Good Control User Self Service Online Help

Version 4.2

©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.

Table of Contents

Overview

Welcome to BlackBerry Dynamics from BlackBerry, Inc.

With Good Control, you can provision access keys that allow you to activate and run BlackBerry Dynamics applications on your mobile devices, upload certificates to authenticate your sessions, manage your devices (when Good device management is active), and more.

This is the online help for the User Self Service portal of Good Control.

Understanding our terminology

The following terminology is used this help and the Good Control console.

Access Key	A one-time 15 character code required to activate a BlackBerry Dynamics application for the first time. When an access key is generated for a user, GC sends the key to the email address it has on file for the user. The access key is also available to the user in the self-service portal.
Application (or BlackBerry Dynamics App)	A specific native application developed with BlackBerry Dynamics. An application can have multiple versions.
Application Group (or Group)	A collection of users to which the same base application permissions are applied.
Container	A secure storage area on the device controlled by the BlackBerry Dynamics framework. Only one application runs in a container, so if a user has multiple applications on a device, the user also has multiple containers.
Device	A phone, tablet, or emulator running one or more BlackBerry Dynamics applications, each in a separate container.
Good Control (GC)	The web-based console for managing access keys and viewing which devices are running which BlackBerry Dynamics applications.
User	An account imported into GC from Active Directory. A user can have more than one device or container and is identified in GC by an email address.

Activating your first BlackBerry Dynamics application

This is a general overview of how to activate an application on your device. Other help topics have more information about this and other aspects of the system.

1. Provision an access key.

   Log into your Good Control account and provision an access key for yourself. The access key is sent in an email to your corporate email address.

2. Download and install the application.

   Depending on how your organization publishes BlackBerry Dynamicsapplications, you can download from the App Store or an enterprise application distribution server. Also, the email with the access key might include a link where the application can be downloaded.

3. Launch and activate the application.

   Launch the application on your device. Enter your email address and access key to activate the application.

Using your account

User accounts - overview

From the account management screen, you can view the following:

- The name of the policy set assigned to you.
- The applications you are permitted or blocked from using.
- The names of any application groups you belong to.
- The applications installed on your devices.
- The history of access keys sent to your email account.
- The history of policy enforcement changes to each of your containers.

See also Managing your devices.

Viewing application permissions

Click the **Applications** tab to view a list of applications that you have been granted or denied access to. Your access is based on a combination of user-level and group-level permissions.

Click the toggle for an application to expand or hide a list of allowed or denied application versions. To view resolved permissions for an application version, click the version number or the **Info** icon. You might see references to Everyone or User or any of the groups you belong to.

Note: The same application can show up in both the allowed and denied lists, because permissions are applied at the version level, not the application level, so some versions of the application can be allowed and others can be denied. You can expand the application in both lists to view which versions are allowed and which are denied.

You can inherit permissions from the Everyone group or application groups created by GC administrators. Groups created by GC administrators can have permissions that refine or override Everyone group permissions. Permissions set at the user level override any permissions set at group level and Everyone group level.

Activating an application

If you want to install and activate an application, you first need permission to run the application. Your IT administrator grants this permission.

In addition, you need an access key. You must enter this key when you run the application for the first time. The access key is a 15 character code sent in an email to your company email address. Access keys have the following characteristics:

- They can only be used once. They are no longer usable after they activated an application.
- They are not specific to an application. For example, a user sent four access keys can use activate any four applications to which he is entitled.
- They cannot be used for re-activation. If you uninstall/reinstall an application on the same device, then you need a new activation. This is also applicable to new or factory-reset devices and to device emulator without persistent state. However, you can use multiple, different keys to activate the same application multiple times.
- They are usually configured to expire after a specified period of time. See the **Access Keys** tab to see when your unused access keys expire.

To provision access keys for yourself, click the **Access Keys** tab, select a number of keys, and click **Provision**.

Activation keys are then sent to your enterprise email address. There is one email message per key. Additionally, the keys are listed on the **Access Keys** tab.

After you have an unexpired key and you have installed a BlackBerry Dynamics application on your device, you can activate the application. When you start an application, the BlackBerry Dynamics user activation interface is displayed. You must enter the activation key and your enterprise email address.

After you enter the correct key, activation finishes, and the key cannot be used again. The application is then usable on the device, and the key is removed from the **Access Keys** tab.

Resending or deleting access keys

When you provision an access key, Good Control sends email to your enterprise email address. This email contains the key that to enter in the BlackBerry Dynamics application on your device to activate it. If this email is lost or is deleted, you can request that it be sent again. Here are some of the actions on the account screen:

- Go to the account screen and open the **Access Keys** tab. Click the **Email** icon for an access key to resend the email.
- If you need to delete an access key, from the **Access Keys** tab, click the **Delete** action for the access key. The key is canceled.
- Expired access keys can be canceled but not resent. If you have lost the provision email, and the access key has expired, cancel the expired key and provision a new key.

Managing your devices

With the Good Control console, you can see which application versions are installed on which devices, and when Good device management is enabled on your Good Control, you can perform device-related actions.

- Go to your account screen, click the **Devices** tab to view a list of the devices that have activated BlackBerry Dynamics applications.
- Expand the toggle for a device to see a list of all BlackBerry Dynamics application versions activated on that device.
- Detailed history is available for each of the application versions. Click the ID of an application or its **Info** icon to view a history log that contains policy compliance information, broken down by event.
- Click the toggle to view messages back and forth from the device and the GC system.

For additional container management actions, please see Locking or wiping an application and Unlocking an application.

Device-related actions

When Good device management is enabled in Good Control, you can perform several device-related actions:

- Lock Device
- Clear Device Password
- Wipe Device

Locking or wiping an application

The Good Control console allows you to lock applications or wipe application data on your devices.

- Go to your account screen, click the **Devices** tab to view a list of the devices that have activated BlackBerry Dynamics applications.
- Expand the toggle for a device to see a list of all BlackBerry Dynamics application versions activated on that device.
- To wipe application data from a your device, click the application version's **Delete** icon to initiate the wipe.
- To lock the application and prevent anyone from accessing it, click the application version's **Lock** icon.

To unlock an application, see Unlocking an application.

Unlocking an application

BlackBerry Dynamics applications on your device can become locked for a variety of reasons, including password authentication failure or your device being out of compliance with a policy. In addition, you or an administrator can explicitly lock the applications.

To unlock an application, make sure the **Devices** tab is active, then click the **Unlock** icon for the application you want to unlock. The console then displays one of the following panels. Follow the appropriate instructions below.

- If a button labeled **Generate** appears, press the button to generate an unlock key. The key is displayed on the console, and it is also sent to your email address.

  Launch the application. Then enter your email address and unlock key to unlock the application.

- However, if a series of small boxes appears, launch the application on your device to receive an unlock code.

  Enter the code from your device into the fields displayed on the GC console. If you enter the code correctly, GC generates another unlock code and displays it on the screen. Enter this code correctly into the unlock screen on the device to unlock the application.

  Note: This procedure can also be used to reset your password.

Troubleshooting application issues

The Good Control console has some useful options for troubleshooting BlackBerry Dynamics applications. To get more information about application related issues, application developers or IT administrators might ask you to do certain actions on the console. These actions are described below.

- To configure an application to generate more verbose, detailed logs, click the **Enable** icon. To disable detailed logging, click the **Disable** icon.
- You can initiate a request that an application upload its logs by clicking the container's **Upload** icon.

Uploading your own PKCS 12 (PKI) certificates to Good Control

Note: By default, PKCS 12 certificates uploaded to the GC must be used within 24 hours before the GC deletes them for security.

You can use your own personal certificates to secure communication between the GC and BlackBerry Dynamics-based applications. You can upload as many certificates as you need.

Certificate requirements and troubleshooting

Make sure your certificates conform to these requirements:

- Certificates must be in PKCS 12 format: Certificate Authority (CA), public key, and private key, all in the same file.
- The PKCS12 file must end with the extension `.p12` or `.pfx`.
- The PKCS 12 file must be password-protected.
- The minimum keylength for the certificates must be 2,048 bytes.

There are many sources of certificates:

- Your own internal certification authority (CA)
- A well-known public CA

- Tools from the Internet, such as OpenSSL's **`keytool`** command. For example, the following is sufficient to generate a PKCS 12 certificate that is usable with Good Control; subsitute your own vlues for alias the keystore name and the keystore password. If in doubt consult information on the Internet about all the possible options on the keytool command:

  ```
  keytool -genkeypair -alias good123 -keystore good123.pfx -storepass good123 -
  validity 365 -keyalg RSA -keysize 2048 -storetype pkcs12
  ```

Beware of weak ciphers from export

Personal Information Exchange files are encrypted, and therefore must be encrypted with FIPS-strength ciphers if to be used when FIPS is enabled on the employee’s security policy.

Note: For their own maximum interoperability with other systems, it is common for third-party applications, for example the Mac OSX keychain, to export identity material (credentials) using weak ciphers.

The administrator or employee can use a tool such as the OpenSSL command line to re-encrypt the file with a FIPS-strength cipher like so, which re-encryts with the AES-128-CBC cipher:

```
openssl pkcs12 -in weak.p12 -nodes -out decrypted.pem
<enter password>
openssl pkcs12 -export -in decrypted.pem -keypbe AES-128-CBC -certpbe AES-128-CBC -out strong.p12
<enter password>
rm decrypted.pem
```

Steps

To upload a PKCS12-format certificate file with either .p12 or .pfx file extension, in Good Control:

1. Click the **Certificates** tab.
2. Click **Upload**.
3. Navigate your computer to find the PKCS-12-format file with either .p12 or .pfx filename extension.
4. Select or open the file.
5. Follow the leading prompts to finish the upload.

GC then displays the date of the upload. GC cannot display more information about the certificate until you use the certificate at least once by entering the password to the certificate file. Until that password is supplied, the certificate is encrypted and details cannot be read from it.

Lifecycle and states of a PKCS 12 certificate

In Good Control, a PKCS 12 certificate can have any of the following states.

State	Description
Uploaded	Certificate has been stored on the GC

State	Description
Delivered	When the certificate has been sent to a GD application container
• Verified • Expired • Failed	After a GD application container has used the certificate. **Note:** Hover your cursor over the "Failed" state to see the reason for the failure.

Security: Close browser on logout

To maintain the security of the Good Control console, after you logout, it is best to close your browser window. This ensures that your session is completely terminated.