Release Notes and Advisories Guide

BlackBerry UEM
Version 12.6 and all maintenance releases

Published: 2017-06-02
SWD-20170602131022342

Contents

About the documentation for this maintenance release

1

Not all of the documentation was updated for BlackBerry UEM 12.6 MR3. The covers of guides that were not updated refer to BlackBerry UEM 12.6 MR1 and BlackBerry UEM 12.6 MR2.

Installing or upgrading the maintenance release

2

You can use the setup application to install BlackBerry UEM version 12.6 MR3 or to upgrade from BES12 version 12.4.x, or BES12 version 12.5.x or BlackBerry UEM version 12.6.x. When you upgrade the software, the setup application stops and starts all the BlackBerry UEM services for you. The BlackBerry UEM setup application backs up the database by default.

Addendum to Administration content

3

The following topics are additions to the Administration content to help administrators:

- host internal apps for Android for Work and devices
- send the root CA certificate to devices

If you host an internal app in BlackBerry UEM for Android for Work devices using a .json file, you must send the BlackBerry UEM root CA certificate to devices. This is added as a prerequisite to the following topic: Send the BlackBerry UEM root CA certificate to devices

Host an internal app for Android for Work devices in BlackBerry UEM using a .json file

To host an internal app for Android for Work devices in BlackBerry UEM, you must generate a .json file for the app, upload the file to Google Play, and get the license key for the published app. Apps that are hosted in BlackBerry UEM can be set only as optional, and you cannot use configuration settings to modify app features and behaviors.

Before you begin:

- Verify that you have OpenSSL, JDK, Python 2.x, and Android Asset Packaging Tool (aapt) installed in a Path location on the computer.
- You need an account to log in to the Google Developers Console. If Android for Work is configured, use the same email address for the developer account that you used to set up Android for Work. For each BlackBerry UEM domain you need a different developer account.
- In BlackBerry UEM, add an internal app to the app list. Select the **Enable the app for Android for Work** option, and in the **App will be hosted by** drop-down list, click **BlackBerry UEM**. Copy and save the URL that is displayed in BlackBerry UEM.

  Note: You need to select **Enable the app for Android for Work** even if you are hosting the app for all Android devices.
- For Android for Work devices, Send the BlackBerry UEM root CA certificate to devices.

1. Generate a .json file for the app. To create the .json file, perform the following actions:
   a. Go to https://github.com/google/play-work/tree/master/externally-hosted-apks.
   b. Click the **externallyhosted.py** file.
   c. Click **Raw**.

d. Save the file to a Path location on the computer.

e. Using a command prompt, navigate to the location where you saved the externallyhosted.py file and type **python externallyhosted.py --apk=*path to apk that you want to host* --externallyHostedUrl=*URL displayed in BlackBerry UEM* >*filename.json*** to run the python file. For example, **python externallyhosted.py --apk=c:\mycompanyapp.apk --externallyHostedUrl=https://enrol-plaintext-<SRPID>.<Country_Code>.bbsecure.com/<SRPID>/mdm/beshosted/afw/app/<App name from UEM>**

2. Log in to the Google Developers Console at https://play.google.com/apps/publish. If Android for Work is configured, use the same email address for the developer account that you used to set up Android for Work.
3. Click **Add new application**.
4. Select the default language.
5. Enter a title for the app.
6. Click **Upload APK**.
7. If applicable, click **Upload your first APK to Production**.
8. Select **I am uploading a configuration for an APK hosted outside of Google Play**.
9. Navigate to and upload the .json file that you generated in step 1.
10. Enter all of the necessary Store Listing and Content Rating information. For example, add screen shots.
11. On the **Pricing & Distribution** tab, in **Restrict Distribution**, select **Only make this application available to my organization (<your organization name>)**.
12. Save draft.
13. Click **Publish app**.
14. To check the status of the app, click **Check status** in the management console to determine whether the license key has been generated. Users can install the app after it is published in Google Play. It may take several hours for the app to be published.
15. Log in to the https://play.google.com/apps/publish.
16. Select the app from the published app list.
17. Click **Services & APIs**.
18. Copy the license key for the app.
19. In the management console, paste the license key in the text box.

Send the BlackBerry UEM root CA certificate to devices

For Android for Work devices, if you want to assign internal apps that are hosted in BlackBerry UEM, you need to send the BlackBerry UEM root CA certificate to devices. Android for Work devices that do not have the root CA certificate installed will not be able to install internal apps that are hosted in BlackBerry UEM.

1. Download the root CA certificate by navigating to the certificate server url as follows: https://<country_code>.bbsecure.com/<SRPID>/ca
2. Create a CA certificate profile using the .cer file that you saved in step 1. See Create a CA certificate profile.
3. Assign the profile to users that require it, or assign the profile to the "All users" group. See Assign a profile to a user group.

What's new in BlackBerry UEM

4

This section contains a list of all the new features that have been introduced in BlackBerry UEM 12.6.

What's new in BlackBerry UEM version 12.6 MR2

Synchronization of Good Control with BlackBerry UEM

After you synchronize Good Control with BlackBerry UEM, the administrator might observe a change in the behavior of app groups and policy sets. For more information, see KB39080.

New IT policy rules

The following new IT policy rules are available in BlackBerry UEM version 12.6 MR2.

Device Type	Group	Name	Description
Android for Work	Device functionality	Allow user-configured VPN in workspace	Specify whether the user can configure a VPN profile in the work space.
Android for Work	Device functionality	Allow mobile data usage while roaming	Specify whether a user can use mobile data while roaming. If this rule is not selected, apps can't connect to the Internet over a wireless network when the device is roaming.
Android for Work	Security and privacy	Allow sending bug reports	Specify whether the user can send bug reports from the device.
Android for Work	Security and privacy	Send bug reports using the BlackBerry DDT app	Specify whether Android devices powered by BlackBerry must use the BlackBerry DDT app to send bug reports to BlackBerry.
BlackBerry devices powered by Android	Device functionality	Allow work apps to access media card	Specify whether work apps can read and write data on the media card.
BlackBerry devices powered by Android	Device functionality	Allow work apps to use USB OTG	Specify whether work apps can read and write data from other devices connected using USB On-The-Go.
BlackBerry devices powered by Android	Device functionality	Adopt attached storage media	Specify whether attached storage media is adopted by the device file system. If this rule is selected, any attached storage media, such as an SD card, is formatted so that it will only work with that device and the device requires the storage media to work as expected. This rule does not take effect until the device restarts or new storage media is attached.

Device Type	Group	Name	Description
			Users have the option to remove the storage media before it is adopted.
BlackBerry devices powered by Android	Device functionality	Allow NFC	Specify whether the device can use NFC.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth	Specify whether the device can use Bluetooth technology.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth A2DP	Specify whether the device can use the Bluetooth A2DP to stream audio files to another Bluetooth enabled device (for example, a headset).
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth AVRCP	Specify whether the device can use the Bluetooth AVRCP to allow a Bluetooth enabled device (for example, a headset) to control the device's media apps.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth discoverable mode	Specify whether the device can use Bluetooth discoverable mode. A device that is discoverable can be found by other Bluetooth enabled devices within range of the device.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth file transfer using OBEX	Specify whether the device can exchange files with other supported Bluetooth OBEX devices.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth pairing	Specify whether the device can connect to another Bluetooth enabled device. If this rule is not selected, the device can't establish new connections with other Bluetooth enabled devices. After a device connects to another Bluetooth enabled device, you can use this rule to prevent the device from connecting to additional Bluetooth enabled devices.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth PAN profile	Specify whether the device can use the Bluetooth PAN profile to allow another Bluetooth enabled device to tether to it.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth SPP	Specify whether the device can use the Bluetooth SPP to connect to another Bluetooth enabled device.
BlackBerry devices powered by Android	Device functionality	Enforce Bluetooth SSP numeric comparison	Specify whether the device must use numeric comparison mode if the device uses Bluetooth SSP to connect to another Bluetooth enabled device.
BlackBerry devices powered by Android	Device functionality	Enforce minimum Bluetooth passkey length	Specify whether the device must use a Bluetooth passkey that is at least 8 digits to connect to another Bluetooth enabled device. If this rule is selected, the device can't connect to another Bluetooth enabled device if the passkey that the Bluetooth enabled device requests or provides is less than 8 digits.
BlackBerry devices powered by Android	Device functionality	Minimum Bluetooth encryption key length	Specify the minimum encryption key length that the device uses to encrypt Bluetooth connections.
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth low energy	Specify whether the device can make Bluetooth low energy connections.

Device Type	Group	Name	Description
BlackBerry devices powered by Android	Device functionality	Allow Bluetooth page scan	Specify if the device can use Bluetooth page scan mode to search for devices that are trying to connect to it. If this rule is not selected, the device never uses page scan for incoming connections, but still permits outgoing connections to paired devices.
BlackBerry devices powered by Android	Device functionality	Allow SMS messages	Specify whether the BlackBerry device can send and receive SMS text messages.
BlackBerry devices powered by Android	Device functionality	Allow MMS messages	Specify whether the BlackBerry device can send and receive MMS messages.
BlackBerry devices powered by Android	Device functionality	SMS/MMS signature	Specify the signature (for example, a web address or a short disclaimer) that is appended to outgoing SMS text messages and MMS messages that a user sends from a device.
BlackBerry devices powered by Android	Device functionality	Allow media streaming	Specify whether users can stream audio and screen content to other devices using the HDMI port, Google Chromecast, or Wi-Fi CERTIFIED Miracast.
BlackBerry devices powered by Android	Device functionality	Allow Hotspot Browser	Specify whether the device can use the Hotspot Browser when it detects a hotspot. If this rule is selected, the device prompts the user to log in to the hotspot and automatically opens the Hotspot Browser. The Hotspot Browser always uses a Wi-Fi connection, regardless of the settings for any other rules. If this rule is not selected, the device can't connect to a hotspot using the Hotspot Browser.
BlackBerry devices powered by Android	Device functionality	Hotspot Browser timeout	Specify the period of time in seconds that the Hotspot Browser connection remains open without user login. If the user doesn't log in to the Hotspot Browser before the time elapses, the Hotspot Browser connection closes.
BlackBerry devices powered by Android	Device functionality	Allow computer to access device using Wi-Fi	Specify whether a computer can access content on the device using a Wi-Fi connection. If this rule is not selected, the computer can't access content on the device using a Wi-Fi connection and the device can't share media content with DLNA Certified devices.
BlackBerry devices powered by Android	Security and privacy	Force workspace and device password to be different	Force the workspace and device password to be different when the workspace password is required.
BlackBerry devices powered by Android	Security and privacy	Allow transfer of work data using NFC, Bluetooth and Wi-Fi Direct	Specify whether the user can transfer work data to another device using NFC, Bluetooth, and Wi-Fi Direct.
BlackBerry devices powered by Android	Security and privacy	Allow personal apps to use work networks	Specify whether personal apps on the device can use a work VPN or work Wi-Fi network to connect to the Internet. If this rule is not selected, personal apps can't use a work VPN or work Wi-Fi network to connect to the Internet and the BBM Video feature can't use work networks.

Device Type	Group	Name	Description
BlackBerry devices powered by Android	Security and privacy	Allow debugging work apps	Specify whether a debugging tool connected to the device can be used to debug work apps.
BlackBerry devices powered by Android	Security and privacy	Allow logging for work apps	Specify whether Android Debug Bridge and developer tools on the device can collect logs from work apps.
BlackBerry devices powered by Android	Security and privacy	Allow voice dictation in work apps	Specify whether the user can use voice dictation in work apps that support this feature.
BlackBerry devices powered by Android	Security and privacy	Allow Turn off work mode	Specify whether the user can disable the work profile using "Turn off work" mode. If "Turn off work" mode is enabled, BlackBerry UEM can't manage the work space on the device.
BlackBerry devices powered by Android	Security and privacy	Allow transfer of work contacts using Bluetooth	Specify whether the device can use Bluetooth to send work contacts to another Bluetooth enabled device.
BlackBerry devices powered by Android	Security and privacy	Allow transfer of work messages using Bluetooth	Specify whether the device can use Bluetooth to send work messages (for example, email messages and instant messages) to another Bluetooth enabled device.

What's new in BlackBerry UEM version 12.6 MR1

Synchronizing BlackBerry UEM and Good Control

- **Synchronizing with a Good Control server**: After you install BlackBerry UEM version 12.6 MR1 in an environment that has an existing Good Control server, you must synchronize Good Control with BlackBerry UEM to enable BlackBerry UEM version 12.6 MR1 features.

Caution: Once you synchronize the Good Control database, you cannot roll back to the original version.

For more information about this feature, see the Configuration content.

BlackBerry Dynamics Integration

- **Onboarding**: You can configure onboarding for users that will use only BlackBerry Dynamics apps.
- **App access keys**: You can generate and send access keys to users so they can activate BlackBerry Dynamics apps.
- **PKI connector:** You can set up a PKI connector that creates a connection between BlackBerry UEM and an internal CA to enroll certificates for BlackBerry Dynamics apps.
- **App Catalog in the BlackBerry Dynamics Launcher**: For devices that are enabled for BlackBerry Dynamics, you can add the work app catalog to the BlackBerry Dynamics Launcher so that users have quick access to a list of their assigned work apps.
- **Gatekeeping:** Gatekeeping is supported with BlackBerry Work when you manage BlackBerry Work in BlackBerry UEM.

For more information about these features, see the Administration content.

Management console

- **Compliance profile**: Several new rules are added to the Compliance profile for iOS, macOS, Android, and Windows devices. The new rules match the compliance policy rules available in BlackBerry Control, which allows you to re-create existing BlackBerry Control compliance policies in BlackBerry UEM.

For more information about these features, see the Administration content.

Licensing

- **BlackBerry Dynamics**: You must have the required SIM or server license to use BlackBerry Dynamics apps.

For more information about these features, see the Licensing content.

iOS

- **Manage notifications for apps on supervised iOS devices**: You can use per-app notification profiles to configure the notification settings for system apps and apps that you manage using BlackBerry UEM. Per-app notification profiles are supported for supervised iOS devices running iOS 9.3 or later.

For more information about these features, see the Administration content.

API changes

When BlackBerry UEM version 12.6 MR1 is integrated with a BlackBerry Control server, the following changes have been made to the BlackBerry Dynamics SOAP APIs:

- All BlackBerry Dynamics SOAP APIs (GC SOAP and CAP SOAP) that are not listed in the following tables have been removed
- All BlackBerry Dynamics MDM REST APIs have been removed
- BlackBerry Dynamics APIs will be available on BlackBerry UEM API port 18084 by default
- Port 18084 uses a different SSL certificate than the one that the BlackBerry Control server uses. API clients must trust the SSL certificate from BlackBerry UEM API port 18084
- Integrated mode does not support BlackBerry Control ‘policyset’. The BlackBerry UEM policies replace that functionality. All BlackBerry Dynamics APIs that managed the ‘policyset’ are impacted. Some are no longer supported and others cannot honor ‘policyset’ related input/output information.
- Integrated mode maps the BlackBerry Control ‘application group’ to the BlackBerry UEM ‘user group’. All BlackBerry Dynamics APIs that managed the ‘application group’ are impacted. Most APIs are supported but are implemented using the BlackBerry UEM ‘user group’ and there are a few that are no longer supported.

- APIs supported in integrated mode will not work with previously persisted entity Ids from a standalone BlackBerry Control server, such as userId, groupId, and containerId

Supported BlackBerry Control SOAP APIs

API Name	Behavior change
generateAccessKeys	Integrated mode uses a new default email template for sending email messages for access keys. Unless the administrator has updated the email template after upgrading to integrated mode, email messages might look different than the ones that BlackBerry Control sends in standalone mode. Any user Ids that the API client system previously persisted, do not work as the “userId” parameter value.
getAccessKeys	Any user Ids that the API client system previously persisted, do not work as the “userId” parameter value. Use the "getUser" API to retrieve the “userId” for users.
removeAccessKey	None
generateUnlockAccessKey	Any user Ids that the API client system previously persisted, do not work as the “userId” parameter value. Use the "getUser" API to retrieve the “userId” for users.
getUnlockAccessKeys	None
lockContainer	None
getActivatedContainers	Any user Ids that the API client system previously persisted, do not work as the “userId” parameter value. Use the "getUser" API to retrieve the “userId” for users.
deleteContainer	None
getDevices	Any user Ids that the API client system previously persisted, do not work as the “userId” parameter value. Use the "getUser" API to retrieve the “userId” for users.
getTempUnlockPassword	None
getAppInfo	The response does not include the “serverList” and “policySetId” elements. This information is not available or applicable in integrated mode.
getApps	The response does not include the “serverList” and “policySetId” elements. This information is not available or applicable in integrated mode.
getGPClusterList	None
getGPClusterServerList	None
getServerList	None
getUser	The response does not include “policySetId” and “policyName”. The “appsGroupCount” element represents the number of BlackBerry UEM user groups that the user belongs to.
sendPinEmail	Integrated mode uses a new default email template for sending email messages for access keys. Unless the administrator has updated the email template after upgrading

API Name	Behavior change
	to integrated mode, email messages might look different than the ones that BlackBerry Control sends in standalone mode.

Supported CAP SOAP APIs

API Name	Behavior change
AddGroup	The API creates the BlackBerry UEM user group. The request parameter “group_type” only supports the value of ‘e’ (Enterprise) and displays an error if you use any other values. The owner identifiers (“enterpriseId”/”organizationId”/”resellerId”) do not support accepting any value from the API client and display an error if you provide a value.
getGroups	The API returns the BlackBerry UEM user groups filtered by group name. The “member_count” in the response indicates the number of BlackBerry UEM users in the user group. The values supported for the “group_Type” parameter are: • E="Everyone" • e="All enterprise groups, except 'Everyone'" • null= "All Groups" The API displays an error if you provide an unsupported value for “group_Type”. The owner identifiers “enterpriseId”/”organizationId”/”resellerId” are not supported.
RemoveGroup	The API deletes the BlackBerry UEM user group. Any group Ids that the API client system previously persisted do not work as the “group_id” parameter value. The API performs checks to be consistent with integrated mode.
AddGroupsUsers	The API adds users to the BlackBerry UEM user groups. Any group Ids and user Ids that the API client system previously persisted do not work as request parameter values. If you set the “replace” parameter to ‘true’, users are removed from any other BlackBerry UEM user groups and are added to the newly specified BlackBerry UEM user group.
AddGroupUser	The API adds users to the BlackBerry UEM user group. Any group Ids and user Ids that the API client system previously persisted do not work as request parameter values.
removeGroupUser	The API removes users from the BlackBerry UEM user group. Any group Ids and user Ids that the API client system previously persisted do not work as request parameter values.
getGroupsForUser	The API returns a list of BlackBerry UEM user groups that a given BlackBerry UEM user is part of. Any user Ids that the API client system previously persisted do not work as request parameter values.
getUsersInGroup	The API returns a list of BlackBerry UEM users that are part of a given BlackBerry UEM user group. Any group Ids that the API client system previously persisted do not work as request parameter values.

API Name	Behavior change
getGroupPermissions	The API returns a list of BlackBerry Dynamics applications assigned to a BlackBerry UEM user group with appropriate permission dispositions (ALLOW and DENY). Any group Ids that the API client system previously persisted do not work as request parameter values. There are a few caveats: • app_version is not returned in the response • only applications with client_type = NATIVE_CONTAINER are supported • organization info is excluded from the response • app_realm value can only be 'E' for enterprise • app_type is 'G' for any apps that start with "com.good" or "com.blackberry" and 'O' for all others
setGroupPermission	The API assigns BlackBerry Dynamics applications with appropriate permission dispositions to a BlackBerry UEM user group. Any group Ids that the API client system previously persisted do not work as request parameter values. There are a few caveats: • app_version_id is not supported in the request • app_id must be provided in the request because the default permissions are not supported in integrated mode • only the following permission dispositions are supported: UNDEFINED, ALLOW, and DENY. UNDEFINED removes the application from the BlackBerry UEM user group
AddApp	The API adds a BlackBerry Dynamics application entitlement with app_type as 'O' (organization), app_realm as 'E' (enterprise), app_visibility as 'PRV' (private), and client_type as 'NativeContainer'. The API displays an error if the request parameters do not match. The API ignores the “purchase_url” request parameter.
RemoveApp	The API removes the BlackBerry Dynamics application entitlement from the system. The API displays errors if the removal fails because of BlackBerry UEM rules; for example, the application is already assigned to a user/group.
getApps	None

What's new in BlackBerry UEM version 12.6

Branding

- **Product name**: BES12 is now BlackBerry UEM.

Android

- **Android for Work**: Enterprise deployment and user enrollment for Android for Work is simplified in BlackBerry UEM. To support Android for Work devices, you no longer need to set up a Google domain and connect it to BlackBerry UEM. You must have the most recent version of the BlackBerry UEM Client installed on your organization's devices before you can use this feature. The first version of the client that will be compatible with this feature will be available in January 2017.
- **Password requirements**: For Android for Work devices running Android OS 7.0 or later, you can now enforce password requirements for work space apps as well as the device. In the management console, you can send commands to the device to specify a work space password.

For more information about these features, see the Administration content.

iOS

- **iOS device activation**: You can use Apple Configurator 2 to prepare devices for activation in BlackBerry UEM. Users can activate the prepared devices without using the BlackBerry UEM Client.
- **Lost Mode for supervised iOS devices**: Lost Mode allows you to lock a device, set a message that you want to display, and view the current location of the lost device. You can enable Lost Mode in BlackBerry UEM for supervised iOS devices running iOS 9.3 or later.
- **iOS Work Apps icon**: You can configure the iOS Work Apps icon so that users can view it in full screen mode on their devices.
- **iOS apps**: For supervised iOS 9.3.2 and later devices, you can specify a list of apps to allow on users' devices. All other apps can be installed but cannot be launched and will not be seen on devices. You can add any built-in apps directly to the allowed or restricted list in a compliance profile.
- **App configurations for iOS**: You can now create an app configuration from an XML template that uses the AppConfig schema, which is a standardized format defined by AppConfig Community, copy another app configuration, or create an app configuration manually.
- **Password autofill option for managed domains profiles**: Managed domains profiles include a new option to allow password autofill for the web domains that are specified in a profile. This option is supported for supervised iOS devices running iOS 9.3 or later.
- **Network usage profile**: When you configure the network usage profile, you now have the option to select apps from a list instead of typing the app package ID.
- **Wi-Fi profile – new QoS settings for iOS 10 devices**: For iOS 10 devices, you can configure QoS settings in Wi-Fi profiles to specify whether traffic can use L2 and L3 marking

For more information about these features, see the Administration content.

Device activation

- **Activate multiple devices**: You can let users activate multiple devices with different activation types by pairing activation passwords with activation profiles. For example, you might want users to activate work devices with a "full control" activation type and activate personal devices with an activation type that allows user privacy. You can now manually expire activation passwords at any time if required.
- **Device activation - certificate**: The device activation process for iOS and Android devices is streamlined. Users no longer need to verify and accept the certificate information to authenticate with BlackBerry UEM. This is now done automatically.

For more information about these features, see the Administration content.

Installation

- **Regional deployment**: You can set up regional connections for enterprise connectivity features by deploying one or more BlackBerry Connectivity Node instances in a dedicated region. This is known as a server group. Each BlackBerry Connectivity Node includes BlackBerry Secure Connect Plus, the BlackBerry Gatekeeping Service, the BlackBerry Secure Gateway Service, BlackBerry Proxy, and the BlackBerry Cloud Connector. You can associate enterprise connectivity and email profiles with a server group so that any users that are assigned those profiles use a specific regional connection to the BlackBerry Infrastructure when using BlackBerry Connectivity Node components. Deploying more than one BlackBerry Connectivity Node in a server group also allows for high availability and load balancing.

For more information about these features, see the Installation and upgrade content.

Management console

- **User list**: You can use Shift+click to select multiple users in the user list.
- **Rate and review apps**: You can specify whether users in your organization can rate and provide reviews of iOS, Android, and Windows 10 apps and see reviews provided by other users for internal custom apps or apps that are downloaded from public app storefronts. You must have the most recent version of the BlackBerry UEM Client installed on your organization's Android and Windows 10 devices before you can use this feature. The first version of the client that will be compatible with this feature will be available in January 2017.
- **Logging**: BlackBerry UEM can now generate log files where you can view phone call and SMS/MMS activity for Android for Work devices activated with “Work space only (Android for Work - Premium)” and Samsung KNOX Workspace devices activated with “Work and personal - full control (Samsung KNOX)” or “Work space only (Samsung KNOX)”. You must have the most recent version of the BlackBerry UEM Client installed on your organization's devices before you can use this feature. The first version of the client that will be compatible with this feature will be available in January of 2017.
- **Remove a Secure Work Space connection:** If you have an existing Secure Work Space connection, you can remove the connection and the menu item from the management console.

- **Restrict BlackBerry Secure Connect Plus to specific work space apps on Android for Work devices**: You can enable per-app VPN for Android for Work devices to restrict the use of BlackBerry Secure Connect Plus to specific work space apps that you add to an allowed list.
- **Additional options for Microsoft Active Directory connections**: When you specify key distribution center (KDC) domain controllers and global catalog servers, you can optionally include the port number that the domain controller uses (for example, kdc01.example.com:88). When you configure the Microsoft Active Directory account for each forest, you can also specify the KDC domain controllers and global catalog servers that you want BlackBerry UEM to use.
- **App deployment reports**: You can export app deployment reports to an .html file from the Apps screen in the management console. The report includes information about apps deployed by BlackBerry UEM and the users that have installed the apps on their devices.

For more information about these features, see the Administration content.

IBM Notes Traveler

- **IBM Notes Traveler support**: iOS devices can now connect to IBM Notes Traveler through BlackBerry Secure Gateway Service.

For more information about these features, see the Administration content.

BlackBerry Connectivity Node

- **The BlackBerry Connectivity Node now includes BlackBerry Proxy:** The BlackBerry Connectivity Node now includes the BlackBerry Proxy component. BlackBerry Proxy maintains a secure connection between your organization and the BlackBerry Dynamics NOC and also supports Direct Connect, which allows BlackBerry Dynamics app data to bypass the BlackBerry Dynamics NOC.

For more information about these features, see the Configuration content.

Ports

- **Updated port requirements:** BlackBerry UEM has new outbound port requirements to support connections to the BlackBerry Dynamics NOC, as well as new listening ports to support additional components like BlackBerry Control and BlackBerry Proxy.

For more information about these features, see the Installation and upgrade content.

Monitoring

- **Monitoring**: You can monitor the status of the BlackBerry Cloud Connector using SNMP.

For more information about these features, see the Administration content.

New IT policy rules

The following new IT policy rules are available in BlackBerry UEM version 12.6.

Device type	Group	Rule name	Description	Activation types
BlackBerry 10	Apps	Allow untrusted connections in browser	Specify whether a device can make untrusted connections to remote websites from the work browser. If this rule is selected, the device may prompt the user to accept a connection when the certificate is not trusted. If this rule is not selected, the device does not prompt the user when the certificate is not trusted and the connection to the remote website fails.	Work and personal - Corporate, Work space only, Work and personal - Regulated
BlackBerry 10	Security and privacy	Require VPN for IPPP traffic	Specify whether all data traffic using IPPP sent between devices and the BlackBerry Infrastructure via BlackBerry UEM must use VPN. If this rule is not selected, data traffic using IPPP sent between devices and the BlackBerry Infrastructure can use any available path.	Work space only, Work and personal - Regulated
BlackBerry 10	Security and privacy	Allow data over USB	Specify whether data traffic can travel over the USB interface of the device. If this rule is not selected, the device is only able to charge over the USB interface.	Work and personal - Corporate, Work space only, Work and personal - Regulated

Device type	Group	Rule name	Description	Activation types
BlackBerry 10	Security and privacy	Require NIAP Common Criteria functionality for browser	Specify whether NIAP Common Criteria functionality must be used by the browser. If this rule is selected, the web browsing experience may be degraded due to restrictions in permitted cipher suites.	Work space only, Work and personal - Regulated
iOS	Device functionality	Allow Bluetooth changes (supervised only)	Specify whether users can change the Bluetooth settings on the device.	MDM controls
Android MDM	Apps	Synchronize SMS/MMS logs	Specify whether the device synchronizes logs for SMS text messages and MMS messages with your EMM server.	Work space only (Samsung KNOX), Work and personal - full control (Work space only), Work space only (Android for Work - Premium)
Android MDM	Apps	Synchronize phone logs	Specify whether the device synchronizes the call log for the Phone app with your EMM server.	Work space only (Samsung KNOX), Work and personal - full control (Work space only), Work space only (Android for Work - Premium)
Android for Work	Password	Synchronize SMS/MMS logs	Specify whether the device synchronizes logs for SMS text messages and MMS messages with your EMM server.	Work space only (Samsung KNOX), Work and personal - full control (Samsung KNOX), Work space only (Android for Work - Premium)
Android for Work	Password	Password requirements	Specify the minimum requirements for a device password. If set to "Something," the user must set a	Work and personal - user privacy (Android for Work), Work and personal - user privacy

Device type	Group	Rule name	Description	Activation types
			password but there are no requirements for length or quality. If set to "Numeric," "Alphabetic," or "Alphanumeric," the password must contain at least the specified character types and can also include other character types. If set to "Complex," the password must contain at least a letter, number and special symbol. If set to "Numeric Complex," the password must contain numeric characters with no repeating sequence (4444) or ordered sequence (1234, 4321, 2468). If set to "Biometric Weak," the password allows for low-security biometric recognition technology.	(Android for Work - Premium)
Android for Work	Password	Maximum failed password attempts	Specify the number of times that a user can enter an incorrect work space password before the device is deactivated and the work profile is removed. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)

Device type	Group	Rule name	Description	Activation types
Android for Work	Password	Maximum inactivity time lock	Specify the number of minutes of user inactivity that must elapse before the device and work space lock. If you set a value for both this rule and the Native OS "Maximum inactivity time lock" rule, both the device and work space will lock when either timer expires. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Password expiration timeout	Specify the maximum amount of time that the work space password can be used. After the specified amount of time elapses, the password expires and the user must set a new password. If set to 0, the password does not expire. This rule takes effect only if the "Password requirements" rule is set to something other than "Unspecified."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Password history restriction	Specify the maximum number of previous passwords that a device checks to prevent a user from reusing a work space password. If set to 0, the device does not check	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)

Device type	Group	Rule name	Description	Activation types
			previous passwords. This rule takes effect only if the "Password requirements" rule is set to "Numeric," "Alphabetic," "Alphanumeric," "Complex," or "Numeric Complex."	
Android for Work	Password	Minimum password length	Specify the minimum number of characters that the work space password must contain. This rule takes effect only if the "Password requirements" rule is set to "Numeric," "Alphabetic," "Alphanumeric," "Complex," or "Numeric Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Minimum uppercase letters required in password	Specify the minimum number of uppercase letters that the work space password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Minimum lowercase letters required in password	Specify the minimum number of lowercase letters that the work space password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)

Device type	Group	Rule name	Description	Activation types
Android for Work	Password	Minimum non-letters in password	Specify the minimum number of non-letter characters (numbers or symbols) required in the password. This rule takes effect only if you set the "Password requirements" rule to "Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Minimum letters required in password	Specify the minimum number of letters that the work space password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Minimum numeric digits required in password	Specify the minimum number of numerals that the work space password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Password	Minimum symbols required in password	Specify the minimum number of non-alphanumeric characters that the work space password must contain. This rule takes effect only if you set the "Password requirements" rule to "Complex."	Work and personal - user privacy (Android for Work), Work and personal - user privacy (Android for Work - Premium)
Android for Work	Device functionality	Allow searching work contacts from personal apps	Specify whether users can search work contacts from apps that	Work and personal - user privacy (Android for Work), Work and personal - user privacy

Device type	Group	Rule name	Description	Activation types
			are not in the work profile.	(Android for Work - Premium)
KNOX MDM	Password	Require lock screen message	Specify whether you set a message to display when the device is locked. If this rule is not selected, the user can choose a message to display on the lock screen.	MDM controls, Work and personal - full control (Samsung KNOX)
KNOX MDM	Password	Lock screen message	Specify the text to display on the device when the device is locked.	MDM controls, Work and personal - full control (Samsung KNOX)
KNOX MDM	Security and privacy	Allow users to deactivate devices	Specify whether the user can deactivate the device and wipe all work data.	MDM controls, Work space only (Samsung KNOX), Work and personal - full control (Samsung KNOX)
KNOX Premium - Device	Security and privacy	Validate end-user installed certificates	Specify whether the device validates certificates installed by end users. If one of the validation checks (for example, certification path, expiration date, or revocation status) fails, the device blocks the installation of the certificate.	Work space only (Samsung KNOX), Work and personal - full control (Samsung KNOX)
Windows	Device functionality	Update installation day	Specify the day that updates are installed. The default is “every day”. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Device functionality	Update installation hour	Specify the hour of the day that updates are installed. The value corresponds to a 24-	MDM controls

Device type	Group	Rule name	Description	Activation types
			hour clock where 0 represents 12 AM. This rule does not apply to Windows 10 smartphones.	
Windows	Device functionality	Active hours start	Specify the start of the range of hours when the user is usually active and Windows update reboots are not scheduled. The value corresponds to a 24-hour clock where 0 represents 12 AM. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Device functionality	Active hours end	Specify the end of the range of hours when the user is usually active and Windows update reboots are not scheduled. The value corresponds to a 24-hour clock where 0 represents 12 AM. This rule does not apply to Windows 10 smartphones.	MDM controls
Windows	Device functionality	Lock screen image provider	Specify the package ID of the lock screen image provider. If you don't set this rule, the user can set the lock screen image. This rule does not apply to Windows 10 computers and tablets.	MDM controls
Windows	Security and privacy	Send activation data to Microsoft	Specify whether the device can send data about its activation	MDM controls

Device type	Group	Rule name	Description	Activation types
			state to Microsoft. This rule applies to Windows 10computers and tablets and to smartphones with Windows 10 Mobile Enterprise.	
Windows	Security and privacy	Allow device to accept pairing and privacy consent prompts	Specify whether the device can automatically accept pairing and privacy user consent prompts when launching apps. If this rule is not selected, the user must manually accept the prompts.	MDM controls
Windows	Security and privacy	Enable Microsoft advertising ID	Specify whether the Microsoft advertising ID is enabled on the device.	MDM controls

REST API changes

For more information about the REST APIs, see the BlackBerry UEM 12.6 REST API Reference.

New REST APIs

API Name	Behavior
Create user	The API creates a user with basic user attributes. The new user gets a self-service role in BlackBerry UEM and is added to the “All Users” group. The new user also receives default policies. By default, the user is enabled for MDM service, but the API allows you to disable MDM service. Note that the BlackBerry Control SOAP API ‘addUser’ is removed and the Create user API provides the required functionality.
Assign policy to user	The API allows assigning: • a policy to one or more users • one or more policies to a user

API Name	Behavior
	Note that the BlackBerry Control SOAP API 'changePolicyUser' is no longer available. The Assign policy to user API provides the required functionality.
Assign policy to group	The API allows assigning: • a policy to one or more user groups • one or more policies to a user group
Replace policies for a user	The API replaces all policies assigned to a user with a new set of policies.
Replace policies for a group	The API replaces all policies assigned to a user group with a new set of policies.
Query policies	The API allows querying policies by: • profile category • user id which returns all profiles assigned to user • group id which returns all profiles assigned to user group Note that the BlackBerry Control SOAP API 'getAllPolicies' is no longer available. The Query policies API provides the required functionality.
Query user groups	The API allows querying user groups by: • group id • group name • profile id which returns all user groups that the profile is assigned to • user id which is assigned to a user group
Assign compliance/security policies to BlackBerry Dynamics app	The API allows assigning compliance and security policies to a BlackBerry Dynamics application entitlement. Note that the BlackBerry Control SOAP API 'changePolicyApp' is no longer available. The Assign compliance/security policies API provides the required functionality
Query activation email templates	The API allows querying activation email templates.
Create device activation password	The API allows creating a device activation password for a user.

Fixed issues

5

This section contains a list of all the issues that have been fixed since the release of BlackBerry UEM version 12.5.

Fixed issues in BlackBerry UEM 12.6 MR3

Installation, upgrade, and migration fixed issues

When you upgraded to BlackBerry UEM version 12.6, the db.properties file might have been overwritten and any mirroring settings in the file might have been lost. (JI 1656979)

Synchronization of Good Control with BlackBerry UEM fixed issues

If you had only one policy set configured in Good Control, after the synchronization of Good Control with BlackBerry UEM was complete, the policy set was not synchronized with BlackBerry UEM. (JI 2155743)

After the synchronization of Good Control with BlackBerry UEM was complete, if you were using Internet Explorer 11 when you opened the Managed devices page, BlackBerry Dynamics apps did not display. (JI 1678646)

For BlackBerry Dynamics apps, hosted binary names displayed alongside BlackBerry Dynamics entitlement names after a sync between Good Control and BlackBerry UEM. (JI 1671642)

User and device management fixed issues

When you removed a binary for an app, a reconciliation rule was not triggered to remove the app from the device. (JI 2156286)

A parse exception might have occurred on the BlackBerry UEM Core when it processed the installed application list from an iOS device. (JI 1687554)

A null pointer exception might have occurred in the BlackBerry UEM Core while it processed a managed application configuration result sent from an iOS device. (JI 1683540)

On an iOS device, when you selected the "Require device management to use BlackBerry Dynamics apps" option in the BlackBerry Dynamics profile, after a user had activated BlackBerry Access using an email address and activation key, and performed an MDM enrollment, when the user started BlackBerry Access, they were prompted for an email address and access key again. (JI 1684366)

A null pointer exception occurred in the BlackBerry UEM Core when an iOS device queried BlackBerry UEM for available OS updates. (JI 1683479)

When expired activation passwords existed in the database, they might have caused non-expired passwords to fail when a user tried to activate a device. (JI 1678237)

After an upgrade of the BlackBerry UEM Client, the user had to accept the IBM Verse app license agreement and re-enter the password for the app. (JI 1535779)

Management console fixed issues

After you added an entitled app, when you navigated to the Apps page and clicked Update apps, the entitled apps that you added might not have displayed. (JI 2155571)

When you created a BlackBerry Dynamics connectivity profile, if you clicked Add in the App servers section and selected a BlackBerry Dynamics app and clicked Save, when you clicked Add at the bottom of the profile page, an error message displayed. (JI 2148088)

When you created a BlackBerry Dynamics profile, if you selected the "Require password when BB Dynamics apps start" option and you also set an app to be an Authentication delegate, no error message displayed. (JI 2143601)

If your organization did not use a TLS connection, when you navigated to Settings > External integration > SMTP server, and set the Supported encryption type option to "Automatic detection of TLS support", when you clicked Test connection, an error displayed. (JI 1696396)

If you used Microsoft Edge to log in to the management console, you might not have been able to use drop-down lists to select options. (JI 1689423)

When you were on the Apps page, if you tapped on a BlackBerry Dynamics app to view the app details, an error message displayed that stated no app details were available. (JI 1681445)

On the Infrastructure page, the incorrect version numbers displayed for the BlackBerry Control service and the BlackBerry Proxy service. (JI 1681317)

After adding an entitlement for a custom BlackBerry Dynamics app, you could not manage the app until the app source files had been uploaded. (JI 1671706)

You could not save any changes to a company directory if any of your domain controllers were unavailable. (JI 1620572)

Fixed issues in BlackBerry UEM 12.6 MR2

Installation, upgrade, and migration fixed issues

After you upgraded to BlackBerry UEM 12.6 MR1 and performed the synchronization of Good Control with BlackBerry UEM, Kerberos Constrained Delegation did not work for BlackBerry Dynamics apps. (JI 1700208)

When you performed the synchronization of Good Control with BlackBerry UEM, a NullPointerException occurred when the BlackBerry UEM Core was retrieving a directory email address that did not have a Microsoft Active Directory mailbox. (JI 1692856)

When you had Good Control and Good Proxy installed on a server and you upgraded to BlackBerry UEM version 12.6, on the Ports screen of the setup application, the Required Ports might have displayed as unavailable. (JI 1660808)

Synchronization of Good Control with BlackBerry UEM fixed issues

After you performed the BlackBerry Control synchronization with BlackBerry UEM 12.6 MR1, if you set the BlackBerry UEM Client as the authentication delegate, the BlackBerry Dynamics compliance profile might have caused the BlackBerry UEM Client to repeatedly stop responding. (JI 2154991)

After the synchronization of Good Control with BlackBerry UEM 12.6 MR1 was complete, app groups that were configured in Good Control were recreated as user groups in BlackBerry UEM and app policies that were configured in Good Control were recreated as app configurations in BlackBerry UEM.

After synchronization, app policies that were assigned to app groups in Good Control remained assigned to users as they were before the synchronization; however, when you viewed the recreated user groups in BlackBerry UEM, an incorrect app configuration was shown in the Assigned apps table for the user group. (JI 1675134)

Note that this is still an issue if you synchronized Good Control with BlackBerry UEM 12.6 MR1. For more information, see KB39080.

This issue is fixed when you synchronize Good Control with BlackBerry UEM using BlackBerry UEM 12.6 MR2. For more information, see KB39080.

After you started the synchronization of Good Control with BlackBerry UEM, a Ready page might have displayed for a few moments before the sync progress screen displayed, and the Start synchronization button might have displayed again. (JI 1685179)

User and device management fixed issues

When you activated an Android device using the Android for Work with work space only activation type and no Google domain, a fake Google account was created on the device. When the user finished enrolling the device, the fake account was not removed and apps were not pushed to the device. (JI 1694616)

On iOS devices, it took a long time to update internal apps and the update might not have happened automatically. (JI 1691422)

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

Management console fixed issues

When you created a BlackBerry Dynamics profile and you did not select the “Do not allow copying data from non BlackBerry Dynamics apps into BlackBerry Dynamics apps” option, after you assigned the profile to a user, some BlackBerry Dynamics apps did not behave as expected. (JI 1691051, JI 1675839)

When you created or edited an OCSP profile, invalid characters such as "???scope.ocsp.OCSP.BB.settings.hostUrl???" displayed on the page. (JI 1687138)

On the Apps page, the scroll bar disappeared when you sorted by the "App rating" column header. (JI 1670473)

Onboarded Microsoft Active Directory users did not receive the custom email message that you selected on the Sync settings tab (Settings > External integration > Company directory). (JI 1666094)

The introductory text in the Certificate Retrieval, CRL, and OSCP profiles stated that the profiles applied to BlackBerry devices powered by Android. However, you could not apply the profiles to BlackBerry devices powered by Android. (JI 1649625)

Fixed issues in BlackBerry UEM 12.6 MR1

Installation, upgrade, and migration fixed issues

In a new installation of BlackBerry UEM, emails with access keys for BlackBerry Dynamics apps were not sent to users. (JI 1656425)

After you upgraded from BES12 version 12.5 MR2 to BlackBerry UEM version 12.6, BlackBerry Dynamics apps might have disappeared. (JI 1591544)

User and device management fixed issues

If you assigned BlackBerry Dynamics apps to a device before you activated the device, the apps were not assigned after the activation completed. (JI 1658991)

After an upgrade of the BlackBerry UEM Client, when a user tried to open the IBM Verse app, the server name and user name were not prepopulated. (JI 1654896)

On Windows 10 devices, the message that displayed when a compliance violation occurred stated that the activation of the device was successful when the activation was actually not successful. (JI 1643283)

On an iOS device, during an upgrade of the BlackBerry UEM Client, the client was referred to as Good for BES12. (JI 1630680)

Users could not activate an unsupervised iOS device that was activated with the MDM activation type because in certain circumstances, the device did not send the ActivationLockByPassCode to BlackBerry UEM. (JI 1624483)

Management console fixed issues

When you had two instances of BlackBerry UEM 12.6 in your environment and you upgraded both instances to BlackBerry UEM 12.6 MR1, if you navigated to Settings > External integration > Android for Work on one of the instances and clicked "Remove Android for Work Connection", the connection might not have been removed. (JI 1673609)

If you configured BlackBerry UEM to support Android for Work and then you removed the Android for Work connection and you removed any information from Google Play for Work, if you then reconfigured the connection and tried to update apps, an error message displayed. (JI 1660788)

When you tried to remove a nested group from a user group, an error message displayed. (JI 1656997)

After you assigned a Good Dynamics profile to a user, when you clicked on "Set activation password" on the User page, in the "Set device activation password" screen the "Access key expiration" and "Email template" drop-down lists displayed and after you clicked "Submit", the access keys were not sent to the user. (JI 1657635)

If you turned on debug logging in the console, the work apps on iOS devices took a long time to load. (JI 1655531)

If you had configured multiple App servers in a BlackBerry Dynamics Connectivity profile, if you removed one of the App servers from the profile and clicked Save, all of the App servers were not removed from the profile. (JI 1643189)

When you added apps from the Apple App Store or Google Play, they might have been added as BlackBerry Dynamics apps and you could not push the apps to non-BlackBerry Dynamics users. (JI 1641959)

In the Compliance profile, under the "Connectivity verification" option, the "Allow authentication delegation" option displayed. However the option should have been named "Base connectivity interval on auth delegate apps". (JI 1635123)

In the Good Dynamics profile, the "Android Fingerprint for Idle Unlock" option did not display. (JI 1634984)

When you were using Internet Explorer 11 to view the management console, when you navigated to the device summary page, no personal apps displayed. (JI 1625357)

Fixed issues in BlackBerry UEM 12.6

Security fixed issues

A vulnerability in the BES12 Core could have allowed a potential attacker to enroll an illegitimate device to BES12, gain access to device parameters for BES12, or send false information to BES12, if the requirements were met for exploitation. This issue is addressed in KB38913: BSRT-2017-001 Vulnerability in BES Core impacts BES12.

A vulnerability in BES12 could have allowed a potential attacker to obtain local or domain credentials of an administrator or user account, if the requirements were met for exploitation. This issue is addressed in KB38914: BSRT-2017-002 Information disclosure vulnerability affects BES12.

Installation, upgrade, and migration fixed issues

If you installed BES12 on one server and integrated with Good Control on another server, if you upgraded the BES12 server to BlackBerry UEM before you upgraded the original Good Control server, the Good Control service might not have started. (JI 1637561)

When you installed BlackBerry UEM 12.6, if you typed an FQDN that ended with ".LOCAL" in the hostname field, an error message displayed. (JI 1625906)

During installation, when you saved the proxy port and proxy domain parameters, the parameters were reversed in the gps.properties file, causing BlackBerry Proxy to not start. (JI 1617539)

When you were performing a new installation of BlackBerry UEM 12.6, the port check for port 17443 failed even though the port was free. (JI 1616172)

When you attempted to upgrade from BlackBerry Proxy to BlackBerry Connectivity Node, the upgrade might have failed. (JI 1610591)

After you upgraded from BlackBerry Proxy to BlackBerry Connectivity Node, if you tried to stop the BlackBerry Connectivity Node an error displayed in the GPS logs and two instances of prunrsv.exe were started. (JI 1606689)

The setup application did not check for available hard disk space before installing the software. If you did not have enough space available the installation did not complete. (JI 1605382)

After you upgraded from a BlackBerry Control server to BlackBerry UEM 12.6, entries for BlackBerry Proxy Server and BlackBerry Control were still listed in the Windows Control Panel. (JI 1603604)

During installation, the setup application did not check if a database existed. If a database did exist the installation failed. (JI 1599804)

After you upgraded from BES12 version 12.4.x, iOS apps that were deployed with the "Do Not Convert" option were removed. (JI 1553783)

After you upgraded to BlackBerry UEM 12.6, the BlackBerry UEM Core might have encountered issues such as transaction timeouts, transaction failures, and NullPointerExceptions. (JI 1524971)

User and device management fixed issues

After you assigned a proxy profile to an enterprise connectivity profile and assigned the profile to an iOS device, on the device the profile displayed as a Global HTTP Proxy. (JI 1647869)

After you enrolled a DEP device, when you clicked 'Compliant' in the BlackBerry UEM Client to view the compliance report, a blank page displayed. (JI 1641459)

When you clicked 'Update device information' in the management console, the BlackBerry UEM Client might have become unmanaged. (JI 1636020)

If you were using an Android device that had the BlackBerry UEM Client installed, when you activated the device using the MDM activation type and the device had a Good Dynamics profile assigned, the activation might have failed and the following error message might have displayed: "BB Dynamics Work environment could not be configured- configure-Retry/close". (JI 1635975)

If you navigated to Settings > App management > Internal app storage, and set a Network location for internal apps, when you tried to add an internal app an error message displayed. (JI 1614947)

You could not always create access keys in BlackBerry UEM Self-Service. (JI 1614650)

On the Device tab, in the License information section, "No licenses found" displayed even though the device was using a license. (JI 1583667)

During a new activation of an iOS 10 device, an error occurred and the activation was unsuccessful. (JI 1583454, JI 1547950)

The Android for Work app configuration page did not display. (JI 1577401)

You could select one or more users to remove from the All users group. (JI 1546460)

When you created a new activation email template or compliance violation email template, if you used the same name as an existing template, the error message that displayed contained unreadable text. (JI 1539595)

When a device that was running iOS 9 or later was activated with the “User privacy” or “Work and personal - user privacy” activation type and you selected the “Allow access to SIM card and device hardware information to enable SIM-based licensing” checkbox, apps sent to the device were not displayed. (JI 1538701)

When a user started the IBM Verse app on a Samsung KNOX device, the servername and username fields were not prepopulated. (JI 1526488)

BlackBerry UEM did not add the Android version of the BlackBerry UEM Client as a required app and therefore users that were activated with an Android for Work activation profile did not receive any BlackBerry UEM Client updates. (JI 1523047)

After you created an internal app directory for Windows 10 apps, when you tried to add apps to the directory a warning message displayed at the top of the page that stated that you must specify a network location. (JI 1519271)

After you pushed the BlackBerry UEM Client client from BlackBerry UEM to an iOS device, when the user opened the client to perform a migration, the client did not detect the BlackBerry UEM configuration for migration and instead automatically started to activate. (JI 1542925, JI 1469968)

Management console fixed issues

You could not remove a Safari domain from an enterprise connectivity profile. (JI 1651476)

When you navigated to Settings > Infrastructure > Instances, the version numbers that displayed for the management console, BlackBerry Control, and BlackBerry Proxy were incorrect.(JI 1640976)

You could not add an internal app if the app name contained an apostrophe ('). When you clicked on Apps > Add an app > Internal app and then browsed to your app and clicked Add, a blank page displayed. (JI 1637185)

After you opened a user's page, and you clicked the BlackBerry Dynamics access keys link, then clicked the Send icon, and on the Resend access key screen you clicked Send, the user did not receive an email message that contained the new access key. Also, the user received two activation email messages. (JI 1634671)

On the user details page, in Advanced view, the version number of the BlackBerry UEM Client Client did not display for activated iOS devices. (JI 1612468)

When you navigated to Settings > Migration > Configuration, on the Add a source page, in the Source type list, there were only two choices available: BES10 and BlackBerry UEM. (JI 1605318)

After you added a VPP account and apps for the VPP account, you could not access the apps. Also, when you tried to access the account the following message displayed: "Please wait while the VPP Store is contacted to retrieve licensing information", and the account information never displayed. (JI 1596686)

You might not have been able to use your credentials to log in to the management console using Microsoft Active Directory authentication. (JI 1582944)

When you navigated to Settings > Licensing > Licensing Settings, the date and time in the Last contact time with licensing infrastructure field was incorrect. (JI 1563972)

When you used the Work space only (Android for Work - Premium) activation type to activate an Android device and you selected the Android for Work email activation template, the instructions in the email message that the user received only applied to Android 5.x devices. (JI 1562341)

When you added an iOS app to the app list, if you set the "Convert installed personal app to work app" field to "Convert", and then you refreshed the list, the setting changed to "Do not convert". This caused previously deployed apps to be removed from the user's device. (JI 1553855)

If you edited a Certificate retrieval profile to add another Service URL, when you clicked Add an error message might have displayed. (JI 1549578)

If you navigated to Settings > External integration > Microsoft Exchange gatekeeping and added a new Microsoft Exchange gatekeeping configuration, after you filled out all the fields and clicked Test connection, a Connection failed message displayed. However, the new gatekeeping instance that you configured worked, it was only the Test connection functionality that did not work. (JI 1545191)

When BlackBerry UEM was connected to a BlackBerry Control server that was in a BlackBerry Control server cluster, if any of the BlackBerry Control servers were unavailable when you set up BlackBerry Dynamics for an iOS or Android device, BlackBerry Dynamics apps might not have been sent to the device and the BlackBerry Dynamics column on the Managed devices page might have displayed "assigned" instead of "configured" for the device. (JI 1544063)

If you were using LDAP, when you were configuring the synchronization settings for company groups, the Activation email template drop-down list did not contain any options. (JI 1543149)

If you configured a Good Dynamics profile, when you selected more than 20 users to send an activation email message to, and you clicked the Autogenerate Good Dynamics access key and send email with instructions option, and set the Number of access keys to generate to 5, when you clicked Send an error message displayed. (JI 1535245)

If you navigated to Settings > App management > Work apps for iOS, and you tried to add a Web icon, an error displayed. (JI 1534177)

If you were using Google Chrome or Mozilla Firefox to view the management console, on the Device page for a user after you clicked View device report, you could not export the device report. (JI 1533428)

When you assigned a role to a user through a group, if the user logged in to the console and clicked the user icon in the upper right hand corner, the user's role name did not display. (JI 1531286)

If you had configured your BlackBerry UEM so that when you created Android for Work users in BlackBerry UEM you also created user accounts in your Google Cloud domain, after you created some users in BlackBerry UEM all of those users might not have been created in the Google Cloud domain. Also, when you deleted users in BlackBerry UEM they might not have been deleted from the Google Cloud domain. (JI 1524871)

When you created a device group and you changed the Value field to Model, if one of the device model names contained an apostrophe, such as the Porsche Design P'9982, when you clicked Save a 500 Internal Server error displayed. (JI 1522346)

BlackBerry Secure Connect Plus fixed issues

When you created an enterprise connectivity profile with the "Enable per-app VPN" and "Allow apps to connect automatically" options selected, and you assigned Google Chrome with per-app VPN to the device, and you assigned the profile to an iOS device, the device might not have connected through BlackBerry Secure Connect Plus. (JI 1632598)

BlackBerry Router fixed issues

The BlackBerry Router might have stopped responding when it was trying to reconnect with the BlackBerry Infrastructure. (JI 1547910)

BlackBerry Connectivity Node fixed issues

After you reinstalled the BlackBerry Connectivity Node, if you navigated to Settings > External integration > BlackBerry Connectivity Nodes, the friendly name of the BlackBerry Connectivity Node that displayed was incorrect. (JI 1533818)

BlackBerry Secure Gateway Service fixed issues

Mail flow was delayed or stopped for iOS device users connecting through the BES12 BlackBerry Secure Gateway Service. (JI 1649003)

BlackBerry Web Services fixed issues

The GetUsers() call might have timed out if you used the LastUserUid property, which caused BlackBerry Web Services to return all users. (JI 1558055)

Known issues

6

Installation, upgrade, and migration known issues

If your organization's environment includes more than one Good Control server and you upgrade a Good Proxy server to BlackBerry UEM, the upgrade will fail if the Good Proxy server's primary Good Control server is not already upgraded and running. For more information see KB44771. (JI 2178154)

When you try to upgrade Good Proxy to BlackBerry UEM, the upgrade might fail because port 17443 might be appended to the gc.server.uri field multiple times in the gps.properties file. (JI 2178125)

Workaround: In c:\good\gps.properties, remove each port instance from the gc.server.uri field, and try the upgrade again.

If you upgrade from BES12 version 12.5 MR1 to BlackBerry UEM, the BlackBerry Router service might be listed twice on the Windows services page; once as "BES12 – BlackBerry Router" and once as "BlackBerry UEM - BlackBerry Router". (JI 2167075)

BlackBerry Control cannot configure a new BlackBerry Proxy server if another unconfigured BlackBerry Proxy server exists in the database with the name "NOT_REGISTERED". For more information see KB39200. (JI 2156273)

If you upgrade from BES12 version 12.5 MR1 to BlackBerry UEM 12.6 MR3, the BlackBerry Secure Connect Plus service might not start. (JI 1686910)

Workaround: Restart the Windows server where you installed the BlackBerry UEM software.

If you upgrade from BES12 version 12.5 MR1 to BlackBerry UEM 12.6 MR3, the BlackBerry Cloud Connector service might be listed on the Windows services page. (JI 1686860)

Workaround: Disable the BlackBerry Cloud Connector service.

If you have the BlackBerry UEM management console and Good Proxy installed on the same virtual machine and you upgrade to BlackBerry UEM 12.6 MR3, the Good Proxy service is stopped but it is not removed. (JI 1685395)

After you install BlackBerry UEM, on the Windows services page, the BlackBerry UEM Router is named BES12 – BlackBerry Router. (JI 1683598)

When you use the setup application to upgrade to BlackBerry UEM 12.6 MR3, on the Ports screen a red X icon might display beside the Required ports section even when the ports are available. (JI 1682985)

Workaround: Click "Check again".

When you migrate more than 1000 users from BES10 to BlackBerry UEM 12.6 MR3, the migration might fail. (JI 1676361)

Workaround: Migrate a maximum of 500 users at a time.

After you upgrade from Good Control to BlackBerry UEM, you cannot delete the old compliance profile from the management console. (JI 1647729)

If you have the Good Proxy server folder nested inside the Good Control server folder, when you upgrade to BlackBerry UEM, the upgrade will fail. (JI 1638535)

After you install BlackBerry UEM version 12.6, if you try to stop or restart the BlackBerry UEM Core an error message displays. (JI 1532799)

Workaround: The BlackBerry UEM Core will eventually stop even though the error message displays. If you were trying to restart the service, you will have to start the service manually after it stops.

The installation of the software will not complete if your domain name contains an ampersand (&). (JI 1532095)

Synchronization of Good Control with BlackBerry UEM known issues

After the synchronization of Good Control with BlackBerry UEM is complete, app groups that have no users assigned do not display the apps that were assigned to the group before the synchronization started. (JI 1681782)

User and device management known issues

Currently Proxy configuration with PAC files does not work for iOS devices. Proxy configuration for iOS devices must use manual configuration with an IP address. (FIRST-12273)

If you host a private app on BlackBerry UEM and you publish the JSON file on the Google Play Store, the app won't install on devices running Android OS 7.x.(JI 2168718)

Workaround: Upload the app as an .apk file to the Google Play Store.

If a user is using an Android device with the BlackBerry UEM Client and BlackBerry Work installed, when the user enters the user certificate password, if the certificate is not configured correctly, a user credential profile record is added to the user's profile in the management console. (JI 2158288)

If a device is not pre-encrypted by a manufacturer, when you activate the device using the Android for Work with work space only activation type and no Google domain, a fake Google account is created on the device, and device enrollment fails and the following message displays: Google Play Store and Google Play Services may be outdated. (JI 2146318)

If you create a BlackBerry Dynamics profile and you do not select the "Allow use of client certificates" option, and you also create a User credential profile, when a user tries to open the BlackBerry Access app on a device, they are prompted to enter a password and the app will not enroll even when the password is correct. (JI 1675832)

If you select the "Allow use of client certificates" option when you create a BlackBerry Dynamics profile, and you allow your BlackBerry Dynamics apps to use user certificates and user credential profiles, if the user enters an incorrect password and then closes the app, when the user restarts the app the password screen might not display again. (JI 1675826)

On an iOS device, after you update a custom BlackBerry Dynamics app, the Update button still displays and the version number is truncated. (JI 1671601)

When you are activating an Android for Work device, if you exceed the limit of allowed users in the Google domain, the device is left in a partially activated state. (JI 1644881)

Workaround: Deactivate the device, and before you attempt to reactivate the device, ensure you have enough room in the Google domain for the user.

When you are downloading apps on an iOS device, the apps might not finish downloading and the following error message might display in the log files: An established connection was aborted by the software in your host machine. (JI 1639292)

BlackBerry UEM cannot synchronize apps on Windows 10 devices if the app is a legacy app that uses the XAP file type. (JI 1531748)

Workaround: Remove the apps from BlackBerry UEM. Users must go to the Windows store and download and install the apps.

When the BlackBerry 2FA server returns HTTP status code 403 to an iOS device, the device stops responding for 30 seconds before reporting the error to the user. (JI 1520503)

Management console known issues

In a BlackBerry UEM 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 BlackBerry UEM and activate a BlackBerry OS device for the user, the BlackBerry OS device information does not display in the BlackBerry UEM management console.

When you are creating a Network usage profile, after you click on the plus sign (+) and you click "Add an app", it might take a long time for the list of apps to load, and the same app might be listed multiple times. (JI 2182214)

The "Manage BlackBerry Dynamics apps" permissions do not work if you select the "Selected groups only" option when you create or edit an administrator role. (JI 2174586)

When you navigate to Settings > BlackBerry Dynamics > Clusters and you create a cluster with a space in the name, if you create a Connectivity (BlackBerry Dynamics) profile and you use the cluster with the space in the name as one of the BlackBerry Proxy clusters, you cannot edit and save the profile. (JI 2171642)

Workaround: Edit the cluster name so that it does not have a space in the name.

When you create a compliance profile, if you select the "Required Security patch level is not installed" option on the Android tab, no plus sign button (+) displays so you cannot add any security patches. (JI 2162863)

If you are using Internet Explorer 11 to use the management console, if you edit a BlackBerry Dynamics app, you cannot save the changes. (JI 2162439)

Workaround: Use Google Chrome or Mozilla Firefox to edit a BlackBerry Dynamics app.

If you disable the “View VPN options” setting when you create an administrator role, after you assign the role to an administrator, an error will display when the administrator clicks on a user that has a VPN profile assigned to them. (JI 2154331)

Workaround: Select the View VPN options setting when you create an administrator role.

If you use Microsoft Edge to view the management console, when you navigate to Settings > BlackBerry Dynamics > App services and click one of the services, then click the back arrow, the Edit app section displays below the app list. (JI 2146075)

When you create a VPN profile and set the "Connection type" to "IKEv2", after you assign the profile to an iOS device, the xml payloads from BlackBerry UEM might not match the xml payloads from Apple Configurator and the VPN connection does not work. (JI 2141874)

When you use Safari to view the management console, the vertical scrollbar is invisible. However, you can click and drag the scrollbar. (JI 1699213)

When you navigate to Settings > BlackBerry Dynamics > Properties, the “Enable job to automatically remove duplicate containers(on/off)" option is selected. If you deselect the option and click Save the option is turned off in the console and in the database. If you then select the option again, the option is turned on in the console but not in the database. (JI 1697835)

When you create a BlackBerry Dynamics profile, if you set BlackBerry Work as primary, BlackBerry Access as secondary, and BlackBerry Connect as tertiary in the App authentication delegation section and you set the “Require password after period of inactivity” to 3 minutes, after the user activates BlackBerry Access on a device, if the user taps on the launcher in BlackBerry Access and taps on the email link to open BlackBerry Work, after the user logs in, the device switches back to BlackBerry Access. (JI 1695800)

If you create a .csv file that includes a user group with the Enterprise Identity app assigned, and use the file to import a user, in the console the user does not display as able to use Enterprise Identity. (JI 1691330)

Workaround: Remove the user from the group, and then add the user back to the group.

The icons for the BlackBerry UEM Client and BlackBerry Connectivity apps have not been updated to the new versions. (JI 1691174)

When you create a company directory connection, if you select the “Enable onboarding” and “Onboard user with BlackBerry Dynamics apps only” options, if you then remove the “Enable onboarding” option and click Save, an error displays. (JI 1690338)

Workaround: Deselect the “Onboard user with BlackBerry Dynamics apps only” option before you click Save.

After you complete the synchronization of Good Control with BlackBerry UEM, if you delete the BlackBerry Dynamics PKI authentication certificate that is created when you performed the synchronization and you navigate to Settings > External integration > Certification Authority and test the connection for the BlackBerry Dynamics PKI connection, the connection fails. (JI 1689126)

Workaround: Upload the BlackBerry Dynamics PKI authentication certificate again.

After you create a BlackBerry Dynamics internal app, if you open the App and click "Upload a template", an error displays. (JI 1688040)

When you are adding a compliance profile, the list of restricted OS versions for OS X does not include build numbers which causes the OS X device to display as Unknown in the OS column on the device page. (JI 1686893)

Some BlackBerry Dynamics apps might display in the app list even if they are unavailable. When you click on one of the apps, an error message displays. (JI 1686386)

When you create a compliance profile that has the same name as an existing profile, after you click Add, the page does not display correctly. (JI 1685537)

If you navigate to Settings > BlackBerry Dynamics > Clusters, and rename one of the clusters and click Save, the change is not saved. (JI 1685129)

If you navigate to Settings > BlackBerry Dynamics > App services, and edit one of the services, after you click Save, the changes are not saved. (JI 1685056)

You cannot create a compliance profile for OS X devices when you select the following options: (JI 1682757)

- "Restricted device model detected"
- Set the "Device model restrictions" list to "Do not allow device selected device models"
- After you click Edit, set the Restricted device model list to "iMac"
- Set the "Enforcement action" list to "Delete all data"
- Do not enter any data in the "Find my Mac PIN" field

If you try to replace directory groups that are associated with your organization's LDAP company directory, the directory groups for your organization's Microsoft Active Directory company directory are removed. Also, if you try to replace directory groups that are associated with your organization's Microsoft Active Directory company directory, the directory groups for your organization's LDAP company directory are removed. (JI 1682078)

Workaround: Add the directory group again.

On the Settings > Email templates page, when you create a custom email template, if you click on the Suggested text link and copy and paste the text into the body of the email message, the formatting of the text is incorrect. (JI 1681468)

On the Apps page, if you click on the BlackBerry Access app, add an app configuration to the app, and then click Save, an error might display. (JI 1678731)

Workaround: Reopen the app, add the app configuration again, and click Save.

When you use the MDM controls activation type to activate a Windows 10 device, after you install an app on the device, the app displays as "Not installed" on the App details page in the console. (JI 1678111)

When you disable detailed logging for a BlackBerry Dynamics app (either by policy set or at the user level), the detailed logging does not display as disabled on the device tab in the BlackBerry Dynamics Apps section. Also, when you enable detailed logging for a BlackBerry Dynamics app (either by policy set or at the user level), the detailed logging displays as Off on the device tab in the BlackBerry Dynamics Apps section. (JI 1677889)

If you assign a BlackBerry Dynamics profile to a user when the BlackBerry Control service is stopped, an error message displays. (JI 1675154)

Workaround: Apply the profile when the BlackBerry Control service has started.

On the Users page, some device models might display as Unknown. (JI 1674410)

When you click Assign to assign a profile to a user, the profile might not get assigned and the console remains on the Assign a profile page. (JI 1673704)

Workaround: Click Assign again.

After you add a BlackBerry Dynamics app to a device, if you add a newer version of the app, on the device tab the app might display as “Not installed” even when the app is installed. (JI 1671581)

Newly added BlackBerry Proxy instances might display as “unassigned BlackBerry Proxy servers” on the Settings > BlackBerry Dynamics > Clusters page. (JI 1671306)

When you add an iOS app, if you try to upload a template without filling out all of the fields, the upload will fail. (JI 1670904)

After you create a web content filter profile and assign the profile to a user, if you click on the profile on the user page, the entries to the "Specific website bookmarks" section are cut off. (JI 1665084)

When you create certain profiles, such as proxy profiles, under the "Show device types to configure the profile for *" label, if you click on one of the device OS labels the corresponding device OS checkbox is not cleared or selected. (JI 1662796)

If you install the BlackBerry UEM Core on one server and the management console on another server, when you navigate to Settings > Infrastructure > BlackBerry Control, the URL for the BlackBerry Control console that displays contains the FQDN of the server where the console is installed instead of the FQDN of the server where the BlackBerry Control Service is installed.

Note that this issue does not display after you upgrade to BlackBerry UEM 12.6 MR1 and perform the synchronization. (JI 1657049)

After you add internal BlackBerry Dynamics apps, on the Apps page the background color for the apps displays in different shades. (JI 1653250)

On a user's page, when you navigate to BlackBerry Dynamics access keys > Send icon, and click Send, on the Resend access key screen, the Send button remains active and you can click the button again even though you don't need to. (JI 1634676)

Workaround: After you click Send once, you can click the X to close the Resend access key screen.

On the Company directory connection page, if you edit a Microsoft Active Directory connection, and then press Enter to save your changes, an error message might display. However, your changes are saved. (JI 1628615)

Workaround: Click Save to save your changes.

On the device page for a user, if you click the App actions drop-down list, there might be a delay of 4-5 seconds before the options display. (JI 1529791)

You can create a user account without enabling a service and specifying a contact email address. If you then enable the user account for device management and set or autogenerate a password that is sent to the user's device, the task appears to complete successfully instead of displaying a warning that an email address is required before the task can be completed. (JI 1507131)

Workaround: Add a contact email address when you create a user account.

UEM Self-Service known issues

If you are using Mozilla Firefox, you cannot access UEM Self-Service. (JI 2177349)

Workaround: Use Google Chrome or Internet Explorer to access UEM Self-Service.

The expiration period for access keys generated in UEM Self-Service is 24 hours instead of 30 days. (JI 1659057)

BlackBerry UEM API known issues

In previous releases of BlackBerry UEM and BES12, the BlackBerry Web Services certificate included the domain name in the Common Name. This practice is no longer supported by certain browsers. For BlackBerry UEM 12.6 MR3 and later, the domain name is now in the SAN of the BlackBerry Web Services certificate.

If you upgraded to BlackBerry UEM 12.6 MR3 and your organization has apps that use the BlackBerry Web Services, you must add the BlackBerry Web Services certificate to the trust store again. For instructions, visit http://help.blackberry.com/detectLang/blackberry-web-services-for-blackberry-uem/current/ to see the *BlackBerry Web Services Development Guide*.

When you call the BlackBerry UEM SOAP API endpoints that are hosted on the BlackBerry UEM Core, if the URL that the client provides ends with a slash (/), the API call fails with a "401 Unauthorized" error. (JI 1701299)

Workaround: Remove the slash from the URL.

When you are using the BlackBerry UEM SOAP APIs, if an authentication failure against a CAP API occurs, the faultCode in the response from BlackBerry UEM is "PROXY_AUTHENTICATION_REQUIRED" which does not accurately describe the reason for the failure. This response is different from the one that Good Control used to provide when an authentication failure occurred. If you have hard coded your application to expect the old Good Control failure response you will need to modify your client code. (JI 1620440)

Critical issue advisories

7

This section contains a list of all the critical issue advisories that have been released for BlackBerry UEM 12.6.

Critical issue advisory JRE 8u121 (KB39003)

Summary

Updating to JRE 8u121 on a BlackBerry UEM 12.6 server or on a BES12 server will cause authentication issues between BlackBerry UEM and your company directory or between BES12 and your company directory.

Impact

If using Windows Authentication, administrators will be prevented from logging into the BlackBerry UEM management console or from the BES12 management console and end users will be prevented from logging into BlackBerry UEM Self-Service or BES12 Self-Service.

Recommendations

Upgrade to BlackBerry UEM 12.6 MR1 before you upgrade to JRE 8u121.

Do not upgrade to JRE 8u121 on BlackBerry UEM 12.6 servers or on BES12 servers. In these cases retain JRE 8u111 as recommended in the BlackBerry UEM Compatibility Matrix.

Critical issue advisory - Device deactivates on upgrade to BlackBerry UEM Client

Summary

On iOS devices, if a user upgrades from the Good for BES12 Client or the BES12 Client to the latest version of the BlackBerry UEM Client, the device is deactivated.

Impact

If your organization is using BES12 or UEM 12.6.0, when an iOS device user upgrades to the latest version of the BlackBerry UEM Client, the device is deactivated.

Resolution

Upgrade your organization's server to BlackBerry UEM 12.6.1, or Contact BlackBerry Technical Support Services to request a QuickFix for BES 12.5.

For more information, see KB38729.

Affected users must reactivate their devices.

Critical issue advisory – BlackBerry Dynamics NOC update KB38917

Summary

With BlackBerry UEM 12.6, an update was made to the BlackBerry Dynamics NOC which allowed the BlackBerry UEM setup application to reuse Good Dynamics license keys and serial numbers when you were installing a second instance of BlackBerry UEM in the same cluster. However, when you added the second instance the request to join the cluster was not authenticated correctly.

On February 24, 2017 an update to the BlackBerry Dynamics NOC will change the way the BlackBerry Dynamics NOC authenticates a host. Due to the change in the BlackBerry Dynamics NOC, after you install a second BlackBerry UEM 12.6 instance, the BlackBerry Control and BlackBerry Proxy services will not start.

Impact

Existing standalone BlackBerry UEM 12.6 servers that were installed before February 24th are not impacted by this change; registrations between the BlackBerry Control and BlackBerry Proxy services and the BlackBerry Dynamics NOC will not be affected.

This issue impacts the following installation or upgrade scenarios:

- When you install BlackBerry UEM 12.6 as an additional node in an existing BlackBerry UEM 12.6 environment
- When you upgrade an earlier version of BES12 to BlackBerry UEM 12.6 and point to an existing Good Control database
- When installing BlackBerry UEM 12.6 as an additional node in an existing BlackBerry Dynamics environment.

Due to the BlackBerry Dynamics NOC update, when you perform any of the installation or upgrade scenarios listed above, the BlackBerry Control and BlackBerry Proxy services cannot successfully register with the BlackBerry Dynamics NOC and will remain in a disabled state.

Resolution

Upgrade from BlackBerry UEM 12.6 to BlackBerry UEM 12.6 MR1. When you upgrade to BlackBerry UEM 12.6 MR1, the BlackBerry Control and BlackBerry Proxy services start correctly.

If you have downloaded the BlackBerry UEM 12.6 software but have not installed it, please download and install the BlackBerry UEM 12.6 MR1 software instead.

For more information, see KB38917.

Critical issue advisory - iOS device users might stop receiving email messages

Summary

After you upgrade from BES12 version 12.5.2 or earlier to any version of BlackBerry UEM, iOS device users who were activated using the MDM controls activation type might stop receiving email messages, which requires them to re-enter their Microsoft Exchange ActiveSync password.

Note: This issue applies to native iOS mail only. It does not impact BlackBerry Work because BlackBerry Work does not leverage email profiles.

Impact

Due to a change in the email profile for iOS devices in BlackBerry UEM, after you upgrade, a new email profile is pushed to devices. Some iOS devices stop receiving email messages when the new email profile is pushed and users must re-enter their Exchange ActiveSync password. Also, replacing the old email profile with the new profile causes a re-synchronization of the users' mailboxes.

Recommendation

Users must re-enter their Exchange ActiveSync passwords and resynchronize their mailboxes. To avoid data use over the mobile network, users should use a Wi-Fi connection when they resynchronize their mailboxes.

Maintenance releases of the BlackBerry Connectivity app

8

The BlackBerry Connectivity app is required for devices to use the BlackBerry Secure Connect Plus feature in BlackBerry UEM. Maintenance releases of the app might occur between BlackBerry UEM releases. To view the Release Notes for the latest maintenance releases of the app, visit http://help.blackberry.com/en/blackberry-connectivity/current/.

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

Legal notice

9

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