry Gateway agent is supported on the following operating systems:

- Windows 10 version 1809 and later
- macOS version 10.14 and later

Users can download the Gateway Agent from the following locations:

- Windows 10 users can download the Gateway Agent from BlackBerry.
- macOS users can download the Gateway Agent from the App Store.

To activate the Gateway Agent, users must sign in to BlackBerry Gateway. Users added from a linked directory use their directory credentials to sign in to Gateway. Users who are members of your organization in *my*Account, use their BlackBerry Online Account credentials to sign in.

After the Gateway Agent is activated, users can enable and disable work mode, view warnings about blocked connections, and view details for connection time, speed, and the amount of data uploaded and downloaded while connected to Gateway.

If a user disables work mode, they can't access network resources, services, and applications that are only accessible to them through Gateway. Users also may not be blocked from connecting to public destinations blocked by the network access control policy and destinations that BlackBerry has determined to be malicious.

BlackBerry Gateway Agent settings

Users can configure some settings for the BlackBerry Gateway Agent.

Note: Setting names may appear differently depending on the device OS.

Setting	Description
Deactivate	Click this button to deactivate the BlackBerry Gateway Agent. When the Agent is deactivated, it can't receive policy updates from BlackBerry Gateway.
Report a Problem	Click this button to send a problem report to BlackBerry.
Use TCP	Select this option to use TCP for connections to BlackBerry Gateway if your organization's firewall doesn't allow UDP connections.
Start BlackBerry Gateway when I sign in	Select this option to start BlackBerry Gateway whenever you log in to your device.
Enable work mode automatically	Select this option to enable work mode whenever BlackBerry Gateway starts.

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