# Maintenance Release Notes

BES12
Version 12.3
Maintenance Release 1

Published: 2015-12-16
SWD-20151216152621036

# Contents

# What's new in BES12 version 12.3 MR1

1

| Item | Description |
| --- | --- |
| VPN profiles for NIAP | VPN profiles for BlackBerry 10 devices have new settings for connecting to NIAP-compliant VPN gateways. |

## About PRIV and BES12

PRIV is a secure device that runs the Android OS. To manage PRIV with BES12, follow the instructions for Android devices in the BES12 in the Configuration content and in the Administration content.

The following activation types are available for PRIV:

- Work and personal - user privacy (Android for Work)
- Work and personal - user privacy (Android for Work - Premium)
- Work space only (Android for Work)
- Work space only (Android for Work - Premium)
- MDM controls

  **Note:** For this activation type, PRIV must use the TouchDown app to have the email account configured automatically.
- Work and personal - full control (Secure Work Space)
- Work and personal - full control (Secure Work Space)

We recommend that you activate PRIV using an Android for Work activation type to achieve the optimum experience.

### Steps to deploy PRIV in your BES12 environment

Deploy PRIV in your BES12 environment as follows:

| Step | Action |
| --- | --- |
| 1 | If you plan to use an Android for Work activation type:<br>• Configure BES12 to support Android for Work. For more information, see the Configuration content.<br>• Set up BES12 to support Android for Work activations. See "Supporting Android for Work activations" in the Administration content. |

| Step | Action |
|---|---|
| 2 | Create an activation profile. For more information, see "Create an activation profile" in the Administration content. BES12 has some profile settings that are specifically for PRIV. Along with the regular Android email profile settings, the BlackBerry Productivity Suite settings and the S/MIME settings apply only to PRIV. |
| 3 | Assign the PRIV productivity apps. See Select the productivity apps used on PRIV devices that use Android for Work. |
| 4 | User activates the device. See "Activate an Android device" in the Administration content.<br>**Note:** The user must make sure to check the notification drawer for the notification about account synchronization and enter the email password. Otherwise, email is not sent to PRIV.<br>For more information about activating PRIV, see the data flow information in the Architecture content.. |

# Using activation types to configure your control over devices

You can use activation types to configure how much control you have over activated devices. This flexibility of control is useful if you want to have full control over a device that you issue to a user or if you want to make sure that you have no control over the personal data on a device that the user owns and brings to work. The following tables list the activation types available for devices.

Activation types do not apply to BlackBerry OS (version 5.0 to 7.1) devices. You can use BlackBerry OS IT policies in the Personal Devices IT policy group to distinguish between work content and personal content on the device. For more information, download the Policy Reference Spreadsheet at help.blackberry.com/detectLang/bes12/current/policy-reference-spreadsheet-zip/.

## BlackBerry 10 devices

| Activation type | Description |
|---|---|
| Work and personal - Corporate | This activation type provides control of work data on devices, while making sure that there is privacy for personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted.<br>You can control the work space on the device using IT administration commands and IT policies, but you cannot control any aspects of the personal space on the device. |
| Work space only | This activation type provides full control of the device and does not provide a separate space for personal data. When a device is activated, the personal space and all work data from any previous activation is removed, a work space is |

| Activation type | Description |
| --- | --- |
| | installed, and the user must create a password to access the device. Work data is protected using encryption and password authentication.<br>You can control the device using IT administration commands and IT policies. |
| Work and personal - Regulated | This activation type provides control of both work and personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication. All work data from any previous activations is deleted.<br>You can control both the work space and the personal space on the device using IT administration commands and IT policies. |

## iOS devices

| Activation type | Description |
| --- | --- |
| MDM controls | This activation type provides basic device management using device controls made available by iOS. A separate work space is not installed on the device, and there is no added security for work data.<br>You can control the device using IT administration commands and IT policies. During activation, users must install a mobile device management profile on the device. |
| Work and personal - full control | This activation type provides full control of devices. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication.<br>You can control the work space, and some other aspects of the device that affect both the personal and work space using IT administration commands and IT policies. During activation, users must install a mobile device management profile. |
| Work and personal - user privacy | This activation type provides control of work data on devices, while making sure that there is privacy for personal data. When a device is activated, a separate work space is created on the device and the user must create a password to access the work space. Work data is protected using encryption and password authentication.<br>You can control the work space on the device using IT administration commands and IT policies, but you cannot control any aspects of the personal space on the device. Users are not required to install a mobile device management profile. |

| Activation type | Description |
| --- | --- |
| | **Note:** If you select this activation type on the **iOS** tab and you select the **Allow query of network information for SIM licenses** option, BES12 can access only the SIM card and device hardware information that is required to check if an appropriate SIM license is available (for example, ICCID and IMEI). In this case, users are required to install a mobile device management profile. |

## Windows 10, Windows 10 Mobile, and Windows Phone devices

| Activation type | Description |
| --- | --- |
| MDM controls | This activation type provides basic device management using device controls made available by Windows 10, Windows 10 Mobile, and Windows Phone. A separate work space is not installed on the device, and there is no added security for work data.<br><br>You can control the device using IT administration commands and IT policies. Windows Phone users must install BES12 Client to activate a device. Windows 10 and Windows 10 Mobile users activate devices through the Windows 10 Work access app. |

## Android devices

When you configure the activation type for Android devices, you can select multiple activation types and rank them to make sure that BES12 assigns the most appropriate activation type for that device. For example, if you rank "Work space only (Samsung KNOX)" first and "MDM controls" second, devices that support Samsung KNOX Workspace receive the first activation type.

**Note:** KNOX MDM allows the device to use the KNOX MDM IT policy rules in BES12 instead of the basic rules available for all Android devices. KNOX Workspace creates a separate work space on the device that keeps work data and apps separate from personal data and apps.

| Activation type | Description |
| --- | --- |
| MDM controls | This activation type applies to:<br><br>• Android devices, including PRIV, and Samsung devices that support KNOX MDM<br><br>This activation type lets you manage the device using IT administration commands and IT policy rules. If the device supports KNOX MDM, this activation type applies the KNOX MDM IT policy rules. A separate work space is not installed on the device, and there is no added security for work data. |

| Activation type | Description |
| --- | --- |
| | During activation, users must grant Administrator permissions to the BES12 Client. |
| Work and personal - full control (Secure Work Space) | This activation type applies to:<br>• Android devices, including PRIV, and Samsung devices that support KNOX MDM<br>This activation type lets you manage the entire device using IT administration commands and IT policy rules. If the device supports KNOX MDM, it will apply the KNOX MDM IT policy rules. This activation type creates a separate work space on the device, and the user must create a password to access the work space. Data in the work space is protected using encryption and password authentication.<br>During activation, users must grant Administrator permissions to the BES12 Client. |
| Work and personal - user privacy (Secure Work Space) | This activation type applies to:<br>• Android devices, including PRIV<br>This activation type maintains privacy for personal data, but it lets you manage work data using IT administration commands and IT policy rules. This activation type does not support the KNOX MDM IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and password authentication.<br>Users do not have to grant Administrator permissions to the BES12 Client. |
| Work and personal - full control (Samsung KNOX) | This activation type applies to:<br>• Samsung devices that support KNOX Workspace<br>This activation type lets you manage the entire device using IT administration commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint.<br>During activation users must grant Administrator permissions to the BES12 Client. |
| Work and personal - user privacy - (Samsung KNOX) | This activation type applies to: |

| Activation type | Description |
| --- | --- |
| | • Samsung devices that support KNOX Workspace<br><br>This activation type maintains privacy for personal data, but it lets you manage work data using IT administration commands and IT policy rules. This activation type does not support the KNOX MDM IT policy rules. This activation type creates a separate work space on the device and the user must create a password to access the work space. Data in the work space is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint. The user must also create a Screen lock password to protect the entire device and will not be able to use USB debugging mode.<br><br>During activation, users must grant Administrator permissions to the BES12 Client. |
| Work space only - (Samsung KNOX) | This activation type applies to:<br><br>• Samsung devices that support KNOX Workspace<br><br>This activation type lets you manage the entire device using IT administration commands and the KNOX MDM and KNOX Workspace IT policy rules. This activation type removes the personal space and installs a work space. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password, PIN, pattern, or fingerprint.<br><br>During activation, users must grant Administrator permissions to the BES12 Client. |
| Work and personal - user privacy (Android for Work) | This activation type applies to:<br><br>• Android devices that support Android for Work, including PRIV<br><br>This activation type maintains privacy for personal data but lets you manage work data using IT administration commands and IT policy rules. This activation type does not support the KNOX MDM IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication.<br><br>This activation type does not support BlackBerry Secure Connect Plus.<br><br>Users do not have to grant Administrator permissions to the BES12 Client. |
| Work and personal - user privacy (Android for Work - Premium) | This activation type applies to:<br><br>• Android devices that support Android for Work, including PRIV |

| Activation type | Description |
| --- | --- |
| | This activation type maintains privacy for personal data but lets you manage work data using IT administration commands and IT policy rules. This activation type does not support the KNOX MDM IT policy rules. This activation type creates a work profile on the device that separates work and personal data. Work and personal data are both protected using encryption and password authentication.<br><br>Users do not have to grant Administrator permissions to the BES12 Client.<br><br>You must use this activation type if you want to support BlackBerry Secure Connect Plus with the features of the Work and personal - user privacy (Android for Work) activation type. |
| Work space only (Android for Work) | This activation type applies to:<br><br>• Android devices that support Android for Work, including PRIV<br><br>If you assign this activation type to a user, you must also assign the Work space only (Android for Work) activation email template to that user. Assigning that template makes sure that the user receives the Google activation code required during the activation process.<br><br>This activation type lets you manage the entire device using IT administration commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating installs a work profile and no personal profile. The user must create a password to access the device. All data on the device is protected using encryption and a method of authentication such as a password.<br><br>During activation the device installs the BES12 Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app. |
| Work space only (Android for Work - Premium) | This activation type applies to:<br><br>• Android devices that support Android for Work, including PRIV<br><br>If you assign this activation type to a user, you must also assign the Work space only (Android for Work) activation email template to that user. Assigning that template makes sure that the user receives the Google activation code required during the activation process.<br><br>This activation type lets you manage the entire device using IT administration commands and IT policy rules. This activation type requires the user to reset the device to factory settings before activating installs a work profile and no personal profile. The user must create a password to access the device. All data on the |

| Activation type | Description |
| --- | --- |
| | device is protected using encryption and a method of authentication such as a password.<br><br>During activation, the device installs the BES12 Client automatically and grants it Administrator permissions. Users cannot revoke the Administrator permissions or uninstall the app.<br><br>You must use this activation type if you want to support BlackBerry Secure Connect Plus with the features of the Work space only (Android for Work) activation type. |

# Select the productivity apps used on PRIV devices that use Android for Work

To be able to use productivity apps on PRIV devices that use Android for Work, you must assign an app group that contains the productivity apps that you want devices to use to users. You have the following options:

- BlackBerry Productivity Suite: The BlackBerry Productivity Suite app group contains the following apps: BlackBerry Hub, BlackBerry Calendar, Contacts by BlackBerry, Notes by BlackBerry, and Tasks by BlackBerry.
- Divide Productivity: The Divide Productivity app group contains the Android for Work apps from Google including mail, calendar, contacts, tasks, and notes.

**Before you begin:**

- Configure BES12 to support Android for Work. For more information about configuring BES12 to support Android for Work, see the Configuration content.
- Assign an activation profile to users or user groups with one of the following activation types:
  - Work and personal - user privacy (Android for Work)
  - Work and personal - user privacy (Android for Work - Premium)
  - Work space only (Android for Work)
  - Work space only (Android for Work - Premium)

1. On the menu bar, click **Apps**.
2. If the Divide Productivity and BlackBerry Productivity Suite app groups already appear in the app list, make sure that the correct apps, as listed in step 4, have been added to the app groups, and then proceed to step 5.
3. If the app groups do not already appear in the app list, you must add the following apps to BES12.
   - https://play.google.com/store/apps/details?id=/com.blackberry.infrastructure
   - https://play.google.com/store/apps/details?id=com.blackberry.hub

- https://play.google.com/store/apps/details?id=com.blackberry.calendar
- https://play.google.com/store/apps/details?id=com.blackberry.contacts
- https://play.google.com/store/apps/details?id=com.blackberry.notes
- https://play.google.com/store/apps/details?id=com.blackberry.tasks
- https://play.google.com/store/apps/details?id=com.google.android.apps.work.pim

4. Depending on the productivity suite that you want to use, create the following app groups. Make sure that you select the **Enable app group for Android for Work** option so that the apps can be installed on Android for Work devices.

| Task | Steps |
| --- | --- |
| Create an app group for the BlackBerry Productivity Suite | Add the following apps:<br>• BlackBerry Hub<br>• BlackBerry Calendar<br>• Contacts by BlackBerry<br>• Notes by BlackBerry<br>• Tasks by BlackBerry |
| Create an app group for Divide Productivity | Add Divide Productivity. |

5. Assign the app groups to users, user groups, or device groups.

# BlackBerry 10: VPN profile settings

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| Server address | This setting specifies the FQDN or IP address of a VPN server. |
| Gateway type | This setting specifies the type of VPN client that the VPN client on a BlackBerry 10 device emulates.<br>Possible values:<br>• Check Point VPN-1<br>• Cisco VPN 3000 Series Concentrator<br>• Cisco Secure PIX Firewall<br>• Cisco IOS Easy VPN |

| BlackBerry 10: VPN profile setting | Description |
|---|---|
| | • Cisco ASA Series<br>• Cisco AnyConnect<br>• Juniper SRX Series (IPsec VPN)<br>• Juniper MAG Series or Juniper SA Series (SSL VPN)<br>• Microsoft IKEv2 VPN server<br>• Generic IKEv2 VPN server<br>• NIAP-compliant IKEv2 VPN server<br><br>The default value is "Check Point VPN-1." |
| Authentication type | This setting specifies the authentication type for the VPN gateway.<br><br>The "Gateway type" setting determines which authentication types are supported and the default value for this setting.<br><br>Possible values:<br><br>• PSK<br>• PKI<br>• XAUTH-PSK<br>• XAUTH-PKI<br>• EAP-TLS<br>• EAP-MS-CHAPv2 |
| Preshared key or Group password | This setting specifies the preshared key or group password for the VPN gateway.<br><br>This setting is valid only if the "Authentication type" setting is set to "PSK" or "XAUTH-PSK." |
| Username | This setting specifies the username that a BlackBerry 10 device uses to authenticate with the VPN gateway. If the profile is for multiple users, you can use the %UserName% variable.<br><br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect" or if the "Authentication type" setting is set to "XAUTH-PSK" or "XAUTH-PKI." |
| Hardware token | This setting specifies whether a user must use a hardware token to authenticate with the VPN gateway.<br><br>This setting is valid only if the "Authentication type" setting is set to "XAUTH-PSK" or "XAUTH-PKI." |
| Password | This setting specifies the password that a BlackBerry 10 device uses to authenticate with the VPN gateway. |

| BlackBerry 10: VPN profile setting | Description |
|---|---|
| | This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect" or if the "Authentication type" setting is set to "XAUTH-PSK" or "XAUTH-PKI" and the "Hardware token" setting is not selected. |
| EAP identity | This setting specifies the EAP identity that a BlackBerry 10 device uses to authenticate with the VPN gateway.<br>This setting is valid only if the "Authentication type" setting is set to "EAP-TLS." |
| EAP-TLS gateway ID | This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Authentication type" setting is set to "EAP-TLS."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| MS-CHAPv2 EAP identity | This setting specifies the MS-CHAPv2 EAP identity that a BlackBerry 10 device uses to authenticate with the VPN gateway.<br>This setting is valid only if the "Authentication type" setting is set to "EAP-MS-CHAPv2." |
| MS-CHAPv2 username | This setting specifies the MS-CHAPv2 username that a BlackBerry 10 device uses to authenticate with the VPN gateway.<br>This setting is valid only if the "Authentication type" setting is set to "EAP-MS-CHAPv2." |
| MS-CHAPv2 password | This setting specifies the MS-CHAPv2 password that a BlackBerry 10 device uses to authenticate with the VPN gateway.<br>This setting is valid only if the "Authentication type" setting is set to "EAP-MS-CHAPv2." |
| Authentication ID type | This setting specifies the authentication ID type for the VPN gateway.<br>This setting is valid only if the "Gateway type" setting is set to "Juniper MAG Series or Juniper SA Series (SSL VPN)," "Microsoft IKEv2 VPN server," "Generic IKEv2 VPN server," or "NIAP-compliant IKEv2 VPN server."<br>The "Gateway type" setting determines which authentication ID types are supported and the default value for this setting.<br>Possible values:<br>• IPv4<br>• Fully qualified domain name<br>• Email address<br>• Identity certificate distinguished name<br>• Identity certificate general name |

| BlackBerry 10: VPN profile setting | Description |
|---|---|
| | • Key ID |
| Authentication ID or Group username | This setting specifies the authentication ID or group username for the VPN gateway.<br>This setting is valid only if the "Gateway type" setting is set to "Juniper MAG Series or Juniper SA Series (SSL VPN)," "Microsoft IKEv2 VPN server," or "Generic IKEv2 VPN server," or if the "Authentication type" setting is set to "PSK" or "XAUTH-PSK." |
| Gateway authentication type | This setting specifies the gateway authentication type for the VPN gateway.<br>This setting is valid only if the "Gateway type" setting is set to "Juniper MAG Series or Juniper SA Series (SSL VPN)," "Microsoft IKEv2 VPN server," or "Generic IKEv2 VPN server."<br>Possible values:<br>• None<br>• PSK<br>• PKI<br>The default value is "None." |
| Enable OCSP/CRL check on the certificates from the VPN | This setting enables certificate revocation checking for the certificates used during authentication.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Authentication type" setting is set to "PKI" or "EAP-TLS."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Gateway preshared key | This setting specifies the gateway preshared key for the VPN gateway.<br>This setting is valid only if the "Gateway authentication type" setting is set to "PSK." |
| Gateway authentication ID type | This setting specifies the gateway authentication ID type for the VPN gateway.<br>This setting is valid only if the "Gateway type" setting is set to "Juniper MAG Series or Juniper SA Series (SSL VPN)," "Microsoft IKEv2 VPN server," "Generic IKEv2 VPN server," or "NIAP-compliant IKEv2 VPN server."<br>Possible values:<br>• IPv4<br>• Fully qualified domain name<br>• Email address<br>• Identity certificate distinguished name |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| | • Identity certificate general name<br>• Key ID<br><br>The default value is "IPv4." |
| Gateway authentication ID | This setting specifies the gateway authentication ID for the VPN gateway.<br><br>This setting is valid only if the "Gateway authentication ID type" setting is set to "Fully qualified domain name" or "Email address." |
| Send requested gateway ID in message 1 of IKEv2 protocol | This setting specifies whether the gateway ID request is sent in the IKEv2 login packet.<br><br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br><br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Requested gateway ID type | This setting specifies the requested gateway ID type for the VPN.<br><br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Send requested gateway ID in message 1 of IKEv2 protocol" setting is selected.<br><br>Possible values:<br>• IPv4<br>• Fully qualified domain name<br>• Email address<br>• Identity certificate distinguished name<br>• Identity certificate general name<br>• Key ID<br><br>The default value is "IPv4."<br><br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Requested gateway ID | This setting requests a specific gateway ID in the first IKE message during login, if the VPN server supports multiple IDs. The requested gateway ID may be different than the gateway ID used for authentication.<br><br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Send requested gateway ID in message 1 of IKEv2 protocol" setting is selected.<br><br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| Secondary username | This setting specifies the username that a BlackBerry 10 device uses for secondary authentication with the VPN gateway. If the profile is for multiple users, you can use the %UserName% variable.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Secondary password | This setting specifies the password that a BlackBerry 10 device uses for secondary authentication with the VPN gateway.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Group name | This setting specifies the password that a BlackBerry 10 device uses for secondary authentication with the VPN gateway.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Enable automatic client certificate processing | This setting specifies whether a client certificate is automatically selected when a VPN connection is made.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Enable IPsec authentication | This setting specifies whether the VPN gateway uses IPsec authentication.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| IPsec authentication type | This setting specifies the authentication type for an IPsec VPN connection.<br>This setting is valid only if the "Enable IPsec authentication" setting is selected.<br>Possible values:<br>• EAP-MS-CHAPv2<br>• EAP-MD5<br>• EAP-GTC<br>• EAP-AnyConnect<br>• IKE-RSA<br>The default value is "EAP-MS-CHAPv2." |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| | The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| EAP authentication ID | This setting specifies the EAP identity that a BlackBerry 10 device uses to authenticate with the VPN gateway.<br>This setting is valid only if the "IPSec authentication type" setting is set to "EAP MSCHAPv2," "EAP MD5," or "EAP GTC." |
| Exclude subnets | This setting specifies whether to exclude specified subnets from using the VPN connection.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Exclusion subnets | This setting specifies the subnets and subnet masks that are not sent through the VPN connection.<br>This setting is valid only if the "Exclude subnets flag" setting is selected. |
| Cisco AnyConnect configuration file (.xml) | This setting specifies the location of the Cisco AnyConnect configuration file to send to BlackBerry 10 devices.<br>This setting is valid only if the "Gateway type" setting is set to "Cisco AnyConnect."<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Allow personal apps to use work networks | This setting specifies whether personal apps on a BlackBerry 10 device can use the VPN connection.<br>This setting is valid only if the "Allow personal apps to use work networks" IT policy rule is selected.<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Untrusted certificate action | This setting specifies whether a BlackBerry 10 device accepts untrusted certificates. If this setting is set to "Allow," the device accepts untrusted certificates automatically. If this setting is set to "Prompt," the user can choose whether to accept untrusted certificates. If this setting is set to "Disallow," the device does not accept untrusted certificates.<br>The "Gateway type" setting determines which untrusted certificate actions are supported and the default value for this setting.<br>Possible values:<br>• Allow<br>• Prompt<br>• Disallow |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| | The minimum requirement is BlackBerry 10 OS version 10.3.2. |
| Client certificate source | This setting specifies how BlackBerry 10 devices can obtain the client certificate. There are four options for devices to obtain client certificates:<br>• If you choose "SCEP," you must also specify the associated SCEP profile that the device can use to download the client certificate.<br>• If you choose “User credential," you must also specify the user credential profile that the device can use to download the client certificate.<br>• If you choose "Smart card," the user must pair the device with a smart card that includes the client certificate.<br>• If you choose "Other," the user must add the client certificate to the device manually.<br>Smart card support is available for devices that are running BlackBerry 10 OS version 10.3.1 and later.<br>This setting is valid only if the "Authentication type" setting is set to "PKI" or "XAUTH-PKI."<br>Possible values:<br>• Smart card<br>• SCEP<br>• User credential<br>• Other<br>The default value is "Other." |
| Associated user credential profile | This setting specifies the associated user credential profile that a BlackBerry 10 device uses to obtain a client certificate to use for authentication with the VPN.<br>This setting is valid only if the "Client certificate source" setting is set to "User credential."<br>The minimum requirement for using a user credential profile is BlackBerry 10 OS version 10.3.1. |
| Associated SCEP profile | This setting specifies the associated SCEP profile that a BlackBerry 10 device uses to obtain a client certificate to authenticate with the VPN.<br>This setting is valid only if the "Client certificate source" setting is set to "SCEP." |
| IKE lifetime | This setting specifies the lifetime, in seconds, of the IKE connection. If you set an unsupported value or a null value, the BlackBerry 10 device default value is used.<br>The possible values are from 1 to 2,147,483,647. |

| BlackBerry 10: VPN profile setting | Description |
|---|---|
| IKE threshold | This setting specifies the percentage of the IKE lifetime at which the VPN client will initiate a new key exchange.<br>Possible values: "0" to "100"<br>The default value is "90."<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| IPsec lifetime | This setting specifies the lifetime, in seconds, of the IPsec connection. If you set an unsupported value or a null value, the BlackBerry 10 device default value is used.<br>The possible values are from 1 to 2,147,483,647. |
| IPsec threshold | This setting specifies the percentage of the IPsec threshold at which the VPN client will initiate a new key exchange.<br>Possible values: "0" to "100"<br>The default value is "90."<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Allow VPN extensions | This setting allows you to enable or disable extensions.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| VPN extensions list | This setting allows you to enter a list of extensions that are used to generate Vendor ID payloads and perform additional certificate validation.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Allow VPN extensions" setting is selected.<br>The minimum requirement is BlackBerry 10 OS OS version 10.3.3. |
| Require vendor ID extension | This setting indicates that the administrator wants to use one of the extensions in the VPN extension list to generate a Vendor ID payload during the login.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Allow VPN extensions" setting is selected. |

| BlackBerry 10: VPN profile setting | Description |
|---|---|
| | The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Require certificate validation extension | This setting indicates that the administrator wants to use one of the extensions to perform additional certificate validation.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Allow VPN extensions" setting is selected.<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Enable session resumption | This setting enables IKEv2 session resumption settings. If the VPN server supports this feature, the VPN client will suspend and resume a session instead of completely disconnecting and reconnecting whenever VPN auto-connect is enabled.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Ticket threshold | This setting specifies at what percentage of the ticket threshold session resumption will occur.<br>Possible values: 0-100%<br>The default value is "90".<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server" and the "Enable session resumption" setting is selected.<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Enable hash-and-URL format certificate payloads during IKE | This setting specifies whether the VPN client advertises to the VPN server that it supports using IKEv2 to exchange certificates using URLs and fetches certificates, if available, from a provided HTTP URL.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Enable strict enforcement of approved algorithms | This setting specifies whether the use of NIAP-approved algorithms is strictly enforced.<br>This setting is valid only if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server."<br>The minimum requirement is BlackBerry 10 OS version 10.3.3. |
| Split tunneling | This setting specifies whether a BlackBerry 10 device can use split tunneling to bypass the VPN gateway, if the VPN gateway supports it. |

| BlackBerry 10: VPN profile setting | Description |
|---|---|
| | This setting is not valid if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server." |
| Disable banner | This setting specifies whether a BlackBerry 10 device blocks the VPN banner.<br>This setting is not valid if the "Gateway type" setting is set to "NIAP-compliant IKEv2 VPN server." |
| Trusted certificate source | This setting specifies the source of the trusted certificate. If this setting is set to "Trusted certificate store," a BlackBerry 10 device can connect to a VPN that uses any certificate in the VPN certificate store.<br>This setting is valid only if the "Authentication type" setting is set to "PKI" or "XAUTH-PKI."<br>Possible values:<br>• None<br>• Trusted certificate store<br>The default value is "None." |
| Automatically determine IP | This setting specifies whether a BlackBerry 10 device automatically determines the IP configuration of the VPN gateway. |
| Private IP | This setting specifies the private IP of the VPN gateway.<br>This setting is valid only if the "Automatically determine IP" setting is not selected. |
| Private IP mask | This setting specifies the private IP mask of the VPN gateway.<br>This setting is valid only if the "Automatically determine IP" setting is not selected. |
| Subnet | This setting specifies the subnet of the VPN gateway.<br>This setting is valid only if the "Automatically determine IP" setting is not selected. |
| Subnet mask | This setting specifies the subnet mask of the VPN gateway.<br>This setting is valid only if the "Automatically determine IP" setting is not selected. |
| Automatically determine DNS | This setting specifies whether a BlackBerry 10 device automatically determines the DNS configuration of the VPN gateway. |
| Primary DNS | This setting specifies the primary DNS server in dot-decimal notation (for example, 192.0.2.0).<br>This setting is valid only if the "Automatically determine DNS" setting is not selected. |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| Secondary DNS | This setting specifies the secondary DNS server in dot-decimal notation (for example, 192.0.2.0).<br>This setting is valid only if the "Automatically determine DNS" setting is not selected. |
| Domain suffix | This setting specifies the FQDN of the DNS suffix.<br>This setting is valid only if the "Automatically determine DNS" setting is not selected. |
| Perfect forward secrecy | This setting specifies whether the VPN gateway supports PFS.<br>If this setting is selected, the "IPsec DH group" setting must not be set to 0. |
| Manual algorithm selection | This setting specifies whether you must set the cryptographic algorithms for the VPN gateway. |
| IKE DH group | This setting specifies the DH group that a BlackBerry 10 device uses to generate key material.<br>This setting is valid only if the "Manual algorithm selection" setting is selected.<br>Possible values:<br>• 1 to 26, except 3, 4, and 6<br>• Custom 1 to Custom 5<br>The default value is "1." |
| Custom IKE DH provider | This setting specifies the name of the provider for custom IKE DH.<br>This setting is valid only if the "IKE DH group" setting is set to one of the Custom values. |
| Enable MOBIKE | This setting specifies whether the VPN gateway supports MOBIKE.<br>This setting is valid only if the "Gateway type" setting is set to "Microsoft IKEv2 VPN server," or "Generic IKEv2 VPN server," the "Authentication type" setting is set to "PKI," and the "IKE DH group" setting is set to one of the Custom values.<br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| IKE cipher | This setting specifies the algorithm that a BlackBerry 10 device uses to generate a shared secret key.<br>This setting is valid only if the "Manual algorithm selection" setting is selected.<br>Possible values:<br>• None<br>• DES (56-bit key)<br>• Triple DES (168-bit key) |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| | • AES (128-bit key)<br>• AES (192-bit key)<br>• AES (256-bit key)<br>The default value is "None." |
| IKE hash | This setting specifies the hash function that a BlackBerry 10 device uses with IKE.<br>This setting is valid only if the "Manual algorithm selection" setting is selected.<br>Possible values:<br>• None<br>• MD5<br>• AES-XCBC<br>• SHA-1<br>• SHA-256<br>• SHA-384<br>• SHA-512<br>The default value is "None." |
| IKE PRF | This setting specifies the PRF that a BlackBerry 10 device uses with IKE.<br>This setting is valid only if the "Manual algorithm selection" setting is selected.<br>Possible values:<br>• None<br>• HMAC<br>• HMAC-MD5<br>• AES-XCBC<br>• HMAC-SHA-1<br>• HMAC-SHA-256<br>• HMAC-SHA-384<br>• HMAC-SHA-512<br>The default value is "None." |
| IPsec DH group | This setting specifies the DH group that a BlackBerry 10 device uses with IPsec. |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| | This setting is valid only if the "Manual algorithm selection" setting is selected.<br>The possible values are from 0 to 26, except 3, 4, and 6.<br>The default value is "0." |
| IPsec cipher | This setting specifies the algorithm that a BlackBerry 10 device uses with IPsec.<br>This setting is valid only if the "Manual algorithm selection" setting is selected.<br>Possible values:<br>• None<br>• DES (56-bit key)<br>• Triple DES (168-bit key)<br>• AES (128-bit key)<br>• AES (192-bit key)<br>• AES (256-bit key)<br>The default value is "None." |
| IPsec hash | This setting specifies the hash function that a BlackBerry 10 device uses with IPsec.<br>This setting is valid only if the "Manual algorithm selection" setting is selected.<br>Possible values:<br>• None<br>• MD5<br>• AES-XCBC<br>• SHA-1<br>• SHA-256<br>• SHA-384<br>• SHA-512<br>The default value is "None." |
| NAT keepalive | This setting specifies how often a device sends a NAT keepalive packet. If you set an unsupported value or a null value, the BlackBerry 10 device default value is used.<br>The possible values are from 1 to 2,147,483,647. |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| DPD frequency | This setting specifies the DPD frequency, in seconds. A BlackBerry 10 device supports a minimum setting of 10 seconds. If you set an unsupported value or a null value, the device default value is used.<br><br>The possible values are from 1 to 2,147,483,647. |
| User can edit | This setting specifies the VPN settings that a BlackBerry 10 device user can change. If this setting is set to "Read only," the user can't change any settings. If this setting is set to "Credentials only," the user can change the username and password.<br><br>Possible values:<br><br>• Read only<br>• Credentials only<br><br>The default value is "Read only." |
| Display VPN information on device | This setting specifies whether VPN information is displayed on a BlackBerry 10 device. If this setting is set to "Visible," most of the VPN profile information appears on the device. If this setting is set to "Invisible," only the profile name appears on the device. If this setting is set to "Credentials only," the profile name and the credential fields appear on the device.<br><br>Possible values:<br><br>• Visible<br>• Invisible<br>• Credentials only<br><br>The default value is "Visible." |
| Data security level | This setting specifies the domain in the work space where the VPN profile is stored when the work space uses advanced data at rest protection. This setting is valid only if the "Force advanced data at rest protection" IT policy rule is selected. If this setting is set to "Always available," the profile is stored in the Startup domain and is available when the work space is locked. If this setting is set to "Available after authentication," the profile is stored in the Operational domain and is available after the work space is unlocked once until the device restarts. If this setting is set to "Available only when work space unlocked," the profile is stored in the Lock domain and can be used for VPN connections only when the work space is unlocked.<br><br>Possible values:<br><br>• Always available<br>• Available after authentication |

| BlackBerry 10: VPN profile setting | Description |
| --- | --- |
| | • Available only when work space unlocked<br><br>The default value is "Always available."<br><br>The minimum requirement is BlackBerry 10 OS version 10.3.1. |
| Associated proxy profile | This setting specifies the associated proxy profile that a BlackBerry 10 device uses to connect to a proxy server when the device is connected to the VPN. |

# Installing or upgrading the maintenance release

2

You can use the setup application to install BES12 version 12.3 MR1 or to upgrade from BES12 version 12.3. When you upgrade the software, the setup application stops and starts all the BES12 services for you. The BES12 setup application backs up the database by default.

For more information, see the Installation and upgrade content.

# Fixed issues

3

## Installation, upgrade, and migration fixed issues

When you installed several BES12 Core and BES12 management console instances, the BlackBerry Affinity Manager sent notifications to the BES12 management console instances. (JI 1357610)

When you attempted to upgrade from BES12 version 12.0 to BES12 version 12.3, the message that displayed was not clear. The message should have stated that you could not upgrade from BES12 version 12.0 to BES12 version 12.3. (JI 1351611)

When you were migrating a large number of BES10 users to BES12, the migration would timeout before you could select the users and devices that you wanted to migrate. (JI 1339985)

After you upgraded to BES12 version 12.3, on the Settings > Infrastructure > BES12 Instances page, the status of the BES12 server displayed as Unavailable. (JI 1336382)

## User and device management fixed issues

When a user was using an Android device with the Secure Work Space apps and with a SCEP profile assigned, during activation if the SCEP PKI connection took longer than 15 seconds to complete, the connection closed and activation did not complete. (JI 1367421)

If the BES12 Core was installed on one server and the BES12 management console was installed on a separate server, when a user opened the Secure Work Space Work apps on an iOS device, a Connection refused message displayed. (JI 1348304)

## Management console fixed issues

If you added a user whose email address contained an apostrophe ('), an error displayed. (JI 1385339)

When you attempted to create a user and the domain portion of the user's email address contained a hyphen, a “The value is invalid” error message displayed above the email address field, and the user was not created. (JI 1377541)

Hosted .ipa apps could not exceed 134 MB in size. (JI 1372132)

When you added a user to a group that contained a WatchDox role, on the User details page there was no indication that the user had any WatchDox capability. (JI 1364169)

Email addresses did not display in CSV log files for BlackBerry 10 devices. (JI 1360158)

In an environment with multiple BES12 instances, if you stopped all of the instances and then started half of the instances, most of the instances entered the election state and their SRPs became disabled. (JI 1352572)

If you looked at the location of a Windows device, when you clicked Device actions unnecessary characters displayed in the Action column. (JI 1341813)

On the dashboard, even if the image for non-compliant devices showed that non-compliant devices existed, when you clicked the image the Device compliance report did not show any non-compliant devices. (JI 1298560)

On the Users and devices tab, the Compliance Violation column was empty for BlackBerry 10 devices that were out of compliance. (JI 1298623)

When you used single sign-on for BES12, in some circumstances when you tried to access the BES12 site, you had to refresh to remove a blank screen to see the console. (JI 1140596)

## BlackBerry Secure Connect Plus fixed issues

When your organization is using BlackBerry 10 devices, the BlackBerry Secure Connect Plus app sometimes continues to use the cellular network when a Wi-Fi network is available. (JI 1077523)

# Known issues

4

## Installation, upgrade, and migration known issues

When you upgrade from BES5 to BES12, the Microsoft Active Directory connection for BES5 is migrated automatically. This connection supports all devices that connect to this directory. You do not have to create a Microsoft Active Directory connection to this directory.

If there are external users in the source BES12 database, those users become candidates for migration. (JI 1335337)

When you are migrating devices, some of the text in the Group column does not wrap correctly and you can't see all of the information. (JI 1320066)

When you install the BES12 version 12.3 software, the installation might stop responding when the services are being installed. (JI 1294980)

**Workaround**: Stop the setup application and run it again.

When you upgrade from BES12 version 12.2 to BES12 version 12.3, the Keymaster tool might generate a SCEP certificate that has the SAN field set to *.hostname instead of *.domain.com <*fqdn*> which causes enrollments to fail. (JI 1274891)

When you install BES12 on a STIG server, the TAP-windows file does not install because its root certificate is not trusted. (JI 1273885)

After you upgrade from BES5 to BES12, if the BlackBerry Administration Service stops, when you restart the BlackBerry Administration Service and log in to the console, the login screen keeps reloading. (JI 788051)

**Workaround**: Log out from BES12 and then after the BlackBerry Administration Service is running, log back in to BES12.

After you upgrade from BES5 to BES12, if you use the Enterprise Transporter tool to move multiple users, when you click **User Summary** > **Advanced Settings** you cannot assign anything to the users. (JI 787042)

## User and device management known issues

When you try to use the Work Space Only - (Samsung KNOX) activation type to activate a Samsung KNOX device that uses KNOX version 2.4, if the user has the Samsung email app configured to use Microsoft ActiveSync on the device, the device will not activate and an "Unexpected internal error" message displays. (JI 1359308)

**Workaround**: Remove the Microsoft ActiveSync email account from the Samsung email app and then re-activate the device.

On Windows 8.x and Windows 10 devices, if you change the SSID in a Wi-Fi profile, the profile is not updated on the device. (JI 1350623)

**Workaround**: Create different Wi-Fi profiles for different SSIDs.

If an iOS device is part of a device group that has the OS type set to iOS, and there is no email profile assigned to the group, if you push an email profile to the device it does not receive the profile. (JI 1321293)

**Workaround**: Make sure that iOS devices are not included in a device group, or assign an email profile to the device group that iOS devices are a part of.

When you upgrade an internal app that is hosted on Google Play and is part of an app group, the app configuration is removed from the app group and is set to None. (JI 1303541)

## Management console known issues

When you are configuring an email profile for Android devices, in the Security type drop-down list the STARTTLS and STARTTLS-Trust All options are available but do not work.

The Maximum failed password attempts IT policy rule does not apply to Windows 10 mobile devices that use Microsoft Passport or with Windows 10 computers or tablets. (JI 1356254)

This issue occurs when you are logged in to the console as a Security Administrator. When you add a Microsoft Active Directory user and click Save and New, and then add a local user and click Save and New, an error message displays and the users are not added. (JI 1354742)

**Workaround**: Add users one at a time.

If you add an internal app that is enabled for Android for Work and you choose to host the app on Google Play, step 7 in the instructions in the administration console is incorrect. Do not select the I am uploading a configuration for an APK hosted outside of Google Play option.( (JI 1348312)

**Workaround**: Ignore step 7.

After you upgrade from BES12 version 12.2 MR1 to BES12 version 12.3, when you create a user the default Enterprise Management Agent profile is not assigned to the user. Also, if you create any profiles, the profiles are not pushed to the user's device. (JI 1347699)

**Workaround**: Create an Enterprise Management Agent profile, push it to the device, and click the synchronize button on the device.

The Windows logo does not display consistently in the management console. For example, on the App management page the logo displays but on the Assign app page the letters "WP" display. (JI 1346667)

For Windows devices, the View location history button does not work. (JI 1346249)

If you are using an LDAP connection, on the User summary page when you click on the arrow beside the user's name and then click Refresh, a message displays that states the email address has been updated. (JI 1344729)

If you use a custom activation email template, and when you add a user you select the Set device activation password option and the custom activation email template, when you preview the activation email the default email displays. (JI 1344206)

**Workaround**: When you select the Autogenerate device activation password and send email with activation instructions option, the custom activation email displays.

When you use the Location service to locate an iOS device, more than one device location might display on the map. (JI 1340051)

When you try to upload an APK file, and error displays on the BES12 management console. (JI 1338666)

When you create an email profile for Android devices, the settings for the BlackBerry Productivity Suite include the S/MIME settings. (JI 1334609)

You cannot create a single sign-on profile. (JI 1328010)

When you export a .csv file of a device report for a Samsung Galaxy Note 4 device, in the file the type of media card available displays a string variable, for example "???.devicehw.storage.memorycard.type". (JI 1326586)

When you create an IT policy and configure password requirements in the policy, after you assign the policy to a BlackBerry 10 device user, the **Specify device password, lock and set message** IT command has to use the same password requirements that you configured in the IT policy. (JI 1304784)

When you add a new version of an optional BES12 hosted app, the old version of the app is removed before the new version is published. When this happens the new version of the app cannot be installed. (JI 1289342)

In a BES12 and BES5 integrated environment, if you delete a BlackBerry OS user from the BlackBerry Administration Service without selecting the Delete the user and remove the BlackBerry information from the user's mail system option, and then you add the same user to BES12 and activate a BlackBerry OS device for the user, the BlackBerry OS device information does not display in the BES12 management console.

When you add a new version of an Android for Work hosted app, the Assigned to users tab displays an incorrect number of devices. (JI 1286689)

When you are using Internet Explorer 11, when you click Assign to assign a profile to a user, the profile is not assigned. (JI 1274473)

**Workaround**: Click Assign again.

The tool tips for the fields in the SCEP profile do not provide enough information. If you want to create a SCEP profile for Android devices that are activated with Secure Work Space, the Subject field in both sections of the profile are required and must be the

same. Similarly, if you include a subject alternative name, you must enter the same information in the SAN fields in the Secure Work Space section and in the Android for Work/Samsung KNOX Workspace section of the profile. (JI 1154684)

If you create an IT policy for Android devices and set the Notification level to Show all information when the work space is locked, the account name and profile name are the only information that displays on the device. (JI 939910)

When you send an email profile that has a description with more than 100 characters to a device, a SQL exception occurs and the profile is not applied to the device. (JI 854774)

**Workaround**: Do not use more than 100 characters in the description field for a profile.

When you enable single sign-on for multiple Microsoft Active Directory connections, if the Microsoft Active Directory accounts use the same passwords single sign-on does not work. (JI 853807)

**Workaround**: Do not use the same password on multiple directory connections.

If you have assigned a user certificate to a user and then edit the user certificate profile to remove the assigned certificate and add a different certificate, the new certificate is not shown in the management console and is not sent to the device. (JI 807990)

If your organization's environment contains BES5 and BES12, when you create users in BES5 and then you view the Directory synchronization report in BES12, the users display in both the User information update on BES12 and User removal from BES12 sections. (JI 795407)

## BlackBerry Secure Connect Plus known issues

When you assign a third-party VPN solution to an Android device that has BlackBerry Secure Connect Plus enabled, you should turn off BlackBerry Secure Connect Plus before you send the profile to the device. When BlackBerry Secure Connect Plus is enabled, the device might not automatically connect to your organization using the third-party VPN solution. You can enable BlackBerry Secure Connect Plus after the device connects to your organization’s network through the third-party VPN solution. (JI 1185934)

## Documentation known issues

In the Licensing content for BES12 version 12.0, and 12.1, in the SIM licenses topic > iOS row, "Work and personal - user privacy" is listed as an activation type when it should not be. Also, in the License requirements for activation types topic > iOS devices table > Work and personal - user privacy row, "Gold SIM license" is listed as a required license when it should not be. (JI 1259757)

In some cases the documentation states that the supported version of Android that Android for Work uses is 5.0, however the supported version is 5.1. For the most current version information, refer to the *Compatibility Matrix*.

# Maintenance releases of the BES12 Secure Connect Plus app

5

The BES12 Secure Connect Plus app is required for devices to use the BlackBerry Secure Connect Plus feature in BES12. Maintenance releases of the app might occur between BES12 releases. To view the Release Notes for the latest maintenance releases of the app, visit http://help.blackberry.com/detectLang/bes12-secure-connect-plus-app/latest/.

For more information about enabling and using BlackBerry Secure Connect Plus, see "Using BlackBerry Secure Connect Plus for secure connections to work resources" in the BES12 Administration content.

# Legal notice

6

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