BlackBerry Dynamics Overview for Administrators and Developers

Version 4.2

Contents

Revision history

BlackBerry Dynamics Platform Overview for Administrators and Developers

Date	Description
2017-09-19	Determining whether you should upgrade to BlackBerry UEM
2017-07-18	Version number updated for new release; no changes to content.
2017-02-14	Cosmetic changes
2017-01-31	Version numbers updated for latest release; no content changes.
2016-07-18	Added clarification in About security of services "in the cloud"
2016-06-29	Version numbers updated for latest release; no content changes.
2016-03-10	Truncated revision history to reduce bulk.
2016-01-15	Version numbers updated for latest release; no content changes.
2015-12-23	Version numbers updated for latest release; no content changes.

Introduction: secure mobile platform

BlackBerry Dynamics is a secure platform for managing mobile devices running unique and customized enterprise applications. Designed to securely access data and services through the enterprise firewall, as well as capable of extending beyond your enterprise intranet to securely access online services and resources available on the web.

Background

Users of enterprise applications are increasingly demanding that their enterprise tools be available to them at all times, whenever and wherever needed, in the office or away from it. And, for the most part, enterprise applications can be adapted to this purpose. This means that a desktop client can be replaced by a mobile application running on a connected mobile device, be it an Android smartphone or tablet, an iPhone, iPad, or Windows Phone device. At the same time, however, mobilizing enterprise data—i.e., making the data available on mobile devices—presents a number of enterprise security concerns.

Potentially, data in transit between a backend server and a mobile device could be intercepted, or a mobile device could be tampered with, with or without the owner's knowledge, in such a way that data at rest on the device can be obtained by someone other than the authorized user. In addition, backend servers accessible to/from the Internet are intrinsically vulnerable to any number of attacks, but locating backend servers behind the enterprise firewall for protection also makes them inaccessible to mobile data connections.

Installing a virtual private network (VPN) may seem like a solution, until you realize that VPN access from an equipped device typically opens the firewall to every application on the device, which could include malicious software of which the device's user is unaware. The attack surface is further expanded and compounded by BYOD ("bring your own device") initiatives pursued in response to the rapidly growing number of enterprise users preferring to use their own mobile devices for running enterprise applications.

Notwithstanding ownership of the device, the enterprise will wish to control its company-sensitive data, even if it cannot control the entire device and the user's personal data. Despite most devices having lock mechanisms requiring a device password or PIN to open, there is no guarantee the user won't disable or weaken these features, most often by setting a password that can be easily guessed. In any case, a device's native lock features generally fail to meet the stringent security measures most enterprises are compelled to enforce to remain competitive within their respective marketplace.

Mobilizing applications may meet the immediate needs of end users, but to meet the needs of the enterprise, such a mobilization of applications must be coupled with security.

About BlackBerry Dynamics software version numbers

The cover of this document shows the base or major version number of the product, but not the full, exact version number (which includes "point releases"), which can change over time while the major version number remains the same. The document, however, is always current with the latest release.

Product	Version
Good Control	4.1.57.49
Good Proxy	4.1.57.51
BlackBerry Dynamics SDK for Android	3.3.0.3073
BlackBerry Dynamics SDK for iOS	3.3.0.3259
BlackBerry Dynamics SDK for macOS	3.0.0.227
BlackBerry Dynamics SDK for Universal Windows Platform	3.0.0.805
BlackBerry Launcher Library for Android	2.6.1.201
BlackBerry Launcher Library for iOS	2.6.1.137
BlackBerry Dynamics SDK for Cordova (formerly also called "PhoneGap")	3.2.0.371
BlackBerry Dynamics Bindings for Xamarin.Android	3.2.0.3073
BlackBerry Dynamics Bindings for Xamarin.iOS	3.3.0.3259
Digital Authentication Framework (DAF) • Android • iOS	 • 3.0.0.13 • 2.0.0.12

If in doubt about the exact version number of a product, check the BlackBerry Developer Network for the latest release.

Mobile application security

BlackBerry Dynamics enables mobile enterprise applications to employ the same industry-leading security employed in the GFE product, including:

- Network Operation Center (NOC) and proxy infrastructure enabling connections between mobile clients and application servers that are behind the enterprise firewall, ending the need for a VPN or open ports in the enterprise firewall.
- end-to-end encryption of data in transit between mobile clients and application servers.
- storing enterprise data on the device in a separate secure container, which can be remotely wiped by an administrator.
- encrypting with AES 256-bit cypher technology protecting data at rest, in the secure container, in addition to protecting data in transit between client and server.
- enforcing password and device compliance policies whenever enterprise data accessed.

These benefits and more can be extended from BlackBerry for Enterprise to other enterprise applications because BlackBerry Dynamics is a platform solution that provides capabilities available to software developers.

This includes the ability to automatically:

- authenticate and manage users.
- communicate between a client on a mobile device and an application server that is behind the enterprise firewall.
- protect data in transit with secure communications.
- protect data at rest with secure storage.
- enforce security measures such as password policies.

BlackBerry Dynamics also provides a number of powerful integration capabilities, such as:

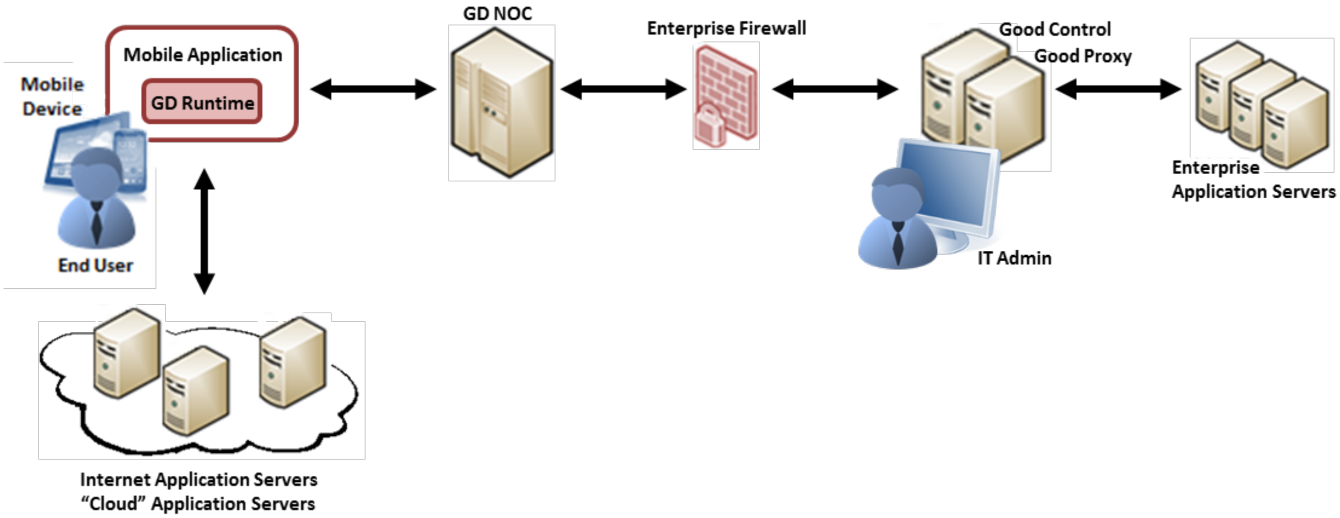
- delegating authentication and password security from a BlackBerry Dynamics application to the BlackBerry for Enterprise (GFE) mobile client.
- securely exchanging data between GFE and a BlackBerry Dynamics application.
- delegating authentication and password security from one BlackBerry Dynamics application to another.
- securely exchanging data between two BlackBerry Dynamics applications.

Platform components

All the aforementioned capabilities are provided through the following BlackBerry Dynamics components:

- **BlackBerry Dynamics Runtime** – included in every BlackBerry Dynamics mobile application, the runtime has an API that gives the application access to user authentication, secure communications, secure storage, and communication behind the firewall, and enforces security policies on behalf of the application.
- **BlackBerry Dynamics Network Operation Center (NOC)** – providing the secure communications infrastructure between the BlackBerry Dynamics Runtime on the device and the BlackBerry Dynamics enterprise servers behind the firewall.
- **BlackBerry Dynamics Enterprise Servers** – two components installed behind the enterprise firewall, namely:
  - **Good Control (GC)** – a server providing management of enterprises users, applications, and security policies.
  - **Good Proxy (GP)** – a server providing the secure communications infrastructure between the NOC and connected application servers behind the enterprise firewall.

Platform components



BlackBerry Dynamics Infrastructure: Platform and Application Components

BlackBerry Dynamics runtime

The BlackBerry Dynamics Runtime is the mobile component of the BlackBerry Dynamics platform. An instance of the BlackBerry Dynamics Runtime is built into every BlackBerry Dynamics mobile application (BlackBerry Dynamics App).

BlackBerry Dynamics Apps are native applications programmed using native tools. To create a BlackBerry Dynamics App for iOS, the developer uses Apple's Xcode IDE, Apple's iOS SDK, and the BlackBerry Dynamics SDK for iOS. To create a BlackBerry Dynamics App for Android, the developer uses the Eclipse IDE or the Android command line tools, the Android SDK Manager, and the BlackBerry Dynamics SDK for Android.

These tools enable the developer to compile and link application code with the BlackBerry Dynamics Runtime library for their chosen platform. The BlackBerry Dynamics Runtime library employs a variety ofApplication Programming Interfaces (APIs).The implementation of the API is necessarily different for different platforms:

- The programming language for BlackBerry Dynamics for iOS is Objective-C, with some APIs also supporting a C interface.
- The programming language for the BlackBerry Dynamics for Android is Java.

Secure communication

BlackBerry Dynamics Apps communicate with application servers that are behind the enterprise firewall by employing either of two technologies for secure communication:

- TCP Sockets
- HTTP Request

As used in BlackBerry Dynamics, communication relay is along three legs, each making use of either a Secure Socket Layer or Transport Layer Security (SSL/TLS):

1. From the runtime to the BlackBerry Dynamics Network Operation Center (NOC), communication is protected by SSL/TLS.
2. From the BlackBerry Dynamics NOC to the enterprise's Good Proxy (GP), communication is likewise protected by SSL/TLS.
3. From the GP to the application server, communication can be protected by SSL/TLS, if required.

In addition, the BlackBerry Dynamics Runtime and the enterprise's GP share a key for AES encryption. This key is not known to the NOC, so secure communication data cannot be intercepted there. Also, the application and its server can use SSL/TLS as endpoints, meaning an SSL/TLS connection can be securely conveyed over the BlackBerry Dynamics infrastructure as a whole.

About security of services "in the cloud"

If necessary and if secure communications are not a paramount concern, BlackBerry Dynamics's secure communication APIs can also connect to servers on the Internet, including "cloud" servers that are not be able to establish secure communications via BlackBerry Dynamics. These communications go directly from the BlackBerry Dynamics Runtime to the Internet server, not via the BlackBerry Dynamics infrastructure. Full end-to-end encryption is not available on these connections. See Application servers for additional detail.

Secure storage

BlackBerry Dynamics Apps can store data securely on the device using the following APIs:

- Secure file system
- Secure SQL database
- Secure Core Data*[1]

The BlackBerry Dynamics Runtime encrypts data in these stores using AES encryption. The encryption key can include a value entered by the user—the BlackBerry Dynamics security password. See Security Password Policies below for additional details. Alternatively, a password replacement value can be supplied through authentication delegation.

The user interface on which the BlackBerry Dynamics security password is entered is part of the BlackBerry Dynamics Runtime. The runtime does not store the password in the device's persistent storage, so the password is never available to an attacker who happens to obtain the device. Nor is ever exposed to the application code.

When authentication delegation is in use, a password replacement value is used instead of the BlackBerry Dynamics security password entered by the user. The delegate will only supply the replacement value after it authenticates the user. Treated like the password by the runtime, because the replacement value is not stored persistently, it is also never exposed to an attacker.

The Secure Storage APIs furnish decrypted data to the application only if the user has already entered the correct security password, if required, or the password replacement has been supplied. This applies whether the device is on-line and connected to the BlackBerry Dynamics infrastructure or not.

[1] Core Data is a native iOS feature that can be made secure with BlackBerry Dynamics. Specific to iOS, Core Data is not available on the Android platform.

Push channel

BlackBerry Dynamics's Push Channel APIs allow mobile clients to receive timely notifications from their application servers, automatically, eliminating the need for BlackBerry Dynamics apps to poll their servers. The BlackBerry Dynamics Runtime itself uses the Push Channel to receive notifications of updates to enterprise policies and user entitlements (see Security Policies).

The Push Channel API has both client and server versions. The client API governs setup and management of Push Channel connections. The server API governs which notifications are sent to clients after a connection is established.

The client API is furnished by the BlackBerry Dynamics Runtime, whereas the sever API is hosted on the BlackBerry Dynamics NOC and presented to application servers through the enterprise's Good Proxy.

The BlackBerry Dynamics Runtime keeps the Push Channel connection open continuously, achieved by sending "heartbeat" messages at an interval that is dynamically optimized for battery and network performance.

Note: The Push Channel service in BlackBerry Dynamics for iOS is different from, and should not be confused with, the Apple Push Notification Service (APNS).

BlackBerry Dynamics runtime object

The BlackBerry Dynamics Runtime object is the link between the application code and the BlackBerry Dynamics platform. This includes the user's authorization to connect to the BlackBerry Dynamics infrastructure. Each time a BlackBerry Dynamics-enabled app starts, the BlackBerry Dynamics Runtime object must be initialized.

The very first time such an app is started on a device, runtime object initialization requires that:

1. The end user's credentials—email address and an access key—are entered in the BlackBerry Dynamics Runtime UI (see Application Activation for more on access keys).
2. The entered credentials are sent to the NOC for validation, as well as verification that this user is entitled to use the BlackBerry Dynamics app just launched. Authorized use of the BlackBerry Dynamics infrastructure for this particular application on this particular device is then enabled, and an infrastructure key is issued to the device.
3. An association is created between the user and their provisioning enterprise. Encryption keys are exchanged between the runtime and the enterprise's GP, enabling communication between the BlackBerry Dynamics Runtime and servers located behind the enterprise firewall.
4. Security policies are retrieved from the enterprise GC server (see Security Policies for more details on what policies are supported by BlackBerry Dynamics).
5. The end user now sets a BlackBerry Dynamics security password, as/if required by the enterprise's policies, unless authentication delegation is enabled. See Authentication Delegation for details.

Once the above processing and communication completes, the issued keys are encrypted and stored on the device. The encryption algorithm used is the same as that used for Secure Storage. For those familiar with GFE, the entry of credentials and setting of a security password during first-time execution follows the same flow as a GFE mobile client.

In subsequent runtime object initializations, the user merely enters their security password, if any. This enables decryption of the stored keys, which in turn enables connection to the BlackBerry Dynamics infrastructure, and to servers behind the enterprise firewall. The runtime then retrieves and applies any outstanding changes to security policies and user entitlement.

Subsequent changes to policies and entitlements made when the runtime is already connected to the BlackBerry Dynamics infrastructure are applied immediately. The runtime is notified of these changes using the BlackBerry Dynamics Push Channel.

The runtime object also implements an inactivity timer, which temporarily suspends the end-user’s authorization when they are idle for an admin-defined interval. The application is notified of this, and of other changes as described above, by the dispatch of an event from the BlackBerry Dynamics Runtime object.

BlackBerry Dynamics network operation center (NOC)

Accessible to the Internet, the BlackBerry Dynamics NOC is the central component of the BlackBerry Dynamics infrastructure. Both clients and servers connect to the NOC as a mediation point for end-to-end communication and management.

The NOC hosts a number of services and data stores used by other components, including:

- Secure communications relay
- Push Channel
- End user access key provisioning
- Entitlement of end users to BlackBerry Dynamics apps
- Associations between enterprises and BlackBerry Dynamics software vendors.

Good Proxy (GP)

Good Proxy (GP) server maintains the secure connection between your enterprise and the NOC. The GP’s connection is used for:

- Secure communication relay.
- Presentation of the BlackBerry Dynamics Push Channel service to enterprise application servers.

Installed behind the enterprise firewall, GP establishes the secure connection outwards, to the NOC, so there is no need to open an inbound port in the firewall and no need to use a VPN.

Multiple GP servers can be installed for high availability and disaster recovery (HA/DR, as well as to add more relay capacity. See Enterprise Server Requirements for details.

Good Control (GC)

Good Control (GC) is BlackBerry Dynamics’s management and configuration component. Every BlackBerry Dynamics enterprise has its own GC server. The functions of the GC include:

- **User Management**
  - add and remove end users
  - manage access keys
  - check application activation for each device
  - reset end-user security passwords
- **Policy Management**
  - set password policies
  - set device compliance policies
  - edit email templates
  - create policy sets
  - assign users to policy sets
  - check delivery and history of policy updates, per end-user device.
- **Application Management**
  - set individual end-user entitlement to specified BlackBerry Dynamics Apps
  - set group entitlements
  - remotely wipe application data on a device
  - remotely lock and unlock applications on a device.
- **Infrastructure Configuration**
  - set accessible enterprise servers, per application or globally
  - automatic configuration of GP servers
- **Role Management** - designate administrator users.

Good Control has two user interfaces. For administrators, there is a full-service dashboard, called the GC console. There is also a limited self-service user interface for end users.

GC requires access to the following enterprise services:

- **Microsoft Active Directory (AD)**, for GC console log-in and end-user account identification. Users log in to the GC console, or self-service user interface, by entering their AD credentials. Only users with accounts on an Active Directory server can be added as BlackBerry Dynamics end-users or administrators.
- **SMTP (Simple Mail Transfer Protocol)** for email. Access keys are sent to end-users by email.

Unlike Good Proxy, GC is not in the relay path of Secure Communication or Push Channel.

Multiple GC servers can be installed, in a cluster, for HA/DR or to increase the capacity for concurrent users. GC servers in a cluster can be placed in a priority order, which means some GC resources can be reserved for fail-over scenarios. GP servers can be allocated between GC servers with relay resources also reserved.

enterprise server requirements

Requirements for your enterprise’s BlackBerry Dynamics servers—GC, GP, and GC database—include:

- GC server software
- GC database
- GP server software

The servers and the database can be installed on the same physical machine, if required. These three primary server components can also be installed separately on two or three different machines.

Supported platforms for the database are restricted to either Oracle 10g/11g or MS SQL Server.

Important: If you are running GFE in parallel with BlackBerry Dynamics, your GC and GP servers cannot be installed on the same physical machine as GFE's BlackBerry Mobile Control (GMC) or BlackBerry Mobile Messaging (GMM) servers.

Application components

Application components use the capabilities of the secure mobile platform components described in Platform components. BlackBerry Dynamics application components include the mobile client running on provisioned devices and the enterprise or internet application server(s) or both supporting it.

Mobile client

The mobile client is the part of the application that runs on a mobile device—a smartphone or tablet. The mobile client makes use of the BlackBerry Dynamics API, which is its link to the BlackBerry Dynamics platform. Every mobile client includes an instance of the BlackBerry Dynamics Runtime discussed in BlackBerry Dynamics runtime.

The mobile client code is written by a software developer as discussed in Application Providers. The code includes the user interface and application logic. BlackBerry Dynamics code will usually include secure communication with one or more application servers using HTTP requests or a TCP socket connection.

The client and code will be different for devices running different mobile operating systems. The mobile client can be coded in any language that is supported by the BlackBerry Dynamics SDK for the operating system of the target device. For iOS, the BlackBerry Dynamics mobile client is typically coded in Objective-C, perhaps including some C++ or plain C. For Android, the BlackBerry Dynamics mobile client is coded in Java, but may link-in pieces written in C++ if the NDK is in use.

A brief description of native development tools is included in BlackBerry Dynamics runtime.

Application servers

Application servers are the backend components with which the mobile client communicates in order to provide service to its user. An application server may itself be the host of data or services required by the end user, or may interface with a separate business system that is the host. In each case, the application server presents an API that is used by the mobile client. A single mobile client can communicate with a number of application servers.

Application servers are created by the developer and do not include any BlackBerry Dynamics code or libraries and can be based on any server-side technology, for example Java (JRE), PHP or Perl.

Server addresses

To communicate with an application server, a mobile client requires a server address. The mobile client may also need a port number. Server addresses can be set in full in the application code, but BlackBerry Dynamics conveniently offers an alternative by allowing the address of an application to be configurable in the GC management console, from which the BlackBerry Dynamics Runtime retrieves the configured address and port number values. These retrieved values are then made available to the application code by the BlackBerry Dynamics Runtime.

Additionally, symbolic server names can be configured in the GC console. The application code then uses a symbolic name; for example “intranet.” This is then mapped to a full address and port number by the GC configuration.

For routing purposes, two categories of server address are in play: Enterprise and Internet. Connections to enterprise server addresses will be routed via the BlackBerry Dynamics infrastructure. Connections to Internet server addresses will be made directly from the device.

Server addresses are identified as enterprise or Internet based on a set of pattern-matching rules. The rules are configured in the GC console, and retrieved by the BlackBerry Dynamics Runtime. Each time the application attempts a connection to a server, the BlackBerry Dynamics Runtime uses the rules to identify the server’s routing category, and then connects in the appropriate manner.

Enterprise application servers

Enterprise application servers are located behind the enterprise firewall. Such servers can be accessed using BlackBerry Dynamics Secure Communications to enforce end-to-end encryption. This involves the enterprise’s GP server as configured from the GC console.

Different BlackBerry Dynamics Apps can be granted access to different enterprise servers. Access is configured by server address and port number. The API that an enterprise application server offers to the mobile client can be based on HTTP requests or TCP sockets. The connection can also be secured using endpoint SSL/TLS, if required, as discussed in Secure communication.

Internet application servers

BlackBerry Dynamics applications can also communicate with servers that located in the Internet, including cloud services. However, Internet servers are not protected by the enterprise firewall, and the client-server connection cannot be end-to-end encrypted by the BlackBerry Dynamics platform.

For convenience, developers can use the BlackBerry Dynamics HTTP and socket APIs to communicate with Internet application servers. The BlackBerry Dynamics Runtime routes communication to non-enterprise servers directly over the Internet, not via the BlackBerry Dynamics infrastructure.

Application server clustering

Multiple application servers can be deployed in a cluster. BlackBerry Dynamics capabilities for application server clustering are similar to its capabilities for GC clustering and deliver the same benefits, supporting both HA/DR and increased capacity.

Server addresses for a clustered application server are entered in the GC console (see Server addresses). Multiple addresses can be entered for a single application. The server addresses can be placed in priority order. GP servers can be allocated between them as a relay resource.

The entire clustering configuration of an application server cluster is retrieved and made available to the application code by the BlackBerry Dynamics Runtime.

Application management

BlackBerry Dynamics's application management capabilities provide in depth monitoring and control of:

- Application Providers
- Application Identification
- Application Entitlement
- Application Activation

All BlackBerry Dynamics applications available to enterprise users are listed in the enterprise GC console. This includes in-house proprietary applications, white-label apps, and BlackBerry Dynamics partner apps published to the enterprise by an independent software vendor (ISV).

Application providers

Three types of providers furnish the BlackBerry Dynamics Apps used by an enterprise: Organization, Partner, and Good.

Organization refers to BlackBerry Dynamics applications provided by in-house developers, i.e. developers within the same enterprise as the end users. Developers could be full-time staff or contractors.

Partner refers to white-label BlackBerry Dynamics applications or apps obtained from an ISV. To be eligible to use ISV applications, the enterprise must execute a legal agreement with the ISV. A vendor connection between the two organizations is then created in the BlackBerry Dynamics NOC, and the ISV can now publish the requested BlackBerry Dynamics Apps to the enterprise. Agreements are mediated through the BlackBerry Dynamics Marketplace.

BlackBerryrefers to BlackBerry Dynamics applications provided directly by BlackBerry.

Application identification

A BlackBerry Dynamics application is identified by its unique BlackBerry Dynamics Application ID.

By convention, the BlackBerry Dynamics Application ID of a given organization's applications begins with a reversal of an Internet domain owned by the organization. For instance, applications provided by BlackBerry have the prefix "com.good", because BlackBerry owns the good.com domain.

Appended to the reversed domain prefix will be a number of further segments, which together are unique within the providing organization. For example, "com.good.gd.example.remotedb" is the BlackBerry Dynamics Application ID of the Remote Database sample application that comes with the BlackBerry Dynamics SDK.

In general, wherever a BlackBerry Dynamics Application ID is used, a version number will also be used. By convention, version numbers are four integers separated by full stops; e.g., “1.0.0.0,” which likely the version number for the first release of a BlackBerry Dynamics application.

Application entitlement

Entitlement of end users to applications is managed in the GC console. GC administrators can entitle individual users to specific BlackBerry Dynamics apps. As well, end users can also be placed in groups, and the groups made entitled to particular BlackBerry Dynamics apps.

Entitlement can be to designated versions of a BlackBerry Dynamics application, or to all versions.

When an end user’s BlackBerry Dynamics application entitlement is changed, GC immediately notifies the NOC, which stores the new entitlement. If an end user’s device is running a BlackBerry Dynamics app to which they are not now entitled, and the application is online, the change is enforced immediately. Otherwise, the change is enforced when the application next connects to the NOC.

Enforcement of removed entitlement includes deleting the enterprise data from the device. See Policy Enforcement Action under Security Policies.

As previously mentioned, users can be grouped for the purposes of granting BlackBerry Dynamics application entitlement. An end user can belong to multiple groups. There is also a special “everyone” group to which all users in the GC are added.

Changes to end-user entitlement will therefore result whenever a user is added to a group, removed from a group, a group application entitlement is granted, or a group application entitlement is revoked.

Any resulting entitlement change is enforced as set forth above.

Application activation

Users must activate every application that they use. To do this, the user runs the application on their mobile device. They will be prompted to enter their email address, and an access key.

The access key must have been generated and sent to the user before they attempt to use the application for the first time. Access keys are generated and managed in the GC console. The GC server requires an SMTP connection to send the key to the user’s email address.

A new access key is required in the following situations:

- Initial application activated by a new user.
- New application activated by existing user. This applies even if the application is being activated on a device on which another BlackBerry Dynamics application is already activated.
- Application activated on a second device, when the user has previously activated the same application on a different device.
- Re-installation of an application that was previously activated on the same device.

Note: BlackBerry Dynamics access keys fulfill the same function as GFE PINs and have the same number of characters. BlackBerry Dynamics access keys, however, are not reusable for reinstallation on the same device.

Security policies

Supporting policies similar to GFE security policies, BlackBerry Dynamics can enforce any number of application security policies. Set in the GC console, security policies are retrieved and enforced by the BlackBerry Dynamics Runtime.

Security password policies

The end user may be required to enter an additional password, the BlackBerry Dynamics security password, to access their BlackBerry Dynamics applications. The BlackBerry Dynamics security password strictly applies to the application, not the device as a whole. This security password, when required, is included in the encryption key used by the BlackBerry Dynamics secure storage features (see Secure storage).

The security password policies enforced by BlackBerry Dynamics include but are not limited to:

- Security password required
- Password expires after a specified number of days
- When changed, a specified number of previously used passwords cannot be used
- Password minimum length
- Maximum number of occurrences of any particular character
- Password cannot be changed more than once a day
- Password must have letters and numbers
- Password must have upper-case and lower-case letters
- Password cannot only be letters and numbers
- Password cannot have sequential numbers
- Password cannot contain personal information.

Access key policies

Used during application activation, access keys are issued by the GC and sent to the end user by email. The following access key policies are supported:

- The time for which a newly issued access key is valid.
- The template used to create the email message to the end user.

Device compliance policies

Enterprises may already enforce security policies relating to the mobile devices on which their end users run mobile applications. The BlackBerry Dynamics Runtime checks that each entitled user’s mobile device complies with all device policies, including:

- Device be must an enterprise-approved make and model.
- Device must be running an enterprise-approved version of the iOS or Android operating system.
- Device must not have a jailbreak in place (iOS).
- Device must not have been rooted (Android).

Miscellaneous policies

In addition to the above policy categories, BlackBerry Dynamics supports:

- Data copied from within the BlackBerry Dynamics application cannot be pasted into another application.
- Device cannot remain disconnected from the BlackBerry Dynamics infrastructure for longer than a specified time interval.

Applying policies

Different BlackBerry Dynamics security policies can apply to different end users. The GC administrator manages the application of security policies by using policy sets.

The GC administrator creates a policy set by selecting and specifying a collection of the policies cited above. End users can then be assigned to the policy set. The policies in the set apply to all BlackBerry Dynamics applications the end user launches and runs on any device.

A GC administrator can create multiple policy sets. Because each end user must be assigned to at least one policy set, there is a designated default policy set that is applied to all new users.

Policy enforcement action

Whenever a BlackBerry Dynamics security policy violation is detected, enforcement action is taken in one of two ways:

- Access to the application data on the device is blocked.
- All application data on the device is deleted (also known as a device wipe).

A block will remain in place until the policy violation is rectified. For example, suppose a block had been put in place when the user had not changed their password when required to do so. The block would be removed when the user actually does change the password. By contrast, a device wipe is immediate and irreversible.

Enforcement actions are executed by the BlackBerry Dynamics Runtime, eliminating any need for the application code to implement enforcement actions.

Changing policies

When the policies in a set change, or when a user is assigned to a different set, the policies now applying to that user might change.

When policies change, the GC immediately attempts to notify any BlackBerry Dynamics apps being run by affected users. Any of the user's BlackBerry Dynamics applications online at the time will receive and enforce the changed policies immediately. Otherwise, the change is enforced when the BlackBerry Dynamics app is online next.

Authentication delegation

A BlackBerry Dynamics application can itself authenticate the end user. It can also delegate authentication to another application.

One benefit of delegation is improved UX. When authentication is delegated, the end user can unlock a number of applications with a single password. Authentication delegation can also be the means to introduce additional security mechanisms, such as hardware accessories.

Controlled by policy configuration, authentication delegation supports delegation from one BlackBerry Dynamics application to another, as well as from a BlackBerry Dynamics app to GFE.

Certain early releases of BlackBerry Dynamics for iOS supported a limited form of authentication delegation: enterprise single sign-on (SSO). Enterprise SSO required a specific build-time configuration by the developer and was not controlled by policies. Enterprise SSO is now deprecated in favor of full authentication delegation.

A value entered by the end user is sometimes required to form an encryption key. When authentication delegation is in use, a password replacement value is supplied by the delegate application instead. The delegate will only supply the password replacement after authenticating the user.

Scenarios

Presented here are four common use-case scenarios illustrating BlackBerry Dynamics's situation-handling capabilities.

New employee

The following is likely to occur when a new member of staff joins the enterprise:

1. The new employee, **Emp1**, is added to the enterprise ActiveDirectory (AD) server. This includes, at minimum, adding their name and email address.
2. An IT administrator, **Admin1**, adds **Emp1** to the enterprise GC server via the GC console, looking up **Emp1**'s details in the enterprise AD server.
3. **Admin1** assigns the default policy set to **Emp1** in the GC console.
4. Next, **Admin1** adds **Emp1** to all required groups in the GC console. This entitles **Emp1** to the BlackBerry Dynamics apps they require.
5. **Admin1** next creates access keys for **Emp1**; as many keys as there are BlackBerry Dynamics apps to which **Emp1** is entitled, multiplied by the number of devices being provisioned for **Emp1**.
6. The GC server sends the access keys to **Emp1**'s email account.

After this, the Activate End-User Application scenario below takes place for each BlackBerry Dynamics application to which the new employee is now entitled.

Activating end-user application

When an end user wants to use a new BlackBerry Dynamics app to which s/he is now entitled, the scenario typically followed is this:

1. An access key, **Key1**, is issued to the end user, **User1**. The user is notified of the key's value in a welcome message sent by email.
2. The mobile client for the new application, **App1**, is installed on the mobile device, **Dev1**, on which **User1** will run the application.

   BlackBerry Dynamics does not have its own system for distribution of executable files. Even so, the client software may be installed using any method that is supported by the target device. For example, software could be installed from an application marketplace like Google Play or the Apple App Store. For iOS, an enterprise App Store may also be available. For Android, loading an installer directly on the device is an option. In addition, GFE or another Mobile Device Management (MDM) mechanism may be in use by the enterprise.
3. **App1** is started on **Dev1**. The BlackBerry Dynamics Runtime opens a user interface that prompts for the email address and access key to be entered.
4. **User1** enters a designated enterprise email address along with **Key1** from the welcome message. **App1** sends these credentials to the NOC.
5. The entitlement of **User1** to **App1** is checked. A secure connection to the enterprise GC is established and policies are retrieved.
6. **User1** enters a security password in accordance with the policy set to which they are assigned in the GC.
7. **Dev1** is checked against the device compliance policies of the policy set to which **User1** is assigned in the GC.

The BlackBerry Dynamics App is now ready for use.

activation with authentication delegation to GFE

Activation of a new end user when authentication is delegated to GFE differs as follows:

Before Step 2, the user must have already installed and activated the GFE mobile client on their device.

In Step 6, the user will enter their GFE password instead of setting a new security password.

In-house application development

A close variation of the following will likely take place as part of the development life cycle of a custom BlackBerry Dynamics application:

1. The developer can begin their work by using enterprise simulation mode. In this mode:
   - Access keys are not required.
   - The mobile client can only be run on a simulator, not on a physical device.
   - Connections to enterprise servers behind the firewall cannot be made through the BlackBerry Dynamics infrastructure, but could be made directly; e.g., if the simulator is running on a machine that is on the enterprise LAN or VPN.

2. When ready for the next stage, the developer stops using enterprise simulation mode. This means that the:
   - Full application activation must take place every time the software is re-installed, which could be frequently. A new access key is required each time.
   - The mobile client can only be run by a user that is entitled to the BlackBerry Dynamics application. This in turn means that:
     - The developer must be added to the GC server as an end user.
     - The BlackBerry Dynamics App must be registered in the GC server, with a unique BlackBerry Dynamics Application ID, see under Application Identification, above.
     - The mobile client can communicate with application servers that are behind the enterprise firewall, via the BlackBerry Dynamics infrastructure. Application servers must be listed in the GC server (see Enterprise application servers).
3. When ready for roll-out to end users:
   - Entitlement to the new BlackBerry Dynamics App is granted to end users requiring access. This could be done individually or by group. See Application entitlement.
   - End users are granted access to a specific version of the BlackBerry Dynamics app; i.e., the production version. Meanwhile, the developer is granted access to a follow-on version of the BlackBerry Dynamics application, the development version.
   - The developer changes this copy of the application code to identify itself as the development version.

Lost device

The following takes place when an end user loses a mobile device on which a BlackBerry Dynamics application is currently installed:

1. The user logs in to the GC self-service user interface.
2. The user sends a device-wipe command to every BlackBerry Dynamics application on the device.
3. The command is received by the BlackBerry Dynamics runtime instances running on the device. Enterprise data is deleted from the device.
4. The user self-issues new access keys.

The user then obtains a new device, and activates all the BlackBerry Dynamics Apps to which s/he is entitled on the new device.

Variant: The IT administrator takes the same actions.