

BlackBerry Dynamics and Fingerprint Authentication

Last updated: Friday, March 31, 2017

Versions: GC 3.0.xx.yy, GP 3.0.xx.yy, and BlackBerry Dynamics SDK 3.0.xxxx



©2017 BlackBerry Limited. Trademarks, including but not limited to BLACKBERRY, BBM, BES, EMBLEM Design, ATHOC, MOVIRTU and SECUSMART are the trademarks or registered trademarks of BlackBerry Limited, its subsidiaries and/or affiliates, used under license, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. All other trademarks are the property of their respective owners. This documentation is provided "as is" and without condition, endorsement, guarantee, representation or warranty, or liability of any kind by BlackBerry Limited and its affiliated companies, all of which are expressly disclaimed to the maximum extent permitted by applicable law in your jurisdiction.

Contents

Revision history	5
BlackBerry Dynamics and fingerprint authentication	6
Standard behavior of fingerprint authentication without BlackBerry Dynamics	6
BlackBerry Dynamics' generalized approach: policy control	6
Application developers: no work necessary	6
Android Fingerprint	8
Considerations about Android Fingerprint	8
Disallowing Android Fingerprint after application coldstart	8
Allowing Android Fingerprint after application coldstart	8
Android Fingerprint policies in Good Control	8
Android Fingerprint policies in BlackBerry UEM	8
User experience when Android Fingerprint is allowed	9
About Samsung Pass	9
Known limitations in Samsung Pass	9
Apple Touch ID	10
Allowing Touch ID after application coldstart	10
Summary of options and comparison of coldstart/warmstart behaviors on iOS	10
Apple Touch ID policies in Good Control	11
Apple Touch ID policies in BlackBerry UEM	11
User experience when Touch ID is allowed	12
Additional use cases and policy interactions	12
Touch ID policy with periodic password enforcement	12
Stolen device	12
Shared device	13
GFE with Apple Touch ID	13
Policies in BlackBerry mobile control	13
GFE/GMC complete control by policy	16

BlackBerry Dynamics documentation 17

Revision history

Revision history

Date	Description
2017-03-20	<ul style="list-style-type: none">• Now refers to both Good Control and BlackBerry UEM• Additional use cases in Apple Touch ID• Clarifications throughout
2016-12-19	Version numbers updated for latest release; no content changes.
2016-06-29	Updated for latest release: <ul style="list-style-type: none">• Android Fingerprint• Changes to Good Control policies governing fingerprint authentication• Renamed <i>BlackBerry Dynamics and Fingerprint Authentication</i>
2016-01-15	Version numbers updated for latest release; no content changes.
2015-06-19	Updated to include information about Touch ID with BlackBerry For Enterprise (GFE) and BlackBerry Mobile Control (GMC).
2015-05-18	Version numbers updated for latest release; no content changes.
2015-04-15	Updated with clarifications about Apple Inc.'s own treatment of the biometric data in its processor's Secure Enclave.
2015-03-26	Updated for latest release: New policy in Good Control to allow Touch ID immediately after application start ("coldstart")
2015-02-27	First issued

BlackBerry Dynamics and fingerprint authentication

This document describes the security of fingerprint recognition technology for user authentication in mobile applications with BlackBerry Dynamics, including the following vendor-specific biometric solutions:

- Android Fingerprint
- Apple Touch ID
- Samsung Pass

This paper should help you make your own decisions about whether or not your organization wants to rely on fingerprint technology with BlackBerry Dynamics.

Standard behavior of fingerprint authentication without BlackBerry Dynamics

The standard behavior of fingerprint recognition without BlackBerry Dynamics software can be generalized as follows:

- If authentication with fingerprint recognition fails a certain number of times in succession, the application prompts the user for a password.
- The user cannot return to the home screen unless the fingerprint recognition dialog is dismissed by either authenticating or by canceling the dialog.

This standard behavior is not changed by BlackBerry Dynamics.

BlackBerry Dynamics' generalized approach: policy control

If a user has not enabled fingerprint recognition on a device, then enabling fingerprint authentication in Good Control or BlackBerry UEM has no effect. That is, the user must indicate the desire to use fingerprint recognition; it is not imposed by the system.

Regardless of the specific platform's implementation of fingerprint recognition, BlackBerry Dynamics takes a generalized approach: administrator-managed policy.

BlackBerry's support for fingerprint recognition is a supplement to standard BlackBerry secure user authentication, not a replacement for it. BlackBerry Dynamics includes the following kinds of policies related to Touch ID. These settings are configured by way of policies in Good Control or BlackBerry UEM.

- Allow or disallow fingerprint authentication for BlackBerry Dynamics-based applications in general
- If fingerprint authentication is allowed in general, you can also allow or disallow it for BlackBerry Dynamics applications immediately after application coldstart. If you do not allow it after application coldstart, the user must enter the password for the application.
- Require the end-user to enter a password after a specified time interval.

Application developers: no work necessary

Developers of BlackBerry Dynamics-based applications benefit from BlackBerry's fingerprint authentication support in several ways:

BlackBerry Dynamics and fingerprint authentication

- No additional programming is required. All necessary work is done by the BlackBerry Dynamics SDK itself.
- Fingerprint authentication can be enabled or disabled quickly in Good Control or BlackBerry UEM by the IT administrator, without the developer's intervention.

Android Fingerprint

Android Fingerprint is a fingerprint recognition system from Google for some Android devices, [discussed from a programming perspective by Google](#).

Considerations about Android Fingerprint

Security ramifications depend on how your Android Fingerprint policies are configured, with options described in [Android Fingerprint policies in Good Control](#) and [Android Fingerprint policies in BlackBerry UEM](#).

Disallowing Android Fingerprint after application coldstart

When Android Fingerprint immediately after application coldstart is not allowed, Android Fingerprint does not alter the security of BlackBerry Dynamics-enabled application data on the device, which remains secure with or without the use of Android Fingerprint. In this case, the application keystore is not used as part of BlackBerry Dynamics's Android Fingerprint integration. The application is secured by the application container's password.

Allowing Android Fingerprint after application coldstart

By contrast, when Android Fingerprint after application coldstart *is* allowed, a BlackBerry Dynamics-based application stores key information in the keystore, which is protected by the device passcode.

This means that the application container's password adds no extra security and the contents of the application container are protected only by the device passcode.

If the device passcode is disabled or removed, the Android-Fingerprint-related information stored by the BlackBerry Dynamics application is removed from the keystore. The end-user can no longer use Android Fingerprint to authenticate to the application after coldstart but must authenticate with the application password instead.

If the user subsequently enables the device passcode, the ability to use Android Fingerprint to unlock an application after coldstart is re-enabled, after the next time the user unlocks the application with the application password.

Android Fingerprint policies in Good Control

The Good Control administrator can specify the behavior of Android Fingerprint via security policy.

Shown below are the clickpaths in Good Control to change the settings.

1. **Policy Sets > *edit a policy* > Security Policies > Password Policies >** checkmark or uncheckmark **Allow Android Fingerprint for Idle Unlock**, . The default is "Not Allowed".
2. The second setting determines if Android Fingerprint is allowed immediately after application coldstart and is displayed only if Android Fingerprint in general is allowed. If Android Fingerprint after application coldstart is not allowed, the user must enter the application password that was set at activation.
3. The third setting determines when a user must periodically enter the password that was set when the application was activated.

Android Fingerprint policies in BlackBerry UEM

The UEM administrator can specify the behavior of Android Fingerprint via the BlackBerry Dynamics profile.

Android Fingerprint

Shown below are the clickpaths in the UEM to change the settings.

1. Navigate to **Policies and profiles > BlackBerry Dynamics profiles > Allow Android fingerprint authentication**. Check the checkbox to enable. The default is "Not Allowed".
2. The second setting determines if Android Fingerprint is allowed immediately after application coldstart and is displayed only if Android Fingerprint in general is allowed. If Android Fingerprint after application coldstart is not allowed, the user must enter the application password that was set at activation.
3. The third setting determines when a user must periodically enter the password that was set when the application was activated.

User experience when Android Fingerprint is allowed

In the case that the "Allow Android Fingerprint" password policy has been set to "Allowed" for the user, the user can choose to enable or disable the use of Android Fingerprint to unlock a BlackBerry Dynamics application at the time the user sets or changes the BlackBerry Dynamics application password. The Android operating system guides the user to the necessary settings to enable Fingerprint, if he so chooses.

Even if Fingerprint is allowed by policy, the user must set an application password when the application is activated.

If the IT administrator allows Android Fingerprint in general and also after an application coldstart, the user is prompted with the Fingerprint screen to authenticate when a BlackBerry Dynamics application is started or idle-locked.

If Android Fingerprint is not allowed in general by the IT administrator, it is never presented as an option to the end-user.

About Samsung Pass

Samsung Pass is Samsung's implementation of fingerprint security on Android.

With BlackBerry Dynamics, Samsung Pass behaves identically to Android Fingerprint and is governed by the same Good Control policies that govern the use of Android Fingerprint.

For Samsung Pass, some programming is required to include a special library that is delivered with the BlackBerry Dynamics SDK for Android.

Known limitations in Samsung Pass

A known limitation in Samsung Pass is that Samsung Pass does not have any API to detect newly added fingerprints and thus never invalidates the previous fingerprints. This means that BlackBerry Dynamics has no mechanism to prompt the user to reactivate an application when a new fingerprint is added. This limitation also applies to the S 5 and Note 4 Samsung devices running Android M, which have recently begun to be supported by BlackBerry.

Apple Touch ID

Apple Touch ID is a fingerprint recognition system for some iOS devices and is [described in great detail by Apple](#).

According to Apple, the Touch ID biometric data is always directly stored by the iOS Touch ID system in the Apple processor (such as, the A7) Secure Enclave and never accessible by any application. More details of Apple's security and the Secure Enclave are in Apple's document at https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Allowing Touch ID after application coldstart

When Touch ID after application coldstart is allowed, a BlackBerry Dynamics-based application stores key information in the keystore, which is protected by the device passcode.

This means that the application container's password adds no extra security and the contents of the application container are protected only by the device passcode.

If the device passcode is disabled or removed, the Touch-ID-related information stored by the BlackBerry Dynamics application is removed from the keychain. The end-user can no longer use Touch ID to authenticate to the application after coldstart but must authenticate with the application password instead. If the user subsequently enables the device passcode, the ability to use Touch ID to unlock an application after coldstart is re-enabled, after the next time the user unlocks the application with the application password.

Summary of options and comparison of coldstart/warmstart behaviors on iOS

The terms *coldstart* and *warmstart* in reference to applications are defined below. In addition, for iOS, the behavior of applications based on the settings of Good Control or BlackBerry UEM are compared.

	Coldstart	Warmstart
Definitions	When an application is terminated by iOS or the end user, and started again, it is considered a <i>coldstart</i> .	When an application remains in memory and is resumed by the user, it is considered a <i>warmstart</i> .
Capability	Allows end users to use fingerprint to login/authenticate to BlackBerry Dynamics-based applications even if the application has been terminated by iOS or the end user.	Allows end user to authenticate using a password on coldstart and fingerprint on warmstart. Warmstart is utilized when the application remains in memory, and not terminated by iOS.
Usage	To use Touch ID user must set a device password between 4 and 6 numbers long.	
Fallback	If the user removes the fingerprint or removes the device passcode, Touch ID is not used by BlackBerry Dynamics application, and the applications fallback to passwords.	
Options	The IT administrator can enable the "Force Password Reentry" policy to required the user to authenticate with a password every hour or at intervals of hours.	
Application password required	The application will prompt for password in these conditions:	Same as coldstart plus: When coldstarted, the application will prompt for a password.

Apple Touch ID

Coldstart	Warmstart
	<ul style="list-style-type: none"> Initial password set on application activation Password change, either initiated by user or password expiration. Device passcode is changed Fingerprint set is changed (iOS 9 or higher and latest versions of the BlackBerry Dynamics SDK) Time interval specified in "Force Password Reentry" policy to reauthenticate with password has expired. See "Options," above. User's entry of fingerprint has failed too many times. User cancels the entry of a fingerprint.
Relation to BlackBerry Dynamics authentication delegation	<p>Multi-authentication delegation in BlackBerry applications allows the administrator to define BlackBerry Dynamics-based applications that can authenticate the user for other BlackBerry Dynamics-based applications.</p> <p>Multi-authentication delegation is not affected by enabling fingerprint authentication, except that the end-user authenticates with a fingerprint rather than a password.</p>

Apple Touch ID policies in Good Control

The Good Control administrator can specify the behavior of Touch ID via security policy for application.

Shown below are the clickpaths in Good Control to change the settings.

1. Device: **Device Policies** > *edit a policy* > **Restrictions** > **iOS heading** > **Edit** > check or uncheck **Allow Touch ID to unlock devices (iOS 7+)**. The default is "Allowed".
2. Good-based Applications, Touch ID settings:
 - **Policy Sets** > *edit a policy* > **Security Policies** > **Password Policies** > checkmark or uncheckmark **Allow Touch ID for Idle Unlock**. The default is "Not Allowed".
 - The second setting determines if Touch ID is allowed immediately after application coldstart and is displayed only if Touch ID in general is allowed. If Touch ID after application coldstart is not allowed, the user must enter the application password that was set at activation.
 - The third setting determines when a user must periodically enter the password that was set when the application was activated. The default is 1 day.

Apple Touch ID policies in BlackBerry UEM

The UEM administrator can specify the behavior of Touch ID via the BlackBerry Dynamics profile.

Shown below are the clickpaths in UEM to change the settings.

Apple Touch ID

1. Navigate to **Policies and profiles > BlackBerry Dynamics Profile > Allow Touch ID**. Check the checkbox to enable. The default is "Not Allowed".
2. The second setting determines if Touch ID is allowed immediately after application coldstart and is displayed only if Touch ID in general is allowed. If Touch ID after application coldstart is not allowed, the user must enter the application password that was set at activation.
3. The third setting determines when a user must periodically enter the password that was set when the application was activated. The default is 1 day.

User experience when Touch ID is allowed

In the case that Touch ID is enabled on the iOS device and the "Allow Touch ID" password policy has been set to "Allowed" for the user, the user can choose to enable or disable the use of Touch ID to unlock a BlackBerry Dynamics application at the time the user sets or changes the BlackBerry Dynamics application password.

Even if Touch ID is allowed by Good Control or UEM policy, the user must set an application password when the application is activated.

If the IT administrator allows Touch ID in general and also after an application coldstart, the user is prompted with the Touch ID screen to authenticate when a BlackBerry Dynamics application is started or idle-locked.

If Touch ID is not allowed in general by the IT administrator, it is never presented as an option to the end-user.

Additional use cases and policy interactions

This section describes the behavior BlackBerry Dynamics's support for Touch ID in some specific use cases.

Touch ID policy with periodic password enforcement

When enabling the policy for Touch ID at cold start, the IT administrator can optionally set a time frame to prompt the user for an application password instead of using Touch ID for authentication. The policy is **Require Password not Fingerprint after N period since Password last used**. Interval can range from 1 hour to 7 days. Default is minimum of every day.

Stolen device

If a device set with the policy to enable Touch ID is stolen when the device is already unlocked or if the thief guesses the password, BlackBerry Dynamics or iOS itself still protect the device:

- The thief cannot access the application containers on the device via Touch ID, because stealing a person's fingerprint is next to impossible.
- If the thief succeeds in adding a new fingerprint, removing a stored fingerprint or disabling Touch ID (for all of which iOS itself requires that the thief authenticate with the fingerprint), iOS prompts for the device passcode. In addition, in this case, the next time a BlackBerry Dynamics application is launched, BlackBerry Dynamics detects the change in fingerprints and prompts the user for the application container's password, as follows: "Due to a device touch ID or Password Settings change, your password is required".
- If the thief's attempts to authenticate with fingerprint fails five times, iOS itself requires the thief to authenticate with the device passcode. The application containers are unaffected. Reference from Apple: "... Touch ID only allows five unsuccessful fingerprint match attempts before you must enter your passcode" at [About Touch ID security on iPhone and iPad](#).

Apple Touch ID

You might consider enforcing a complex password scheme to increase the security of the passwords.

Shared device

Apple allows up to five fingerprints, which can belong to different users (see forum discussion at <https://forums.developer.apple.com/thread/65847>), but iOS does not support the “multi-user OS” concept; that is, multiple fingerprints do not map to multiple users.

Likewise, BlackBerry Dynamics does not support the concept of multiple users sharing the same applications on a device; that is, the relation of application to device to policy to user is 1:1:1:1. Only a single instance of an application can be installed on the device.

Thus, the users sharing the device can login with separate fingerprints but the underlying password for fallback is identical, the enforcement of the password policies is identical, the encryption of the “shared” application containers is identical because in reality the device is not truly “shared”; it belongs to a “single” user. All users who access the device share the same data.

GFE with Apple Touch ID

Described here are aspects of Apple Touch ID fingerprint authentication with BlackBerry Mobile Control (GMC) and BlackBerry For Enterprise (GFE).

Policies in BlackBerry mobile control

The BlackBerry Mobile Control administrator can specify the behavior of Touch ID via policy for the device and authentication policy for the GFE application.

These policies are independent of one another.

Shown below are the clickpaths in BlackBerry Mobile Control to change the settings.

1. Device: **Policies** > *edit a policy set* > **Restrictions** > **Mobile Device Management heading** > **iOS Configuration** > **Policies** tab > check or uncheck **Allow fingerprint for unlock**. The default is “Allowed”.


Platform Support

General | **Passcode** | **Restrictions** | WiFi

Restriction policy settings are enforced by iOS and cannot be modified
*** Changing these options will require the user to install a new MDM Profile**

Enable Restrictions *

Device Functionality
Enable use of device features

- Allow installing apps**
- Allow use of camera**
 - Allow FaceTime** ⚠
- Allow screen capture**
- Allow syncing of consumer email accounts while roaming** ⚠
- Allow voice dialing** ⚠
- Allow In-App purchases** ⚠
- Allow Siri Assistant** ⚠
 - Allow Siri while device locked** ⚠
- Allow multiplayer gaming** ⚠
- Allow adding Game Center friends** ⚠
- Allow Passbook While Device Locked** ⚠
- Allow lock screen notifications view** ⚠
- Allow lock screen today view** ⚠
- Allow fingerprint for unlock** ⚠ 
- Allow lock screen control center** ⚠

iTunes Settings

2. GFE settings:

- **Policies > edit a policy set > BlackBerry For Enterprise Policies heading > BlackBerry for Enterprise Authentication > Lock Screen Protection Show>> > Allow Touch ID**, as shown below. The default is "Not Allowed".
- The second setting determines if Touch ID is allowed immediately after application coldstart and is displayed only if Touch ID in general is allowed. If Touch ID after application coldstart is not allowed, the user must enter the application password that was set at activation.



GFE/GMC complete control by policy

With GFE and GMC the user cannot cannot disable Touch ID as a substitute for password authentication from within the GFE device client. The settings are completely controlled by the policies in GMC.

BlackBerry Dynamics documentation

Category	Title	Description
Cross-platform	<ul style="list-style-type: none"> Getting Started Guide for Marketplace Partners Good Control/Good Proxy Platform Overview for Administrators and Developers 	Overviews of the BlackBerry Dynamics system
	<ul style="list-style-type: none"> Good Control Device and Application Management Good Control Device Management Enrollment: Good Agent for iOS Good Control Device Management Enrollment: Good Agent for Android 	Device and application management on Good Control, including app distribution, with client-side device enrollment details
Security	BlackBerry Dynamics Security White Paper	Description of the security aspects of BlackBerry Dynamics
	BlackBerry Dynamics and Fingerprint Authentication	Discussion of the implementation of BlackBerry security with fingerprint recognition systems: Apple Touch ID and Android Fingerprint
BlackBerry UEM	BlackBerry UEM Administration Guide	Approaches to administering the BlackBerry Unified Endpoint Manager
	Getting Started with BlackBerry UEM and BlackBerry Dynamics	Introductory material to administering the BlackBerry UEM with the BlackBerry Dynamics profile
Good Control	<ul style="list-style-type: none"> BlackBerry Secure Enterprise Planning Guide BlackBerry Secure Servers Compatibility Matrix BlackBerry Performance Calculator 	Guidelines and tools for planning your BlackBerry Secure Enterprise deployment
	Good Control/Good Proxy Server Preinstallation Checklist	Same checklist extracted from the installation guide below
	Good Control/Good Proxy Server Installation	Details on installing Good Control, Good Proxy, and the GC database
	Kerberos Constrained Delegation for Good Control	Configuration details for integrating the Kerberos authentication system with BlackBerry Dynamics

BlackBerry Dynamics documentation

Category	Title	Description
	Direct Connect for Good Control	Configuring BlackBerry Dynamics servers to securely access internal resources from the external Internet
	Good Control Easy Activation Overview	A look at the Easy Activation feature
	Good Control/Good Proxy Server Backup and Restore	Minimal steps for backing up and restoring the BlackBerry Dynamics system
	Good Control Online Help	Printable copy of the GC console online help
	PKI Cert Creation via Good Control: Reference Implementation	A reference implementation in Java for creating end-user PKI certificates via Good Control and a Certificate Authority (CA)
	Good Control Cloud Online Help	Printable copy of the Cloud GC console online help
	Technical Brief: BlackBerry Dynamics Application Policies	Description of formatting application policies for use in Good Control, with examples.
	Good Control Web Services	<p>Programmatic interfaces on Good Control</p> <ul style="list-style-type: none"> • Basic control and application management: SOAP over HTTPS. Documentation is in the WSDL files included with GC. • Device management: HTTP API (with JSON) for device management. Zipfile of API reference.
Software Development	Developer Bootstrap: Good Control Essentials	Bare minimum of information that a developer of BlackBerry Dynamics applications needs to get started with the Good Control server to test applications.
	BlackBerry Dynamics Shared Services Framework	Description of the BlackBerry Dynamics shared services framework for software developers
Android	<ul style="list-style-type: none"> • Getting Started with the BlackBerry Dynamics SDK for Android • API Reference for Android 	Working with the BlackBerry Dynamics SDK for Android and the essential reference for developers
iOS	<ul style="list-style-type: none"> • Getting Started with the BlackBerry Dynamics SDK for iOS • API Reference for iOS 	Working with the BlackBerry Dynamics SDK for iOS and the essential reference for developers
macOS	<ul style="list-style-type: none"> • Getting Started with the BlackBerry Dynamics SDK for macOS • API Reference for macOS 	Working with the BlackBerry Dynamics SDK for macOS and the essential reference for developers

BlackBerry Dynamics documentation

Category	Title	Description
Windows	<ul style="list-style-type: none"> Getting Started with the BlackBerry Dynamics SDK for Universal Windows Platform (UWP) API Reference for UWP 	Working with the BlackBerry Dynamics SDK for Universal Windows Platform (UWP) and the essential reference for developers
iOS, Android	BlackBerry Launcher Library	Source code and header files for implementing the popular BlackBerry Launcher interface
Cross-platform	BlackBerry Dynamics Cordova for iOS and Android	Working with the BlackBerry Dynamics SDK and the Cordova plugins
	BlackBerry Dynamics Secure HTML5 Bundle Getting Started Guide for Developers	Working with the BlackBerry Dynamics SDK and the secure HTML5 bundle
	BlackBerry Dynamics Bindings for Xamarin.Android	Working with the BlackBerry Dynamics SDK and the Xamarin cross-platform integrated development environment For Xamarin.Android, no separate API reference is needed; see the standard BlackBerry Dynamics SDK API Reference for Android
	BlackBerry Dynamics Bindings for Xamarin.iOS and the API Reference for Xamarin.iOS	Working with the BlackBerry Dynamics SDK and the Xamarin cross-platform integrated development environment