



BlackBerry UEM

Planning Guide

12.15

Contents

- Start here..... 5**
 - I am a new customer (no previous version of BlackBerry UEM).....5
 - I am upgrading from one of the last two releases of BlackBerry UEM.....7
 - I am upgrading from an older version of BES12 or BlackBerry UEM.....7
 - I have Good Control (standalone).....8
 - I have a BES10 environment.....8
 - I need a disaster recovery environment.....8

- Planning tools..... 9**
 - BlackBerry UEM Readiness Tool.....9
 - BlackBerry UEM Configuration Tool.....9
 - BlackBerry UEM Performance Calculator.....10

- BlackBerry UEM installation options..... 11**

- Device management modes..... 13**

- Designing a deployment plan for BlackBerry UEM.....17**
 - Installing or upgrading to BlackBerry UEM..... 17
 - Considerations for upgrades from BlackBerry UEM..... 17
 - Upgrading BlackBerry UEM with BlackBerry Dynamics devices..... 17
 - Upgrading from Good Control or Good Proxy to BlackBerry UEM..... 17
 - Installing the BlackBerry Enterprise Mobility Server.....18
 - Installing a BlackBerry Connectivity Node instance.....18
 - Migrating data to BlackBerry UEM..... 19
 - High availability and disaster recovery.....19
 - Log files.....20
 - BlackBerry Secure Connect Plus.....20
 - Third-party software requirements..... 20
 - Considerations for deployments with a large number of BlackBerry 10 devices.....20

- Planning high availability for a BlackBerry UEM domain.....21**
 - Architecture: High availability for BlackBerry UEM.....22
 - High availability and the BlackBerry UEM Core.....24
 - Configuring high availability for the management console.....24
 - High availability and the BlackBerry Connectivity Node.....24
 - Load-balancing data for BlackBerry 10 devices without BSCP.....25
 - How BlackBerry UEM evaluates the health of components.....25
 - Configuring database high availability using Microsoft SQL Server AlwaysOn.....26
 - AlwaysOn high availability.....26
 - AlwaysOn requirements.....28

Configuring database high availability using database mirroring.....	28
Database mirroring requirements.....	29

Preinstallation and preupgrade requirements.....30

Hardware requirements.....33

Hardware requirements: BlackBerry UEM.....	33
Small deployments.....	33
Medium deployments.....	35
Large deployments.....	37
Hardware requirements: BEMS.....	39
Small deployments.....	39
Medium deployments.....	41
Large deployments.....	42
Hardware requirements: BlackBerry Router.....	43

Port requirements..... 44

Server configuration.....	44
Global IP ranges.....	45
Mobile device configuration (Wi-Fi requirements).....	48
Reserved IP address ranges.....	50
Outbound connections: BlackBerry UEM to the BlackBerry Infrastructure.....	51
Outbound connections: BlackBerry UEM to the BlackBerry Dynamics NOC.....	54
Outbound connections: Devices on a work Wi-Fi network.....	54
Intranet connections.....	56
How BlackBerry UEM selects listening ports during installation.....	57
BlackBerry UEM listening ports.....	57
Minimum ports to open between BlackBerry UEM instances.....	61

Supporting the deployment..... 64

Hardware issues.....	64
Software issues.....	64
Network issues.....	65
User, device, device control, and license issues.....	65
Database issues.....	66
Returning to a previous environment.....	66

Legal notice..... 67

Start here

Start here to plan your installation of BlackBerry UEM.

- [I am a new customer](#) (no previous version of BlackBerry UEM)
- [I am upgrading from the last release of BlackBerry UEM](#)
- [I am upgrading from an older version of BES12 or UEM](#)
- [I have Good Control \(standalone\)](#)
- [I have a BES10 environment](#)
- [I need a disaster recovery environment](#)

I am a new customer (no previous version of BlackBerry UEM)

If you are new to BlackBerry UEM, review the checklist below.

Overview information and training	
General product information	BlackBerry documentation
Training	BlackBerry Training
Support	BlackBerry Support

Base requirements	
Overview	Preinstallation and preupgrade requirements
Software	Compatibility matrixes
Hardware	Hardware requirements

Infrastructure	
On-premises	BlackBerry UEM on-premises documentation
Cloud	BlackBerry UEM Cloud documentation

BlackBerry UEM components	
Manage devices	MDM
Access internal corporate resources	BlackBerry Connectivity Node and enterprise connectivity (BlackBerry UEM Configuration Guide)

BlackBerry UEM components

- | | |
|------------------------|--|
| Secure individual apps | <ul style="list-style-type: none">• BlackBerry Dynamics• BlackBerry Enterprise Mobility Server (BlackBerry Enterprise Mobility Server documentation)• Microsoft Intune |
|------------------------|--|

Devices and activation types

- | | |
|--|--|
| User privacy and BYOD | <ul style="list-style-type: none">• Android Enterprise with work profile• App/container management (BlackBerry Dynamics)• iOS work email only (BlackBerry Secure Gateway) |
| Organization-managed | <ul style="list-style-type: none">• Android Enterprise with work profile• Android Enterprise fully managed device with work profile• iOS MDM controls• macOS MDM controls |
| Organization-owned | <ul style="list-style-type: none">• Apple DEP• iOS supervised mode• Android Enterprise fully managed device• Android Enterprise fully managed device with work profile |
| Deprecated management types for legacy devices | <ul style="list-style-type: none">• Android device administrator• Samsung Knox |

Licensing

[BlackBerry Enterprise Licensing Guide](#)

[Managing licensing for devices](#)

High availability and disaster recovery

- | | |
|-------------------------------------|--|
| Active redundancy in the local site | Planning high availability for a BlackBerry UEM domain |
| Remote site failover | BlackBerry UEM Disaster Recovery Guide |

Network segmentation

- | | |
|-----|--|
| DMZ | Installing BlackBerry UEM in a DMZ |
|-----|--|

Network segmentation

Direct Connect/DEC [Configure Direct Connect or a web proxy for BlackBerry Proxy connections](#)

I am upgrading from one of the last two releases of BlackBerry UEM

If you are upgrading from the release of BlackBerry UEM previous to this one or the one before that, review the following checklist.

Updates

New features [What's new](#)

Fixed and known issues [Release notes and advisories](#)

Upgrading

Planning [Installing or upgrading to BlackBerry UEM](#)

Upgrade

- [Preinstallation and preupgrade requirements](#)
- [Steps to upgrade BlackBerry UEM](#)

I am upgrading from an older version of BES12 or BlackBerry UEM

If you are upgrading from BES12 or from a version of BlackBerry UEM that is more than two releases previous to this version, review the following checklist.

Updates

New features [What's new](#)

Fixed and known issues [Release notes and advisories](#)

Upgrading

Planning [Preinstallation and preupgrade requirements](#)

Upgrade [Supported upgrade environments](#)

I have Good Control (standalone)

If you have Good Control (standalone), review the following checklist. Determine whether you can upgrade to BlackBerry UEM or whether you must migrate your users and devices to BlackBerry UEM.

General information	
General product information	BlackBerry documentation
Training	BlackBerry Training
Support	BlackBerry Support

Upgrade	
Planning	Upgrading from Good Control or Good Proxy to BlackBerry UEM
Upgrade	Supported upgrade environments

Migration	
Planning	Migrating data to BlackBerry UEM
Migration	<ul style="list-style-type: none">• Supported upgrade environments• Migrating users, devices, groups, and other data from a source server

I have a BES10 environment

If you have a BES10 environment and you want to move to BlackBerry UEM, review:

- [Supported upgrade environments](#)
- [BlackBerry Software Lifecycle Overview](#)

You must migrate users, devices, groups and other data to UEM version 12.9, then migrate or upgrade by two UEM versions at a time (for example, 12.9 to 12.11, 12.11 to 12.13, and so on) to the latest UEM version.

I need a disaster recovery environment

If you want to set up a disaster recovery environment, review the [BlackBerry UEM Disaster Recovery Guide](#).

Planning tools

In addition to all of your planning considerations, BlackBerry UEM has some tools that you can use to assist you in planning your BlackBerry UEM installation or upgrade:

- BlackBerry UEM Readiness Tool
- BlackBerry UEM Configuration Tool
- BlackBerry UEM Performance Calculator

BlackBerry UEM Readiness Tool

You can use the BlackBerry UEM Readiness Tool to check system requirements before you run the BlackBerry UEM setup application. The BlackBerry UEM Readiness Tool is included with the BlackBerry UEM software. You can also download the tool from *myAccount*.

The BlackBerry UEM Readiness Tool checks the following requirements:

- Proxy server setting validation
- Minimum operating system requirements
- Minimum hard disk space
- Secure connection
- SRP connection
- Connection to the BlackBerry Dynamics NOC
- Required ports
- Account permissions
- Database validation

Note:

- The BlackBerry UEM Readiness Tool does not check for Microsoft .NET Framework 4.5.
- The BlackBerry UEM Readiness Tool performs a simple CONNECT to determine that ports are open. It does not validate that traffic will flow properly. For example, the Readiness Tool cannot detect issues related to traffic monitoring, SSL termination, or other systems that might reactively close sessions.

BlackBerry UEM Configuration Tool

If your organization plans to support more than 500 BlackBerry 10 devices, use the BlackBerry UEM Configuration Tool to calculate the number of SRP IDs you require. After you install BlackBerry UEM, run the BlackBerry UEM Configuration Tool to import the SRPs into the BlackBerry UEM database before you add or migrate users. The BlackBerry UEM Configuration Tool is included with the BlackBerry UEM software. You can also download the tool from *myAccount*.

The BlackBerry UEM Configuration Tool allows you to:

- Update or change the following BlackBerry UEM database properties:
 - Microsoft SQL Server name
 - Database name
 - Port configuration
 - Database authentication
 - Windows username

- Windows password
- Calculate the number of SRP IDs required for BlackBerry UEM based on the projected total number of BlackBerry 10 devices
- Import extra SRP IDs into the BlackBerry UEM database

For more details on the BlackBerry UEM Configuration Tool, [visit support.blackberry.com/community](http://support.blackberry.com/community) to read article 36443.

For more information about obtaining and importing SRP IDs, [visit support.blackberry.com/community](http://support.blackberry.com/community) to read article 36435.

BlackBerry UEM Performance Calculator

The BlackBerry UEM Performance Calculator contains BlackBerry UEM performance models and SPEC CPU conversions. You can use the [Performance Calculator for BlackBerry UEM](#) to determine the minimum number of BlackBerry UEM instances and BlackBerry Connectivity Node instances for your device configuration and workload.

BlackBerry UEM installation options

You can install all BlackBerry UEM components on one server, or you can install the components on separate servers. The setup application allows you to install the primary BlackBerry UEM components, the management console, and the device connectivity components separately. You can install BlackBerry UEM components on separate server for security reasons or if your server has system resource limitations.

Note:

- You must install the BlackBerry UEM primary components on one server before you install the management console or BlackBerry Connectivity Node on separate servers.
- When the primary components and management console are installed on the same server, the management console permanently binds to the local BlackBerry UEM Core. The result is that the management console will not try to use any other instances of the BlackBerry UEM Core unless the local BlackBerry UEM Core is shut down.
- You cannot install only the management console and the device connectivity components on the same server.
- For instructions on installing the components, and for instructions on configuring the BlackBerry Connectivity Node, [see the Installation and upgrade content](#).

Installation options	Primary BlackBerry UEM components	Management console	Device connectivity components
For a smaller organization, install all three components on one server.	√	√	√
Install the primary BlackBerry UEM components and the management console on one server if your organization does not require the BlackBerry Connectivity Node.	√	√	
Install only the primary BlackBerry UEM components and the device connectivity components on one server. This configuration can provide better performance and scalability for large organizations and allows you to manage access to servers that host BlackBerry UEM components.	√		√
Install only the primary BlackBerry UEM components on a server. You must also install the management console on another server for BlackBerry UEM to function.	√		
Install only the management console on a server. You must also install the primary BlackBerry UEM components on another server for BlackBerry UEM to function.		√	

Installation options	Primary BlackBerry UEM components	Management console	Device connectivity components
Install only the BlackBerry Connectivity Node for better performance and scalability for large organizations with BlackBerry UEM components installed in different regions.			√

The following table lists the subcomponents that are installed with each of the three main components. For detailed information about each subcomponent, [see the Architecture content](#).

Subcomponents	Primary BlackBerry UEM components	Management console	Device connectivity components
BlackBerry UEM Core	√		
Management console		√	
BlackBerry UEM Core (for UI only)		√	
BlackBerry Gatekeeping Service	√		√
BlackBerry Proxy			√
BlackBerry Secure Connect Plus			√
BlackBerry Secure Gateway			√
BlackBerry Cloud Connector			√

Device management modes

The following tables list the device management modes to help you plan your environment. Some of these options can be combined or used in conjunction, and some modes are exclusive. For more information about and instructions to configure these features, see the [Administration content](#).

iOS

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
MDM controls	Enterprise email only	Yes iOS email app only: BlackBerry Secure Gateway
MDM controls	Device-wide VPN for email and apps	Yes <ul style="list-style-type: none"> iOS email app: BlackBerry Secure Gateway Additional apps: BlackBerry Secure Connect Plus
MDM controls	Device Control and App Deployment (BlackBerry UEM Client)	No Behind the firewall with VPN profile
MDM controls	BlackBerry Dynamics	Yes BlackBerry Dynamics apps: BlackBerry Proxy
MDM controls	iOS Supervised - DEP	Yes <ul style="list-style-type: none"> Email only: BlackBerry Secure Gateway Email and apps: BlackBerry Secure Connect Plus Dynamics apps: BlackBerry Proxy
MDM controls	iOS Supervised - Apple Configurator 2	Yes <ul style="list-style-type: none"> Email and apps: BlackBerry Secure Connect Plus Dynamics apps: BlackBerry Proxy

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
MDM controls	Microsoft Intune	Yes <ul style="list-style-type: none"> Email and apps: BlackBerry Secure Connect Plus Dynamics apps: BlackBerry Proxy
User privacy	Enterprise email only	Yes iOS email app only: BlackBerry Secure Gateway
User privacy	Work Apps catalog (BlackBerry UEM Client)	No <ul style="list-style-type: none"> Behind the firewall with Activation Profile: Allow VPN management VPN profile
User privacy	BlackBerry Dynamics	Yes Dynamics apps: BlackBerry Proxy
User privacy	Microsoft Intune	Yes Dynamics apps: BlackBerry Proxy
Device registration for BlackBerry 2FA only	BlackBerry 2FA only	No

Android

The activation types in this section support Samsung Knox policies on Samsung devices and BlackBerry Dynamics for additional security in the work profile.

You can use the User privacy activation type to activate Chrome OS devices to allow you to install and manage Android BlackBerry Dynamics apps.

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
Work and personal - user privacy (Android Enterprise with work profile)	Android Enterprise	No Third-party VPN
Work and personal - user privacy (Android Enterprise with work profile) (Premium)	Android Enterprise	Yes Email and apps: BlackBerry Secure Connect Plus

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
Work space only (Android Enterprise fully managed device)	Android Enterprise <ul style="list-style-type: none"> Manual user activation Zero-touch enrollment 	No Third-party VPN
Work space only (Android Enterprise fully managed device) (Premium)	Android Enterprise <ul style="list-style-type: none"> Manual user activation Zero-touch enrollment 	Yes Email and apps: BlackBerry Secure Connect Plus
Work and personal - full control (Android Enterprise fully managed device with work profile)	Android Enterprise	No Third-party VPN
Work and personal - full control (Android Enterprise fully managed device with work profile) (Premium)	Android Enterprise	Yes Email and apps: BlackBerry Secure Connect Plus

Android legacy management types

As of Android10, Google has deprecated the use of Android device administrator for Samsung Knox and MDM controls.

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
MDM controls	Device Control and App Deployment (BlackBerry UEM Client)	No
MDM controls	BlackBerry Dynamics	Yes Email and apps: BlackBerry Proxy
MDM controls	Microsoft Intune	Yes <ul style="list-style-type: none"> Email and apps: BlackBerry Secure Connect Plus Dynamics apps: BlackBerry Proxy
Work and personal - full control	Samsung Knox	Yes Email and apps: BlackBerry Secure Connect Plus
Work and personal - user privacy	Samsung Knox	Yes Email and apps: BlackBerry Secure Connect Plus

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
Work space only	Samsung Knox	Yes Email and apps: BlackBerry Secure Connect Plus
User privacy	Microsoft Intune	Yes Email and apps: BlackBerry Proxy
Device registration for BlackBerry 2FA only	BlackBerry 2FA only	No

macOS/OS X

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
MDM controls	Device management	No Behind the firewall with VPN profile

Windows

Activation type	Device management mode	UEM service for behind-the-firewall enterprise connectivity
MDM controls	Device management	No Behind the firewall with VPN profile (Windows 10)
MDM controls	BlackBerry Dynamics	Yes Dynamics apps: BlackBerry Proxy
MDM controls	Microsoft Intune	No (unless combined with BlackBerry Dynamics) Behind the firewall with VPN profile (Windows 10)

Designing a deployment plan for BlackBerry UEM

You can deploy BlackBerry UEM in your organization's environment in several ways, depending on whether or not you have other EMM solutions from BlackBerry installed.

Note:

- You cannot install BlackBerry UEM on a computer that has both BES5 and BES10 installed on it.
- You cannot install BlackBerry UEM on a computer that has the BlackBerry Cloud Connector installed on it.

Follow the instructions in [the Installation and upgrade content](#) to install BlackBerry UEM or to upgrade to the latest version of BlackBerry UEM. After the installation is complete, [see the Configuration content](#) to finish setting up your BlackBerry UEM.

Installing or upgrading to BlackBerry UEM

You can use the UEM setup application to install the UEM software and database or to upgrade from up to two previous versions of UEM.

Considerations for upgrades from BlackBerry UEM

If you are upgrading from a previous version of BlackBerry UEM, make sure your servers meet the requirements for the BlackBerry UEM configuration you are upgrading to.

Note: If you have any inactive BlackBerry Connectivity Nodes, either activate them or remove them from the environment. If you do not activate them before upgrading, any devices they manage will be removed.

Upgrading BlackBerry UEM with BlackBerry Dynamics devices

If you are upgrading an environment that has activated BlackBerry Dynamics applications on devices, connections to the application servers, including the mail server, will continue to be supported. For example, the BlackBerry Work application will continue to receive email during the upgrade.

BlackBerry Dynamics applications cannot be activated during the upgrade. All servers in the environment must be upgraded before any BlackBerry Dynamics applications can be activated.

Upgrade all servers in the environment within 24 hours of the first server upgrade.

Upgrading from Good Control or Good Proxy to BlackBerry UEM

To upgrade Good Control or Good Proxy version 4.0 and later to the latest version of UEM, you must first upgrade Good Control and Good Proxy instances to UEM 12.8.1, synchronize the environment, then upgrade by two UEM versions at a time to the latest UEM version.

If your environment has a version of BES12 that is integrated with Good Control, you must first upgrade to UEM version 12.8.1, synchronize the environment, then upgrade by two UEM versions at a time to the latest UEM version. Use the setup application to upgrade both BES12 and Good Control. Do not use the Good Control setup application to upgrade Good Control in this scenario.

Note: For details about supported upgrade paths, visit support.blackberry.com/community to read article 38980. For information about performing Good Control synchronization, visit support.blackberry.com/community to read article 39172.

Considerations for upgrades from Good Control and Good Proxy

If you are upgrading to BlackBerry UEM from Good Control or Good Proxy, make sure your servers meet the requirements for the BlackBerry UEM configuration you are upgrading to.

Note: When you upgrade a Good Proxy node, it is upgraded to a BlackBerry Connectivity Node. You must activate the new BlackBerry Connectivity Node on BlackBerry UEM to enable the functionality. A Good Control node is upgraded to a BlackBerry UEM node that includes primary components and management console, without a BlackBerry Connectivity Node.

For upgrades from a Good Control node that is **not** integrated with BES12 version 12.5, consider migrating your data, users, and devices to BlackBerry UEM instead:

1. Upgrade Good Control to Good Control version 5.0.
2. Migrate your data from Good Control to BlackBerry UEM.

Using this method minimizes the hardware requirements for the upgrade, and reduces the number of post-upgrade decommissioning tasks. This method also allows you to move data, users, and devices in stages.

Important: To determine if this is an appropriate course of action for your environment, first read the information about migration in the [Configuration content](#).

Installing the BlackBerry Enterprise Mobility Server

You can install the BlackBerry Enterprise Mobility Server (BEMS) in your BlackBerry UEM environment to provide additional services for BlackBerry Dynamics apps. BEMS integrates the following services: BlackBerry Push Notifications, BlackBerry Connect, BlackBerry Presence, and BlackBerry Docs.

For information about sizing your environment for BEMS and determining whether you should install BEMS on a separate server, see [Hardware requirements: BEMS](#). For information about installing BEMS, see the [BlackBerry Enterprise Mobility Server Installation and configuration content](#).

Note: When you upgrade BlackBerry UEM, you may also have to upgrade BEMS. See the [BlackBerry UEM Compatibility Matrix](#) for information about which versions of BEMS are compatible with your version of BlackBerry UEM.

Installing a BlackBerry Connectivity Node instance

You can install one or more instances of the BlackBerry Connectivity Node to add additional capacity for device connectivity, for the purposes of regionalizing device connectivity, or for the purpose of high availability or disaster recovery.

Each BlackBerry Connectivity Node instance contains the following BlackBerry UEM components:

- BlackBerry Secure Connect Plus
- BlackBerry Gatekeeping Service
- BlackBerry Secure Gateway
- BlackBerry Proxy
- BlackBerry Cloud Connector

Each BlackBerry Connectivity Node instance provides another active instance of these components to the BlackBerry UEM domain that can process and manage secure device connections (by default, the BlackBerry Gatekeeping Service in a BlackBerry Connectivity Node instance is disabled).

Enterprise connectivity can be maintained by creating server groups for BlackBerry Secure Connect Plus connectivity or BlackBerry Proxy clusters for BlackBerry Dynamics connectivity.

A server group contains one or more instances of the BlackBerry Connectivity Node. When you create a server group, you specify the regional data path that you want the components to use to connect to the BlackBerry Infrastructure. You can associate email and enterprise connectivity profiles with a server group. Any device that is assigned those profiles uses that server group's regional connection to the BlackBerry Infrastructure when it uses any of the components of the BlackBerry Connectivity Node.

Optionally, you can designate each BlackBerry Connectivity Node in a server group to handle a single connection type: BlackBerry Secure Connect Plus only, BlackBerry Secure Gateway only, or BlackBerry Proxy only. This frees up server resources to allow fewer servers required for the same number of users or containers.

A BlackBerry Proxy cluster contains one or more instances of the BlackBerry Connectivity Node. When you create a BlackBerry Proxy cluster, you specify the BlackBerry Proxy servers included in the cluster, as well as whether that cluster will be used for BlackBerry Dynamics activation, or only for application server connectivity.

After you install a BlackBerry Connectivity Node, you must register it before it can be used.

Migrating data to BlackBerry UEM

For instructions and considerations about migrating data to a BlackBerry UEM domain, see the [Configuration content](#).

To move data from Good Control to UEM, the source Good Control server must be at version 5.0 and must not be integrated with BES12 or UEM in any way. You can move Good Control data only from a standalone Good Control server.

You can migrate data from BES10 to UEM version 12.9, then upgrade or migrate by two UEM versions at a time to the latest UEM version.

High availability and disaster recovery

It is important to understand the difference between high availability and disaster recovery.

High availability means that each service has some form of redundancy within a BlackBerry UEM environment. For BlackBerry UEM, high availability is active-active. High availability could mean N+1 or N+N (where N is the number of servers for your environment as defined by the Performance Calculator), depending on how much fault tolerance is acceptable. All nodes in a high availability configuration exist within the same physical location and have minimal latency between nodes. In high availability, the database server is collocated (with low latency) to all online Core nodes. All running core nodes must be within 5ms of the database at all times (for more information, see [Hardware requirements](#)).

Disaster Recovery means servers located in an alternate physical site that can be failed over to in the event of a disaster in the primary site (complete site failure). Disaster recovery servers for BlackBerry UEM must remain offline and must have a mirrored/clustered copy of the database in the disaster recovery site. Failing over to the disaster recovery site is "all or nothing". For example, if the database fails over, the BlackBerry UEM Core servers also need to be brought up in the disaster recovery site and brought down in the primary site.

For more information, see [Planning high availability for a BlackBerry UEM domain](#) and the [Disaster recovery content](#).

Log files

The size of log files for BlackBerry UEM varies based on the number of devices in your organization's environment, the level of user activity on devices, and the logging levels that BlackBerry UEM uses. It is a best practice to monitor and control the amount of disk space that the BlackBerry UEM log files take up. For more information about configuring logging, [see the Administration content](#).

BlackBerry Secure Connect Plus

If your BlackBerry UEM domain will support more than 1000 devices per server using BlackBerry Secure Connect Plus at the same time, you must install Windows Server 2012 R2 or later on the computers that host BlackBerry UEM.

Third-party software requirements

For more information about which third-party software is compatible with BlackBerry UEM, [see the Compatibility matrixes](#).

Considerations for deployments with a large number of BlackBerry 10 devices

BlackBerry UEM enterprise connectivity traffic for BlackBerry 10 devices includes email, organizer data, and browser network traffic. All of this traffic flows from the BlackBerry Dispatcher (one for each BlackBerry UEM instance), to the active BlackBerry Affinity Manager within the BlackBerry UEM domain, to the BlackBerry Infrastructure, and then to the device. In the path between the BlackBerry Affinity Manager and the BlackBerry Infrastructure, network conditions such as latency, packet loss, and packet reordering reduce the rate at which data can be transmitted over a single TCP connection due to the nature of the TCP/IP protocols.

Adding SRPs allows the BlackBerry Affinity Manager to establish multiple connections to the BlackBerry Infrastructure, known as SRP connections. Each connection must have an SRP ID associated with it. By having multiple connections, you can compensate for these network effects by reducing the amount of data each connection must carry between the BlackBerry Affinity Manager and the BlackBerry Infrastructure. The BlackBerry UEM Configuration Tool helps estimate how many SRP connections you need for your particular domain size and network conditions.

It is a best practice to establish the correct number of SRP connections before you install BlackBerry UEM, to allow for a good distribution of BlackBerry 10 devices across the SRP connections. BlackBerry 10 devices are statically assigned to the least loaded SRP connection during activation. If an extra SRP connection is added later, new devices are assigned to the new SRP connection when they are activated until the new SRP connection reaches the same load as the other SRP connections.

Planning high availability for a BlackBerry UEM domain

BlackBerry UEM uses an active-active high availability model to minimize service interruptions for device users. To configure high availability, you install multiple instances of BlackBerry UEM, each on a separate computer. Each instance connects to the BlackBerry UEM database and actively manages user accounts and devices.

High availability in BlackBerry UEM includes the following features:

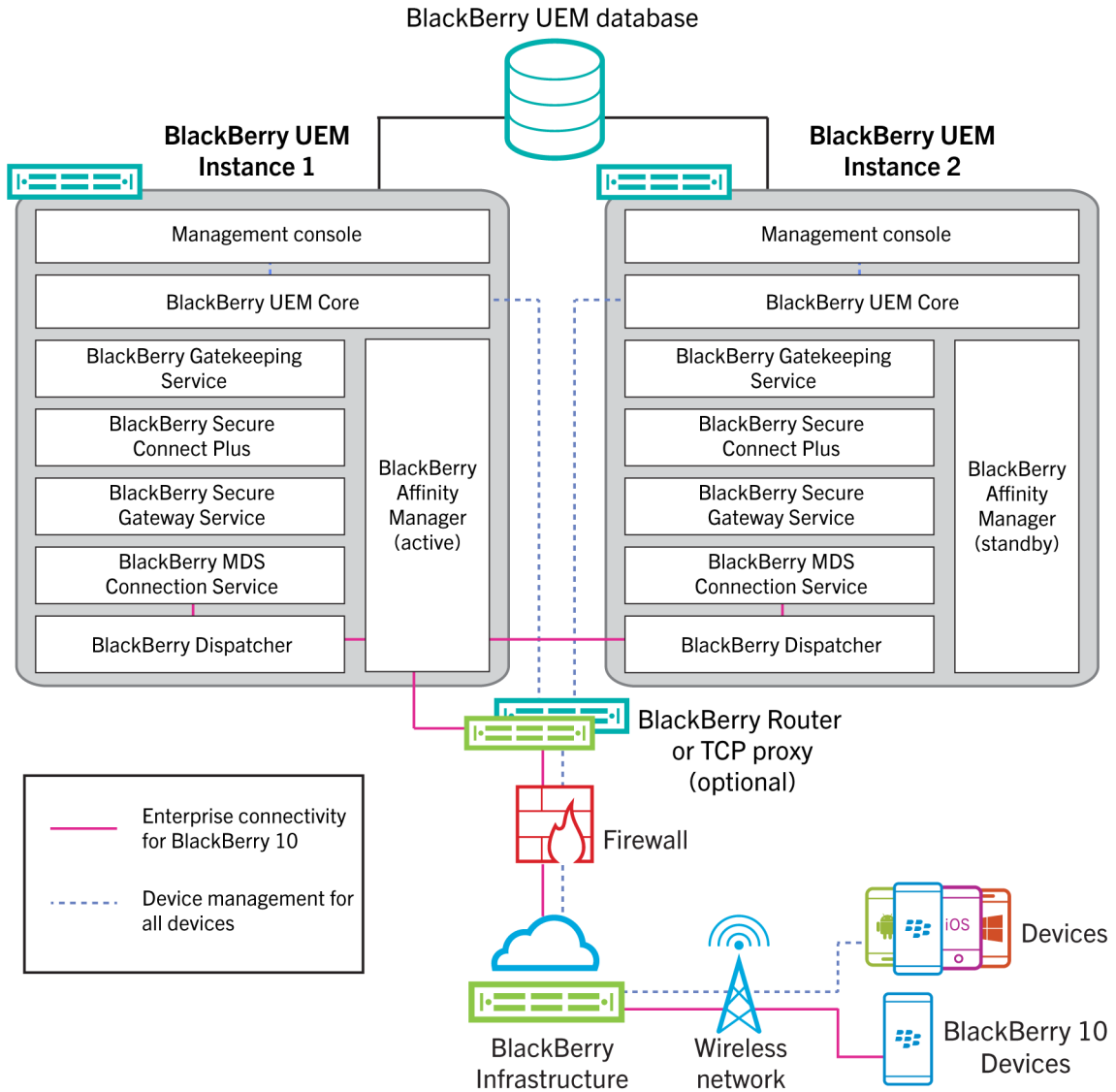
Feature	Description
iOS, Android, and Windows devices can connect to any BlackBerry UEM instance	iOS, Android, and Windows devices can connect to any BlackBerry UEM Core instance to receive device management, policy, and configuration updates. If one or more BlackBerry UEM Core instances is unhealthy, iOS, Android, and Windows devices connect to one of the healthy instances. Load balancing is performed automatically. As a result, device management services continue uninterrupted.
Access the management console and BlackBerry UEM Self-Service from any BlackBerry UEM instance	If there is a problem with the management console or BlackBerry UEM Core for a BlackBerry UEM instance, you can continue to access the management console and the BlackBerry UEM Core of any healthy instance.
Round-robin DNS pool for the management console	You can use third-party software to configure a round-robin DNS pool that connects to the management console in each BlackBerry UEM instance. If there is a problem with a console, the pool makes sure that you connect to a working console.
Round-robin DNS pool for the web services API	You can use third-party software to configure a round-robin DNS pool that connects to the web services API in each BlackBerry UEM instance. If there is a problem with one web services API, using the pool makes sure that you connect to a working web services API. If there is a problem using the web services API pool, check the round robin mechanism to ensure the web services API is correctly connected.
BlackBerry Connectivity Node	You can install one or more instances of the BlackBerry Connectivity Node to add additional instances of the device connectivity components to your organization's domain. You can also create server groups to specify regional data paths for secure connectivity and to set up high availability for the components of the BlackBerry Connectivity Node. For more information, see High availability and the BlackBerry Connectivity Node .

Feature	Description
BlackBerry 10 devices	<p>If BlackBerry 10 devices on a BlackBerry UEM instance cannot connect to work resources using enterprise connectivity, those devices are reassigned to healthy BlackBerry UEM instances. BlackBerry 10 devices can use enterprise connectivity to access email and calendar data, the work browser, and the organization's network. Most management tasks (for example, assigning profiles) require enterprise connectivity to complete successfully.</p> <p>The BlackBerry Affinity Manager assigns BlackBerry 10 devices to a BlackBerry UEM instance, monitors enterprise connectivity for each instance, and moves BlackBerry 10 users if there are issues with enterprise connectivity. The BlackBerry Affinity Manager cannot assign iOS, Android, or Windows devices to a specific BlackBerry UEM instance.</p> <p>Only one BlackBerry Affinity Manager is active. The other BlackBerry Affinity Manager instances are on standby. If there is a problem with the active BlackBerry Affinity Manager, each standby instance starts an election process to become active. The instance that completes the election process first becomes the active BlackBerry Affinity Manager.</p>

When BlackBerry UEM is completing a recovery action, affected users experience a short service interruption. The duration depends on a number of factors, including the number of BlackBerry 10 devices and the number of BlackBerry UEM instances. When BlackBerry 10 users are reassigned to another instance, the average down-time is 3 minutes. When a BlackBerry Affinity Manager failover occurs, the average down-time is 10 minutes.

Architecture: High availability for BlackBerry UEM

The following diagram shows a high availability domain with two BlackBerry UEM instances. You can install any number of BlackBerry UEM instances. This topic explains how specific components are involved in a high availability configuration. For more information about the BlackBerry UEM architecture and components, [see the Architecture content](#).



Components	Description
BlackBerry UEM database	Each BlackBerry UEM instance connects to the BlackBerry UEM database to access user and device data.
Management console and BlackBerry UEM Core	<p>You can use any management console to manage the domain's user accounts and devices. The BlackBerry UEM Core associated with that console carries out the management tasks.</p> <p>You can configure a round-robin DNS pool that connects to each console. If there is a problem with a console, the pool connects to a working console.</p>

High availability and the BlackBerry UEM Core

High availability is automatic when you set up a second BlackBerry UEM Core. For a larger environment, install N +1 core nodes. All active core nodes need to be local to DB. Configuration of failover is not required.

Configuring high availability for the management console

To configure high availability for the BlackBerry UEM management consoles, you can use your organization's hardware load balancer or DNS server to configure a round-robin pool that connects to each management console in the domain. If a management console is not available, the load balancer or DNS server connects to one of the other available consoles.

For more information about setting up a round-robin pool, consult the documentation for your organization's hardware load balancer or DNS server.

After you configure a round-robin pool, it is a best practice to update the %AdminPortalURL% and %UserSelfServicePortalURL% variables in the management console (Settings > General settings > Default variables) with the pool name. If you do, email messages that use these variables to link to the management console and BlackBerry UEM Self-Service can use the round-robin pool.

If you enabled single sign-on, you must update the SPNs for the Microsoft Active Directory account with the pool name and restart the BlackBerry UEM services on each computer that hosts a BlackBerry UEM instance.

A BlackBerry UEM management console instance in the round-robin pool can disconnect from the BlackBerry UEM domain if the DNS server assigns a different IP address to that instance. The instance is disconnected because the new IP address doesn't recognize the user's login information. If this happens, the user must log out and log back in again.

High availability and the BlackBerry Connectivity Node

You can install one or more instances of the BlackBerry Connectivity Node to add additional instances of the device connectivity components to your organization's domain. This includes BSCP traffic for enterprise connectivity and BlackBerry Dynamics traffic for BlackBerry Dynamics devices. Each BlackBerry Connectivity Node contains the following BlackBerry UEM components: BlackBerry Secure Connect Plus, the BlackBerry Gatekeeping Service, the BlackBerry Secure Gateway, BlackBerry Proxy, and the BlackBerry Cloud Connector.

Each BlackBerry Connectivity Node provides another active instance of these components to the BlackBerry UEM domain that can process and manage secure device connections. For information about installing a BlackBerry Connectivity Node, see the [the Installation and upgrade content](#).

You can also create server groups. A server group contains one or more instances of the BlackBerry Connectivity Node. When you create a server group, you specify the regional data path that you want the components to use to connect to the BlackBerry Infrastructure. For example, you can create a server group to direct device connections for BlackBerry Secure Connect Plus and the BlackBerry Secure Gateway to use the path for the United States to the BlackBerry Infrastructure. You can associate email and enterprise connectivity profiles with a server group. Any device that is assigned those profiles uses that server group's regional connection to the BlackBerry Infrastructure when it uses any of the components of the BlackBerry Connectivity Node.

Optionally, you can designate each BlackBerry Connectivity Node in a server group to handle a single connection type: BlackBerry Secure Connect Plus only, BlackBerry Secure Gateway only, or BlackBerry Proxy only. This frees up server resources to allow fewer servers required for the same number of users or containers.

If a server group contains multiple instances of the BlackBerry Connectivity Node, devices can use any instance that is running. Device connections are load balanced across the available instances in the group. If no instances

are available, devices cannot use those components for secure connections. At least one of the instances must be available.

Load-balancing data for BlackBerry 10 devices without BSCP

If you install multiple instances of BlackBerry UEM in the same domain, data for BlackBerry 10 devices is load-balanced approximately equally across all healthy, running instances. For example, if you install three instances of BlackBerry UEM and the domain includes 3000 BlackBerry 10 devices, BlackBerry UEM assigns approximately 1000 devices to each of the three running instances.

BlackBerry UEM load-balances when the number of devices on a specific server is more than 500 devices above the average device count per server.

You cannot manually assign BlackBerry 10 devices to a specific instance. The BlackBerry Affinity Manager determines which instances manage BlackBerry 10 devices.

If an instance is temporarily unavailable, the remaining instances manage user and device data.

Each BlackBerry UEM instance uses the same SRP ID and connects to the same BlackBerry UEM database. The components on each instance are all running and actively managing data for all device types, except for the BlackBerry Affinity Manager. Only one instance of the BlackBerry Affinity Manager is active.

You can view the status of each instance in the management console.

How BlackBerry UEM evaluates the health of components

The following BlackBerry UEM components have health scores that are used to determine whether a recovery action is required:

Components	Health monitored by	Health score factors	Action if health is below threshold
BlackBerry MDS Connection Service and BlackBerry Dispatcher (aggregate health score)	Active BlackBerry Affinity Manager	<ul style="list-style-type: none"> Whether the components are running Whether they can connect to the active BlackBerry Affinity Manager Whether they can connect to BlackBerry 10 devices Whether they can connect to the database 	The BlackBerry Affinity Manager moves BlackBerry 10 devices from the unhealthy BlackBerry UEM instance to the healthy instances.

Components	Health monitored by	Health score factors	Action if health is below threshold
Active BlackBerry Affinity Manager	Each standby BlackBerry Affinity Manager	<ul style="list-style-type: none"> The status of the BlackBerry Affinity Manager (active, standby, or in election to become active) Whether it can connect to the BlackBerry Dispatcher Whether it can receive calls from the BlackBerry UEM Core and each standby BlackBerry Affinity Manager Whether it can connect to the BlackBerry Infrastructure Whether it can connect to and load configuration settings from the database 	The standby instances initiate a failover and one becomes the active BlackBerry Affinity Manager.

Configuring database high availability using Microsoft SQL Server AlwaysOn

Before you install BlackBerry UEM, decide if you want to configure high availability for the BlackBerry UEM database. Database high availability allows you to retain database service and data integrity if issues occur with the BlackBerry UEM database.

You can use one of the following Microsoft SQL Server features for database high availability:

- AlwaysOn Failover Cluster Instances (FCI) for Microsoft SQL Server 2014 or 2016 (Standard Edition)
- AlwaysOn Availability Groups for Microsoft SQL Server 2014 or 2016 (Enterprise Edition)
- Database mirroring for Microsoft SQL Server 2014

If you want to use an AlwaysOn feature, you must complete configuration steps before you install BlackBerry UEM. This section gives you instructions for configuring database high availability using AlwaysOn.

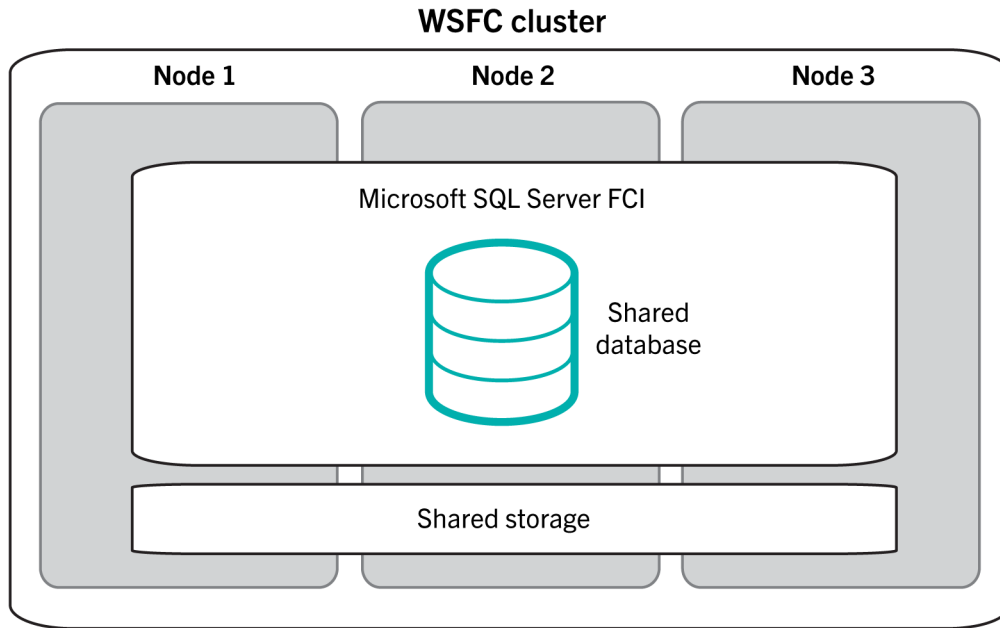
You can configure database mirroring any time after you install BlackBerry UEM. For instructions, see the [Configuration content](#).

Note: Microsoft recommends using AlwaysOn because database mirroring will be deprecated in a future version of Microsoft SQL Server.

AlwaysOn high availability

BlackBerry UEM supports AlwaysOn using a Failover Cluster Instance (FCI) or availability group. Both methods require a Windows Server Failover Clustering (WSFC) cluster where independent servers interact to provide a high availability solution for databases. For more information about WSFC, visit the [MSDN Library](#) to see [Windows Server Failover Clustering \(WSFC\) with SQL Server](#).

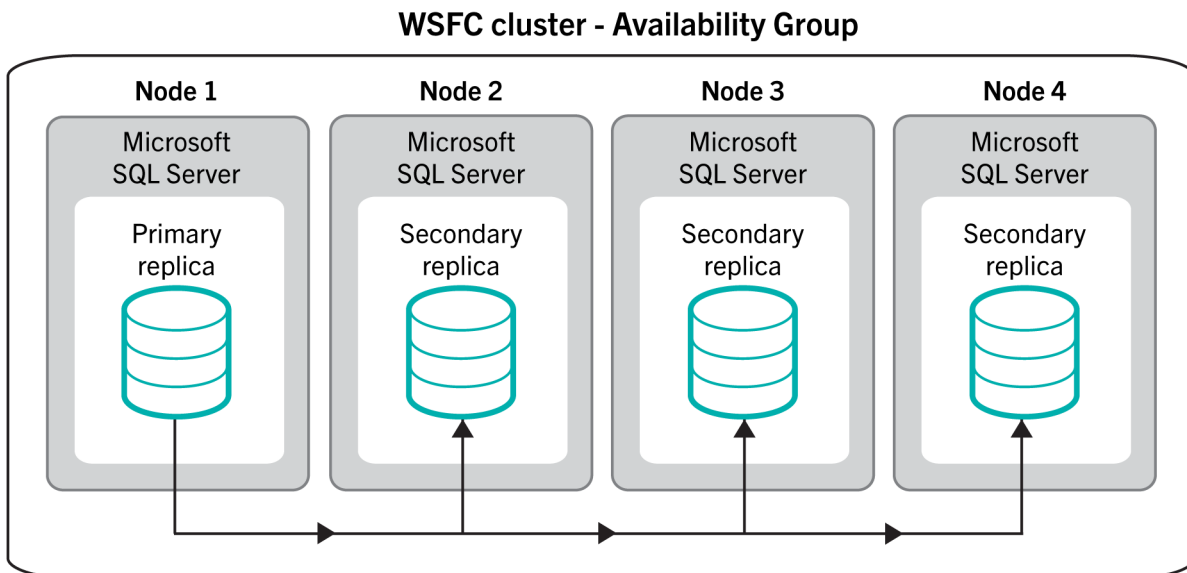
Instance-level high availability using an AlwaysOn Failover Cluster Instance



An FCI is an instance of Microsoft SQL Server that is installed across multiple computers (or “nodes”) in a WSFC cluster. The nodes are members of a resource group, and all nodes have shared access to the BlackBerry UEM database. One of the nodes has ownership of the resource group and gives the BlackBerry UEM components access to the BlackBerry UEM database. If the node that owns the resource group becomes unavailable (for example, a hardware or OS failure), a different node takes ownership of the resource group. As a result, BlackBerry UEM database service continues with minimal interruption.

For more information, visit the [MSDN Library](#) to see [AlwaysOn Failover Cluster Instances \(SQL Server\)](#).

Database-level high availability using an AlwaysOn availability group



To use an availability group, you configure a WSFC cluster with multiple nodes. Each node is a separate computer that has an instance of Microsoft SQL Server. One of the nodes hosts the primary BlackBerry UEM database and

gives the BlackBerry UEM components read-write access. This node is the “primary replica.” The WSFC cluster can have one to eight other nodes, each hosting a secondary database. These nodes are “secondary replicas.”

The primary database synchronizes data with the secondary databases. Data is synchronized with each secondary database independently. If one secondary database is unavailable, it does not affect the other secondary databases. You can configure the data synchronization to be asynchronous (delayed synchronization with minimal transaction latency) or synchronous (faster synchronization with increased transaction latency). BlackBerry recommends the synchronous configuration. Automatic failover requires the primary replica and secondary replicas to use synchronous-commit mode.

If you configure an availability group for automatic failover and the primary database becomes unavailable, one of the secondary replicas becomes the primary replica. That replica’s secondary database becomes the primary database. As a result, BlackBerry UEM database service continues with minimal interruption.

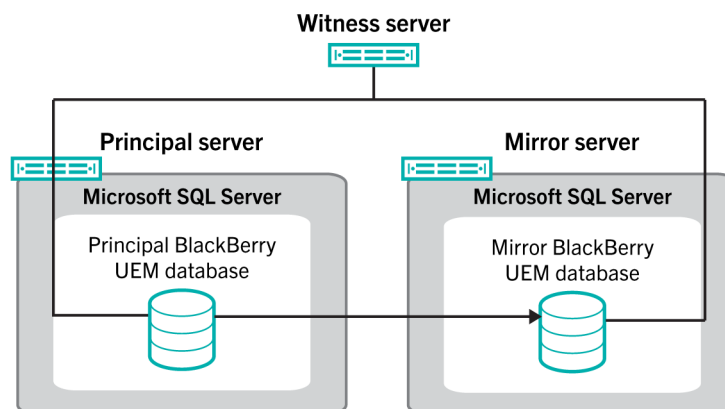
For more information, visit the [MSDN Library](#) to see [Overview of AlwaysOn Availability Groups \(SQL Server\)](#) and [AlwaysOn Availability Groups \(SQL Server\)](#).

AlwaysOn requirements

Review the following requirements for configuring AlwaysOn in a BlackBerry UEM environment:

- Create a WSFC cluster. It is recommended to use static port 1433 for the database server. For requirements and instructions, visit the [Technet Library](#) to see [Create a Failover Cluster](#).
- If you want to use an AlwaysOn FCI:
 - Verify that your environment meets Microsoft requirements. Visit the [MSDN Library](#) to see [Before Installing Failover Clustering](#).
 - Configure the FCI. Visit the [MSDN Library](#) to see [Create a New SQL Server failover Cluster \(Setup\)](#).
- If you want to use an AlwaysOn availability group:
 - Verify that your environment meets Microsoft requirements. Visit the [MSDN Library](#) to see [Prerequisites, Restrictions, and Recommendations for AlwaysOn Availability Groups \(SQL Server\)](#).
 - Enable the availability groups feature and complete the initial setup tasks, including creating an availability group listener. You will set up the primary replica and secondary replicas after you install BlackBerry UEM and create the BlackBerry UEM database. Visit the [MSDN Library](#) to see [Getting Started with AlwaysOn Availability Groups](#).

Configuring database high availability using database mirroring



You can use database mirroring to provide high availability for the BlackBerry UEM database. Database mirroring is a Microsoft SQL Server feature that allows you to retain database service and data integrity if issues occur with the BlackBerry UEM database.

Note: Microsoft plans to deprecate database mirroring in future versions of Microsoft SQL Server, and recommends using the AlwaysOn feature for database high availability. Using AlwaysOn requires configuration steps before you install BlackBerry UEM. For more information about using AlwaysOn, [Configuring database high availability using Microsoft SQL Server AlwaysOn](#). The AlwaysOn feature cannot be used if you upgrade from BES5 to BlackBerry UEM (the BES5 database is upgraded to a BlackBerry UEM database). AlwaysOn is not supported for the components that manage BlackBerry OS devices.

When you configure database mirroring, you back up the principal BlackBerry UEM database (the database created during installation) and you use the backup files to create a mirror database on a different computer. You then configure a mirroring relationship between the two databases so that the mirror database performs the same actions and stores the same data.

To enable automatic failover, you set up a witness server to monitor the principal database. If the principal database stops responding, the witness starts an automatic failover to the mirror database. The BlackBerry UEM components connect to the mirror database and device service continues without interruption. A role switch occurs: the mirror database becomes the principal database, and the original principal database becomes the mirror database. This role switch can occur several times during a mirroring session.

To learn more about database mirroring, visit technet.microsoft.com/sqlserver to read [Database Mirroring Witness – SQL Server 2012](#) or [Database Mirroring Witness – SQL Server 2014](#).

Database mirroring requirements

Item	Requirement
Microsoft SQL Server	BlackBerry UEM supports database mirroring using one of the following: <ul style="list-style-type: none"> • Microsoft SQL Server 2012 • Microsoft SQL Server 2014
SQL Server Native Client	The SQL Server 2012 Native Client must be installed on each computer that hosts a BlackBerry UEM instance. The BlackBerry UEM setup application installs the SQL Server 2012 Native Client.
Version parity	The Microsoft SQL Server that hosts the mirror database must be the same version and edition as the Microsoft SQL Server that hosts the principal database.
Database location	Make sure that the active copy of the mirror database is always in the local datacenter.
Operating mode	Configure database mirroring using high-safety mode with automatic failover.
Witness	A witness server is required for automatic failover. The witness must be a different server than the principal server and the mirror server. For more information, see Database Mirroring Witness – SQL Server 2012 or Database Mirroring Witness – SQL Server 2014 .

Preinstallation and preupgrade requirements

Review the following checklists before you begin installing or upgrading BlackBerry UEM.

Hardware requirements

Review and complete the [Performance Calculator for BlackBerry UEM](#).

The performance calculator provides minimum recommendations based on the values you enter. If you require additional capacity, redundancy, or room for growth, enter values that reflect these needs to accommodate any near future large app and user deployment projects.

Ensure your environment meets the [hardware requirements](#) for your needs.

Ensure that database latency requirements are met. BlackBerry UEM Core servers must have less than 5ms latency to the database server.

Third-party software requirements

Verify that your computer is running [an operating system that supports BlackBerry UEM](#).

Verify that you have [a supported browser](#) on the computers that host the BlackBerry UEM management console.

The browser must support configuration of the following settings:

- Support for JavaScript
- Cookies turned on
- Support for TLS
- SSL certificate installed to permit trusted connections to the consoles

If you have a requirement to use a proxy server in your organization, verify that you have a supported proxy solution.

Ensure that Windows is up to date and that you perform any reboot required for the update.

Verify that your computer is running Windows PowerShell 2.0 or later for the following:

- RRAS for BlackBerry Secure Connect Plus setup during the BlackBerry UEM installation
- Exchange ActiveSync gatekeeping (optional)

Verify that you have installed JRE 8 on the servers where you will install BlackBerry UEM. Visit support.blackberry.com to review article 52117.

For more information about supported JRE versions, see the [Compatibility matrix](#).

Verify that you have [a mail server that supports BlackBerry UEM](#).

Verify that [the Exchange ActiveSync version meets the minimum requirements](#).

Environment configuration requirements

Verify that the [BlackBerry UEM listening ports](#) are configured.

Verify that you opened the necessary ports on your organization's firewall. For more information about port and firewall requirements, visit support.blackberry.com/community to read article 36470.

Note: BlackBerry UEM services do not support SSL Termination, SSL Offloading, SSL Packet Inspection or Deep Packet Inspection. Ensure these endpoint services are not enabled on your proxy/firewall.

Verify that the TCP/IP network protocols are turned on for your BlackBerry UEM database.

Verify that you have DNS support for resolving IP addresses into host names.

If you perform the installation or upgrade process on a computer that has more than one NIC, verify that the production NIC is first in the bind order in the Windows network settings.

If a Windows host operating system is configured in a workgroup instead of a domain, verify that you configured the primary DNS suffix. For information on configuring the primary DNS suffix, visit the Microsoft support website.

Ensure that the no count setting for the Microsoft SQL Server is disabled.

Verify that the BlackBerry UEM service account has local administrator permissions on each computer.

The Microsoft SQL Server account must have dbo as its default schema.

Ensure antivirus exclusions have been made for both the extracted installation files and the target installation and logging directories.

For more information, visit support.blackberry.com/community to read article 36596.

If you previously upgraded from a legacy Good Control environment and modified the Java Heap value, make note of the existing value. You will need to reapply the change after upgrade. For more information, visit support.blackberry.com/community to read article 56641.

Additional considerations

Review all current [Critical Issue Advisories](#). Contact BlackBerry Technical Support if you are unsure whether a particular advisory applies to you.

Review the [Release Notes](#).

Review the [BlackBerry UEM Compatibility Matrix](#) and the [Mobile/Desktop OS Compatibility Matrix](#).

Review the [Installation and Upgrade Guide](#).

Review the information about [supported upgrade environments](#).

If you plan to install BlackBerry UEM in a DMZ, read [Installing BlackBerry UEM in a DMZ](#).

Additional considerations

Plan for an appropriate amount of downtime based on the number of servers in your environment.

Upgrading the first server may take 45-60 minutes. Additional servers may take 15-45 minutes depending on which components are installed and whether or not these components can be installed in parallel. Consider adding additional time to account for rolling back servers if troubleshooting is required.

Verify that you have [the appropriate licenses](#).

Visit support.blackberry.com/community to read article 38341 about licensing.

Make sure that your perpetual licenses are supported. Visit support.blackberry.com/community to read article 36537.

Perpetual licenses are issued for specific versions of BlackBerry UEM and are not compatible with later versions. If perpetual licenses are covered by a valid support contract, automatic version updates are supported.

Visit support.blackberry.com/community to review article 38980 about upgrades.

If your organization uses a proxy server for Internet access, verify that you have the computer name, port number, and credentials for the proxy server.

If your organization uses Apple VPP accounts, after the upgrade you must generate a new .vpp token file and edit your Apple VPP account information at Apps > iOS App licenses.

If you are planning a multistage upgrade, review the upgrade documentation for the versions you are upgrading to.

Decommission surplus nodes, if applicable. For more information, visit support.blackberry.com/community to read article 46210 and see the [Installation and upgrade content](#) for instructions on how to remove BlackBerry UEM software.

Hardware requirements

BlackBerry UEM hardware requirements depend on the size of your environment. BlackBerry UEM also has requirements for third-party software compatibility.

To determine the CPU and disk space requirements for BlackBerry UEM, you must consider the number of devices that you plan to activate, the types of connection that devices use, and the level and type of user activity on devices. To calculate hardware requirements for a BlackBerry UEM environment, use the [Performance Calculator for BlackBerry UEM](#).

- [Hardware requirements: BlackBerry UEM](#)
- [Hardware requirements: BEMS](#)
- [Hardware requirements: BlackBerry Router](#)

Hardware requirements: BlackBerry UEM

The following sections list the hardware requirements for BlackBerry UEM.

Note: If you are installing BlackBerry UEM on virtual machines, the servers require dedicated or reserved hardware resources.

Small deployments

A small BlackBerry UEM deployment consists of 2000 or fewer devices. All BlackBerry UEM components are typically installed on one server; however, you can install the BlackBerry Connectivity Node and Microsoft SQL Server on separate servers.

Hardware requirements for up to 500 devices

For up to 500 devices, install the BlackBerry UEM primary components, BlackBerry UEM management console, BlackBerry Connectivity Node, and Microsoft SQL Server or Microsoft SQL Server Express on one server. A domain with this configuration can have a maximum of 500 devices.

Note: You may need to adjust the -Xmx values of the UI and Core services for this configuration.

Server	Requirement
BlackBerry UEM primary components, BlackBerry UEM management console, BlackBerry Connectivity Node, and Microsoft SQL Server or Microsoft SQL Server Express	<ul style="list-style-type: none">• 6 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent• 20 GB of available memory• 64 GB of disk space

Hardware requirements for up to 1000 devices

For up to 1000 devices, install the BlackBerry UEM primary components, the BlackBerry UEM management console, and the BlackBerry Connectivity Node on one server, and Microsoft SQL Server on another server. A domain with this configuration can have a maximum of 1000 devices. The servers that host BlackBerry UEM must be physically located near the server with the Microsoft SQL Server databases (less than 5ms latency).

Note: You may need to adjust the -Xmx values of the UI and Core services for this configuration.

BlackBerry UEM server	Requirement
BlackBerry UEM primary components, BlackBerry UEM management console, and BlackBerry Connectivity Node	<ul style="list-style-type: none"> • 6 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 24 GB of available memory • 64 GB of disk space

Database server	Requirement
Microsoft SQL Server	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 6 GB of available memory • 64 GB of disk space

Hardware requirements for up to 2000 devices

For a domain with up to 2000 devices, you can install all BlackBerry UEM components on one server, or you can install the BlackBerry UEM primary components and management console on one server, and the BlackBerry Connectivity Node on another server.

In both types of deployment, install Microsoft SQL Server on a separate server. The server that hosts BlackBerry UEM must be physically located near the server with the Microsoft SQL Server databases (less than 5ms latency).

BlackBerry UEM servers	Requirement
All BlackBerry UEM components on one server	
BlackBerry UEM primary components, management console, and BlackBerry Connectivity Node	<ul style="list-style-type: none"> • 8 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 28 GB of available memory • 64 GB of disk space
BlackBerry UEM components on separate servers	
BlackBerry UEM primary components and BlackBerry UEM management console	<ul style="list-style-type: none"> • 4 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 16 GB of available memory • 64 GB of disk space
BlackBerry Connectivity Node	<ul style="list-style-type: none"> • 4 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

Database server	Requirement
Microsoft SQL Server	<ul style="list-style-type: none"> • 4 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 8 GB of available memory • 64 GB of disk space

Medium deployments

A medium BlackBerry UEM deployment consists of between 2000 and 25,000 devices. You can install all the BlackBerry UEM components on one server, or have a separate server for the BlackBerry Connectivity Node. Microsoft SQL Server is installed on a separate server. You can install multiple instances of BlackBerry UEM and multiple instances of the BlackBerry Connectivity Node.

Hardware requirements for up to 5000 devices

For a domain with up to 5000 devices, you can install all BlackBerry UEM components on one server, or you can install the BlackBerry UEM primary components and management console on one server, and the BlackBerry Connectivity Node on one or two additional servers.

You can have multiple instances of BlackBerry UEM and multiple instances of the BlackBerry Connectivity Node. Multiple instances require increased database CPU and memory.

In both types of deployment, install Microsoft SQL Server on a separate server. The servers that host BlackBerry UEM must be physically located near the server with the Microsoft SQL Server databases (less than 5ms latency).

BlackBerry UEM servers	Requirement
All BlackBerry UEM components on one server	
BlackBerry UEM primary components, management console, and BlackBerry Connectivity Node	<ul style="list-style-type: none"> • 10 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 28 GB of available memory • 64 GB of disk space
BlackBerry UEM components on separate servers	
BlackBerry UEM primary components and BlackBerry UEM management console	<ul style="list-style-type: none"> • 4 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 16 GB of available memory • 64 GB of disk space
BlackBerry Connectivity Node	<ul style="list-style-type: none"> • 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

Database server	Requirement
Microsoft SQL Server	<ul style="list-style-type: none"> • 8 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 16 GB of available memory • 64 GB of disk space

Hardware requirements for up to 25,000 devices

For a domain with up to 25,000 devices, you can install all BlackBerry UEM components on one server, or you can install the BlackBerry UEM primary components and management console on one server, and the BlackBerry Connectivity Node on another server.

In both types of deployment, install Microsoft SQL Server on a separate server. The servers that host BlackBerry UEM must be physically located near the server with the Microsoft SQL Server database (less than 5ms latency).

One instance of BlackBerry UEM can support:

- Up to 25,000 Android, Windows 10, or BlackBerry 10 devices with MDM-only activation (no BlackBerry Dynamics)
- Up to 25,000 Android, iOS, Windows 10, or macOS devices with BlackBerry Dynamics-only activation (no MDM)
- Up to 20,000 Android devices with MDM and BlackBerry Dynamics
- Up to 10,000 iOS devices with MDM (with or without BlackBerry Dynamics)

Specific features may also limit the number of devices that one instance can support. Use the [Performance Calculator for BlackBerry UEM](#) to determine the number of instances required.

One standard instance of the BlackBerry Connectivity Node can support up to 5000 iOS, macOS, Android, Windows, or BlackBerry 10 devices.

However, if you enable single-service performance mode, the BlackBerry Connectivity Node can support up to 10,000 devices per instance.

BlackBerry UEM server	Requirement
All BlackBerry UEM components on one server	
BlackBerry UEM primary components, management console, and BlackBerry Connectivity Node (5000 devices per instance)	<ul style="list-style-type: none"> • 10 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 28 GB of available memory • 64 GB of disk space
BlackBerry UEM components on separate servers	
BlackBerry UEM primary components and BlackBerry UEM management console (25,000 devices per instance for MDM-only or BlackBerry Dynamics-only, 20,000 Android devices per instance for MDM and BlackBerry Dynamics, 10,000 iOS devices per instance for MDM and BlackBerry Dynamics. Use the Performance Calculator for BlackBerry UEM for details.)	<ul style="list-style-type: none"> • 8 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 16 GB of available memory • 64 GB of disk space

BlackBerry UEM server	Requirement
BlackBerry Connectivity Node (5000 devices per instance)	<ul style="list-style-type: none"> • 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Proxy only (10,000 devices per instance)	<ul style="list-style-type: none"> • 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Secure Connect Plus only (10,000 devices per instance)	<ul style="list-style-type: none"> • 4 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Secure Gateway only (10,000 devices per instance)	<ul style="list-style-type: none"> • 8 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

Database server	Requirement
Microsoft SQL Server	<ul style="list-style-type: none"> • 12 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 30 GB of available memory • 64 GB of disk space

Large deployments

A large BlackBerry UEM deployment consists of between 25,000 and 150,000 devices. You can install all the BlackBerry UEM components on one server, or have a separate server for the BlackBerry Connectivity Node. Microsoft SQL Server is installed on a separate server. You can install multiple instances of BlackBerry UEM and multiple instances of the BlackBerry Connectivity Node.

Hardware requirements for up to 150,000 devices

For a domain with up to 150,000 devices, you can install multiple instances of all BlackBerry UEM components, or you can install multiple instances of the BlackBerry UEM primary components and management console, and multiple instances of the BlackBerry Connectivity Node.

In both types of deployment, install Microsoft SQL Server on a separate server. The servers that host BlackBerry UEM must be physically located near the server with the Microsoft SQL Server database (less than 5ms latency). The BlackBerry UEM servers do not need to be near the mail and messaging servers.

One instance of BlackBerry UEM can support:

- Up to 25,000 Android, Windows 10, or BlackBerry 10 devices with MDM-only activation (no BlackBerry Dynamics)
- Up to 25,000 Android, iOS, Windows 10, or macOS devices with BlackBerry Dynamics-only activation (no MDM)

- Up to 20,000 Android devices with MDM and BlackBerry Dynamics
- Up to 10,000 iOS devices with MDM (with or without BlackBerry Dynamics)

Specific features may also limit the number of devices that one instance can support. Use the [Performance Calculator for BlackBerry UEM](#) to determine the number of instances required.

One instance of the BlackBerry Connectivity Node can support up to 5000 iOS, macOS, Android, Windows, or BlackBerry 10 devices.

However, if you enable single-service performance mode, the BlackBerry Connectivity Node can support up to 10,000 devices per instance.

BlackBerry UEM servers	Requirement
All BlackBerry UEM components on one server	
BlackBerry UEM primary components, management console, and BlackBerry Connectivity Node (5000 devices per instance)	Install enough instances of BlackBerry UEM to support the number of devices. <ul style="list-style-type: none"> • 10 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 28 GB of available memory • 64 GB of disk space
BlackBerry UEM components on separate servers	
BlackBerry UEM primary components and BlackBerry UEM management console (25,000 devices per instance for MDM-only or BlackBerry Dynamics-only, 20,000 Android devices per instance for MDM and BlackBerry Dynamics, 10,000 iOS devices per instance for MDM and BlackBerry Dynamics. Use the Performance Calculator for BlackBerry UEM for details.)	Install enough instances of BlackBerry UEM to support the number of devices. <ul style="list-style-type: none"> • 8 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 16 GB of available memory • 64 GB of disk space
BlackBerry Connectivity Node (5000 devices per instance)	Install enough instances of BlackBerry Connectivity Node to support the number of devices. <ul style="list-style-type: none"> • 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Proxy only (10,000 devices per instance)	<ul style="list-style-type: none"> • 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
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Secure Connect Plus only (10,000 devices per instance)	<ul style="list-style-type: none"> • 4 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

BlackBerry UEM servers	Requirement
BlackBerry Connectivity Node with single-service performance mode enabled for BlackBerry Secure Gateway only (10,000 devices per instance)	<ul style="list-style-type: none"> • 8 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

Database server	Requirement
Microsoft SQL Server Note: Microsoft SQL Server has compute capacity limits on the number of processor cores that specific editions support. Ensure that the edition of Microsoft SQL Server you are using supports 24 processor cores.	<ul style="list-style-type: none"> • 24 processor cores, E5-2670 (2.6 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 30 GB of available memory • 64 GB of disk space

Hardware requirements: BEMS

The following sections list the hardware requirements for BEMS.

Note:

- If you are installing BEMS on virtual machines, the servers require dedicated or reserved hardware resources.
- You can compress the log files that are generated and saved in the default log folder or folder you specified during the installation of BEMS. For more information, see ["Enabling log file compression" in the BEMS-Core configuration content](#).

Small deployments

A small BEMS deployment consists of 2000 or fewer devices.

BEMS hardware requirements for up to 500 devices

For up to 500 devices, install BEMS (with BlackBerry Push Notifications and BlackBerry Presence only) on the same server as the BlackBerry UEM primary components, BlackBerry UEM management console, BlackBerry Connectivity Node, and Microsoft SQL Server or Microsoft SQL Server Express. A domain with this configuration can have a maximum of 500 devices.

Note: You may need to adjust the -Xmx values of the UI and Core services for this configuration.

Note: To add BlackBerry Connect, you must meet the hardware requirements for 2000 or 5000 devices, which require a separate server for BEMS.

Server	Requirement
BEMS (with BlackBerry Push Notifications and BlackBerry Presence), BlackBerry UEM primary components, BlackBerry UEM management console, BlackBerry Connectivity Node, and Microsoft SQL Server or Microsoft SQL Server Express	<ul style="list-style-type: none"> • 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 22 GB of available memory • 64 GB of disk space

BEMS hardware requirements for up to 1000 devices

For up to 1000 devices, install BlackBerry UEM and BEMS (with BlackBerry Push Notifications and BlackBerry Presence) on one server and Microsoft SQL Server on another server. The BlackBerry UEM and BEMS server must be physically located near the server that hosts the Microsoft SQL Server database.

Note: You may need to adjust the -Xmx values of the UI and Core services for this configuration.

BlackBerry UEM and BEMS server	Requirement
BlackBerry UEM and BEMS (with BlackBerry Push Notifications and BlackBerry Presence)	<ul style="list-style-type: none"> • 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 26 GB of available memory • 64 GB of disk space

Database server	Requirement
Microsoft SQL Server	<ul style="list-style-type: none"> • 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 2 GB of available memory • 64 GB of disk space

BEMS hardware requirements for up to 2000 devices

For up to 2000 devices, install BEMS on its own server. The BEMS server must be physically located near the server that hosts the Microsoft SQL Server database.

Note: If you install both BEMS with BlackBerry Push Notifications and BEMS with BlackBerry Connect, install BlackBerry Presence on only one of those two servers.

BEMS servers	Requirement
BEMS with BlackBerry Push Notifications and optional BlackBerry Presence	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 6 GB of available memory • 64 GB of disk space
BEMS with BlackBerry Connect and optional BlackBerry Presence	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 6 GB of available memory • 64 GB of disk space

Database servers	Requirement
Microsoft SQL Server for BEMS with BlackBerry Push Notifications	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 4 GB of available memory • 64 GB of disk space
Microsoft SQL Server for BEMS with BlackBerry Connect	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 4 GB of available memory • 64 GB of disk space

Medium deployments

A medium BEMS deployment consists of between 2000 and 25,000 devices. You must install BEMS on its own server, and you can deploy multiple BEMS servers.

BEMS hardware requirements for up to 5000 devices

For up to 5000 devices, install BEMS on its own server. The BEMS server must be physically located near the server that hosts the Microsoft SQL Server database.

Note: If you install both BEMS with BlackBerry Push Notifications and BEMS with BlackBerry Connect, install BlackBerry Presence on only one of those two servers.

BEMS servers	Requirement
BEMS with BlackBerry Push Notifications and optional BlackBerry Presence	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 8 GB of available memory • 128 GB of disk space
BEMS with BlackBerry Connect and optional BlackBerry Presence	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 8 GB of available memory • 64 GB of disk space

Database servers	Requirement
Microsoft SQL Server for BEMS with BlackBerry Push Notifications	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 6 GB of available memory • 64 GB of disk space
Microsoft SQL Server for BEMS with BlackBerry Connect	<ul style="list-style-type: none"> • 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent • 6 GB of available memory • 64 GB of disk space

BEMS hardware requirements for up to 25,000 devices

For up to 25,000 devices, install BEMS on its own server. This configuration requires multiple BEMS servers (not including high availability or disaster recovery scenarios). One dedicated instance of BEMS can support approximately 10,000 devices. To support more devices, add more instances of BEMS.

Use the [BEMS Performance Calculator](#) to determine the minimum number of BEMS instances for your device configuration and workload.

The servers that BEMS is installed on must be physically located near the server that hosts the Microsoft SQL Server database (less than 5 ms latency).

Note: If you install both BEMS with BlackBerry Push Notifications and BEMS with BlackBerry Connect, install BlackBerry Presence on only one of those two servers.

BEMS servers	Requirement
BEMS with BlackBerry Push Notifications and optionally BlackBerry Presence	<ul style="list-style-type: none">• 4 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent• 8 GB of available memory• 250 GB of disk space
BEMS with BlackBerry Connect and optionally BlackBerry Presence	<ul style="list-style-type: none">• 4 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent• 8 GB of available memory• 64 GB of disk space

Database servers	Requirement
Microsoft SQL Server for BEMS with BlackBerry Push Notifications	<ul style="list-style-type: none">• 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent• 8 GB of available memory• 64 GB of disk space
Microsoft SQL Server for BEMS with BlackBerry Connect	<ul style="list-style-type: none">• 2 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent• 8 GB of available memory• 64 GB of disk space

Large deployments

A large BEMS deployment consists of between 25,000 and 150,000 devices. You must install BEMS on its own server, and you can deploy multiple BEMS servers.

BEMS hardware requirements for up to 150,000 devices

For up to 150,000 devices, install BEMS on its own server. This configuration requires multiple BEMS servers (not including high availability or disaster recovery scenarios). One dedicated instance of BEMS can support approximately 10,000 devices. To support more devices, add more instances of BEMS.

Use the [BEMS Performance Calculator](#) to determine the minimum number of BEMS instances for your device configuration and workload.

The servers that BEMS is installed on must be physically located near the server that hosts the Microsoft SQL Server database (less than 5 ms latency).

Note: If you install both BEMS with BlackBerry Push Notifications and BEMS with BlackBerry Connect, install BlackBerry Presence on only one of those two servers.

BEMS servers	Requirement
BEMS with BlackBerry Push Notifications and optionally BlackBerry Presence (one for every 10,000 devices)	<ul style="list-style-type: none"> 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent 8 GB of available memory 250 GB of disk space
BEMS with BlackBerry Connect and optionally BlackBerry Presence	<ul style="list-style-type: none"> 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent 8 GB of available memory 64 GB of disk space

Database servers	Requirement
Microsoft SQL Server for BEMS with BlackBerry Push Notifications	<ul style="list-style-type: none"> 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent 12 to 24 GB of available memory, depending on the size of EWS SyncState, up to 60 KB 64 GB of disk space
Microsoft SQL Server for BEMS with BlackBerry Connect	<ul style="list-style-type: none"> 6 processor cores, E5-2670 v2 (2.5 GHz), E5-2683 v4 (2.1 GHz), or equivalent 8 GB of available memory 64 GB of disk space

Hardware requirements: BlackBerry Router

The following requirements apply to the computer that you install a standalone BlackBerry Router on.

Number of activated devices	Requirement
1 to 150,000	<ul style="list-style-type: none"> One processor, Quad Core, 2.7 GHz (4 cores) or 4 vCPU 4 GB of available memory 64 GB of disk space

Port requirements

Before you install or upgrade BlackBerry UEM, you should familiarize yourself with how BlackBerry UEM uses ports.

The BlackBerry UEM components use various ports to communicate with the BlackBerry Infrastructure, the BlackBerry Dynamics NOC, and internal resources (for example, your organization's messaging software). The topics in this section indicate the default ports that BlackBerry UEM uses for outbound connections and also describe the internal connections that you should verify. These port connections are required whether or not BlackBerry UEM is installed in a DMZ.

BlackBerry Enterprise Mobility Server (BEMS) must be installed in BlackBerry UEM environments that use BlackBerry Dynamics. BEMS has port requirements for communication with BlackBerry UEM and the BlackBerry Dynamics NOC.

For more information about BlackBerry UEM and BEMS ports, visit support.blackberry.com/kb to read article 36470.

Server configuration

The recommended and least restrictive firewall configuration is to enable the listed TCP ports to carry outbound-initiated bidirectional communications to the blackberry.com and bbsecure.com subdomains.

Usage	TCP port	Protocol	Domain
BlackBerry UEM Core, BlackBerry Proxy, app servers	443	TCP	gdmdc.good.com
BlackBerry Proxy	443	TCP	gdrelay.good.com
BlackBerry Proxy	443	TCP	gdentgw.good.com
BlackBerry UEM Core, BlackBerry Proxy, BlackBerry Enterprise Mobility Server	443	TCP	gdweb.good.com
BlackBerry Enterprise Mobility Server	443	TCP	login.good.com
BlackBerry Enterprise Mobility Server	443	TCP	gwupload.good.com
BlackBerry Enterprise Mobility Server	443	TCP	gwmonitor.good.com
BlackBerry Enterprise Mobility Server	443	TCP	fcm.googleapis.com
BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<country>.srp.blackberry.com
BlackBerry UEM Core	3101	TCP	<region>.bbsecure.com
BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com
BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com

Usage	TCP port	Protocol	Domain
BlackBerry Secure Connect Plus with Knox Workspace	443	TCP	api.samsungapps.com

Note: <region> represents a unique region code depending on the EULA selected during installation. For example, if Canada was selected, then <region> is ca. To find a specific country code, see the [ISO Standard](#).

Global IP ranges

Region	Usage	TCP port	Protocol	Domain	IP address
All	BlackBerry UEM Core, BlackBerry Proxy, app servers	443	TCP	gdmdc.good.com	206.124.114.93
	BlackBerry Proxy	443	TCP	gdrelay.good.com	206.124.114.91
	BlackBerry Proxy	443	TCP	gdentgw.good.com	206.124.114.89
	BlackBerry UEM Core, BlackBerry Proxy, BlackBerry Enterprise Mobility Server	443	TCP	gdweb.good.com	206.124.114.92
	BlackBerry Enterprise Mobility Server	443	TCP	login.good.com	206.124.122.112
	BlackBerry Enterprise Mobility Server	443	TCP	gwupload.good.com	206.124.122.73
	BlackBerry Enterprise Mobility Server	443	TCP	gwmonitor.good.com	206.124.122.73
Asia Pacific region (APAC) excluding Saudi Arabia and UAE	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<country>.srp.blackberry.cc	216.9.240.6 68.171.240.33
	BlackBerry Secure Connect Service	3101	TCP	<region>.bbsecure.com	103.246.200.136
	BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com	103.246.200.136

Region	Usage	TCP port	Protocol	Domain	IP address
	BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com	103.246.200.138 103.246.200.139 103.246.201.138 103.246.201.139
Canada	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	ca.srp.blackberry.com	216.9.242.6 68.171.242.6
	BlackBerry Secure Connect Service	3101	TCP	ca.bbsecure.com	216.9.242.244
	BlackBerry Connectivity Node	3101	TCP	ca.bbsecure.com	216.9.242.244
	BlackBerry Secure Connect Plus	3101	TCP	ca.turnb.bbsecure.com	216.9.242.242 216.9.242.243 74.82.72.242 74.82.72.243
Europe, the Middle East, and Africa region (EMEA)	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<region>.srp.blackberry.com	93.186.25.33 193.109.81.33
	BlackBerry Secure Connect Service	3101	TCP	<region>.bbsecure.com	93.186.19.240
	BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com	93.186.19.240
	BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com	93.186.19.242 93.186.19.243 93.186.17.242 93.186.17.243
India and Southern Asia	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<region>.srp.blackberry.com	216.9.240.6 68.171.240.33
	BlackBerry Secure Connect Service	3101	TCP	<region>.bbsecure.com	93.186.19.240
	BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com	93.186.19.240

Region	Usage	TCP port	Protocol	Domain	IP address
	BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com	93.186.19.242 93.186.19.243 93.186.17.242 93.186.17.243
Latin America and the Caribbean	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<region>.srp.blackberry.com	216.9.242.32 68.171.242.32
	BlackBerry Secure Connect Service	3101	TCP	<region>.bbsecure.com	216.9.242.244
	BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com	216.9.242.244
	BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com	216.9.242.242 216.9.242.243 74.82.72.242 74.82.72.243
Saudi Arabia	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<region>.srp.blackberry.com	5.100.168.48 5.100.168.49
	BlackBerry Secure Connect Service	3101	TCP	<region>.bbsecure.com	93.186.19.240
	BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com	93.186.19.240
	BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com	93.186.19.242 93.186.19.243 93.186.17.242 93.186.17.243
United Arab Emirates	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	<region>.srp.blackberry.com	131.117.168.48 131.117.168.49
	BlackBerry Secure Connect Service	3101	TCP	<region>.bbsecure.com	>93.186.19.240
	BlackBerry Connectivity Node	3101	TCP	<region>.bbsecure.com	93.186.19.240
	BlackBerry Secure Connect Plus	3101	TCP	<region>.turnb.bbsecure.com	93.186.19.242 93.186.19.243 93.186.17.242 93.186.17.243

Region	Usage	TCP port	Protocol	Domain	IP address
United States	BlackBerry Affinity Manager, BlackBerry Dispatcher	3101	TCP	us.srp.blackberry.com	216.9.242.33 68.171.242.33
	BlackBerry Secure Connect Service	3101	TCP	us.bbsecure.com	216.9.242.240
	BlackBerry Connectivity Node	3101	TCP	us.bbsecure.com	216.9.242.240
	BlackBerry Secure Connect Plus	3101	TCP	us.turnb.bbsecure.com	74.82.72.202 74.82.72.203 68.171.242.202 68.171.242.203

Mobile device configuration (Wi-Fi requirements)

The port requirements in this section are for mobile devices to connect to the BlackBerry Infrastructure. These addresses and ports may not be required by the BlackBerry UEM server components. For example, in a typical Wi-Fi network setup, connectivity to the internet on port 443 is allowed, but connectivity to APNs may be blocked.

Mobile devices managed by UEM also have specific connectivity requirements. Whether the device is attempting a connection over the mobile network or a Wi-Fi network, the port requirements must be met.

Note: <region> represents a unique region code depending on the EULA selected during installation. For example, if Canada was selected, then <region> is ca. To find a specific country code, see the ISO Standard.

Device OS	TCP port	Protocol	Domain
BlackBerry 10 OS, iOS, Android OS, iOS, Windows Phone OS	443	HTTPS/TLS ¹	<region>.bbsecure.com
iOS	5223	TCP	gateway.push.apple.com
EMM/Google APIs ²	443	TCP	android.apis.google.com
Google Play ²	TCP/443 TCP,UDP/5228-5230	TCP, UDP	play.google.com, googleusercontent.com, google-analytics.com, gstatic.com, android.com, gvt1.com, gvt2.com, ggph.com
Google authentication ²	443	TCP	accounts.google.com
Google Cloud Messaging ²	TCP/443,5228-5230, 5235,5236	TCP	gcm-http.googleapis.com, gcm-xmpp.googleapis.com, android.googleapis.com

Device OS	TCP port	Protocol	Domain
Google Firebase Cloud Messaging ²	TCP/443,5228-5230	TCP	fcm.googleapis.com, fcm-xmpp.googleapis.com
Googlecertificate revocation ²	443	TCP	pki.google.com, clients[1-9].google.com
BlackBerry 10 OS (version 10.3.2 and later) and Android OS (Android for Work/Samsung Knox)	443	TCP	<region>.turnd.bbsecure.com
BlackBerry 10 OS (BlackBerry World for Work)	80	HTTP	appworld.blackberry.com
BlackBerry 10 OS (version 10.3.1 and later)	80	HTTP	icc.blackberry.com/v1/wifi/
BlackBerry Dynamics apps	49152	TCP	gdmdc.good.com
BlackBerry Dynamics apps	443	TCP	gdmdc.good.com
BlackBerry Dynamics apps	15000	TCP	gdrelay.good.com
BlackBerry Dynamics apps	443	TCP	gdrelay.good.com
BlackBerry Dynamics apps	443	TCP	gdweb.good.com
BlackBerry Dynamics apps	443	TCP	gdentgw.good.com
BlackBerry Analytics ³	443	TCP	analytics.blackberry.com receiver.analytics.blackberry.com
BlackBerry UEM Client	443	HTTPS	discoveryservice.blackberry.com
BlackBerry Android certificate server	80	HTTP	pki.services.blackberry.com
BlackBerry Protect	443	HTTPS	score.cylance.com
BlackBerry Enterprise Identity	443	HTTPS	idp.blackberry.com

¹ In addition to standard HTTPS traffic, BlackBerry UEM components may also need to make an HTTP CONNECT and HTTP OPTIONS call on port 443. Because some firewalls are configured to block non-HTTPS traffic detected on port 443, this traffic may need to be explicitly allowed. Similarly, some firewalls incorrectly recognize TLS traffic on port 3101 as nonstandard and block the traffic. Ensure that necessary allow lists are in place on your firewall or other network appliances.

² When using Samsung Knox with BlackBerry Secure Connect Plus, all device traffic, including HTTP and TCP traffic, is redirected to the BlackBerry UEM server. The device-side TCP ports must be allowed from the BlackBerry UEMserver. For more information, visit support.blackberry.com/community to read article 46317.

³ To open the firewall to specific IP addresses, for analytics.blackberry.com use 74.82.73.148, and for receiver.analytics.blackberry.com use 74.82.73.149.

Reserved IP address ranges

BlackBerry may add new IP addresses to the Global IP ranges. BlackBerry has reserved IP address ranges, identified below for this purpose. BlackBerry recommends that you add these IP address ranges in the firewall rules to ensure that future changes do not impact server connectivity.

Region	Current and future IP addresses
All	68.171.242.252 206.124.114.1 to 206.124.114.254 (206.124.114.0/24) 206.124.122.1 to 206.124.122.254 (206.124.122.0/24)
Asia Pacific region (APAC) excluding Saudi Arabia and UAE	103.246.200.136/30 103.246.201.136/30 68.171.240.33/29 68.171.240.33
Canada	216.9.242.240/29 74.82.72.240/29 68.171.242.192/29 68.171.242.216/29 216.9.242.6 68.171.242.6
Europe, the Middle East, and Africa region (EMEA)	93.186.19.240/29 93.186.17.240/29 93.186.25.33 193.109.81.33
India and Southern Asia	93.186.19.240/29 93.186.17.240/29 68.171.240.33/29 68.171.240.33

Region	Current and future IP addresses
Latin America and the Caribbean	216.9.242.240/29 74.82.72.240/29 68.171.242.192/29 68.171.242.216/29 68.171.242.208/29 74.82.72.208/29 216.9.242.32 68.171.242.32
Saudi Arabia and United Arab Emirates	93.186.19.240/29 93.186.17.240/29 131.117.168.128/29 5.100.168.128/29 131.117.168.48 131.117.168.49 5.100.168.48 5.100.168.49
United States only	68.171.242.200/29 74.82.72.200/29 216.9.242.240/29 68.171.242.216/29 216.9.242.33 68.171.242.33

Outbound connections: BlackBerry UEM to the BlackBerry Infrastructure

BlackBerry UEM must connect with and receive data from the BlackBerry Infrastructure to perform tasks. BlackBerry UEM connects with the BlackBerry Infrastructure over the outbound-initiated, two-way port 3101 (TCP).

Your organization's firewall must allow outbound two-way connections over port 3101 to `<region>.srp.blackberry.com`, `<region>.bbsecure.com`, and `<region>.turnb.bbsecure.com`.

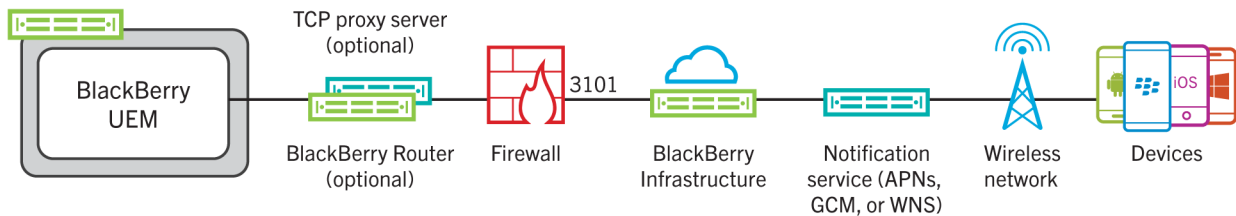
Note: If you install the device connectivity components (the BlackBerry Connectivity Node) on a separate computer, your organization's firewall must allow connections from that computer over port 443 through the BlackBerry Infrastructure (`<region>.bbsecure.com`) to activate the BlackBerry Connectivity Node. All other outbound connections from the BlackBerry Connectivity Node use port 3101 through the BlackBerry Infrastructure (`<region>.bbsecure.com`). 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 (<region>.bbsecure.com) and to the same bbsecure.com region as the Core server.

You have the option of routing data from BlackBerry UEM through your organization's TCP proxy server or the BlackBerry Router to the BlackBerry Infrastructure. If you choose to send data through a proxy server, configure the firewall to allow the following outbound two-way connections:

- Use port 3102 as the default listening port to connect the BlackBerry UEM components to the TCP proxy server or the BlackBerry Router
- Use port 3101 as the default listening port to connect the components that manage BlackBerry OS devices to the TCP proxy server or the BlackBerry Router

If you configure BlackBerry UEM to use a TCP proxy server or the BlackBerry Router, verify that the proxy allows connections over port 3101 to <region>.srp.blackberry.com, <region>.bbsecure.com, and <region>.turnb.bbsecure.com.



Activities initiated by the BlackBerry UEM Core over the port 3101 connection to the BlackBerry Infrastructure

Purpose	Description
Authenticate BlackBerry UEM	Connect to the authentication service to authenticate the BlackBerry UEM installation and allow the components to use the BlackBerry Infrastructure services.
Enable licenses	Connect to the licensing infrastructure to activate your organization's server licenses and to enable BlackBerry 10, iOS, Android, and Windows devices to use SIM licenses obtained from your service provider.
Request a signed CSR	Connect to the signing infrastructure so you can request a certificate signing request (CSR) from BlackBerry. You use the signed CSR to obtain and register an Apple Push Notification Service (APNs) certificate, which you require to manage iOS devices.
Activate and manage BlackBerry 10 devices	Connect to the BlackBerry Infrastructure to: <ul style="list-style-type: none"> • Activate and manage BlackBerry 10 devices • Enable the work space on BlackBerry 10 devices
Communicate with notification services	Connect to the BlackBerry Infrastructure to send data to the appropriate notification service for supported device types (APNs, FCM, or WNS).
Communicate with the BlackBerry push data service	Connect to the BlackBerry push data service so that you can manage and configure settings for BlackBerry 10 devices.
Discover server connection during activation	Connect to the discovery service so that BlackBerry UEM can find and use the server connection automatically when users activate devices. If you turn off this connection, users must specify the server manually when they activate devices.

Purpose	Description
Update device OS data	Connect to the BlackBerry Infrastructure every 24 hours to check a hosted metadata file for new device or OS data. Updates are downloaded to the BlackBerry UEM database.
Search for apps	Connect to the BlackBerry Infrastructure and then to the App Store or BlackBerry World so that you can search for apps to add to the available app list.
Purchase and push apps to iOS devices	Connect to the BlackBerry Infrastructure and then to the App Store to allow you to buy and push apps to iOS devices.

Activities initiated by the BlackBerry Affinity Manager over the port 3101 connection to the BlackBerry Infrastructure

Purpose	Description
Send and receive data for BlackBerry 10 devices	Connect to the BlackBerry Infrastructure to send and receive data for BlackBerry 10 devices, including Exchange ActiveSync data and enterprise connectivity data (for example, intranet browsing and third-party app data).

Activities initiated by BlackBerry Secure Connect Plus over the port 3101 connection to the BlackBerry Infrastructure

Purpose	Description
Secure connection from work apps to work resources	Connect to the BlackBerry Infrastructure to provide BlackBerry 10, Android Enterprise, and Knox Workspace devices with a secure connection to work resources using BlackBerry Secure Connect Plus.

Activities initiated by the components of the BlackBerry Connectivity Node over the port 3101 connection to the BlackBerry Infrastructure

Purpose	Description
Establish secure device connections to work resources	<p>You can install one or more instances of the BlackBerry Connectivity Node to add additional instances of the device connectivity components to your organization's domain. Each BlackBerry Connectivity Node contains the following BlackBerry UEM components:</p> <ul style="list-style-type: none"> • BlackBerry Secure Connect Plus: Connects to the BlackBerry Infrastructure to provide devices with a secure connection to work resources • BlackBerry Secure Gateway: connects to the BlackBerry Infrastructure to provide iOS devices with the MDM controls activation type with a secure connection to your organization's mail server • BlackBerry Gatekeeping Service: Connects through the BlackBerry Infrastructure to the primary BlackBerry UEM components and the Microsoft Exchange Server or Microsoft Office 365 for Exchange ActiveSync gatekeeping • BlackBerry Cloud Connector: Connects to the BlackBerry Infrastructure to allow the BlackBerry Connectivity Node components to communicate with the primary BlackBerry UEM components <p>The BlackBerry Connectivity Node also includes the BlackBerry Proxy, which maintains the secure connection between your organization and the BlackBerry Dynamics NOC. The BlackBerry Proxy does not use the 3101 connection.</p>

Outbound connections: BlackBerry UEM to the BlackBerry Dynamics NOC

Your organization's firewall must allow TCP connections to the appropriate IP ranges so that the BlackBerry Proxy can connect to the BlackBerry Dynamics NOC. Refer to [Reserved IP address ranges](#) for details.

Alternatively, you can configure your organization's firewall to allow connections to host names specifically for BlackBerry Dynamics apps, listed in [Mobile device configuration \(Wi-Fi requirements\)](#).

If you do not configure a web proxy server for a BlackBerry Proxy instance, your organization's internal and external firewalls must allow connections over port 17533. If you configure BlackBerry Proxy to use BlackBerry Dynamics Direct Connect, your organization's external firewalls must allow connections over port 17533. For more information about configuring BlackBerry Proxy, [see the Configuration content](#).

Outbound connections: Devices on a work Wi-Fi network

BlackBerry 10, iOS, Android, and Windows devices that use your work Wi-Fi network use the following outbound ports to connect to the BlackBerry Infrastructure and external services. Configure your organization's firewall to allow outbound two-way connections over these ports.

Refer to [Mobile device configuration \(Wi-Fi requirements\)](#) for details about outbound connections for devices with BlackBerry Dynamics apps, devices using BlackBerry Protect, and for BlackBerry Analytics.

From	To	Purpose	Protocol	Port
BlackBerry 10	BlackBerry Infrastructure	To connect to *.rdns.blackberry.net and primary DNS host iceberg.blackberry.com if "Use cloud services to find more info about the contacts that you add to the Contacts app" is enabled in the Contacts settings.	<ol style="list-style-type: none"> 1. HTTP CONNECT to BlackBerry Infrastructure; creates tunnel from device to BlackBerry UEM outbound to BlackBerry Infrastructure 2. TLS session between device and BlackBerry UEM 	443
BlackBerry 10 iOS Android Windows devices	BlackBerry Infrastructure	To connect to the <region>.bbsecure.com subdomain when activating the device.	<ol style="list-style-type: none"> 1. HTTP CONNECT to BlackBerry Infrastructure; creates tunnel from device to BlackBerry UEM 2. TLS session between device and BlackBerry UEM 	443
BlackBerry 10 Android	BlackBerry Infrastructure	To connect to the <region>.bbsecure.com subdomain so that administration commands can be applied to the devices.	<ol style="list-style-type: none"> 1. HTTP CONNECT to BlackBerry Infrastructure; creates tunnel from device to BlackBerry UEM 2. TLS session between device and BlackBerry UEM 	443
iOS	BlackBerry Infrastructure	To connect to the <region>.bbsecure.com subdomain so that administration commands can be applied to the devices.	TLS	443
Windows devices	BlackBerry Infrastructure	To connect to the <region>.bbsecure.com subdomain so that administration commands can be applied to the devices.	HTTPS; includes TLS handshake using SNI	443
iOS	APNs	To connect to gateway.push.apple.com to receive notifications from APNs.	TCP	5223

From	To	Purpose	Protocol	Port
Android	FCM	To connect to android.apis.google.com (ports 5228 and 5229) and android.googleapis.com (port 5230) to receive notifications from FCM.	TCP	5228 5229 5230

Intranet connections

Connections initiated by the BlackBerry UEM Core

To simplify administration and support certain device features, the BlackBerry UEM Core must be able to connect to your organization's intranet applications. Examples of intranet applications include Microsoft Active Directory, an LDAP directory, Microsoft Exchange, or an SMTP server.

Consult the documentation or support resources for your organization's applications to identify the ports that BlackBerry UEM must be able to access.

Intranet port configurations for BlackBerry Proxy

On each computer that hosts BlackBerry Proxy, verify that the following inbound ports are open, available, and not used by other servers or processes:

- 17080
- 17433

The computer that hosts BlackBerry Proxy should have at least 30,000 ports in the dynamic TCP port allocation for outbound connections to the BlackBerry Dynamics NOC (when Direct Connect is configured, these ports become inbound).

To route connections from BlackBerry Dynamics apps through a web proxy server, the proxy server must support the HTTP Connect command and must not require authentication. Your organization's internal firewall must allow connections over port 17533. If you do not configure a web proxy server for a BlackBerry Proxy instance, your organization's internal and external firewalls must allow connections over port 17533. For more information about configuring BlackBerry Proxy, [see the Configuration content](#).

Connections initiated by BlackBerry 10 devices

BlackBerry 10 devices can access your organization's internal applications through BlackBerry UEM using the outbound-initiated port 3101 connection. Examples of internal applications include your organization's messaging software, or work browser access to intranet sites (HTTP/HTTPS).

Consult the documentation or support resources for your organization's applications to identify additional ports that BlackBerry UEM must be able to access.

How BlackBerry UEM selects listening ports during installation

When you install BlackBerry UEM for the first time, the setup application determines whether default listening ports are available for use. If a default port is not available, the setup application assigns a port value from the range of 12000 to 12999. The setup application stores the port values in the BlackBerry UEM database.

When you install an additional BlackBerry UEM instance in the domain, the setup application retrieves the listening port values from the database and uses those values for the current installation. If a defined listening port is not available, you receive an error message stating that you cannot complete the installation until the port is available for use.

The default values of some listening ports may have changed over the course of BlackBerry UEM releases. When you upgrade BlackBerry UEM to a new version, the upgrade process retains the listening port values that were defined by the original installation.

BlackBerry UEM listening ports

The following is a list of the default ports that the BlackBerry UEM setup application tries to use when you install the first BlackBerry UEM instance in your organization's domain. If a default port is not available, the setup application assigns a port from the range of 12000 to 12999. Some listening ports require the default port and cannot be assigned a different port value (see notes in the table below).

To check the minimum ports that must be open between BlackBerry UEM instances, or any assigned listening port, see [Check the ports assigned by the BlackBerry UEM setup application](#).

Note: BlackBerry UEM uses port 8889 for identity management for BlackBerry 10 devices and to handle SCEP requests for BlackBerry Secure Connect Plus. BlackBerry UEM must be able to access this port to support devices running BlackBerry 10 OS version 10.3 or later.

Default port	Name in database	Purpose
1610	mdm.snmp.monitoring.udpport	The BlackBerry UEM Core uses this port to provide SNMP monitoring data.
1611	com.rim.p2e.snmp.monitoring.udpport	SNMP clients can use this port to query monitoring data for BlackBerry Secure Connect Plus.
1612	com.rim.asp.snmp.monitoring.udpport	This is the default port that is used for SNMP monitoring for the BlackBerry Secure Gateway. This port can be changed in the management console.
1613	com.rim.platform.mdm.zed.snmp.monitoring.udpport	This is the default port that is used for SNMP monitoring for the BlackBerry Cloud Connector.
1620	mdm.snmp.eventing.ipv4.udpport	The BlackBerry UEM Core uses this port to send SNMP notifications in an IPv4 environment.

Default port	Name in database	Purpose
8000 443	ui.port.ssp ui.port.admin	BlackBerry UEM Self-Service and the management console listen for HTTPS connections on this port. If 443 is not available, the setup application tries to use port 8008. If port 8008 is not available, the setup application assigns a port from the range of 12000 to 12999.
8087	com.rim.asp.proxy.listenPort	The primary BlackBerry UEM components and any BlackBerry Connectivity Node instances send BlackBerry Secure Gateway traffic to this port.
8095	tomcat.public.https.port	This port is reserved for secure REST communication between external systems and BlackBerry UEM plug-ins.
8100	ui.port.healthcheck	The BlackBerry UEM Core uses this port to check the status of the UEM management console.
8102	com.rim.p2e.monitoringservice.listenerPort	The BlackBerry UEM Core uses this port to check the status of BlackBerry Secure Connect Plus.
8103	com.rim.asp.monitoringservice.listenPort	The BlackBerry UEM Core uses this port to obtain the status of the BlackBerry Secure Gateway. The status is displayed in the management console.
8182	bcs.mgmt.port	The BlackBerry UEM Core uses this port to obtain the status of the BlackBerry Collaboration Service.
8448	ui.port.internal-api	The BlackBerry UEM Core and the management console and BlackBerry UEM Self-Service use this port for internal communication.
8543		The BlackBerry UEM management console uses this port when an administrator or user logs in to the management console or BlackBerry UEM Self-Service using certificate-based authentication.
8881	tomcat.bdmi.certicom.https.port	The BlackBerry UEM Core uses this port to receive management requests for BlackBerry 10 devices. The connection uses mutual authentication with ECC certificates.

Default port	Name in database	Purpose
8882	tomcat.enrol.http.port	The BlackBerry UEM Core uses this port to receive enrolment requests for BlackBerry 10 devices.
8883	tomcat.enrol.https.port	The BlackBerry UEM Core uses this port to receive enrolment requests for iOS, Android, and Windows Phone devices.
8884	tomcat.bdmi.bouncycastle.https.port	The BlackBerry UEM Core uses this port to receive management requests for iOS, Android, and Windows Phone devices. The connection uses mutual authentication with RSA certificates.
8885	tomcat.applemdm.https.port	The BlackBerry UEM Core uses this additional port to receive management requests for iOS devices. The connection uses mutual authentication with RSA certificates.
8887	tomcat.ipc.https.port	The BlackBerry UEM Core and the management console use this port for authenticated connections to check the status of BlackBerry UEM instances.
8889	tomcat.scep.https.port	<p>The BlackBerry UEM Core uses this port for identity management for BlackBerry 10 devices and to handle SCEP requests for BlackBerry Secure Connect Plus (the BlackBerry UEM Core acts as the CA).</p> <p>Note: BlackBerry UEM must be able to access port 8889 to support devices running BlackBerry 10 OS version 10.3 or later.</p>
8890	tomcat.e2c.https.port	When BlackBerry Secure Connect Plus and the BlackBerry Gatekeeping Service are installed remotely as part of a BlackBerry Connectivity Node, these components use this port to obtain configuration and authorization data and certificates. The BlackBerry Gatekeeping Service also uses this port for gatekeeping operations.
8891	tomcat.i2c.https.port	Certain BlackBerry Infrastructure services use this mutually authenticated port to connect with BlackBerry UEM.

Default port	Name in database	Purpose
8892	tomcat.e2c.local.https.port	When BlackBerry Secure Connect Plus and the BlackBerry Gatekeeping Service are installed with the primary BlackBerry UEM components, they use this port to obtain configuration and authorization data and certificates. The BlackBerry Gatekeeping Service also uses this port for gatekeeping operations.
8893	tomcat.bb2fa.local.http.port	This port supports connections to the BlackBerry UEM Core from the BlackBerry 2FA app on BlackBerry 10 devices (10.3.2 or earlier).
8894	tomcat.core.health.check.http.port	The BlackBerry UEM Core health can be collected on this port. This functionality is available only for deployments of BlackBerry UEM Cloud.
8895	tomcat.i2c.basic.https.port	The BlackBerry UEM Core uses this port is to receive requests from external services such as BEMS, BlackBerry Connect, and BlackBerry Workspaces.
8896	tomcat.dynamics.apps.https.port	BlackBerry UEM listens on this port for REST requests from BlackBerry Dynamics apps. This port uses GDAuthToken-based authentication.
8897	tomcat.bdmi.wp8.https.port	BlackBerry UEM listens on this port when you are upgrading BlackBerry UEM so that it can communicate with Windows Phone 8 devices. For more information, visit support.blackberry.com/community to read article 48098.
8900	winservice.bgs.https.port	The BlackBerry Gatekeeping Service listens on this secure SSL port.
11001	com.rim.p2e.endpoint.listenerPort	BlackBerry Secure Connect Plus uses this port to listen for signaling requests from the BlackBerry Infrastructure.
17080	good.proxy.appservers.http.listening.port	BlackBerry Proxy listens on this port for connections from application servers. Note: The default port must be used. The setup application does not assign an alternate port if the default port is not available.

Default port	Name in database	Purpose
17317	good.control.container.management.listening.port	BlackBerry UEM listens on this port for BlackBerry Dynamics container management data. Note: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17433	good.proxy.appservers.ssl.listening.port	BlackBerry Proxy listens on this port for SSL connections from application servers. Note: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
17533	good.proxy.container.ssl.listening.port	BlackBerry Proxy listens on this port for SSL connections. Note: The default port must be used. The setup application does not assign an alternate port if the default port is not available.
18084	tomcat.bws.port	Applications can use this port to send data to the BlackBerry Web Services.
38082	com.rim.platform.mdm.core.proxy.adam.endpoint.port	The BlackBerry UEM Core listens on this port to route email notification traffic through the BlackBerry Infrastructure to the APNs for iOS devices.
38083	com.rim.platform.mdm.core.proxy.direct.endpoint.port	The BlackBerry UEM Core listens on this port for migration requests when you move devices from BES10 to BlackBerry UEM.
38086	com.rim.platform.mdm.core.proxy.apns.endpoint.port	Your organization's TCP proxy server listens on this port for data that BlackBerry UEM sends to the APNs.
38087	com.rim.platform.mdm.core.proxy.cirr.endpoint.port	The BlackBerry UEM Core listens on this port to route traffic for BlackBerry Enterprise Identity through the BlackBerry Infrastructure.

Minimum ports to open between BlackBerry UEM instances

If your organization's domain has more than one BlackBerry UEM instance, note the following requirements:

- If you install the device connectivity components (the BlackBerry Connectivity Node) on a separate computer, your organization's firewall must allow connections from that computer over port 443 through the BlackBerry Infrastructure (<region>.bbsecure.com) to activate the BlackBerry Connectivity Node. All other outbound connections from the BlackBerry Connectivity Node use port 3101 through the BlackBerry Infrastructure (<region>.bbsecure.com).

- If you are migrating data from one BlackBerry UEM instance to another, the ports that must be open between the source and destination servers are 8887 (TCP) and 35844 (TCP) for BlackBerry UEM and static ports 1433 (TCP) and 1434 (UDP) for Microsoft SQL Server.
- The following listening ports must be open between each instance. The default port values are listed. After you install the first instance, you can verify the listening port values that the setup application defined. For instructions, see [Check the ports assigned by the BlackBerry UEM setup application](#).

Default port	Name in database	Purpose
8000	ui.port.ssp	BlackBerry UEM Self-Service and the management console listen for HTTPS connections on this port.
443	ui.port.admin	If 443 is not available, the setup application tries to use port 8008. If port 8008 is not available, the setup application assigns a port from the range of 12000 to 12999.
8448	ui.port.internal-api	The BlackBerry UEM Core, the management console, and BlackBerry UEM Self-Service use this port for internal communication.
8887	tomcat.ipc.https.port	BlackBerry UEM uses this port for authenticated connections to check the status of BlackBerry UEM instances.
8896	tomcat.dynamics.apps.https.port	BlackBerry UEM listens on this port for REST requests from BlackBerry Dynamics apps. This port uses GDAuthToken-based authentication.
17080	good.proxy.appservers.http.listening.port	BlackBerry Proxy listens on this port for connections from application servers. Note: The default port value must be used. The setup application does not assign an alternate port value if the default port is not available.
17317	good.control.container.management.listening	BlackBerry Control listens on this port for BlackBerry Dynamics container management data. Note: The default port value must be used. The setup application does not assign an alternate port value if the default port is not available.
17433	good.proxy.appservers.ssl.listening.port	BlackBerry Proxy listens on this port for SSL connections from application servers. Note: The default port value must be used. The setup application does not assign an alternate port value if the default port is not available.

Default port	Name in database	Purpose
17533	good.proxy.container.ssl.listening.port	BlackBerry Proxy listens on this port for SSL connections. Note: The default port value must be used. The setup application does not assign an alternate port value if the default port is not available.

Supporting the deployment

Many of the items to consider when planning the support of your BlackBerry UEM deployment are similar to items you looked at when you assessed your organization's environment.

Hardware issues

Possible issue	Mitigation options
<ul style="list-style-type: none">• The hardware does not work or does not meet BlackBerry UEM requirements• Not all hardware is available	<p>Before the planned installation date:</p> <ul style="list-style-type: none">• Check all hardware before the planned installation date to verify that it is in working order and that it meets all BlackBerry UEM hardware requirements.• Prepare one or two extra computers in case a computer stops working on the planned installation date. <p>During installation:</p> <ul style="list-style-type: none">• If you must install multiple instances of BlackBerry UEM, stage the deployment so that you complete a full installation on one computer first to make sure that all hardware is working.• Install the BlackBerry Router later (if applicable).

Software issues

Possible issue	Mitigation options
<ul style="list-style-type: none">• Port conflicts• The computer's operating system does not meet BlackBerry UEM requirements• The BlackBerry UEM setup application does not work	<p>Before the planned installation date:</p> <ul style="list-style-type: none">• Run the BlackBerry UEM Readiness Tool on the computers you plan to install BlackBerry UEM on. The BlackBerry UEM Readiness Tool helps you determine whether or not the computers meet the minimum requirements for installing BlackBerry UEM.• Make sure all application servers, such as Exchange ActiveSync and the mail servers, are active, running, and tested.

Network issues

Possible issue	Mitigation options
<ul style="list-style-type: none"> • Required firewall ports are not open • BlackBerry UEM instances cannot communicate with each other • BlackBerry UEM cannot communicate with the BlackBerry Infrastructure • BlackBerry UEM cannot communicate with application or content servers 	<p>Before the planned installation date:</p> <ul style="list-style-type: none"> • Run the BlackBerry UEM Readiness Tool on the computers you plan to install BlackBerry UEM on. The BlackBerry UEM Readiness Tool helps you determine whether or not the computers meet the minimum requirements for installing BlackBerry UEM. • Create a detailed list of the ports that are required. Confirm with your networking team that the ports are open. • BlackBerry UEM services do not support SSL Termination, SSL Offloading, SSL Packet Inspection or Deep Packet Inspection. Ensure these endpoint services are not enabled on your proxy/firewall. For more information, visit support.blackberry.com/community to read article 36470.

User, device, device control, and license issues

Possible issue	Mitigation options
<ul style="list-style-type: none"> • Users were added between the time of planning and the time of deployment • The type of activation planned for each user group was changed • Test activations are not working 	<p>Depending on device type, number of devices, and activation type, you may have fewer licenses than you need when it is time to activate devices. In this case, you can activate only the key users and add more licenses as soon as possible.</p> <p>When dealing with activation, app, IT policy, or profile issues during deployment, make sure that:</p> <ul style="list-style-type: none"> • You have enough licenses for the activation type. • You have created or imported the correct IT policies and profiles and assigned them to the user that you are testing. • If you are not registering users with the BlackBerry Infrastructure, make sure that you have the correct BlackBerry UEM web address to enter during activation. • Application servers are accessible by the devices and by BlackBerry UEM. • The devices are compatible with BlackBerry UEM.

Database issues

Possible issue	Mitigation options
The BlackBerry UEM database does not install	<p>Before the planned installation date:</p> <ul style="list-style-type: none">• Check all hardware before the planned installation date to verify that it is in working order and that it meets all BlackBerry UEM hardware requirements.• Make sure that SQL Server permissions are set to allow the creation of the database.• Install and test the database using createdb. For instructions, see the Installation and upgrade content.• Test all connectivity between the computer that will host BlackBerry UEM and the database.

Returning to a previous environment

Most organizations cannot afford a long service interruption while troubleshooting. Therefore, before a database upgrade, you should plan for the ability to return to the previous environment, in case any issues arise.

Returning to the previous environment is not as simple as stopping the upgrade, especially if data was being migrated when an issue occurred.

To prepare to return to your previous environment, before the planned installation date:

- Back up the existing databases. (By default, the BlackBerry UEM setup application backs up the existing database.)
- If you use a virtual environment, take a snapshot of it.

If you encounter an issue during or after installing BlackBerry UEM, collect data about the issue before you return to your previous environment so that you can determine its root cause.

For more information about backing up the BlackBerry UEM database, [see the Installation and upgrade content](#).

For more information about troubleshooting installation and upgrade, visit support.blackberry.com/community to read article 49655.

Legal notice

©2021 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.

Android is a trademark of Google Inc. Apple and OS X are trademarks of Apple Inc. iOS is a trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. iOS® is used under license by Apple Inc. Microsoft, ActiveSync, SQL Server, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Wi-Fi is a trademark of the Wi-Fi Alliance. 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 web sites (collectively the "Third Party Products and Services"). RIM 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 RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS,

LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM 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 RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM 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 RIM OR ANY AFFILIATES OF RIM 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 RIM'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 RIM'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 RIM and RIM 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 RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry® Enterprise Server, BlackBerry® Desktop Software, and/or BlackBerry® Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM 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