Contents

About this guide ........................................................................................................................................... 7

Getting started ........................................................................................................................................... 8

Configuring BES12 for the first time ........................................................................................................... 8
Configuration tasks for managing BlackBerry OS devices ............................................................................ 10
Administrator permissions you need to configure BES12 ............................................................................ 12
Obtaining and activating licenses .............................................................................................................. 12
Managing WorkLife by BlackBerry .............................................................................................................. 12

Adding trusted certificates ........................................................................................................................... 13
Changing the certificate that the BES12 consoles use ................................................................................... 13
Change the certificate that the BES12 consoles use .................................................................................... 13
Changing the certificate that BES12 uses to sign the MDM profile sent to iOS devices .................................. 14
Change the certificate that BES12 uses to sign the MDM profile on iOS devices .......................................... 14

Configuring BES12 to use a proxy server ................................................................................................. 15
Configuring a proxy server when logging in to BES12 for the first time ...................................................... 16
Comparing TCP proxies .............................................................................................................................. 16
Configuring the TCP proxy server ............................................................................................................ 16
Configure BES12 to use a transparent TCP proxy server .......................................................................... 17
Enable SOCKS v5 on a TCP proxy server .................................................................................................. 17
Configuring the BlackBerry Router ............................................................................................................ 18
Configure BES12 to use the BlackBerry Router ....................................................................................... 18

Connecting to your company directories ................................................................................................. 19
Steps to configure a company directory connection ................................................................................... 19
Configuring Microsoft Active Directory authentication in an environment that includes a resource forest ... 20
Connect to a Microsoft Active Directory instance .................................................................................... 20
Connect to an LDAP directory .................................................................................................................... 22
Enabling directory-linked groups .............................................................................................................. 25
Enable directory-linked groups ................................................................................................................. 27
Synchronize a company directory connection .......................................................................................... 28
View a directory synchronization report .................................................................................................. 29
Adding a synchronization schedule .......................................................................................................... 29
Best practices: Migrating IT policies, profiles, and groups from a source database.......................................................... 74
Migrate IT policies, profiles, and groups from a source database.......................................................................................... 76
Best practices: Migrating users from a source database..................................................................................................... 77
Migrate users from the source database........................................................................................................................................ 78
Migrate devices from the source database.......................................................................................................................... 78
Migrating DEP devices................................................................................................................................................................. 79
  Migrate DEP devices that have the BES12 Client installed.................................................................................................. 79
  Migrate DEP devices that do not have the BES12 Client installed...................................................................................... 79

Configuring how data is pushed to BlackBerry 10 devices...................................................................................................... 81
Steps to configure the BlackBerry MDS Connection Service.................................................................................................. 81
Configuring the BlackBerry MDS Connection Service.......................................................................................................... 82
  Component information settings................................................................................................................................................ 82
  Configure the BlackBerry MDS Connection Service........................................................................................................... 82
Configuring BlackBerry MDS Connection Service push information........................................................................................ 83
  Push information settings......................................................................................................................................................... 84
  Configure push information.................................................................................................................................................... 85
Configuring the BlackBerry MDS Connection Service keystore............................................................................................. 87
  Keystore settings...................................................................................................................................................................... 87
  Configure the keystore............................................................................................................................................................ 88
Configure BlackBerry MDS Connection Service proxy mappings.......................................................................................... 89
  Rank proxy mappings............................................................................................................................................................ 90

Monitoring BES12........................................................................................................................................................................ 91
Supported SNMP operations......................................................................................................................................................... 91
System requirements: SNMP monitoring........................................................................................................................................ 92
MIBs for BES12............................................................................................................................................................................ 93
Compile the MIB and configure the SNMP management tool................................................................................................ 93
Using SNMP to monitor the BES12 Core and BlackBerry Secure Connect Plus........................................................................ 94
  Configure SNMP to monitor the BES12 Core and BlackBerry Secure Connect Plus............................................................ 94

Glossary..................................................................................................................................................................................... 96

Legal notice............................................................................................................................................................................... 98
BES12 helps you manage BlackBerry 10, BlackBerry OS (version 5.0 to 7.1), iOS, Android, and Windows devices for your organization. This guide provides instructions for configuring BES12 to meet your organization's needs.

This guide is intended for senior IT professionals who are responsible for setting up and deploying the product. Before you can complete the tasks in this guide, you need to install the product and activate licenses. For installation instructions, see the Installation and upgrade content. For more information about activating licenses, see the Licensing content.

After you complete the tasks in this guide, see the Administration content to learn how to manage the BES12 domain.
# Getting started

## Configuring BES12 for the first time

The following table summarizes the configuration tasks covered in this guide. The tasks are optional based on your organization’s needs. Use this table to determine which configuration tasks you should complete.

After you complete the appropriate tasks, you are ready to set up administrators, set up device controls, create users and groups, and activate devices.

<table>
<thead>
<tr>
<th>Task</th>
<th>Required or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replace default certificates with trusted certificates</td>
<td>Optional</td>
<td>You can replace the default SSL certificate used by the BES12 consoles and the default certificate that BES12 uses to sign the MDM profile for iOS devices with trusted certificates.</td>
</tr>
<tr>
<td>Configure BES12 to send data through a proxy server</td>
<td>Optional</td>
<td>You can configure BES12 to send data through a proxy server behind your organization’s firewall.</td>
</tr>
<tr>
<td>Connect BES12 to company directories</td>
<td>Optional</td>
<td>You can connect BES12 to one or more company directories, such as Microsoft Active Directory or an LDAP directory, so that BES12 can access user data to create user accounts.</td>
</tr>
<tr>
<td>Configure single sign-on for BES12</td>
<td>Optional</td>
<td>If you connect BES12 to Microsoft Active Directory, you can configure single sign-on authentication to permit administrators or users to bypass the login webpage and access the management console or BES12 Self-Service directly.</td>
</tr>
<tr>
<td>Obtain and register an APNS certificate</td>
<td>Optional</td>
<td>If you want to manage and send data to iOS devices, you must obtain a signed CSR from BlackBerry, use it to obtain an APNs certificate from Apple, and register the APNs certificate with the BES12 domain.</td>
</tr>
<tr>
<td>Configure BES12 for Apple’s Device Enrollment Program</td>
<td>Optional</td>
<td>If you want to use the BES12 management console to manage iOS devices that your organization purchased from Apple for DEP, you must configure BES12.</td>
</tr>
<tr>
<td>Connect BES12 to an SMTP server</td>
<td>Optional</td>
<td>If you want BES12 to send activation emails and other notifications to users, you must specify the SMTP server settings that BES12 can use.</td>
</tr>
<tr>
<td>Task</td>
<td>Required or Optional</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set up BES12 Self-Service</td>
<td>Optional</td>
<td>If you want to allow users to perform certain management tasks such as changing their passwords, you can set up and distribute the BES12 Self-Service web application.</td>
</tr>
<tr>
<td>Configure high availability</td>
<td>Optional</td>
<td>To minimize service interruptions for users, you can install more than one active BES12 instance.</td>
</tr>
<tr>
<td>Configure database mirroring</td>
<td>Optional</td>
<td>To retain database service and data integrity if issues occur with the BES12 database, you can install and configure a failover database that serves as a backup to the principal database.</td>
</tr>
<tr>
<td>Configure BES12 to send notifications to iOS devices with Secure Work Space</td>
<td>Optional</td>
<td>If you want BES12 to send notifications to iOS devices with Secure Work Space, you must configure the BlackBerry Work Connect Notification Service and set up an SSL connection between BES12 and the Microsoft Exchange Server.</td>
</tr>
<tr>
<td>Configure BES12 to support Android for Work</td>
<td>Optional</td>
<td>To support Android for Work, you need to configure your Google Apps for Work or Google for Work domain to support third-party mobile device management providers and configure BES12 to communicate with your Google Apps for Work or Google for Work domain.</td>
</tr>
<tr>
<td>Configure your network to simplify Windows 10 activations</td>
<td>Optional</td>
<td>You can simplify the process for activating Windows 10 devices by making configuration changes to your network so that users don’t need to type a server address.</td>
</tr>
<tr>
<td>Configure support for Microsoft Exchange gatekeeping</td>
<td>Optional</td>
<td>If you configured Microsoft Exchange to block devices from accessing work email and organizer data unless the devices are added to an allowed list, you must create a Microsoft Exchange configuration in BES12.</td>
</tr>
<tr>
<td>Migrate users, groups, and other data from BES10</td>
<td>Optional</td>
<td>If your organization is moving from BES10 to BES12, you can migrate IT policies, profiles, group names, users, and devices from BES10.</td>
</tr>
<tr>
<td>Configure how data is pushed to BlackBerry 10 devices</td>
<td>Optional</td>
<td>You can customize how BES12 sends push data to BlackBerry 10 devices.</td>
</tr>
<tr>
<td>Configure SNMP monitoring</td>
<td>Optional</td>
<td>You can use third-party SNMP tools to monitor the activity of BES12 components.</td>
</tr>
</tbody>
</table>
## Configuration tasks for managing BlackBerry OS devices

If your organization’s BES12 domain will support BlackBerry OS (version 5.0 to 7.1) devices, you can customize the management of BlackBerry OS devices. If you upgraded from BES5 to BES12, any configuration of the BES5 components completed before the upgrade remain intact after the upgrade, so you may not need to complete additional configuration tasks.

For instructions for each task in the table, visit help.blackberry.com/detectLang/category/enterprise-services to read the BlackBerry Enterprise Server 5 Installation and Configuration Guide or the BlackBerry Enterprise Server 5 Administration Guide.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Resource</th>
</tr>
</thead>
</table>
| Specify which service manages calendar data. | **Installation and Configuration Guide**  
By default, Microsoft Exchange Web Services manage calendar data for BlackBerry OS devices. If a user is not permitted to use this service, the user’s calendar data is managed using MAPI and CDO libraries. You can choose to have calendar data managed by Microsoft Exchange Web Services only or by MAPI and CDO libraries only. |
| Use the SNMP service to monitor the components that manage BlackBerry OS devices. | **Installation and Configuration Guide**  
- Post-installation tasks: Configuring a computer for monitoring |
| Use an Enterprise Service Policy to control which BlackBerry OS devices can access BES12. | **Administration Guide**  
- Configuring security options: Managing device access to the BlackBerry Enterprise Server |
| Configure the BlackBerry MDS Connection Service, BlackBerry Collaboration Service, and BlackBerry Administration Service to send data through a proxy server. | **Administration Guide**  
- Configuring the BlackBerry Enterprise Server environment |
| Configure high availability for the components that manage BlackBerry OS devices. | **Administration Guide**  
- Configuring BlackBerry Enterprise Server high availability  
- Configuring high availability for BlackBerry Enterprise Server components |
<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change how the BlackBerry MDS Connection Service for BlackBerry OS devices...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change how the BlackBerry MDS Connection Service manages push data...</td>
<td>• Configuring BlackBerry Configuration Database high availability</td>
</tr>
<tr>
<td>Change how the BlackBerry MDS Connection Service allows users to access...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change how the BlackBerry MDS Connection Service manages push data and allows users to access web content.</td>
<td>• Managing how users access enterprise applications and web content</td>
</tr>
<tr>
<td>Use extension plug-ins to process and make changes to email messages...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Use extension plug-ins to process and make changes to email messages and...</td>
<td>• Setting up the messaging environment: Extension plug-ins for processing messages</td>
</tr>
<tr>
<td>Use extension plug-ins to process and make changes to...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Allow BlackBerry OS devices to enroll certificates to authenticate with...</td>
<td>• Configuring BlackBerry devices to enroll certificates over the wireless network</td>
</tr>
<tr>
<td>Allow BlackBerry OS device users to perform self-service tasks using...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Allow BlackBerry OS device users to perform self-service tasks using the BlackBerry Web Desktop Manager.</td>
<td>• Making the BlackBerry Web Desktop Manager available to users</td>
</tr>
<tr>
<td>Allow BlackBerry OS device users to perform self-service tasks using...</td>
<td>• Configuring the BlackBerry Web Desktop Manager</td>
</tr>
<tr>
<td>Change how apps, OS updates, and settings are sent to BlackBerry OS devices.</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change how apps, OS updates, and settings are sent to BlackBerry devices...</td>
<td>• Managing the delivery of BlackBerry Java Applications, BlackBerry Device Software, and device settings to BlackBerry devices</td>
</tr>
<tr>
<td>Change organizer data synchronization for BlackBerry OS device users.</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change organizer data synchronization for BlackBerry OS device users.</td>
<td>• Managing organizer data synchronization</td>
</tr>
<tr>
<td>Change mail configuration and attachment support for the...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change mail configuration and attachment support for the...</td>
<td>• Managing your organization’s messaging environment and attachment support</td>
</tr>
<tr>
<td>Change mail configuration and attachment support for the components that...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change mail configuration and attachment support for the components that...</td>
<td>• Managing your organization’s messaging environment and attachment support</td>
</tr>
<tr>
<td>Change various log file settings, including the location, level of...</td>
<td><strong>Administration Guide</strong></td>
</tr>
<tr>
<td>Change various log file settings, including the location, level of...</td>
<td>• BlackBerry Enterprise Server log files</td>
</tr>
<tr>
<td>Change various log file settings, including the location, level of...</td>
<td>• BlackBerry Enterprise Server log files</td>
</tr>
</tbody>
</table>
### Administrator permissions you need to configure BES12

When you perform the configuration tasks in this guide, log in to the management console using the administrator account that you created when you installed BES12. If you want more than one person to complete configuration tasks, you can create additional administrator accounts. For more information about creating administrator accounts, see the Administration content.

If you create additional administrator accounts to configure BES12, you should assign the Security Administrator role to the accounts. The default Security Administrator role has the necessary permissions to complete any configuration task.

### Obtaining and activating licenses

To activate devices in your organization's BES12 domain, you must obtain and activate the necessary licenses. You should activate licenses before you follow the configuration instructions in this guide, and before you add user accounts.

For more information about the different types of licenses and how to activate licenses, see the Licensing content.

### Managing WorkLife by BlackBerry

WorkLife by BlackBerry is a Virtual SIM Platform (VSP) that allows organizations to separate work numbers and personal numbers on BlackBerry 10, iOS, or Android devices, making it easy to separate and split the cost of voice minutes, SMS, and data between an organization and its employees.

For more information about how to manage WorkLife by BlackBerry in BES12, see the WorkLife by BlackBerry content.
Adding trusted certificates

During the installation process, the setup application generates two self-signed certificates:

- An SSL certificate that the BES12 consoles use to establish HTTPS connections
- A certificate that BES12 uses to sign the MDM profile that is sent to iOS devices

Because these certificates are self-signed, users receive warning messages indicating that the certificates aren’t trusted. You can replace these certificates with trusted certificates.

Changing the certificate that the BES12 consoles use

When you install BES12, the setup application generates an SSL certificate that the following components can use to authenticate with browsers:

- BES12 management console
- BES12 Self-Service
- BlackBerry Web Services

You can change the certificate if you want to establish trust so that administrators and users don’t get a message from their browsers indicating that the certificate can’t be verified. You can import a self-signed SSL certificate or a trusted certificate that a CA signs.

Change the certificate that the BES12 consoles use

**Before you begin:** Generate or obtain a trusted certificate that a CA signs. The certificate must be in a keystore format (.pfx, .pkcs12). If you configure high availability, you must generate an SSL certificate that uses the name of the BES12 domain. You can find the BES12 domain name in the management console under **Settings > Infrastructure > BES12 Instances**.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > Server certificates**.
3. Under **SSL certificate for consoles and BlackBerry Web Services**, click **View details**.
4. Click **Replace certificate**.
5. Browse to the certificate file and type the password.
6. Click **Replace**.
7. Restart the BES12 services. Do not stop and start the **BES12 - BlackBerry Work Connect Notification Service**; this service is automatically restarted when you restart the **BES12 - BlackBerry Affinity Manager** service.

### Changing the certificate that BES12 uses to sign the MDM profile sent to iOS devices

When you install BES12, the setup application generates a certificate that BES12 can use to sign the MDM profile that users must accept when activating iOS devices.

You can change the certificate if you want to establish trust so that users don’t get a warning message indicating that the certificate can’t be verified.

You can import a self-signed certificate or a trusted certificate that a CA signs.

### Change the certificate that BES12 uses to sign the MDM profile on iOS devices

**Before you begin:** Generate a self-signed certificate or a trusted certificate that a CA signs. The certificate must be in a keystore format (.pfx, .pkcs12).

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > Server certificates**.
3. Under **Apple profile signing certificate**, click **View details**.
4. Click **Replace certificate**.
5. Browse to the certificate file and type the password.
6. Click **Replace**.
Configuring BES12 to use a proxy server

By default, BES12 is not configured to use a proxy server. If you want to use a proxy server with BES12, you can install the BlackBerry Router to act as a proxy server, or you can use a TCP proxy server that is already installed in your environment. You configure BES12 components to support the type of proxy server.

You install the BlackBerry Router or the proxy server outside your organization’s firewall in the DMZ. Installing the BlackBerry Router or a TCP proxy server in the DMZ provides an extra level of security for BES12. Only the BlackBerry Router or the proxy server connects to BES12 from outside the firewall. All connections over the BlackBerry Infrastructure between BES12 and devices go through the BlackBerry Router or the proxy server.

By default, BES12 makes a direct connection to the BlackBerry Infrastructure over port 3101 and you do not need to install more routing components. However, if your organization’s security policy requires that internal systems cannot make connections directly to the Internet, you can install the BlackBerry Router or a TCP proxy server. The BlackBerry Router or TCP proxy server act as an intermediary between BES12 and the BlackBerry Infrastructure.

For BlackBerry OS (version 5.0 to 7.1) devices, the BlackBerry Router also sends data directly to and receives data from devices that are connected to a work Wi-Fi network or to a computer that has the BlackBerry Device Manager.

![Diagram](image-url)
Configuring a proxy server when logging in to BES12 for the first time

You may be prompted to configure your initial BlackBerry Router instance or TCP proxy server instance when you log in to the management console for the first time. If you configure the proxy server, you may need to perform extra configuration for the BlackBerry Router or TCP proxy server in the management console. You can configure more BlackBerry Router or TCP proxy server instances after you have logged in to the management console.

Comparing TCP proxies

<table>
<thead>
<tr>
<th>Proxy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent TCP proxy</td>
<td>• Intercepts normal communication at the network layer without requiring any special client configuration</td>
</tr>
<tr>
<td></td>
<td>• Requires no client browser configuration</td>
</tr>
<tr>
<td></td>
<td>• Usually located between the client and the Internet</td>
</tr>
<tr>
<td></td>
<td>• Performs some of the functions of a gateway or router</td>
</tr>
<tr>
<td></td>
<td>• Often used to enforce acceptable use policy</td>
</tr>
<tr>
<td></td>
<td>• Commonly used by ISPs in some countries to save upstream bandwidth and improve customer response times through caching</td>
</tr>
<tr>
<td>SOCKS v5 proxy</td>
<td>• An Internet protocol for handling Internet traffic through a proxy server</td>
</tr>
<tr>
<td></td>
<td>• Can be handled with virtually any TCP/UDP application, including browsers and FTP clients that supports SOCKS</td>
</tr>
<tr>
<td></td>
<td>• Can be a good solution for Internet anonymity and security</td>
</tr>
<tr>
<td></td>
<td>• Routes network packets between a client and server through a proxy server</td>
</tr>
<tr>
<td></td>
<td>• Can provide authentication so only authorized users can access a server</td>
</tr>
<tr>
<td></td>
<td>• Proxies TCP connections to an arbitrary IP address</td>
</tr>
<tr>
<td></td>
<td>• Can anonymize UDP protocols and TCP protocols like HTTP</td>
</tr>
</tbody>
</table>

Configuring the TCP proxy server

If you choose to use a TCP proxy server, then the TCP proxy server must be transparent or use SOCKS v5 (no authentication).
You can configure a transparent TCP proxy server for the BES12 Core service and another transparent TCP proxy server for the BlackBerry Affinity Manager service. These services require an outbound connection and may also have different ports configured. You cannot install or configure multiple transparent TCP proxy server instances for each service.

You can configure multiple TCP proxy server instances configured with SOCKS v5 (no authentication) to connect to BES12. Multiple TCP proxy server instances configured with SOCKS v5 (no authentication) can provide support if one of the active proxy server instances is not functioning correctly.

You configure only a single port that all SOCKS v5 (no authentication) service instances must listen on. If you are configuring more than one TCP proxy server instance with SOCKS v5 (no authentication), each TCP proxy server instance with SOCKS v5 must share the proxy listening port.

### Configure BES12 to use a transparent TCP proxy server

**Before you begin:** Install a compatible transparent TCP proxy server in the BES12 domain.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > BlackBerry Router and proxy**.
3. Select the **Proxy server** option.
4. Type the proxy server host IP address and port number that the BES12 Core connects to.
5. Type the proxy server host IP address and port number that the BlackBerry Affinity Manager connects to.
6. Click **Save**.

### Enable SOCKS v5 on a TCP proxy server

**Before you begin:** Install a compatible TCP proxy server with SOCKS v5 (no authentication) in the BES12 domain.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > BlackBerry Router and proxy**.
3. Select the **Proxy server** option.
4. Select **Enable SOCKS v5**.
5. Click +.
6. In the **Server address** field, type the IP address or host name of the SOCKS v5 proxy server.
7. Click **Add**.
8. Repeat steps 1 to 7 for each SOCKS v5 proxy server instance that you want to configure.
9. In the **Port** field, type the port number.
10. Click **Save**.
Configuring the BlackBerry Router

You can configure multiple BlackBerry Router instances to connect to BES12. If one of the active BlackBerry Router instances is not functioning correctly, additional BlackBerry Router instances can provide support. You configure only one port for BlackBerry Router service instances to listen on.

BES12 does not support a BlackBerry Router that was originally used with BES5.

By default, BES12 connects to the BlackBerry Router as follows:

- Over port 3102 to connect to BES12 services
- Over port 3101 to connect to BES5 services

If you connect BES12 services to the BlackBerry Router, the BlackBerry Router supports all outbound traffic from the BES12 Core and BlackBerry Affinity Manager services.

**Note:** If you want to use a port other than the default port for the BlackBerry Router, visit [http://support.blackberry.com/kb](http://support.blackberry.com/kb) to read article KB36385.

Configure BES12 to use the BlackBerry Router

**Before you begin:** Install the BlackBerry Router in the BES12 domain. For more information about installing the BlackBerry Router, see the Installation and upgrade content.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > BlackBerry Router and proxy**.
3. Select the **BlackBerry Router** option.
4. Click **+**.
5. In the **Router address** field, type the IP address or host name of the BlackBerry Router instance that you want to connect to BES12.
6. Click **Add**.
7. Repeat steps 1 to 6 for each BlackBerry Router instance that you want to configure.
8. In the **Port** field, type the port number that all BlackBerry Router instances listen on. The default value is 3102.
9. Click **Save**.
Connecting to your company directories

You can connect BES12 to your organization's Microsoft Active Directory or LDAP directory so that it can access the list of users in your organization. When your company directory is connected, BES12 can authenticate administrators for the management console and users for BES12 Self-Service. BES12 also supports connections to multiple directories. The directories can be a combination of both Microsoft Active Directory and LDAP.

If you do not connect BES12 to a company directory, you can manually create local user accounts and authenticate administrators using default authentication.

Steps to configure a company directory connection

To connect a company directory to BES12, perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a connection to a Microsoft Active Directory instance or to an LDAP directory. If your environment includes a resource forest, see Configuring Microsoft Active Directory authentication in an environment that includes a resource forest.</td>
</tr>
<tr>
<td>2</td>
<td>Enable directory-linked groups.</td>
</tr>
<tr>
<td>3</td>
<td>Create a sync schedule.</td>
</tr>
</tbody>
</table>
Configuring Microsoft Active Directory authentication in an environment that includes a resource forest

If your organization’s environment includes a resource forest that is dedicated to running Microsoft Exchange, you can configure Microsoft Active Directory authentication for user accounts that are located in trusted account forests.

If a resource forest exists in your organization’s environment, you must install BES12 in the resource forest. In the resource forest, you create a mailbox for each user account and associate the mailboxes with the user accounts. When you associate the mailboxes in the resource forest with user accounts in the account forests, the user accounts obtain full access to the mailboxes and the user accounts in the account forests are connected to the Microsoft Exchange server.

To authenticate users who log in to BES12, BES12 must read the user information that is stored in the global catalog servers that are part of the resource forest. To configure BES12 to authenticate user accounts that are associated with mailboxes in the resource forest, you must create a Microsoft Active Directory account for BES12 that is located in a Windows domain that is part of the resource forest. You provide the Windows domain, username, and password for the Microsoft Active Directory account, and, if required, the names of the global catalog servers that BES12 can use.

For more information, visit technet.microsoft.com to read Manage linked mailboxes.

Connect to a Microsoft Active Directory instance

**Before you begin:** Create a Microsoft Active Directory account that BES12 can use. The account must meet the following requirements:

- It must be located in a Windows domain that is part of the Microsoft Exchange forest.
- It must have permission to access the user container and read the user objects stored in the global catalog servers in the Microsoft Exchange forest.
- Configure the password settings for the account so the password does not expire and does not need to be changed at the next login.
- If you enable single sign-on, configure constrained delegation for the account.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Company directory**.
3. Click **Add a Microsoft Active Directory connection**.
4. In the **Directory connection name** field, type the name for the directory connection.
5. In the **Username** field, type the username of the Microsoft Active Directory account.
6. In the **Domain** field, type the name of the Windows domain that is a part of the Microsoft Exchange forest. Enter the domain name in DNS format (for example, example.com).

7. In the **Password** field, type the password for the Microsoft Active Directory account.

8. In the **Domain controller discovery** drop-down list, perform one of the following actions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To permit BES12 to search for the domain controllers</td>
<td>1. Click <strong>Automatic</strong>.</td>
</tr>
</tbody>
</table>
| To control which domain controller BES12 searches | 1. Click **Select from the list below**.  
2. In the **Server names** field, type the name of the domain controller in DNS format (for example, example.com).  
3. To add more domain controllers, click + and type the name of the domain controller. |

9. In the **Global catalog search base** field, perform one of the following actions:
   - To permit BES12 to search the entire global catalog, leave the field blank.
   - To control which user accounts BES12 can authenticate, type the distinguished name of the user container (for example, OU=sales,DC=example,DC=com).

10. In the **Global catalog discovery** drop-down list, perform one of the following actions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you want BES12 to find all of the global catalog servers in the Microsoft Exchange forest automatically</td>
<td>1. Click <strong>Automatic</strong>.</td>
</tr>
</tbody>
</table>
| To control which user accounts BES12 can authenticate | 1. Click **Select from list below**.  
2. In the **Server names** field, type the DNS name of the global catalog server that you want BES12 to access (for example, globalcatalog01.example.com). You must type the DNS name of a global catalog server that is located in the Windows domain that the Microsoft Active Directory account is located in.  
3. To add more global catalog servers, click + and type the DNS name of the global catalog server. |

11. In the **Support for linked Microsoft Exchange mailboxes** drop-down list, perform one of the following actions:
Connecting to your company directories

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable support for linked Microsoft Exchange mailboxes</td>
<td>1. Click <strong>No.</strong></td>
</tr>
<tr>
<td>Enable support for linked Microsoft Exchange mailboxes</td>
<td>1. Click <strong>Yes.</strong></td>
</tr>
</tbody>
</table>

To configure the Microsoft Active Directory account for each forest that you want BES12 to access, perform the following actions:

1. In the **List of account forests** section, click **+**.
2. In the **Add account forests** window, in the **User domain** field, type the user domain name. The user may belong to any domain in the account forest.
3. In the **Username** field, type the username for the Microsoft Active Directory account.
4. In the **Password** field, type the password for the Microsoft Active Directory account.
5. Click **Add**.

12. To enable single sign-on, select the **Enable Windows single sign-on** check box.

13. Perform the following actions:
   a. Click **Save**.
   b. If you enabled single sign-on, click **Save**.

BES12 validates the information for Microsoft Active Directory authentication. If the information is invalid, BES12 prompts you to specify the correct information.

14. Click **Close**.

**After you finish:** If you enabled single sign-on, perform the following actions:
- Restart the BES12 services on each computer that hosts a BES12 instance.
- Instruct administrators and BES12 Self-Service users to configure their browsers to support single sign-on for BES12.

**Related information**
- Configure constrained delegation for the Microsoft Active Directory account to support single sign-on, on page 32
- Browser requirements: Single sign-on, on page 34

**Connect to an LDAP directory**

**Before you begin:** Create an LDAP account for BES12 that is located in the relevant LDAP directory. The account must meet the following requirements:
• The user has permission to read all users in the directory.
• The user is not required to change the password at next login.
• The user’s password never expires.

If the LDAP connection is SSL encrypted, make sure that you have the server certificate for the LDAP connection.

**Note:** The LDAP attribute values in the following steps may be different from the attributes you must type. The values you must type depend on the LDAP environment your organization uses.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Company directory**.
3. Click **Add an LDAP connection**.
4. In the **Directory connection name** field, type a name for the directory connection.
5. In the **LDAP server discovery** drop-down list, perform one of the following actions:
   - To automatically discover the LDAP server, click **Automatic**. In the **DNS domain name** field, type the domain name for the server that hosts the company directory.
   - To specify a list of LDAP servers, click **Select server from list**. In the **LDAP server** field, type the name of the LDAP server. To specify more LDAP servers, click `+`.
6. In the **Enable SSL** drop-down list, perform one of the following actions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| If the LDAP connection is SSL encrypted | 1. Click **Yes**.  
|                                      | 2. Beside the **LDAP server SSL certificate** field, click **Browse**.  
|                                      | 3. Select the LDAP server certificate.  
|                                      | 4. Click **Open**.                                          |
| If the LDAP connection is not SSL encrypted | 1. Click **No**.                                            |

7. In the **LDAP Port** field, type the TCP port number for communication (for example, 636 for SSL enabled or 389 for SSL disabled).
8. In the **Authorization required** drop-down list, perform one of the following actions:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If authorization is required for the connection</td>
<td>1. Click <strong>Yes</strong>.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>2.</td>
<td>In the <strong>Login</strong> field, type the DN of the user who has authorization to log in to LDAP (for example, an=admin,o=Org1).</td>
</tr>
<tr>
<td>3.</td>
<td>In the <strong>Password</strong> field, type the password.</td>
</tr>
</tbody>
</table>

If authorization is not required for the connection |
| 1.     | Click **No**. |

9. In the **User Search base** field, type the value to use as the base DN for user information searches.

10. In the **LDAP user search filter** field, type the LDAP search filter that is required to find user objects in your organization’s directory server. For example, in IBM Domino Directory, type `(objectClass=Person)`.

    **Note:** If you want to exclude disabled user accounts from the search results, you must type `(&(objectclass=user)(logindisabled=false))`.

11. In the **LDAP user search scope** drop-down list, perform one of the following actions:

    • To search all objects following the base object, click **All levels**. This value is the default setting.
    • To search objects that are one level directly following the base DN, click **One level**.

12. In the **Unique identifier** field, type the name of the attribute that uniquely identifies each user in your organization’s LDAP directory. This attribute must be a string that is immutable and globally unique. For example, in IBM Domino LDAP 7 and later, you may type `dominoUNID`; in Microsoft Active Directory use may type `objectGUID`.

13. In the **First name** field, type the attribute for each user’s first name (for example, `givenName`).

14. In the **Last name** field, type the attribute for each user’s last name (for example, `sn`).

15. In the **Login attribute** field, type the login attribute to use for authentication (for example, `uid`).

16. In the **Email address** field, type the attribute for each user’s email address (for example, `mail`). If you do not set the value, a default value is used.

17. In the **Display name** field, type the attribute for each user’s display name (for example, `displayName`). If you do not set the value, a default value is used.

18. In the **Email profile account name** field, type the attribute for each user’s email profile account name (for example, `mail`).

19. In the **User Principal Name** field, type the user principal name for SCEP (for example, `mail`).

20. To enable directory-linked groups, select the **Enable directory-linked groups** check box and complete the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group search base</strong></td>
<td>Specify the value to use as the base DN for group information searches.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LDAP group search filter</td>
<td>Type the LDAP search filter that is required to find group objects in your company directory. For example, for IBM Domino Directory, type <em>(objectClass=dominoGroup)</em>.</td>
</tr>
<tr>
<td>Group Unique Identifier</td>
<td>Type the attribute for each group’s unique identifier. This attribute must be immutable and globally unique (for example, type <em>cn</em>).</td>
</tr>
<tr>
<td>Group Display name</td>
<td>Type the attribute for each group’s display name (for example, type <em>cn</em>).</td>
</tr>
<tr>
<td>Group Membership attribute</td>
<td>Type the attribute for each group’s membership identifier. This attribute must be immutable and globally unique (for example, type <em>member</em>).</td>
</tr>
<tr>
<td>Test Group Name</td>
<td>Type an existing group name for validating the group attributes specified.</td>
</tr>
</tbody>
</table>

21. Click **Save**.
22. Click **Close**.

**Enabling directory-linked groups**

You can create groups that are linked to groups in your company directory. You can configure BES12 to automatically synchronize the membership of a directory-linked group to its associated company directory groups. When you enable directory-linked groups, you can enable onboarding and offboarding, force the synchronization process, set the maximum number of changes per synchronization, and set the number of nested levels for the linked groups.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable onboarding   | Onboarding allows you to automatically add user accounts to BES12 based on user membership in a company directory group. You must add company directory groups to the Onboarding directory groups section. User accounts from those company directory groups are automatically added to BES12 during the synchronization process.  
You can configure onboarded users to either receive an email with an autogenerated device activation password or you can choose to not set a device activation password.  
**Offboarding**  
Optionally, you can set up offboarding. Offboarding occurs when a user is removed from all company directory groups in the Onboarding directory groups list and offboarding is enabled. |
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can select the following the enforcement action options you want BES12 to take when a user is offboarded:</td>
<td></td>
</tr>
<tr>
<td>• Delete device data when the user is removed from all onboarding directory groups</td>
<td></td>
</tr>
<tr>
<td>◦ Delete only work data</td>
<td></td>
</tr>
<tr>
<td>◦ Delete all device data</td>
<td></td>
</tr>
<tr>
<td>◦ Delete all device data for corporate owned/delete only work data for individually owned</td>
<td></td>
</tr>
<tr>
<td>• Delete user when the user is removed from all onboarding directory groups</td>
<td></td>
</tr>
<tr>
<td>Depending on the offboarding settings, company directory users, their devices, or both, they are automatically deleted from BES12 when they are deleted from all company directory groups configured for onboarding. They will be removed from BES12 if they do not belong to a company directory group configured for onboarding. The offboarding settings also apply to existing directory users in BES12. It is recommended that you click the preview icon to generate the directory synchronization report to verify the changes.</td>
<td></td>
</tr>
<tr>
<td>Force synchronization</td>
<td>Force synchronization determines the synchronization behavior when a company directory group is deleted from the company directory. If a company directory group no longer exists when force synchronization is enabled, the company directory group is removed from the onboarding directory groups list and from any directory-linked groups during the synchronization process.</td>
</tr>
<tr>
<td>When force synchronization is enabled, and if all the company directory groups linked to it are no longer in your company directory, a directory-linked group is converted to a local group.</td>
<td></td>
</tr>
<tr>
<td>When force synchronization is disabled and a company directory group is not found in your company directory, the synchronization process is canceled.</td>
<td></td>
</tr>
<tr>
<td>Sync limit</td>
<td>If the number of changes exceeds the maximum number of changes for each synchronization, you can prevent the synchronization process from running.</td>
</tr>
<tr>
<td>Before the synchronization process begins, the total number of changes that will occur are calculated by adding together the number of users onboarded, the number of users offboarded, the number of users added to groups, and the number of users removed from groups.</td>
<td></td>
</tr>
<tr>
<td>The default value is 5. If you want no limit to the number of changes, you must enter a value of 0.</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Maximum nesting level of directory groups | You can configure the maximum number of levels in a company directory group that you want directory-linked groups to link to. You can link to an unlimited number of nested levels. Examples:  
  - The default is -1. Returns all levels.  
  - Entering 0 returns the top level only.  
  - Entering 1 returns the top level and the first nested level.  
  For example, if a company directory group has 5 levels and you want to link to all the levels you type -1 in the field provided. If you want to link to the top level only you enter 0, or if you wanted to link to the top level and the first 4 levels, you type 4. |

For more information about creating directory-linked groups, see the Administration content.

**Enable directory-linked groups**

**Before you begin:** Verify that a company directory synchronization is not in progress. You cannot save the changes you make to the company directory connection until the synchronization is complete.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Company directory**.
3. Click the company directory name you want to edit.
4. Click **Sync settings**.
5. To enable directory-linked groups, select **Enable directory-linked groups**.
6. To enable onboarding, select **Enable onboarding** and perform the following actions for each group you want to onboard:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable onboarding | 1. In the **Onboarding directory groups** section, click **+**.  
2. In the **Search group from directory** field, type the company directory group name.  
3. Click **Q**.  
4. Select the company directory group in the search results list.  
5. Click **Add**.  
6. If necessary, select **Link nested groups**. |
7. In the **Device activation** section, choose one of the following:
   - To send users an email with an automatically generated activation password, click **Auto-generate device activation password and send email with activation instructions**. Enter the time an activation password remains valid and choose an activation email template.
   - To not set a device activation password, select **Do not set device activation password**.

8. To delete device data when a user is offboarded, select **Delete device data when the user is removed from all onboarding directory groups** and choose from the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| To delete all the data on a user's device when they are removed from a group | 1. Select one of the following options:  
   a. **Delete only work data**  
   b. **Delete all device data**  
   c. **Delete all device data for corporate owned/delete only work data for individually owned** |
| To delete a user account from BES12 when a user is removed from all onboarding groups | Select **Delete user when the user is removed from all onboarding directory groups**. |

9. To force the synchronization of directory-linked groups, select **Force synchronization**.

10. In the **Sync limit** field, type the maximum number of changes you want to allow in one directory synchronization.

   **Note:** The default value is 5. This means that the synchronization will not be performed if there are more than 5 changes. For example, if you leave this value at five and there are more than 5 changes, the synchronization will not run. If you enter a value of 0, this means there is no limit on the number of changes that a synchronization will complete.

11. In the **Maximum nesting level of directory groups** field, enter the number of nested levels for company directory groups. The default is -1, which means all levels. If you want the top level, type 0; if you want the top level and the first level, type 1, and so on.

12. Click **Save**.

   **After you finish:** For information about creating directory-linked groups, see the Administration content.

---

**Synchronize a company directory connection**

1. On the menu bar, click **Settings**.

2. In the left pane, click **External integration > Company directory**.
3. In the **Sync** column, click 🌟.

### View a directory synchronization report

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Company directory**.
3. In the **Last report** column, click the date.

### Adding a synchronization schedule

BES12 lets you set up synchronization schedules that automatically synchronize BES12 and your company directory. There are three types of synchronization schedules that you can add:

<table>
<thead>
<tr>
<th>Schedule type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interval</strong></td>
<td>Interval lets you choose the length of time between each synchronization and the time frame you want the synchronization to occur. You can select the days of the week that you want synchronizations to occur. You can select more than one day.</td>
</tr>
<tr>
<td><strong>Once a day</strong></td>
<td>Once a day lets you choose the time of day the synchronization starts and the days of the week that you want the synchronizations to occur. You can select more than one day.</td>
</tr>
<tr>
<td><strong>No recurrence</strong></td>
<td>No recurrence lets you configure a one time synchronization that starts on a time and day you select.</td>
</tr>
</tbody>
</table>

On the Company directory screen, you can manually synchronize BES12 and your company directory at any time.

### Add a synchronization schedule

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Company directory**.
3. Click the company directory name you want to edit.
4. On the **Sync schedule** tab, click 📦.
5. In the **Recurrence** field, perform one of the following actions:
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Interval** | 1. Select *Interval*.  
               2. Type the time in minutes between synchronizations.  
               3. In the *Synchronize between (UTC)* field, select the time to start the synchronizations and the time to stop the synchronizations.  
               4. Select the days of the week when you want synchronizations to occur. |
| **Once a day** | 1. Select *Once a day*.  
               2. Select the time when you want the synchronization to start.  
               3. Select the days of the week when you want the synchronizations to occur. |
| **No recurrence** | 1. Select *No recurrence*.  
               2. Select the time when you want the synchronization to start.  
               3. Select the day when you want the synchronization to occur. |

6. Click **Add**.
Configuring single sign-on for BES12

If you connect BES12 to Microsoft Active Directory, you can configure single sign-on authentication to permit administrators or users to bypass the login webpage and access the management console or BES12 Self-Service directly. When administrators or users log in to a computer using their Microsoft Active Directory credentials, the browser uses these credentials to authenticate them with BES12 automatically.

If you upgraded from BES5 and previously enabled single sign-on, you must enable it in BES12 for the Microsoft Active Directory connection that was moved from BES5.

Before you enable single sign-on for a Microsoft Active Directory connection, you must configure constrained delegation for the Microsoft Active Directory account that BES12 uses for the directory connection.

**Note:** If you enable single sign-on, any changes that you make to the Microsoft Active Directory account will require that you restart the BES12 services on each computer that hosts a BES12 instance. Administrators and users must log out from their computers and log in again to use single sign-on for BES12.

Steps to configure single sign-on for BES12

When you configure single sign-on for BES12, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure constrained delegation for the Microsoft Active Directory account to support single sign-on.</td>
</tr>
<tr>
<td>2</td>
<td>Enable single sign-on for a Microsoft Active Directory connection.</td>
</tr>
<tr>
<td>3</td>
<td>Verify browser requirements for single sign-on.</td>
</tr>
</tbody>
</table>
Configure constrained delegation for the Microsoft Active Directory account to support single sign-on

To support single sign-on for BES12, you must configure constrained delegation for the Microsoft Active Directory account that BES12 uses for the directory connection. Constrained delegation allows browsers to authenticate with BES12 on behalf of administrators or users when they access the management console or BES12 Self-Service.

1. Use the Windows Server ADSD Edit tool to add the following SPNs for BES12 to the Microsoft Active Directory account:
   - HTTP/<host_FQDN_or_pool_name> (for example, HTTP/domain123.example.com)
   - BASPLUGIN111/<host_FQDN_or_pool_name> (for example, BASPLUGIN111/domain123.example.com)

   If you configured high availability for the management consoles in a BES12 domain, specify the pool name. Otherwise, specify the FQDN of the computer that hosts the management console.

   **Note:** Verify that no other accounts in the Microsoft Active Directory forest have the same SPNs.

2. Open Microsoft Active Directory Users and Computers.

3. In the Microsoft Active Directory account properties, on the **Delegation** tab, select the following options:
   - Trust this user for delegation to specified services only
   - Use Kerberos only

4. Add the SPNs from step 1 to the list of services.

**Related information**

Configuring high availability for the management console, on page 51

Configure single sign-on for BES12

When you configure single sign-on for BES12, you configure it for the management console and BES12 Self-Service.

**Before you begin:**
- Configure constrained delegation for the Microsoft Active Directory account that BES12 uses for the directory connection.
- If you enable single sign-on for multiple Microsoft Active Directory connections, verify that there are no trust relationships between the Microsoft Active Directory forests.

1. On the menu bar, click **Settings**.
2. In the left pane, expand **External integration**.

3. Click **Company directory**.

4. In the **Configured directory connections** section, click the name of a Microsoft Active Directory connection.

5. On the **Authentication** tab, select the **Enable Windows single sign-on** check box.

6. Click **Save**.

7. Click **Save**.
   
   BES12 validates the information for Microsoft Active Directory authentication. If the information is invalid, BES12 prompts you to specify the correct information.

8. Click **Close**.

**After you finish:**

- Restart the BES12 services on each computer that hosts a BES12 instance.
- Instruct administrators and BES12 Self-Service users to configure their browsers to support single sign-on for BES12.

**Related information**

- [Configure constrained delegation for the Microsoft Active Directory account to support single sign-on](#), on page 32
- [Browser requirements: Single sign-on](#), on page 34

### Console URLs for single sign-on

If you configure single sign-on for BES12, you must instruct administrators to access the management console and users to access BES12 Self-Service using the following URLs:

<table>
<thead>
<tr>
<th>Console</th>
<th>URL for single sign-on authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>BES12 management console</td>
<td>https://&lt;host_FQDN_or_pool_name&gt;:&lt;port&gt;/admin</td>
</tr>
<tr>
<td>BES12 Self-Service</td>
<td>https://&lt;host_FQDN_or_pool_name&gt;:&lt;port&gt;/mydevice</td>
</tr>
</tbody>
</table>

Single sign-on authentication takes precedence over other authentication methods that permit administrators to log in to the management console and users to log in to BES12 Self-Service. If your organization’s security standards require that administrators or users use another authentication method, you must instruct them to access the management console or BES12 Self-Service using the following URLs:

<table>
<thead>
<tr>
<th>Console</th>
<th>URL for other authentication methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>BES12 management console</td>
<td>https://&lt;host_FQDN_or_pool_name&gt;:&lt;port&gt;/admin?sso=n</td>
</tr>
<tr>
<td>BES12 Self-Service</td>
<td>https://&lt;host_FQDN_or_pool_name&gt;:&lt;port&gt;/mydevice?sso=n</td>
</tr>
</tbody>
</table>
# Browser requirements: Single sign-on

If you configure single sign-on for BES12, the following requirements apply to the browsers used by administrators and BES12 Self-Service users.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Browser</strong></td>
<td>Any of the following:</td>
</tr>
<tr>
<td></td>
<td>• Internet Explorer</td>
</tr>
<tr>
<td></td>
<td>• Mozilla Firefox</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome</td>
</tr>
<tr>
<td></td>
<td>For more information about supported versions, see the Compatibility matrix.</td>
</tr>
<tr>
<td><strong>Browser settings</strong></td>
<td>Internet Explorer with the following settings:</td>
</tr>
<tr>
<td></td>
<td>• The management console and BES12 Self-Service URLs are assigned to the local intranet zone (Internet Options &gt; Security).</td>
</tr>
<tr>
<td></td>
<td>• Enable Integrated Windows Authentication is selected (Internet Options &gt; Advanced).</td>
</tr>
<tr>
<td></td>
<td>Firefox with the following settings:</td>
</tr>
<tr>
<td></td>
<td>• In the about:config list, https://, <code>&lt;host_FQDN_or_pool_name&gt;</code> is added to the &quot;network.negotiate-auth.trusted-uris&quot; preference. For more information, visit <a href="http://kb.mozillazine.org/about:config">kb.mozillazine.org/about:config</a>.</td>
</tr>
<tr>
<td></td>
<td>Google Chrome uses the local intranet zone settings from Internet Explorer. The management console and BES12 Self-Service URLs must be assigned to the local intranet zone (Internet Options &gt; Security).</td>
</tr>
</tbody>
</table>
Obtaining an APNs certificate to manage iOS devices

APNs is the Apple Push Notification Service. You must obtain and register an APNs certificate if you want to use BES12 to manage iOS devices. If you set up more than one BES12 domain, each domain requires an APNs certificate.

You can obtain and register the APNs certificate using the first login wizard or by using the external integration section of the administration console.

**Note:** Each APNs certificate is valid for one year. The administration console displays the expiry date. You must renew the APNs certificate before the expiry date, using the same Apple ID that you used to obtain the certificate. If the certificate expires, iOS devices do not receive data from BES12. If you register a new APNs certificate, iOS device users must reactivate their devices to receive data.

For more information, visit https://developer.apple.com to read *Issues with Sending Push Notifications* in article TN2265.

It is a best practice to access the administration console and the Apple Push Certificates Portal using the Google Chrome browser or the Safari browser. These browsers provide optimal support for requesting and registering an APNs certificate.

Data flow: Sending data to an iOS device

1. BES12 sends a notification to the APNs.
2. The APNs authenticates BES12 using the APNs certificate that you registered.
3. The APNs sends the notification to the iOS device.
4. The iOS device receives the notification and retrieves the data from BES12.

Steps to obtain an APNs certificate to manage iOS devices

To obtain and register an APNs certificate, perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Obtain a signed CSR from BlackBerry.</td>
</tr>
</tbody>
</table>
## Obtain a signed CSR from BlackBerry

You must obtain a signed CSR from BlackBerry before you can obtain an APNs certificate.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > iOS management**.
3. Click **Get APNs Certificate**.
   - If you want to renew the current APNs certificate, click **Renew certificate** instead.
4. In the **Step 1 of 3 - Download signed CSR certificate from BlackBerry** section, click **Download certificate**.
5. Click **Save** to save the signed CSR file (.scsr) to your computer.

**After you finish:** Request an APNs certificate from Apple.

## Request an APNs certificate from Apple

**Before you begin:** Download and save the signed CSR provided by BlackBerry.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > iOS management**.
3. In the **Step 2 of 3 - Request APNs certificate from Apple** section, click **Apple Push Certificate Portal**. You are directed to the Apple Push Certificates Portal.
4. Sign in to the Apple Push Certificates Portal using a valid Apple ID.
5. Follow the instructions to upload the signed CSR (.scsr).
6. Download and save the APNs certificate (.pem) on your computer.

**After you finish:** Register the APNs certificate.
Register the APNs certificate

Before you begin: Request an APNs certificate from Apple using the signed CSR from BlackBerry and save the APNs certificate on your computer.

1. On the menu bar, click Settings.
2. In the left pane, click External integration > iOS management.
3. In the Step 3 of 3 - Register APNs certificate section, click Browse. Navigate to and select the APNs certificate (.pem).
4. Click Submit.

After you finish:
- To test the connection between BES12 and the APNs server, click Test APNS certificate.
- To view the status and expiry date of the APNs certificate, click Settings > External integration > iOS management.

Renew the APNs certificate

The APNs certificate is valid for one year. You must renew the APNs certificate each year before it expires.

Before you begin: Obtain a new signed CSR from BlackBerry (see Obtain a signed CSR from BlackBerry).

1. On the menu bar, click Settings.
2. In the left pane, click External integration > iOS management.
4. Sign in to the Apple Push Certificates Portal using the same Apple ID that you used to obtain the original APNs certificate.
5. Follow the instructions to renew the APNs certificate (.pem). You will need to upload the new signed CSR.
6. Download and save the renewed APNs certificate on your computer.
7. In the Step 3 of 3 - Register APNs certificate section, click Browse. Navigate to and select the renewed APNs certificate.
8. Click Submit.

After you finish:
- To test the connection between BES12 and the APNs server, click Test APNS certificate.
- To view the status and expiry date of the APNs certificate, click Settings > External integration > iOS management.
Troubleshooting APNs

This section helps you troubleshoot APNs issues.

The APNs certificate does not match the CSR. Provide the correct APNs file (.pem) or submit a new CSR.

Description

You may receive an error message when you try to register the APNs certificate if you did not upload the most recently signed CSR file from BlackBerry to the Apple Push Certificates Portal.

Possible solution

If you downloaded multiple CSR files from BlackBerry, only the last one that you downloaded is valid. If you know which CSR is the most recent, return to the Apple Push Certificates Portal and upload it. If you are not sure which CSR is the most recent, obtain a new one from BlackBerry, then return to the Apple Push Certificates Portal and upload it.

I cannot activate iOS devices

Possible cause

If you are unable to activate iOS devices, the APNs certificate may not be registered correctly.

Possible solution

Perform one or more of the following actions:

- In the administration console, on the menu bar, click Settings > External integration > iOS management. Verify that the APNs certificate status is "Installed." If the status is not correct, try to register the APNs certificate again.
- Click Test APNS certificate to test the connection between BES12 and the APNs server.
- If necessary, obtain a new signed CSR from BlackBerry and a new APNs certificate.
Configuring BES12 for DEP

You must configure BES12 to use Apple’s Device Enrollment Program before you can synchronize BES12 with DEP. After you configure BES12, you can use the BES12 management console to manage the activation of the iOS devices that your organization purchased for DEP.

Steps to configure BES12 for DEP

When you configure BES12 for Apple’s Device Enrollment Program, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a DEP account.</td>
</tr>
<tr>
<td>2</td>
<td>Download a public key.</td>
</tr>
<tr>
<td>3</td>
<td>Generate a server token.</td>
</tr>
<tr>
<td>4</td>
<td>Register the server token with BES12.</td>
</tr>
<tr>
<td>5</td>
<td>Add an enrollment configuration.</td>
</tr>
</tbody>
</table>

Create a DEP account

1. On the menu bar, click Settings.
2. In the left pane, click External integration > Apple Device Enrollment Program.
3. In step 1 of 4: Create an Apple DEP account, click Create an Apple DEP account.
4. Complete the fields and follow the prompts to create your account.

After you finish: Download a public key.
Download a public key

**Before you begin:** Create a DEP account.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. In step **2 of 4: Download a public key**, click **Download public key**.
4. Click **Save**.

**After you finish:** Generate a server token.

Generate a server token

**Before you begin:** Download a public key.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. In step **3 of 4: Generate a Server Token from Apple DEP account**, click **Open the Apple DEP portal**.
4. Sign in to your DEP account.
5. Follow the prompts to generate a server token.

**After you finish:** Register the server token with BES12.

Register the server token with BES12

BES12 uses a server token for authentication when it communicates with Apple's Device Enrollment Program.

**Before you begin:** Generate a server token.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Apple Device Enrollment Program**.
3. In step **4 of 4: Register the server token with BES12**, click **Browse**.
4. Select the .p7m server token file.
5. Click **Open**.
6. Click **Next**.
After you finish: Add an enrollment configuration.

Add an enrollment configuration

Before you begin: Register the server token with BES12 before you add your first enrollment configuration.

After you register a server token, BES12 automatically displays the window where you add your first enrollment configuration.

1. Complete the fields and select the check boxes for the items you want to include in the enrollment configuration.
   - If you select "Automatically assign new devices to this configuration", BES12 automatically assigns the enrollment configuration to iOS devices when you register the devices in Apple's Device Enrollment Program. If you do not automatically assign an enrollment configuration, you can use the BES12 management console to assign enrollment configurations to iOS devices registered in DEP. For more information about assigning enrollment configurations, see the Administration content.
   - If you do not select either "Enable supervised mode" or "Allow removal of MDM profile" in the Device configuration section, BES12 prompts you to select one of the items when you save the enrollment configuration. You must select at least one of the items. Optionally, you can select both items.

2. Click Save.

3. If you selected "Automatically assign new devices to this configuration," click Yes.

After you finish: Activate iOS devices. For more information about activating devices, see the Administration content.

Update the server token

The server token is valid for one year. You must renew the token each year before it expires. To see the status of the token, see the Expiry date in the Apple Device Enrollment Program window.

Before you begin: If the public key has changed, Download a new public key.

1. On the menu bar, click Settings.

2. In the left pane, click External integration > Apple Device Enrollment Program.

3. In the Expiry date section, click Update server token.

4. In Step 1 of 2: Generate a Server Token from Apple DEP account, click Open the Apple DEP portal.

5. Sign in to your account for DEP.

6. Follow the prompts to generate a server token.

7. In step 2 of 2: Register the Server Token with BES12, click Browse.

8. Select the .p7m server token file.
9. Click Open.
10. Click Save.

Remove the DEP connection

**CAUTION:** If you remove the DEP connection, you cannot activate new iOS devices in Apple’s Device Enrollment Program. If you assigned enrollment configurations to devices and the configurations have not been applied, BES12 removes the enrollment configurations assigned to the devices. Removing the connection does not affect devices that are active on BES12.

If your organization no longer deploys iOS devices that use DEP, you can remove the BES12 connection to DEP.

1. On the menu bar, click Settings.
2. In the left pane, click External integration > Apple Device Enrollment Program.
3. Click Remove DEP connection.
4. Click Remove.
5. Click OK.
Connecting to an SMTP server to send email notifications

To allow BES12 to send email notifications, you must connect BES12 to an SMTP server.

BES12 uses email notifications to send activation instructions to users. You can also configure BES12 to send passwords for BES12 Self-Service and device compliance warnings, and you can send email messages to individuals.

If you don't connect BES12 to an SMTP server, BES12 cannot send passwords, activation messages, or email messages. You can still configure BES12 to send compliance warnings directly to devices.

For more information about activation messages, device compliance warnings, and sending individual email messages, see the Administration content.

Connect to an SMTP server to send email notifications

1. On the menu bar, click Settings.
2. In the left pane, click External integration > SMTP server.
3. Click .
4. In the Sender display name field, type a name to use for BES12 email notifications. For example, donotreply or BES12 Admin.
5. In the Sender address field, type the email address you want BES12 to use to send email notifications.
6. In the SMTP server field, type the FQDN of the SMTP server. For example, mail.example.com.
7. In the SMTP server port field, type the SMTP server port number. The default port number is 25.
8. In the Supported encryption type drop-down menu, select the encryption type you want to apply to email messages.
9. If the SMTP server requires authentication, in the Username field, type the SMTP server login name. In the Password field, type the SMTP server password.
10. If necessary, import an SMTP CA certificate:
   a. Copy the SSL certificate file for your organization’s SMTP server to the computer that you are using.
   b. Click Browse.
   c. Browse to the SSL certificate file and click Upload.
11. Click **Save**.

**After you finish:** Click **Test connection** if you want to test the connection to the SMTP server and send a test email message. BES12 sends the message to the email address you specified in the **Sender address** field.
Setting up BES12 Self-Service for users

BES12 Self-Service is a web-based application that you can make available to users so that they can perform management tasks such as creating activation passwords, remotely locking their devices, or deleting data from their devices. Users do not need to install any software on their computers to use BES12 Self-Service. You must provide the web address and login information to users.

You can force users to read and accept a login notice before they can log in to BES12 Self-Service. For more information about the advisory notice, see the Administration content.

Set up BES12 Self-Service

Set up BES12 Self-Service so that users can log in and perform some self-service tasks.

1. On the menu bar, click **Settings**.
2. In the left pane, click **General settings > Self-Service**.
3. Verify that **Allow users to access the self-service console** is selected.
4. To allow users to create activation passwords, select **Allow users to activate devices in the self-service console** and complete the following tasks:
   a. Specify the number of minutes, hours, or days that a user can activate a device before the activation password expires.
   b. Specify the minimum number of characters required in an activation password.
   c. In the **Minimum password complexity** drop-down list, select the level of complexity required for activation passwords.
5. Click **Save**.

After you finish: Provide the BES12 Self-Service web address and login information to users.
# Configuring high availability for a BES12 domain

BES12 uses an active-active high availability model to minimize service interruptions for device users. To configure high availability, you install multiple instances of BES12, each on a separate computer. Each instance connects to the BES12 database and actively manages user accounts and devices.

High availability in BES12 includes the following features:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically move BlackBerry 10 devices to a healthy BES12 instance</td>
<td>If BlackBerry 10 devices on a BES12 instance cannot connect to work resources using enterprise connectivity, those devices are reassigned to healthy BES12 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.</td>
</tr>
<tr>
<td>iOS, Android, and Windows devices can connect to any BES12 instance</td>
<td>iOS and Android devices with Secure Work Space can use enterprise connectivity to connect to any healthy BES12 instance to access email and calendar data, the work browser, and the organization’s network. If one or more BES12 instances are unhealthy, iOS and Android devices (with or without Secure Work Space) and Windows devices connect to one of the healthy instances. As result, device service continues uninterrupted.</td>
</tr>
<tr>
<td>BlackBerry Affinity Manager failover</td>
<td>The BlackBerry Affinity Manager assigns BlackBerry 10 devices to a BES12 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 BES12 instance. 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 starts an election process to become active. The instance that completes the election process first becomes the active BlackBerry Affinity Manager.</td>
</tr>
<tr>
<td>Manage devices from any BES12 instance</td>
<td>If there is a problem with the management console or BES12 Core for a BES12 instance, you can continue to manage any device (BlackBerry 10, iOS, Android, and Windows devices) using the management console and BES12 Core of any healthy instance.</td>
</tr>
</tbody>
</table>
### Feature | Description
--- | ---
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 BES12 instance. If there is a problem with a console, the pool makes sure that you connect to a working console.

When BES12 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 BES12 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.

### High availability for the components that manage BlackBerry OS devices

If you configured high availability for BES5 before you upgraded BES5 to BES12, the configuration continues to work as expected after you complete the upgrade. The high availability configuration applies only to the components that manage BlackBerry OS devices.

For more information about configuring high availability for the components that manage BlackBerry OS devices, visit help.blackberry.com/detectLang/category/enterprise-services to read the *BlackBerry Enterprise Server 5 Administration Guide*.

### Architecture: High availability for BES12

The following diagram shows a high availability domain with two BES12 instances. You can install any number of BES12 instances. This topic explains how specific components are involved in a high availability configuration. For more information about the BES12 architecture and components, see the Architecture content.
Components

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BES12 database</td>
<td>Each BES12 instance connects to the BES12 database to access user and device data.</td>
</tr>
<tr>
<td>Management console and BES12 Core</td>
<td>You can use any management console to manage the domain’s user accounts and devices. The BES12 Core associated with that console carries out the management tasks. 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. Any healthy BES12 instance can manage enterprise connectivity for iOS and Android devices with Secure Work Space. Each instance manages enterprise connectivity for the</td>
</tr>
</tbody>
</table>
### Components and Description

<table>
<thead>
<tr>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlackBerry 10</td>
<td>BlackBerry 10 devices that are assigned to it by the BlackBerry Affinity Manager. Any healthy instance can process device management tasks for all device types.</td>
</tr>
<tr>
<td>BlackBerry MDS Connection Service and BlackBerry Dispatcher</td>
<td>These components allow BlackBerry 10 devices to connect to and use work resources.</td>
</tr>
<tr>
<td>BlackBerry Affinity Manager</td>
<td>The BlackBerry Affinity Manager is responsible for:</td>
</tr>
<tr>
<td></td>
<td>- Assigning BlackBerry 10 devices to BES12 instances</td>
</tr>
<tr>
<td></td>
<td>- Maintaining a connection with the BlackBerry Infrastructure</td>
</tr>
<tr>
<td></td>
<td>- Configuring and starting the active BlackBerry Work Connect Notification Service</td>
</tr>
<tr>
<td></td>
<td>- Checking the health of the BlackBerry MDS Connection Service and BlackBerry Dispatcher in each instance to monitor enterprise connectivity</td>
</tr>
<tr>
<td></td>
<td>Only one BlackBerry Affinity Manager is active (the others are on standby). If the active instance finds a problem with enterprise connectivity, it reassigns BlackBerry 10 users to the healthy BES12 instances.</td>
</tr>
<tr>
<td></td>
<td>Each standby BlackBerry Affinity Manager monitors the active BlackBerry Affinity Manager. If there is a problem with the active BlackBerry Affinity Manager, a failover occurs and one of the standby instances becomes active.</td>
</tr>
</tbody>
</table>

### Load-balancing data for BlackBerry 10 devices

When you install multiple instances of BES12 in a domain, the active BlackBerry Affinity Manager distributes BlackBerry 10 devices equally across the healthy instances. For example, if you install three instances of BES12 and the domain includes 3000 BlackBerry 10 devices, the active BlackBerry Affinity Manager assigns 1000 devices to each instance. Load-balancing occurs only if the domain includes more than 500 BlackBerry 10 devices.

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

Each BES12 instance connects to the same BES12 database. The components on each instance are all running and actively managing data for all device types, except for the BlackBerry Affinity Manager and BlackBerry Work Connect Notification Service. Only one instance of the BlackBerry Affinity Manager and the BlackBerry Work Connect Notification Service are active. You can view the status of each instance in the management console.

If an instance is temporarily unavailable, the remaining instances manage user and device data.
Load-balancing device connections for iOS and Android devices with Secure Work Space

When you install multiple instances of BES12, device connections for iOS and Android devices with Secure Work Space are distributed across the available, healthy instances in the domain. If one or more instances are unhealthy, the BlackBerry Infrastructure redirects device connections to the healthy BES12 instances.

How BES12 evaluates the health of components

The following BES12 components have health scores that are used to determine whether a recovery action is required:

<table>
<thead>
<tr>
<th>Components</th>
<th>Health monitored by</th>
<th>Health score factors</th>
<th>Action if health is below threshold</th>
</tr>
</thead>
</table>
| BlackBerry MDS Connection Service and BlackBerry Dispatcher (aggregate health score) | Active BlackBerry Affinity Manager                | • 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 BES12 instance to the healthy instances. |
| Active BlackBerry Affinity Manager              | Each standby BlackBerry Affinity Manager          | • 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 BES12 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. |
Install an additional BES12 instance

To install additional BES12 instances to create a high availability domain, see the Installation and upgrade content. Verify that the computer satisfies the system requirements for installing a BES12 instance, and complete the necessary preinstallation and postinstallation tasks. For compatibility details, see the Compatibility matrix.

When you install additional BES12 instances:

- Install each instance on a separate computer.
- In the setup application, on the Setup type screen, select Use an existing domain.
- On the Database information screen, specify the information for the BES12 database that you created when you installed the original BES12 instance.

After you install an additional BES12 instance and complete the necessary postinstallation tasks, active-active high availability is available in the domain. User and device data is load-balanced across the BES12 instances, the active BlackBerry Affinity Manager monitors the enterprise connectivity of each instance, and the standby BlackBerry Affinity Manager instances monitor the active instance to determine whether a failover is required.

Configuring high availability for the management console

To configure high availability for the BES12 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 BES12 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 BES12 services on each computer that hosts a BES12 instance.

A BES12 management console instance in the round-robin pool can disconnect from the BES12 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.

Related information
Configure constrained delegation for the Microsoft Active Directory account to support single sign-on, on page 32
View the status of BES12 instances

1. On the menu bar, click Settings.
2. In the left pane, click Infrastructure > BES12 instances.
   For each BES12 instance in the domain, you can view the following information:
   - Whether each BES12 component is running or stopped
   - Whether the BlackBerry Affinity Manager is the primary instance or a standby instance
   - Whether the primary BlackBerry Affinity Manager is connected to the BlackBerry Infrastructure
   - Whether the BES12 Core is connected to the BlackBerry Infrastructure
   - Whether the components are connected to the BES12 database
3. To refresh the information on the page, click ⌁.

Remove a BES12 instance from the database

If you uninstall a BES12 instance, you must complete the following steps to remove the data for that instance from the BES12 database. If you do not, the BES12 log files indicate that the instance that you removed is not available.

**Before you begin:** Uninstall a BES12 instance.

1. On the menu bar, click Settings.
2. In the left pane, click Infrastructure > BES12 instances.
3. For the BES12 instance that you removed, click 🗑.
4. Click Delete.
Configuring database high availability using database mirroring

You can use database mirroring to provide high availability for the BES12 database. Database mirroring is a Microsoft SQL Server feature that allows you to retain database service and data integrity if issues occur with the BES12 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 BES12. For more information about using AlwaysOn, see the Installation and upgrade content. Note that the AlwaysOn feature cannot be used if you upgrade from BES5 to BES12 (the BES5 database is upgraded to a BES12 database). AlwaysOn is not supported for the components that manage BlackBerry OS devices.

When you configure database mirroring, you back up the principal BES12 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 BES12 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.

This section explains how to create a mirror database and configure the BES12 components to support database mirroring. You also have the option of configuring database mirroring for the components that manage BlackBerry OS devices. For more information, see Database high availability for components that manage BlackBerry OS devices.

To learn more about database mirroring, visit technet.microsoft.com/sqlserver to read Database Mirroring - SQL Server 2008 R2 or Database Mirroring - SQL Server 2012.
Database high availability for components that manage BlackBerry OS devices

The BES12 components that manage BlackBerry 10, iOS, Android, and Windows devices use the same database as the components that manage BlackBerry OS devices. The components that manage BlackBerry OS devices use a different method to connect to the mirror database. If you want to configure database mirroring for the components that manage BlackBerry OS devices, you can complete additional steps after you finish this section.

Visit help.blackberry.com/detectLang/category/enterprise-services to read “Configuring BlackBerry Configuration Database high availability” in the BlackBerry Enterprise Server 5 Administration Guide. The chapter gives instructions for connecting the components that manage BlackBerry OS devices to the mirror database.

Note: “Configuring BlackBerry Configuration Database high availability” includes references to Microsoft SQL Server 2005. This version of Microsoft SQL Server is no longer supported.

If you configured database mirroring for BES5 before you upgraded BES5 to BES12, the configuration continues to work as expected after you complete the upgrade. The configuration applies only to the components that manage BlackBerry OS devices.

Steps to configure database mirroring

To configure database mirroring, perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Verify that the BES12 domain meets the system requirements and prerequisites.</td>
</tr>
<tr>
<td>2</td>
<td>Create the mirror database, start a mirroring session, and set up a witness server.</td>
</tr>
<tr>
<td>3</td>
<td>Configure each BES12 instance to connect to the mirror database.</td>
</tr>
</tbody>
</table>
# System requirements: Database mirroring

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>BES12 supports database mirroring using one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft SQL Server 2012</td>
</tr>
<tr>
<td>SQL Server Native Client</td>
<td>The SQL Server 2012 Native Client must be installed on each computer that hosts a BES12 instance. The BES12 setup application installs the SQL Server 2012 Native Client.</td>
</tr>
<tr>
<td>Version parity</td>
<td>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.</td>
</tr>
<tr>
<td>Single data center</td>
<td>The principal and mirror database must be located in the same data center.</td>
</tr>
<tr>
<td>Database location</td>
<td>Create the mirror database on a different computer than the principal database.</td>
</tr>
<tr>
<td>Operating mode</td>
<td>Configure database mirroring using high-safety mode with automatic failover.</td>
</tr>
<tr>
<td>Witness</td>
<td>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 <a href="https://example.com">Database Mirroring Witness – SQL Server 2008 R2</a> or <a href="https://example.com">Database Mirroring Witness – SQL Server 2012</a>.</td>
</tr>
</tbody>
</table>

# Prerequisites: Configuring database mirroring

- Configure the principal server and mirror server to permit access from remote computers.
- Configure the principal server and mirror server to have the same permissions.
- Set up a witness server that you will use to monitor the principal server. For more information, see [Database Mirroring Witness – SQL Server 2008 R2](https://example.com) or [Database Mirroring Witness – SQL Server 2012](https://example.com).
- Configure the Microsoft SQL Server Agent to use a domain user account with the same local administrative permissions as the Windows account that runs the BES12 services.
- Verify that the domain user account has permissions for both the principal server and mirror server.
- Verify that the DNS server is running.
• On each computer that hosts a BES12 database instance, in the SQL Server 2012 Native Client, turn off the Named Pipes option. If you choose to not turn off the Named Pipes option, visit http://support.blackberry.com/kb to read article KB34373.

• To review additional prerequisites for your organization’s version of Microsoft SQL Server, visit technet.microsoft.com/sqlserver to read Database Mirroring - SQL Server 2008 R2 or Database Mirroring - SQL Server 2012.

• If the mirror database uses the default instance, the BES12 components can connect to the mirror database using the default port 1433 only, not a custom static port. This is due to a limitation of Microsoft SQL Server 2005 and later. For more information about this issue, see SQL 2005 JDBC Driver and Database Mirroring.

Create and configure the mirror database

**Before you begin:** To maintain database integrity while you create and configure the mirror database, stop the BES12 services on every computer that hosts a BES12 instance.

1. In Microsoft SQL Server Management Studio, browse to the principal database.

2. Change the Recovery Model property to FULL.

3. In the query editor, run the `ALTER DATABASE `<BES_db>` SET TRUSTWORTHY ON` query, where `<BES_db>` is the name of the principal database (for example, bes).

4. Back up the principal database. Change the Backup type option to Full.

5. Copy the backup files to the mirror server.

6. On the mirror server, restore the database to create the mirror database. When you restore the database, select the **NO RECOVERY** option.

7. Verify that the name of the mirror database matches the name of the principal database.

8. On the principal server, in Microsoft SQL Server Management Studio, right-click the principal database and select the **Mirror** task. On the **Mirroring** page, click **Configure Security** to launch the Configure Database Mirroring Security wizard.

9. Start the mirroring process. For more information, see Setting up Database Mirroring – SQL Server 2008 R2 or Setting Up Database Mirroring – SQL Server 2012.

10. To enable automatic failover, add a witness to the mirroring session. For more information, see Database Mirroring Witness – SQL Server 2008 R2 or Database Mirroring Witness – SQL Server 2012.

**After you finish:**

• To verify that failover works correctly, manually fail over service to the mirror database and back to the principal database.

• Restart the BES12 services on every computer that hosts a BES12 instance. Do not stop and start the BES12 - BlackBerry Work Connect Notification Service; this service is automatically restarted when you restart the BES12 - BlackBerry Affinity Manager service.
Connect BES12 to the mirror database

You must repeat this task on every computer that hosts a BES12 instance. If the only BES12 component on a computer is the BlackBerry Router, you do not need to complete this task on that computer.

Before you begin:
- Create and configure the mirror database.
- Verify that the mirror server is running.

1. On the computer that hosts the BES12 instance, navigate to <drive>:\Program Files\BlackBerry\BES\common-settings.
2. In a text editor, open DB.properties.
3. In the section optional settings to use failover, after configuration.database.ng.failover.server=, type the FQDN of the mirror server (for example, configuration.database.ng.failover.server=mirror_server.domain.net).
4. If necessary, perform one of the following actions:
   - If you specified a named instance for the principal database during installation, and the mirror database uses the default instance, delete the value after configuration.database.ng.failover.instance=.
   - If the principal database uses a default instance and the mirror database uses a named instance, after configuration.database.ng.failover.instance=, type the named instance.
5. Save and close DB.properties.

After you finish:
- Restart the BES12 services. Do not stop and start the BES12 - BlackBerry Work Connect Notification Service; this service is automatically restarted when you restart the BES12 - BlackBerry Affinity Manager service.
- Repeat this task on every computer that hosts a BES12 instance.
- Verify that each computer that hosts a BES12 instance can connect to the mirror server using the server shortname.

Configuring a new mirror database

If you create and configure a new mirror database after a role switch has occurred (that is, the BES12 components failed over to the existing mirror database and the existing mirror database became the principal database), repeat Connect BES12 to the mirror database on each computer that hosts a BES12 instance.

If necessary, configure the components that manage BlackBerry OS devices to connect to the new mirror server (see Database high availability for components that manage BlackBerry OS devices).
Configuring BES12 to send notifications to iOS devices with Secure Work Space

The BlackBerry Work Connect Notification Service communicates with Microsoft Exchange to provide email and organizer notifications to the Work Connect app on iOS devices with Secure Work Space. To enable notifications, you must complete the following configuration tasks:

- Configure the BlackBerry Work Connect Notification Service
- Enable an SSL connection between BES12 and your organization’s Microsoft Exchange Server

Configure the BlackBerry Work Connect Notification Service

iOS devices do not allow apps to run in the background (with specific exceptions, such as the default messaging app), so work space apps receive new data only if the app is open or if the notification comes from the APNs. The BlackBerry Work Connect Notification Service uses Microsoft Exchange Web Services to receive notifications from the Microsoft Exchange Server and sends the notifications through the BlackBerry Infrastructure to the APNs. The APNs notifies the Work Connect app on the device.

Before you begin:

- Any firewall between BES12 and the Microsoft Exchange CAS must allow an SSL connection over port 8091.
- Configure a Microsoft Exchange account with permissions to impersonate all users. BES12 can use this account to request and receive notifications from the Microsoft Exchange Server when new or updated items are available in a user’s mailbox. For more information about configuring an impersonation account on Microsoft Exchange 2007, Microsoft Exchange 2010, or Microsoft Exchange 2013 (CU2 or later), visit http://support.blackberry.com/kb to read article KB36432 (Part 2).

1. On the menu bar, click Settings.
2. In the left pane, click External integration > Work Connect Notification.
3. For each Microsoft Exchange Server that you want to monitor, perform the following actions:
   a. In the Add Exchange Web Services and import Microsoft Exchange Server certificates section, click +.
   b. In the Exchange Web Services URL field, type the Microsoft Exchange Web Services URL (for example, https://cas.domain.com/EWS/Exchange.asmx).
c. In the **Microsoft Exchange version** drop-down list, select the version of the Microsoft Exchange Server.

d. In the **Username** field, type the domain name and the username for the Microsoft Exchange account that has impersonation permissions. Use the following format: `domain_name\username`.

e. In the **Password** field, type the password for the Microsoft Exchange account that has impersonation permissions.

f. Click **Save**.

## Enable an SSL connection with Microsoft Exchange Server

BES12 registers with your organization's Microsoft Exchange Server on behalf of device users to receive new mail notifications. To enable an SSL connection between BES12 and a Microsoft Exchange Server, you must export the BlackBerry Work Connect Notification Service Root and Intermediate certificates (both contained in a .p7b file) and import them into the Microsoft Exchange Server certificate stores.

If the Microsoft Exchange Server uses a self-signed or CA-signed certificate, you must import the certificate into the BlackBerry Work Connect Notification Service certificate store.

1. In the management console, on the menu bar, click **Settings**.
2. In the left pane, click **External integration > Work Connect Notification**.
4. Transfer the .p7b file to the computer that hosts the Microsoft Exchange Server.
5. Use the Microsoft Management Console to import the .p7b file into the Trusted Root Certification Authorities certificate store. Then export the Intermediate certificate (.cer) from the Trusted Root Certification Authorities certificate store and import it into the Intermediate Certification Authorities certificate store (Certificates folder). Afterwards, delete the Intermediate certificate from the Trusted Root Certification Authorities certificate store. For instructions, visit the [Microsoft Developer Network](https://developer.microsoft.com) to see the Microsoft Management Console (MMC) documentation.

If your organization uses Microsoft Exchange Server 2007 or 2010 with a CAS array, repeat this step on each server in the array. If your organization uses Microsoft Exchange Server 2013, repeat this task on each Mailbox server.

6. For each Microsoft Exchange Server that uses a self-signed or CA-signed certificate, perform the following actions:
   a. Export the Microsoft Exchange Server certificate in an X.509 format (*.cer, *.der). For instructions, visit the [Microsoft Developer Network](https://developer.microsoft.com) to see Microsoft Management Console (MMC) documentation. Store the certificate in a location that you can access from the BES12 management console.
   b. In the management console, on the menu bar, click **Settings**.
   c. In the left pane, click **External integration > Work Connect Notification**.
d. Under **Add Exchange Web Services and import Microsoft Exchange Server certificates**, click the appropriate Exchange Web Services URL.

e. Click ✏.

f. Select the **Import Microsoft Exchange Server certificate** check box.

g. Click **Browse**.

h. Select the Microsoft Exchange Server certificate that you exported in X.509 format (*.cer, *.der).

i. Click **Save**.
Configuring BES12 to support Android for Work

BES12 supports the Android for Work feature in Android OS 5.1 (Lollipop) and later. Android for Work is a feature developed by Google that provides additional security for organizations that want to manage Android devices and allow their data and apps on Android devices. With Android for Work, you can unify work and personal requirements on Android devices that might not be owned by your organization. For example, you can use Android for Work to set up work email on personal devices and still ensure that work data is secure.

To support Android for Work in your organization, you must have a Google for Work domain or Google Apps for Work domain configured to support third-party mobile device management providers. To configure BES12 to support Android for Work, you must:

- Create a Google service account that BES12 can use to connect to your Google for Work or Google Apps for Work domain.
- Configure your Google for Work or Google Apps for Work domain to support mobile device management.
- Generate a token that BES12 uses when it connects to your Google for Work or Google Apps for Work domain.
- If you want to allow BES12 to create user accounts in your Google for Work domain, configure the permissions for the Google service account to allow updates to the user directory.
- Connect BES12 to the Google for Work or Google Apps for Work domain.

After you complete these tasks, you can add Android for Work activation types to your activation profiles. When a user activates a device with an Android for Work activation type, the device receives a work profile that separates and encrypts work data. If you remove the Android for Work connection in BES12, you also deactivate all devices that were activated with an Android for Work activation type.

For instructions on how to perform the required tasks, visit http://support.blackberry.com/kb to read article 37748. For more information about Google for Work, visit https://www.google.com/work/.

Note: You can connect only one BES12 instance to your Google for Work or Google Apps for Work domain. Before you connect another BES12 instance, you must remove the connection to the first instance. Remove the connection before you uninstall BES12, or before you revert to a virtual machine snapshot that you created before you established the connection. If you do not remove the connection, you may be unable to connect your Google domain to a new BES12 instance.
Deploying a discovery service to simplify Windows 10 activations

You can use a Java web application from BlackBerry as a discovery service to simplify the activation process for users with Windows 10 devices. If you use the discovery service, users don’t need to type a server address during the activation process. If you choose not to deploy this web application, users can still activate Windows 10 devices by typing the server address when asked.

Steps to deploy a discovery service web application

You can use different operating systems and web application tools to deploy a discovery service web application. This topic describes the high-level steps. See Deploy a discovery service to simplify Windows 10 activations for an example of the specific steps you would take using certain common operating systems and tools.

When you deploy a discovery service web application, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a static DNS Host A record for the Java application server. The record must specify <code>enterpriseenrollment.&lt;emaildomain&gt;</code> where <code>&lt;emaildomain&gt;</code> corresponds to email addresses of your users.</td>
</tr>
<tr>
<td>2</td>
<td>If you want to allow users to activate while they are outside your network, configure the computer that hosts the discovery service to listen externally on port 443.</td>
</tr>
<tr>
<td>3</td>
<td>Create and install a certificate to secure TLS connections between the Windows 10 device and the discovery service.</td>
</tr>
<tr>
<td>4</td>
<td>Download the file <code>W10AutoDiscovery-1.0.6.exe</code> from <a href="http://docs.blackberry.com/bes12tools">http://docs.blackberry.com/bes12tools</a>. Run the file to extract a <code>.war</code> file and deploy it to the root of your Java application server.</td>
</tr>
<tr>
<td>5</td>
<td>Update the <code>wpd.properties</code> file of the discovery service web application to include a list of your organization’s SRP IDs.</td>
</tr>
</tbody>
</table>
Deploy a discovery service to simplify Windows 10 activations

The following steps describe how to deploy the discovery service web application in the environment described below.

**Before you begin:** Verify that the following software is installed and running in your environment:

- Windows Server 2012 R2
- Java JRE 1.8 or later
- Apache Tomcat 8 Version 8.0 or later

1. Configure a static IP address for the computer that will host the discovery service.

   **Note:** If you want to allow users to activate devices when they are outside your organization’s network, the IP address must be externally accessible on port 443.

2. Create a DNS Host A record for the name `enterpriseenrollment.<email domain>` that points to the static IP address that you configured in Step 1.

3. In the directory where you installed Apache Tomcat, search the server.xml file for `8080` and apply comment tags as shown in the example below:

   ```xml
   <!--
   <Connector port="8080" protocol="HTTP/1.1"
   connectionTimeout="20000"
   redirectPort="8443" />
   -->
   ```

4. Search `server.xml` and change all instances of `8443` to `443`.

5. Search for the `<Connector port="443"` section, remove the comment tags above and below, and modify it as shown in the example below:

   ```xml
   maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS" keystoreFile="C:\Users\<account name>\.keystore" />
   ```

6. While logged in as the account you specified in the example above, generate a certificate by running the two commands shown in the example below. When asked for your first and last name, type `enterpriseenrollment.<email domain>` as shown in the step result below:

   ```bash
   C:\Program Files (x86)\Java\jre1.8.0_60\bin>keytool -genkey -alias tomcat -keyalg RSA -keysize 2048
   ```
C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias tomcat -keyalg RSA -file <filename>.csr

C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -genkey -alias tomcat -keyalg RSA -keysize 2048
Enter keystore password: changeit
What is your first and last name?
[Unknown]: enterpriseenrollment.example.com
What is the name of your organizational unit?
[Unknown]: IT Department
What is the name of your organization?
[Unknown]: Manufacturing Co.
What is the name of your City or Locality?
[Unknown]: Waterloo
What is the name of your State or Province?
[Unknown]: Ontario
What is the two-letter country code for this unit?
[Unknown]: CA
Is CN=enterpriseenrollment.example.com, OU=Business Unit, O=Example Company, L=Waterloo, ST=Ontario, C=CA correct?
[no]: yes

C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -certreq -alias tomcat -keyalg RSA -file <enterpriseenrollment.example.com>.csr
Enter key password for <enterpriseenrollment.example.com> (RETURN if same as keystore password):

7. Send the certificate signing request to a certification authority. The certification authority will send back a .p7b file. For the example above, the certification authority would return the file enterpriseenrollment.example.com.p7b.
   • If you send the certificate signing request to a major external certification authority, users should not have to take any additional action to trust this certificate during the activation process.
   • If you send the certificate signing request to an internal certification authority, users must install the CA certificate on the device before starting the activation process.

8. Install the certificate using the command shown in the example below:
   C:\Program Files (x86)\Java\jre1.8.0_60\bin> keytool -import -trustcacerts -alias tomcat -file <filename>.p7b


10. Download and run the file W10AutoDiscovery-1.0.6.exe. You can get the file from http://docs.blackberry.com/bes12tools.
This will extract the file W10AutoDiscovery-1.0.6.war to C:\BlackBerry.

11. In the directory where you installed Apache Tomcat, check for the folder \webapps\ROOT. If it already exists, delete the \ROOT folder.

12. Rename W10AutoDiscovery-1.0.6.war as ROOT.war. Move it to the folder \webapps in the directory where you installed Apache Tomcat.
   Apache Tomcat will deploy the new webapp and create a `webapp\ROOT` folder.

14. Run notepad.exe as administrator. In the directory where you installed Apache Tomcat, open `webapps\ROOT\WEB-INF\classes\config\wdp.properties`.

15. Add the Host ID for your BES12 domain to the line `wdp.whitelisted.srpid` as shown in the example below. You can find the Host ID for your BES12 domain in the BES12 management console. If you have multiple BES12 domains, specify the Host ID for each one. Perform the following actions:
   a. On the **Settings** tab, expand **Licensing > Licensing summary**.
   b. Click **Activate licenses**.
   c. In the **Licensing activation method** drop-down list, click **Host ID**.

   ```
   wdp.whitelisted.srpid=<Host ID>, <Host ID>, <Host ID>
   ```

Using the BlackBerry Gatekeeping Service

You can stop unauthorized devices from using Exchange ActiveSync unless they are explicitly added to the allowed list. Devices that are not on the allowed list cannot access work email and organizer data. Using the BlackBerry Gatekeeping Service makes sure that only devices managed by BES12 can access work email and other work information on the device.

To use the BlackBerry Gatekeeping Service, you must create a Microsoft Exchange configuration and assign an email profile to users that has the automatic gatekeeping server selected.

If a device does not comply with your organization’s security policies, it is not added to the allowed list. If a device becomes out of compliance with your organization’s security policies, it is automatically removed from the allowed list. For example, if the email profile is removed from the device, the device does not meet the settings in the compliance profile, or if the device is deactivated, the device is removed from the allowed list.

For more information about adding an automatic gatekeeping server to an email profile, viewing the connection status of a device, and allowing or blocking devices that are not automatically added to the allowed list, see the Administration content.

Steps to configure Exchange ActiveSync and the BlackBerry Gatekeeping Service

When you configure the BlackBerry Gatekeeping Service, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure Microsoft Exchange permissions for gatekeeping.</td>
</tr>
<tr>
<td>2</td>
<td>Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync.</td>
</tr>
<tr>
<td>3</td>
<td>Configure Microsoft IIS permissions for gatekeeping.</td>
</tr>
<tr>
<td>4</td>
<td>Create a Microsoft Exchange configuration.</td>
</tr>
<tr>
<td>5</td>
<td>Create an email profile that has an automatic gatekeeping server selected. For instructions, see the Administration content.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>6</td>
<td>Assign the email profile to a user account, user group, or device group. For instructions, see the Administration content.</td>
</tr>
<tr>
<td>7</td>
<td>Optionally, configure Microsoft Office 365 for gatekeeping.</td>
</tr>
</tbody>
</table>

## Configure Microsoft Exchange permissions for gatekeeping

To use Exchange ActiveSync gatekeeping, you must configure management roles in Microsoft Exchange Server 2010 or later with the correct permissions to manage mailboxes and client access for Exchange ActiveSync. To perform this task, you must be a Microsoft Exchange administrator with the appropriate permissions to create and change management roles.

**Before you begin:** On the computer that hosts Microsoft Exchange, create an account and mailbox to manage gatekeeping in BES12 (for example, BES12Admin). You must specify the login information for this account when you create an Exchange ActiveSync configuration.

WinRM must be configured with the default settings on the computer that hosts the Microsoft Exchange Server that you configure for gatekeeping. You must run the command `winrm quickconfig` from a command prompt as an administrator. When the tool displays `Make these changes [y/n]`, type `y`. After the command is successful, you see the following message.

```
WinRM has been updated for remote management.
WinRM service type changed to delayed auto start.
WinRM service started.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
```

1. On a computer that hosts the Microsoft Exchange Management Shell, open the Microsoft Exchange Management Shell.
2. Type `New-ManagementRole -Name "<new_role_mail>" -Parent "Mail Recipients"`. Press ENTER.
3. Type `New-ManagementRole -Name "<new_role_ca>" -Parent "Organization Client Access"`. Press ENTER.
4. Type `New-ManagementRole -Name "<new_role_exchange>" -Parent "Exchange Servers"`. Press ENTER.
5. Type `Get-ManagementRoleEntry "<new_role_mail>\*" | Where {$_.-Name ne "Get-ADServerSettings"} | Remove-ManagementRoleEntry`. Press ENTER.
6. Type `Get-ManagementRoleEntry "<new_role_ca>\*" | Where {$_.-Name ne "Get-CasMailbox"} | Remove-ManagementRoleEntry`. Press ENTER.
7. Type `Get-ManagementRoleEntry "<new_role_exchange>\*" | Where {$_.-Name ne "Get-ExchangeServer"} | Remove-ManagementRoleEntry`. Press ENTER.
8. Type `Add-ManagementRoleEntry "<new_role_mail>\Get-ActiveSyncDeviceStatistics" -Parameters Mailbox`. Press ENTER.

9. Type `Add-ManagementRoleEntry "<new_role_mail>\Get-ActiveSyncDevice" -Parameters Identity`. Press ENTER.

10. Perform this step only if you are using Microsoft Exchange 2013. Type `Add-ManagementRoleEntry "<new_role_mail>\Get-MobileDeviceStatistics" –Parameters Mailbox`. Press ENTER.

11. Perform this step only if you are using Microsoft Exchange 2013. Type `Add-ManagementRoleEntry "<new_role_mail>\Get-MobileDevice" –Parameters Mailbox`. Press ENTER.

12. Type `Add-ManagementRoleEntry "<new_role_ca>\Set-CasMailbox" -Parameters Identity, ActiveSyncBlockedDeviceIDs, ActiveSyncAllowedDeviceIDs`. Press ENTER.

13. Type `New-RoleGroup "<new_group>" -Roles "<new_role_mail>", "<new_role_ca>", "<new_role_exchange>". Press ENTER.

14. Type `Add-RoleGroupMember -Identity "<new_group>" -Member "BES12Admin"`. Press ENTER.

Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync

You must configure Microsoft Exchange Server 2010 or later to allow only authorized devices to access Exchange ActiveSync. Devices for existing users that are not explicitly added to the allowed list in Microsoft Exchange must be quarantined until BES12 allows them access.

To perform this task, you must be a Microsoft Exchange administrator with the appropriate permissions to configure the Set-ActiveSyncOrganizationSettings. For information about how to allow only authorized devices to access Exchange ActiveSync, visit https://technet.microsoft.com to read article Enable a Device for Exchange ActiveSync.

**Before you begin:** Verify with your Microsoft Exchange administrator whether or not there are any users currently using Exchange ActiveSync.

If your organization’s default access level for Exchange ActiveSync is set to allow and you have users setup and successfully synchronizing their devices, you must make sure that these users have a personal exemption or device rule associated to their user account or device before you set the default access level to quarantine. If they do not, then they are quarantined and their devices do not synchronize until they are allowed by BES12.

For more information about setting the default access level for Exchange ActiveSync to quarantine, visit http://support.blackberry.com/kb to read article KB36800.

1. On a computer that hosts the Microsoft Exchange Management Shell, open the Microsoft Exchange Management Shell.

2. Type `Set-ActiveSyncOrganizationSettings –DefaultAccessLevel Quarantine`. Press ENTER.
Configure Microsoft IIS permissions for gatekeeping

BES12 uses Windows PowerShell commands to manage the list of allowed devices in Microsoft Exchange. To use the BlackBerry Gatekeeping Service, you must configure Microsoft IIS permissions. Perform the following actions on the computer that hosts the Microsoft client access server role.

1. Open the Microsoft Internet Information Services (IIS) Manager.
2. In the left pane, expand the server.
3. Expand Sites > Default Web Site.
4. Right-click the PowerShell folder. Select Edit Permissions.
5. Click the Security tab. Click Edit.
6. Click Add and enter the <new_group> that was created when you configured the Microsoft Exchange permissions for gatekeeping.
7. Click OK.
8. Confirm that Read & execute, List folder contents, and Read are selected. Click OK.
10. Select Windows Authentication. Click Enable.
11. Close the Microsoft Internet Information Services (IIS) Manager.

Create a Microsoft Exchange gatekeeping configuration

You can create a Microsoft Exchange configuration so that devices that comply with your organization’s security policies can connect to the Microsoft Exchange Server.

Before you begin:
- Configure Microsoft Exchange permissions for gatekeeping.
- Configure Microsoft Exchange to allow only authorized devices to access Exchange ActiveSync.
- Configure Microsoft IIS permissions for gatekeeping.

1. On the menu bar, click Settings.
2. In the left pane, click External integration > Microsoft Exchange gatekeeping.
3. Click +
4. In the **Server name** field, type the name of the Microsoft Exchange Server that you want to manage access to.
5. Type the username and password for the Microsoft Exchange account that you created to manage Exchange ActiveSync gatekeeping.
6. In the **Authentication type** drop-down list, select the type of authentication that is used on the Microsoft Exchange Server.
7. Select **Use SSL** to enable SSL authentication between BES12 and the Microsoft Exchange Server. Optionally, select more certificate checks.
8. In the **Proxy type** drop-down list, select the type of proxy configuration, if any, that is used between BES12 and the Microsoft Exchange Server.
9. If you selected a proxy configuration in the previous step, select the authentication type that is used on the proxy server.
10. If necessary, select **Authentication required** and type the username and password.
11. Click **Test Connection** to verify that the connection is successful.
12. Click **Save**.

**Test a Microsoft Exchange gatekeeping configuration**

Test an Microsoft Exchange gatekeeping configuration to verify that BES12 can use this configuration to connect to the Microsoft Exchange Server.

**Before you begin:** Create or edit an Microsoft Exchange gatekeeping configuration.

1. On the menu bar, click **Settings**.
2. In the left pane, click **External integration > Microsoft Exchange gatekeeping configuration**.
3. Click the server name of the Microsoft Exchange Server configuration that you want to test.
4. Click **Test Connection**.

The results of the test are displayed in the console beside the test connection button.

**Configure Microsoft Office 365 for gatekeeping**

To use the BlackBerry Gatekeeping Service with Microsoft Office 365, you must configure the mobile device access policy in Microsoft Office 365 to quarantine devices by default.

1. Log in to the Microsoft Office 365 administration portal
2. In the side menu, click **Admin**.
3. Click **Exchange**.
4. In the Mobile section, click mobile device access.
5. Click Edit.
6. Click Quarantine - Let me decide to block or allow later.
Migrating users, devices, groups, and other data from a source BES10 or BES12 database

After you install a new instance of BES12, use the management console to migrate users, devices, groups, and other data from a source BES10 or BES12 database.

Steps to migrate users, devices, groups, and other data from a source BES10 or BES12 database

To migrate users, devices, groups, and other data from a source BES10 or BES12 database, perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connect to a source database.</td>
</tr>
<tr>
<td>2</td>
<td>Optionally, migrate IT policies, profiles, and groups.</td>
</tr>
<tr>
<td>3</td>
<td>Migrate users.</td>
</tr>
<tr>
<td>4</td>
<td>Migrate devices.</td>
</tr>
</tbody>
</table>

Prerequisites: Migrating users, devices, groups, and other data from a source BES10 or BES12 database

Complete the following prerequisites before beginning a migration.
### Connect to a source database

You must connect BES12 to the BES10 or BES12 database that you are migrating data from. You can add multiple source databases, but only one database at a time can be the active source database.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Migration > Configuration**.
3. Click **+**.
4. In the **Source type** drop-down list, select the type of source database, BES10 or BES12.
5. In the **Display name** field, type a descriptive name for the source database.
6. In the **Database server** field, type the name of the computer that hosts the source database, using the `<host>\<instance>` format for a dynamic port and the `<host>:<port>` format for a static port.
7. In the **Database authentication type** drop-down list, select the type of authentication you use to connect to the source database.
8. Do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| If you selected a BES10 source database | 1. If you selected SQL authentication, in the **Username** and **Password** fields, type your login information to connect to the source database.  
2. In the **BDS database name** field, type the name of the source database (for example, BDSMgmt). |
| If you selected a BES12 source database | 1. If you selected SQL authentication, in the **SQL username** and **SQL password** fields, type your login information to connect to the source database.  
2. In the **Database name** field, type the name of the source database.  
3. In the **Source BES12 authentication type** drop-down list, select the authentication type that is used to log in to the source BES12 management console.  
4. In the **Username** and **Password** fields, type your login information to log in to the source BES12 management console.  
5. If you selected Microsoft Active Directory authentication, in the **Domain** field type the name of the domain where the source BES12 management console is located. |

9. Click **Save**.

10. Optionally, to test the connection between the source database and the destination database, click **Test connection**.

11. Click **Save**.

## Best practices: Migrating IT policies, profiles, and groups from a source database

When you migrate BES10 IT policies, profiles, and groups to BES12, consider the following guidelines:

<table>
<thead>
<tr>
<th>Item</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Migrated groups retain the IT policies and profiles assigned to them.</td>
</tr>
</tbody>
</table>
| Users  | Migrated users do not retain the IT policies, profiles, and groups assigned to them.  
After migration, you must reassign users to each group in BES12. |
<table>
<thead>
<tr>
<th>Item</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT policy passwords</td>
<td>If any of the source IT policies you selected for iOS or Android devices has a minimum password length of less than 4 or more than 16, no BES10 IT policies or profiles can be migrated. Deselect or update the source IT policy and restart the migration.</td>
</tr>
<tr>
<td>Custom variables</td>
<td>During migration, BES12 maps the BES10 custom variables %custom1% through %custom5% to the BES12 custom password variables %custom_pswd1% through %custom_pswd5%. To prevent errors with passwords, if you used these variables in BES10, make sure you use them in the same way in BES12. For example, if %custom1% was used for ActiveSync email profile password in BES10, %custom_pswd1% in BES12 must be used for the same purpose. These variables are encrypted in the BES12 database.</td>
</tr>
<tr>
<td>Shared certificate profiles</td>
<td>After migration, shared certificate profiles that contain a SCEP certificate appear in the SCEP section.</td>
</tr>
<tr>
<td>Activation profiles</td>
<td>Activation profiles are not migrated. After migration, you must assign each user an activation profile with the same activation type that the user had in BES10.</td>
</tr>
<tr>
<td>CA certificates</td>
<td>In BES12, you must manually assign any migrated CA certificates to devices (CA certificates were automatically assigned in BES10). Before you can assign a migrated CA certificate to users or a group that contains users who have iOS, Android, or Windows devices, you must first open the CA certificate profile in BES12, click Edit, then click Save.</td>
</tr>
<tr>
<td>IT policy rules</td>
<td>The following IT policy rules cannot be migrated from BES10 to BES12:</td>
</tr>
<tr>
<td></td>
<td>• Backup and Restore Device</td>
</tr>
<tr>
<td></td>
<td>• Backup and Restore Work Space</td>
</tr>
<tr>
<td></td>
<td>• Cloud Storage Access from Work Space</td>
</tr>
<tr>
<td></td>
<td>• Hotspot WPA2-Personal Security Type</td>
</tr>
<tr>
<td></td>
<td>• Two-Factor Encryption Key Generation</td>
</tr>
<tr>
<td></td>
<td>• WebGL</td>
</tr>
</tbody>
</table>

When you migrate BES12 IT policies, profiles, and groups to another BES12 domain, consider the following guidelines:

<table>
<thead>
<tr>
<th>Item</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT policy passwords</td>
<td>If any of the source IT policies you selected for Android devices has a minimum password length of less than 4 or more than 16, no BES12 IT policies or profiles can be migrated. Deselect or update the source IT policy and restart the migration.</td>
</tr>
<tr>
<td></td>
<td>For BES12 version 12.1 IT policies, if the Password requirements field in the KNOX MDM section in the Android tab is set to &quot;Unspecified&quot; or &quot;Something,&quot; after migration to BES12 version 12.2 the value is changed to &quot;Numeric.&quot; The values of &quot;Unspecified&quot; and &quot;Something&quot; are not available in BES12 version 12.2.</td>
</tr>
</tbody>
</table>
### Migrate IT policies, profiles, and groups from a source database

Optionally, you can migrate the IT policies, profiles, and groups from a source database.

A migration copies selected IT policies, Email profiles, Wi-Fi profiles, VPN profiles, Proxy profiles, CA certificate profiles, Shared certificate profiles, SCEP profiles, User credential profiles, and Certification authority settings to the destination database. Any policies and profiles that are associated with the policies and profiles you select are also migrated.

**Note:** For migrations from BES10, all groups are migrated. For groups from BES12, user, role, and software configuration assignments, and BlackBerry OS attributes are not migrated.

1. On the menu bar, click **Settings**.
2. If you have more than one source database configured, in the left pane, click **Migration > Configuration** and then select the radio button beside the name of the database that you want to migrate data from.
3. In the left pane, click **Migration > IT policies, profiles, groups**.
4. Click **Next**.
5. Select the check boxes for the items you want to migrate.
   - The name of the source database is appended to each policy and profile name when it is migrated to the destination database.
6. Click **Preview** to review the policies and profiles you selected.
7. Click **Migrate**.
   - The **Migration status** screen displays the progress of the migration.
8. To configure the IT policies, profiles, and groups, click **Configure IT policies and profiles** to go to the **Policies and Profiles** screen.
## Best practices: Migrating users from a source database

Keep the following things in mind when migrating users to a destination BES12 database:

<table>
<thead>
<tr>
<th>Item</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number to migrate</td>
<td>You can migrate a maximum of 2000 users at a time from a source database. If the destination database is a BES12 database that has been upgraded from a BES5 database, you can migrate a maximum of 300 users at a time.</td>
</tr>
<tr>
<td></td>
<td>If you select more than the maximum number of users, only the maximum number are migrated to the destination BES12 database. The remaining users are skipped. Repeat the migration process as many times as necessary to migrate all the users from the source database.</td>
</tr>
<tr>
<td>Email address</td>
<td>• Users must have an email address before they can be migrated.</td>
</tr>
<tr>
<td></td>
<td>• You cannot migrate a user who already uses the same email address in the destination BES12 database.</td>
</tr>
<tr>
<td></td>
<td>• If two users in the source database have the same email address, only one user is displayed on the Migrate users screen.</td>
</tr>
<tr>
<td></td>
<td>• If two users in the source database have the same email address, the user information displayed on the Migrate devices screen could be the information for either of the users.</td>
</tr>
<tr>
<td></td>
<td>• If two users in a BES10 integrated company directory have the same email address, the first user discovered is the user that is migrated. This user may not be the same user that was originally created in the source database.</td>
</tr>
<tr>
<td>Device</td>
<td>• If a user in the source database has both a BlackBerry 10 device and an iOS or Android device, and the devices use the same email address with different usernames, some of the devices are not migrated.</td>
</tr>
<tr>
<td></td>
<td>• After migration, if a user had both a BlackBerry 10 device and an iOS, Android, or Windows device, the user must use the same login information for BES12 Self-Service that they used for BES10 Self-Service or BES12 Self-Service before migration.</td>
</tr>
<tr>
<td>Password</td>
<td>After migration, local users must change their password after the first time they log in to BES12 Self-Service. Users who did not have permission to access BES12 Self-Service before migration are not automatically granted permission after migration.</td>
</tr>
</tbody>
</table>
Migrate users from the source database

You can migrate users from the source database to the destination BES12 database. The users remain in both databases after the migration is complete.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Migration > Users**.
3. On the **Migrate users** screen, click **Next**.
4. On the **Migrate users** screen, select the users to migrate.
5. Click **Next**.
6. Assign one or more groups, or assign an IT policy and one or more profiles to the selected users.
   For more information, read the Administration content.
7. Click **Preview**.
8. Click **Migrate**.

Migrate devices from the source database

After you migrate users from the source database to the destination BES12 database, you can migrate their devices. The devices move from the source database to the destination BES12 database and are no longer in the source database after the migration.

Before you migrate devices verify that:

- The users exist in the destination BES12 domain
- The devices have the latest version of the BES12 Client installed
- BES12 supports the device type and OS
- All iOS devices are trusted (untrusted iOS devices cannot be migrated)

**Note:**

- You cannot migrate more than five devices per user at the same time.
- Devices activated with "MDM controls" temporarily lose access to email when the migration begins. Email services are restored when the migration is complete.

**Before you begin:** Notify iOS device users that they must open the BES12 Client to start the migration to BES12 and that they must keep the BES12 Client open until the migration is complete.

1. On the menu bar, click **Settings**.
2. In the left pane, click Migration > Devices.
3. On the Migrate devices screen, click Next.
4. Select the devices to migrate.
5. Click Preview.
6. Click Migrate.
7. To view the status of the devices being migrated, in the left pane, click Migration > Status.

Migrating DEP devices

You can migrate iOS devices that are enrolled in Apple’s Device Enrollment Program (DEP) from a source BES12 database to another BES12 database. To migrate DEP devices, both BES12 instances must be at version 12.2 or later.

Migrate DEP devices that have the BES12 Client installed

You can migrate iOS devices that are enrolled in Apple’s Device Enrollment Program (DEP) and are activated with the “Work and personal - full control” or “MDM controls” activation types.

Before you begin: In the settings for the BES12 Client, clear the Remove the app from the device when the device is removed from BES12 check box.

1. In the DEP portal, create a new virtual MDM server.
2. Connect the destination BES12 instance to the new virtual MDM server. For more information, see the Configuration content.
   Make sure that the DEP profile of the destination BES12 instance matches the DEP profile of the source BES12 instance.
3. Move the DEP devices from the source virtual MDM server to the new virtual MDM server.
4. In the BES12 management console, migrate the DEP devices from the source BES12 instance to the destination BES12 instance.

Migrate DEP devices that do not have the BES12 Client installed

iOS devices that are enrolled in Apple’s Device Enrollment Program (DEP) and do not have the BES12 Client installed appear in the list of devices that are unsupported for migration.

1. In the DEP portal, create a new virtual MDM server.
2. Connect the destination BES12 instance to the new virtual MDM server. For more information, see the Configuration content.
   Make sure that the destination BES12 instance has the same DEP profile as the source BES12 instance.

3. Move the DEP devices from the source virtual MDM server to the new virtual MDM server.

4. Perform a factory reset of each DEP device.

5. Reactivate each DEP device.
Configuring how data is pushed to BlackBerry 10 devices

The BlackBerry MDS Connection Service connects apps on BlackBerry 10 devices with server-side push applications. Push applications are hosted on an organization's web or application servers, and are capable of pushing data to apps on devices. For more information about push applications, see the developer documentation at developer.blackberry.com.

You can configure push initiators and push rules that define which server-side push applications can send application data and updates to devices.

All BlackBerry MDS Connection Service instances for BlackBerry 10 devices use DNS round robin to load balance the traffic being pushed to devices.

The BlackBerry MDS Connection Service enforces an 8K limitation on the size of push data. Push requests larger than 8K receive an error in the HTTP response. For data larger than 8K, apps can use the push and pull method, which pushes a notification to the device that there are updates so that the device pulls down the new updates.

For more information on push and pull and the 8K limitation, visit the BlackBerry developer blog at devblog.blackberry.com and search for Enterprise Push and Pull.

Steps to configure the BlackBerry MDS Connection Service

When you configure the BlackBerry MDS Connection Service, you perform the following actions:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configure component information settings.</td>
</tr>
<tr>
<td>2</td>
<td>Configure push information.</td>
</tr>
<tr>
<td>3</td>
<td>Configure the BlackBerry MDS Connection Service keystore.</td>
</tr>
<tr>
<td>4</td>
<td>Configure and rank proxy mappings.</td>
</tr>
</tbody>
</table>
Configuring the BlackBerry MDS Connection Service

The settings that you specify apply to all instances of the BlackBerry MDS Connection Service that are installed in the BES12 domain. There are no specific settings that apply to one instance.

Component information settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server listen port</td>
<td>Use this option to specify the port number that the BlackBerry MDS Connection Service server listens on for HTTP requests from server-side push applications. You should change the default port only if there is a conflict with another service on the same computer.</td>
</tr>
<tr>
<td>Web server SSL listen port</td>
<td>Use this option to specify the port number that the BlackBerry MDS Connection Service web server listens on for SSL requests from server-side push applications. You should change the default port only if there is a conflict with another service on the same computer.</td>
</tr>
<tr>
<td>Thread pool size</td>
<td>Use this option to specify the maximum number of threads that a BlackBerry MDS Connection Service instance uses to process requests from BlackBerry 10 devices.</td>
</tr>
<tr>
<td>Maximum simultaneous scalable sockets</td>
<td>Use this option to specify the maximum number of scalable socket connections that can be opened at the same time between BlackBerry 10 devices and target servers. The more socket connections you allow, the more system resources will be used.</td>
</tr>
<tr>
<td>Database admin configuration cycle timer (minutes)</td>
<td>Use this option to specify how often a BlackBerry MDS Connection Service polls the BES12 database for changes to the configuration settings.</td>
</tr>
<tr>
<td>Maximum number of push messages stored</td>
<td>Use this option to specify set the maximum number of push messages that can be stored in the BES12 database when Store push submissions setting is set to True.</td>
</tr>
<tr>
<td>Maximum push message age (minutes)</td>
<td>Use this option to specify set the maximum length of time, in minutes, that you want the BlackBerry MDS Connection Service to store a push request before the request is deleted from the BES12 database.</td>
</tr>
</tbody>
</table>

Configure the BlackBerry MDS Connection Service

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > MDS Connection Service**.

3. In the **Component information** section, change any of the following settings as required for your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server listen port</td>
<td>9080</td>
</tr>
<tr>
<td>Web server SSL listen port</td>
<td>9443</td>
</tr>
<tr>
<td>Thread pool size</td>
<td>400</td>
</tr>
<tr>
<td>Maximum simultaneous scalable sockets</td>
<td>20000</td>
</tr>
<tr>
<td>Database admin configuration cycle timer</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Maximum number of push messages stored</td>
<td>100000</td>
</tr>
<tr>
<td>Maximum push message age</td>
<td>720 minutes</td>
</tr>
</tbody>
</table>

4. Click **Save**.

**Configuring BlackBerry MDS Connection Service push information**

The BlackBerry MDS Connection Service receives push application requests from server-side push applications and sends the requests to applications on BlackBerry 10 devices. You can control how the BlackBerry MDS Connection Service processes, stores, and sends push application requests.

By default, a BlackBerry MDS Connection Service sends push requests from server-side push applications to applications on BlackBerry 10 devices. BlackBerry 10 devices can receive application data and application updates without users requesting the content.

You can configure your organization's environment so that only specific server-side push applications can send push requests to BlackBerry 10 devices. You can turn on push authentication to prevent a BlackBerry MDS Connection Service from sending push requests from unauthorized push initiators, and create push initiators that permit specific server-side applications to send push requests to BlackBerry 10 devices.

For more information about push applications, see the developer documentation at [https://developer.blackberry.com](https://developer.blackberry.com).
Push information settings

The BlackBerry MDS Connection Service supports secure enterprise push capability which allows push initiators to send push requests securely using HTTPS.

### Push information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push authentication</td>
<td>Use this option to specify whether content from server-side push applications can be sent to BlackBerry 10 devices with or without authentication. When push authentication is turned on, push applications cannot send content to BlackBerry 10 devices until you set up push initiators.</td>
</tr>
<tr>
<td>Push encryption</td>
<td>Use this option to turn on SSL for the BlackBerry MDS Connection Service to encrypt the push requests that server-side push applications send to the BlackBerry MDS Connection Service.</td>
</tr>
<tr>
<td>Store push submissions</td>
<td>Use this option to store push requests in the BES12 database.</td>
</tr>
<tr>
<td>Maximum number of active connections</td>
<td>Use this option to specify the maximum number of push connections that a BlackBerry MDS Connection Service can process at the same time.</td>
</tr>
<tr>
<td>Maximum number of queued connections</td>
<td>Use this option to specify the maximum number of push connections that a BlackBerry MDS Connection Service can queue.</td>
</tr>
</tbody>
</table>

### Push initiators

A push initiator is an application that creates request messages (such as a push request, cancel request, or status-query request) and response messages (such as a result-notification response) using the server-side library, and submits them to the BlackBerry MDS Connection Service.

When push authentication is enabled, push applications use the credentials set for the push initiator to authenticate with the BlackBerry MDS Connection Service.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Assign a name to the push initiator. This should be the username for the push initiator.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the push initiator</td>
</tr>
<tr>
<td>Credentials</td>
<td>Enter the password required for the push initiator.</td>
</tr>
</tbody>
</table>
These credentials must be added to every push request by an app in order to validate whether or not the app is allowed to push content to a managed device.

### Push initiator certificates

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push initiator certificates</td>
<td>A push initiator certificate is a server SSL certificate used by server-side push applications. This certificate allows the BlackBerry MDS Connection Service to communicate with server-side push applications over the SSL protocol, if required. The push initiator certificates are imported into the Java keystore created and maintained by the BlackBerry MDS Connection Service. If you selected Manual keystore management override, you are expected to import SSL certificates used by push applications into a manually created and maintained Java keystore file. Note: To add a push initiator certificate you need a .cert file</td>
</tr>
</tbody>
</table>

### Configure push information

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > MDS Connection Service**.
3. Under the **Push information** section, change the following settings as required for your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push authentication</td>
<td>False</td>
</tr>
<tr>
<td></td>
<td>• True: Enabled</td>
</tr>
<tr>
<td></td>
<td>• False: Disabled</td>
</tr>
<tr>
<td>Push encryption</td>
<td>False</td>
</tr>
<tr>
<td></td>
<td>• True: Enabled</td>
</tr>
<tr>
<td></td>
<td>• If push encryption is enabled you have the ability to <strong>Generate certificate</strong> and <strong>Regenerate certificate</strong> in order to create the SSL certificate for the Java keystore file</td>
</tr>
<tr>
<td></td>
<td>• False: Disabled</td>
</tr>
<tr>
<td>Store push submissions</td>
<td>False</td>
</tr>
</tbody>
</table>
### Option Default value

<table>
<thead>
<tr>
<th>Option</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>True: Enabled</td>
<td></td>
</tr>
<tr>
<td>False: Disabled</td>
<td></td>
</tr>
<tr>
<td>Maximum number of active connections</td>
<td>1000</td>
</tr>
<tr>
<td>Range: 1 to 65535. Increasing the default value will use more system resources.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of queued connections</td>
<td>100000</td>
</tr>
<tr>
<td>Range: 1 to 10000000. Increasing the default value will use more system resources.</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **Save**.

**After you finish:** Create push initiators for push applications.

**Create push initiators for push applications**

When push authentication is turned on, every server-side push application has to authenticate with the BlackBerry MDS Connection Service for a push request. You can specify authentication credentials by creating a push initiator account. You can configure several server-side push applications to use the same push initiator (that is, to use the same authentication password) if your organization's development environment permits it. Verify that the authorization HTTP header in push requests from server-side push applications matches the name and password that you specify for the push initiator.

**Before you begin:** Turn on push authentication for the BlackBerry MDS Connection Service.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > MDS Connection Service**.
3. Click **+** under **Push initiators**.
4. Enter the name, description, and the credentials for the push initiator.
5. Click **Add**.
6. Click **Save**.

**After you finish:** Create a push initiator for each server-side push application that you want to permit to send push requests to BlackBerry 10 devices.

**Add push initiator certificates**

Push initiator certificates are required only when the server-side push application notification listener is running on an SSL port.

**Note:** If you enable **Manual keystore management override** in the **MDS connection service keystore**, then you will be unable to add push initiator certificates.
**Before you begin:** Set **Push encryption** to True.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > MDS Connection Service**.
3. Click under **Push initiator certificates**.
4. Browse to the push certificate. The push certificate must be a .cert file.
5. Click **Add**.
6. Click **Save**.

### Configuring the BlackBerry MDS Connection Service keystore

Push applications can use a BlackBerry MDS Connection Service certificate to open HTTPS connections to the BlackBerry MDS Connection Service to push application data and application updates to BlackBerry 10 devices.

To permit push applications to make trusted connections to a BlackBerry MDS Connection Service, you must create the `webserver.keystore` file on the computer that hosts the BlackBerry MDS Connection Service. This keystore stores the certificate and permits HTTPS connections from push applications.

### Keystore settings

Two options are available for providing SSL certificates to the BlackBerry MDS Connection Service:

- Use the Generate certificate option when Push encryption is enabled
- Use Manual keystore management override to manually create an SSL certificate and a Java keystore file to maintain the SSL certificate

The BlackBerry MDS Connection Service expects a Java keystore file named "webserver.keystore" located at `<drive>\Program Files\BlackBerry\MDS\webserver\`. When the Generate certificate option is used, the BlackBerry MDS Connection Service generates a Java keystore file with the SSL certificate in the folder. When the Manual keystore management override is used, you must create a Java keystore file with SSL certificate for the BlackBerry MDS Connection Service.

The BlackBerry MDS Connection Service can use the self-signed certificate that is generated when you create the keystore or you can use the Java keytool to add a signed certificate from a trusted public CA. When you select Manual keystore management override, the SSL certificate within the Java keystore file must be identified by the alias name **mdscs_ssl** for the BlackBerry MDS Connection Service to successfully enable encrypted push. You must use the Java keytool to export the certificate from the keystore and import the certificate to the keystores that the Java push applications use.

For more information about using the Java keytool, visit [java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html](http://java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html). For more information about the requirements, visit [tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html](http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html).
**Setting** | **Description**
--- | ---
Manual keystore management override | If you select Manual keystore management override, you cannot use push initiator certificates. The BlackBerry MDS Connection Service uses the Java keystore file as a truststore. You are expected to import the server-side push application SSL certificates into the Java keystore so that the BlackBerry MDS Connection Service can successfully communicate with server-side push applications over an SSL port, if required.
Keystore password | Enter the password for the keystore. The default password is "changeit". If a manually created Java keystore file is used, it must use the default password or a configured password.
Keystore confirm password | Confirm the password for the keystore.

**Configure the keystore**

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > MDS Connection Service**.
3. Under **MDS connection service keystore** section, change the following settings as required for your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manual keystore management override | Default: Disabled  
  - Enabled: Cannot add push initiator certificates  
  - Disabled: Can add push initiator certificates |
| Keystore password | Enter the keystore password, if required. |
| Keystore confirm password | Confirm the keystore password. |

4. Click **Save**.

*After you finish: Add push initiator certificates*, if required.
Configure BlackBerry MDS Connection Service proxy mappings

1. On the menu bar, click Settings.
2. In the left pane, click Infrastructure > MDS Connection Service.
3. Under Proxy mappings click +.
4. Configure Add proxy mapping, change the following settings as required for your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal resource indicator</td>
<td>Specify the Java regular expression for the web addresses that the proxy mapping rule controls. The wildcard * forces the server to redirect all traffic to the specified proxy. You can also use wildcards for each domain, such as <em>.example.com/</em>, to redirect all traffic for any server and any directory of the example.com domain to the specified proxy.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of your universal resource indicator. For example: This proxy mapping redirects all traffic for the example.com domain to the primary proxy server.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Specify the username and password that the BlackBerry MDS Connection Service can use to connect to the proxy server that is defined for the web address.</td>
</tr>
<tr>
<td>Proxy type</td>
<td>Select the type of proxy server:</td>
</tr>
<tr>
<td></td>
<td>• Auto (default)</td>
</tr>
<tr>
<td></td>
<td>• Direct</td>
</tr>
<tr>
<td></td>
<td>• PAC: Requires a PAC file address</td>
</tr>
<tr>
<td></td>
<td>• Proxy: Requires a proxy server host name or IP address</td>
</tr>
<tr>
<td>+</td>
<td>Add additional proxy types, if required.</td>
</tr>
</tbody>
</table>

5. Click Add.
6. Click Save.

After you finish: If there are multiple proxy mappings, Rank proxy mappings.
Rank proxy mappings

When there are multiple proxy mappings, you rank them to determine the order in which BES12 uses them.

1. On the menu bar, click Settings.
2. In the left pane, in the Infrastructure section, click MDS Connection Service.
3. Use the arrows to rank the proxy mappings.
4. Click Save.
Monitoring BES12

You can use third-party SNMP tools to monitor the activity of the BES12 Core, BlackBerry Secure Connect Plus, and BES12 enterprise connectivity components.

SNMP monitoring requires an SNMP service and an SNMP management tool. You run the SNMP service on the computers that host BES12. The SNMP service, located in the Windows Services, includes an SNMP agent that collects data from the BES12 components.

You use an SNMP management tool (for example, a MIB browser) to view and analyze the data that is received from the agent. The management tool typically includes an SNMP trap management tool that is used to retrieve and interpret trap messages from the agent. The management tool can be installed on the computer that hosts BES12 or on a separate computer.

There are two places where you configure SNMP:

- To monitor the BES12 Core and BlackBerry Secure Connect Plus, you configure SNMP in the management console.
- To monitor BES12 enterprise connectivity components, you configure the SNMP service.

By default, the management tool displays the OID of a condition, which is a sequence of integers that identify a class value in a class hierarchy. All SNMP OIDs and SNMP traps for BES12 begin with a class value of 1.3.6.1.4.1.3530.8. A suffix (for example, 25.1.1), uniquely identifies each OID value.

MIBs specify the conditions that the SNMP agent monitors. A MIB is a database that defines and describes the variables and management data of BES12 components, including what each SNMP trap value represents. The MIB determines the types of data the SNMP service can collect about the components. When you configure SNMP monitoring, you use the management tool to compile the MIB.

To learn about network security for SNMP, visit support.microsoft.com to read articles KB324261 and KB324263.

Supported SNMP operations

You can use SNMP operations to collect data from the SNMP agent that runs on the computers where BES12 is installed. BES12 supports the following SNMP operations:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get</td>
<td>Retrieves the value for a specific MIB item.</td>
</tr>
<tr>
<td>Get next</td>
<td>Retrieves the value and OID of items in the order that they appear in the MIB file.</td>
</tr>
<tr>
<td>Trap</td>
<td>Sends SNMP trap messages from the SNMP agent to the SNMP trap management tool. SNMP trap messages contain data about specific actions that a BES12 component performs.</td>
</tr>
</tbody>
</table>
## System requirements: SNMP monitoring

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported BES12 components</td>
<td>You can configure SNMP monitoring for the following BES12 components:</td>
</tr>
<tr>
<td></td>
<td>• BES12 Core</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Secure Connect Plus</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Affinity Manager</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Dispatcher</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry MDS Connection Service</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Router</td>
</tr>
<tr>
<td></td>
<td>Other BES12 components do not support SNMP monitoring.</td>
</tr>
<tr>
<td>SNMP management tool</td>
<td>If the management tool does not include a MIB compiler, install a MIB compiler on the computer that hosts the management tool.</td>
</tr>
<tr>
<td></td>
<td>If you want the SNMP service to send trap messages to report on server activity, verify that the management tool includes an SNMP trap management tool. Alternatively, you can install a standalone SNMP trap management tool on a computer that hosts BES12, or on a separate computer.</td>
</tr>
<tr>
<td>Network access</td>
<td>The computer that hosts the SNMP management tool, or a standalone SNMP trap management tool, must be able to access and receive data from the computers where BES12 is installed.</td>
</tr>
<tr>
<td>SNMP service</td>
<td>On the computers where BES12 is installed, install an SNMP service that includes an SNMP agent and SNMP trap service. An SNMP service is available in most versions of Windows. For more information, visit support.microsoft.com.</td>
</tr>
<tr>
<td>SNMP service settings</td>
<td>On the computers where BES12 is installed, in the Windows Services, configure the following SNMP service settings:</td>
</tr>
<tr>
<td></td>
<td>• A valid SNMP community name</td>
</tr>
<tr>
<td></td>
<td>• A minimum of read-only permission for the SNMP community</td>
</tr>
<tr>
<td></td>
<td>• The IP addresses of names of the computers that the SNMP service can accept SNMP data from.</td>
</tr>
</tbody>
</table>
MIBs for BES12

By default, the MIBs for BES12 are on the computer where BES12 is installed, in `<drive>\Program Files\BlackBerry\BES\Monitoring\bin\mib`.

BES12 includes six possible MIBs that you can use to analyze data from BES12 components.

<table>
<thead>
<tr>
<th>MIB file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BES-CoreMIB-SMIV2</td>
<td>Contains a definition of the OID tree root for the SNMP interface of the BES12 Core</td>
</tr>
<tr>
<td>BES-CoreMonitoringMIB-SMIV2</td>
<td>Contains definitions of the managed objects that are accessible and retrievable using the SNMP management tool</td>
</tr>
<tr>
<td>BES-CoreEventingMIB-SMIV2</td>
<td>Contains definitions of the traps and notifications that the BES12 Core issues</td>
</tr>
<tr>
<td>BES-EC-MIB-SMIV2</td>
<td>Contains definitions of the managed objects, traps, and notifications that the following enterprise connectivity components of BES12 issues:</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Affinity Manager</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Dispatcher</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry MDS Connection Service</td>
</tr>
<tr>
<td></td>
<td>• BlackBerry Router</td>
</tr>
<tr>
<td>BES-BSCPMIB-SMIV2</td>
<td>Contains a definition of the OID tree root for the SNMP interface of BlackBerry Secure Connect Plus</td>
</tr>
<tr>
<td>BES-BSCPMonitoringMIB-SMIV2</td>
<td>Contains definitions of the managed BlackBerry Secure Connect Plus objects that are accessible and retrievable using the SNMP management tool</td>
</tr>
</tbody>
</table>

Compile the MIB and configure the SNMP management tool

To enable your organization’s SNMP monitoring software to monitor BES12 components, you must use the SNMP management tool to compile the MIB files of BES12. If the tool does not include an MIB compiler, install a MIB compiler on the computer that hosts the tool.

**Before you begin:** Read the documentation for the SNMP management tool to learn how to use the tool to compile a MIB.

1. On the computer that hosts BES12, browse to `<drive>\Program Files\BlackBerry\BES\Monitoring\bin\mib`. 


2. Use the SNMP management tool (or the MIB compiler that you installed separately) to compile the .mib files.

Using SNMP to monitor the BES12 Core and BlackBerry Secure Connect Plus

The BES12 Core consists of several subcomponents responsible for managing devices. BlackBerry Secure Connect Plus provides a secure IP tunnel between work space apps on BlackBerry 10, KNOX Workspace, and Android for Work devices and your organization’s network.

To monitor the BES12 Core and BlackBerry Secure Connect Plus using SNMP, you must configure the settings in the BES12 management console.

Configure SNMP to monitor the BES12 Core and BlackBerry Secure Connect Plus

To use SNMP to monitor the BES12 Core and BlackBerry Secure Connect Plus, you must configure the settings in the management console.

1. On the menu bar, click **Settings**.
2. In the left pane, click **Infrastructure > SNMP**.
3. Expand **Global settings** and select the **Enable SNMP monitoring** check box. By default, the checkbox is not selected.
4. In the **Community** field, replace the default by typing a new community name.
5. In the IP address field, type the IPv4 UDP address for the server where the trap management tool is installed.
6. In the **Port** field, type the port number for the trap management tool. By default, the port number is 1620.
7. Click **Save**.
8. Expand each BES12 instance name, and complete the following tasks:
   - To monitor the BES12 Core: In the **UDP port to access SNMP monitoring data for the BES12 Core service** field, type the port number that you want BES12 to use to listen for SNMP data requests. By default, the port number is 1610.
   - To monitor BlackBerry Secure Connect Plus: In the **UDP port to access SNMP monitoring data for the BlackBerry Secure Connect Plus service** field, type the port that you want BES12 to use to listen for SNMP data requests. By default, the port is 1611.
9. Click **Save**.

*After you finish:* Complete one of the following tasks:
• If you enable monitoring for the BES12 Core, in the Windows Services, restart the **BES12 - BES12 Core** service.
• If you enable monitoring for BlackBerry Secure Connect Plus, in the Windows Services, restart **BES12 - BlackBerry Secure Connect Plus** service.
<table>
<thead>
<tr>
<th>Glossary</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSI</td>
<td>Active Directory Service Interfaces</td>
</tr>
<tr>
<td>APNs</td>
<td>Apple Push Notification service</td>
</tr>
<tr>
<td>BES5</td>
<td>BlackBerry Enterprise Server 5</td>
</tr>
<tr>
<td>BES10</td>
<td>BlackBerry Enterprise Service 10</td>
</tr>
<tr>
<td>BES12</td>
<td>BlackBerry Enterprise Service 12</td>
</tr>
<tr>
<td>BES12 instance</td>
<td>BES12 instance refers to all BES12 components installed on one computer except the BlackBerry Router, which is an optional component that is installed separately. A BES12 instance is sometimes referred to as a &quot;unit of scale.&quot;</td>
</tr>
<tr>
<td>CAS</td>
<td>Client Access Server</td>
</tr>
<tr>
<td>CSR</td>
<td>certificate signing request</td>
</tr>
<tr>
<td>DEP</td>
<td>Device Enrollment Program</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>FQDN</td>
<td>fully qualified domain name</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol over Secure Sockets Layer</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft Management Console</td>
</tr>
<tr>
<td>OID</td>
<td>object identifier</td>
</tr>
<tr>
<td>PAC</td>
<td>proxy auto-configuration</td>
</tr>
<tr>
<td>PAP</td>
<td>Push Access Protocol</td>
</tr>
<tr>
<td>SCEP</td>
<td>simple certificate enrollment protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used with POP or IMAP to send and receive email messages over a network, such as the Internet.</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SPN</td>
<td>A Service Principal Name (SPN) is an attribute of a user or group in Microsoft Active Directory that supports mutual authentication between a client of a Kerberos enabled service and the Kerberos enabled service. A Microsoft Active Directory account can have one or more SPNs.</td>
</tr>
<tr>
<td>SRP</td>
<td>Server Routing Protocol</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol (TCP/IP) is a set of communication protocols that is used to transmit data over networks, such as the Internet.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
© 2015 BlackBerry. Trademarks, including but not limited to BLACKBERRY, EMBLEM Design, BBM, BES, MANYME, VIRTUAL SIM PLATFORM, WORKLIFE, MOVIRUT, SECUSMART, SECUSMART & Design, SECUSUITE, WATCHDOX, WATCHDOX & Design and WATCHDOX & EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, the exclusive rights to which are expressly reserved.

Microsoft, Active Directory, ActiveSync, Internet Explorer, Microsoft Exchange, Microsoft Exchange Server, Microsoft Exchange Management Console, Microsoft Internet Information Services, SQL Server, Windows, Windows Phone, Windows PowerShell, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. 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. Apple is a trademark of Apple Inc. Android and Google Chrome are trademarks of Google Inc. Mozilla and Firefox are trademarks of Mozilla Foundation. KNOX and Samsung KNOX are trademarks of Samsung Electronics Co., Ltd. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available on the BlackBerry website provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by BlackBerry Limited and its affiliated companies ("BlackBerry") and BlackBerry assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect BlackBerry proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of BlackBerry technology in generalized terms. BlackBerry reserves the right to periodically change information that is contained in this documentation; however, BlackBerry makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). BlackBerry does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthy, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by BlackBerry of the Third Party Products and Services or the third party in any way.

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

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL BLACKBERRY BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA, FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH BLACKBERRY PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF BLACKBERRY PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF BLACKBERRY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, BLACKBERRY SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO BLACKBERRY AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED BLACKBERRY DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF BLACKBERRY OR ANY AFFILIATES OF BLACKBERRY HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with BlackBerry’s products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with BlackBerry's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by BlackBerry and BlackBerry assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with BlackBerry.

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

BlackBerry Enterprise Software incorporates certain third-party software. The license and copyright information associated with this software is available at http://worldwide.blackberry.com/legal/thirdpartysoftware.jsp.

BlackBerry Limited
2200 University Avenue East
Waterloo, Ontario
Canada N2K 0A7

BlackBerry UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada