This walkthrough describes how you can enrol your mobile device or a iDENprotectPLUS Token as an iDENprotect Device to access iDENprotect-secured services and resources.

By successfully enrolling an iDENprotect Device, you can authenticate yourself in iDENprotect-secured systems by using a biometric sensor on your mobile device such as Touch ID fingerprint scan, or by entering your personal PIN code.

iDENprotect Devices are commonly integrated into enterprise solutions with MAM (Mobile Application Management) software. In this guide, the iDENprotect for BlackBerry application - available in App Store for iOS - is used as an example on how to enrol the device.

After successful enrolment, whenever you’re trying to access an iDENprotect-secured resource, the iDENprotect for BlackBerry App launches and requests your authentication.

Some BlackBerry products used in this walkthrough were known as Good products earlier. They are being rebranded at the moment, and old names may still be present in screenshots or applications.

Overview

The enrollment process requires actions from the Device User and iDENprotect Administrator. The following diagram presents a brief overview of the process:

Figure 1. iDENprotect Enrolment Process

Full details are found later in this document. This walkthrough describes what steps the User and the Administrators must perform during the enrolment process, and in what order.
Preparation

To successfully register and enrol the device, the User needs to know several essential pieces of information. It is the Administrator's responsibility to provide these to the User:

- iDENprotect Server URL
- BlackBerry Access Key

The user also needs iDENprotect for BlackBerry App, which is available in App Store for iOS.

BlackBerry Access Key is generated in BlackBerry Control Dashboard or BlackBerry Control Quick Start. It is a 15-character alphanumeric One-Time Password which expires after it has been used in iDENprotect enrolment.

When BlackBerry Access Key is generated, it is delivered to the User via email. We recommend adding iDENprotect Server URL and other organization-specific information in the email, so that the User has all the necessary information in a single resource.

Figure 2. Creating an Invite Email

To generate a BlackBerry Access Key to the User, the Administrator has to:

1. Log in to your organization's BlackBerry Control
2. Open Users and Groups
3. Find the user you want to enable iDENprotect authentication for. If the user doesn’t exist yet, you need to create the user account first.
4. Open Access Keys
5. Press New Access Key. The user receives an email containing the BlackBerry Access Key.
Now, the User should have installed iDENprotect for BlackBerry App, and received the BlackBerry Access Key by email.

Only generate BlackBerry Activation codes on the same server that is used to manage the BlackBerry Dynamics ecosystem.
Registering Device

Full network connectivity is required for the enrolment process. If there are problems with the network, a persistent spinning wheel or error dialog will appear.

The use of Touch ID requires a light placement of the finger on the sensor. Pressing too hard will send the application to background and interrupt the enrolment sequence.

To Register the Device, the User has to:

1. Launch iDENprotect for BlackBerry
2. Select Locally installed security

![Launch Screen](image)

Figure 4. Launch Screen

3. Enter email address and the iDENprotect server URL

![Entering iSPA Details](image)

Figure 5. Entering iSPA Details

4. Press Register and wait for the BlackBerry screen to appear
5. Enter email address and BlackBerry Access Key, received in an earlier email
6. Click **Continue**

The mobile device is now **Registered** in the iDENprotect\textsuperscript{SERVER}, and the iDENprotect for BlackBerry displays an Activation Code screen.

---

**Figure 6. Logging into BlackBerry Dynamics**

---

**Figure 7. Activation Code Screen**

---

Keep the Activation Code screen on the foreground until you have finished enrolment.

The next steps differ slightly, depending on whether LDAP authentication has been enabled on the iDENprotect\textsuperscript{SERVER}.

If LDAP is enabled, the User's identity in the organization's LDAP directory is validated automatically. You can continue to section **Enrolling Device**.

If LDAP is not enabled, the iDENprotect Administrator must manually verify that the recently registered device and its User are valid for the organization, and **assign** the device to the User.
Assigning Device

If you are using LDAP directory lookup with auto-enrolment, skip this section.

Before the User can continue with enrolling the device, the iDENprotect Administrator has to:

1. Log in to your organisation's iDENprotect Management Console. iDENprotect Management Console is the web interface for managing iDENprotect server, usually located in URL https://your.idenprotectserver.url
2. Open Manage Users tab
3. Locate the recently registered Device. Usually this can be recognised as one of the few devices in REGISTERED state.

4. Press Assign
5. Enter the user’s First Name and Last Name. If you have set up LDAP lookup, you can search for the user from the LDAP directory.

Figure 8. Users View - Note the Different Device States

Figure 9. Assigning the Device to the User
6. Press **Submit**

After this step, iDENprotect Server sends an email that contains the Activation Code to the User. The email is sent to the address listed in **Email Address** field. The default value for this is the email address entered by the user during device registration.

The Activation Code consists of 8 digits.

Note that the User cannot proceed further with enrolment before the Administrator has **assigned** the device. The User’s **iDENprotect for BlackBerry** application remains in the Activation Code screen.
Enroling Device

The User must have kept iDENprotect for BlackBerry in the foreground to continue successfully from this point onwards. When iDENprotect for BlackBerry is put to background before the enrolment process is finished, the application resets any progress and returns to the first menu.

If you have closed iDENprotect for BlackBerry in the meantime, restart the process from section Registering Device. If you have trouble re-registering, see Troubleshooting.

After the User has received the Activation Code via email, the User has to:

1. Enter the Activation Code. The enrolment starts.

2. Enter a PIN code that the User will use for authentication in future iDENprotect transactions, if biometric identification is not available. The PIN must be at least 4 digits long.

3. Confirm the PIN by entering it a second time.
4. Select whether to use Touch ID instead of PIN when Touch ID is available.
5. Press the Unlock icon in the middle of the screen.
6. Authenticate with Touch ID
You may have to perform Touch ID authentication twice due to device security requirements.

7. Click on the Synchronize with BlackBerry button.

8. Authenticate with Touch ID one final time.

![Figure 12. Final Steps](image)

After the User has successfully synchronised the mobile device with BlackBerry framework, the enrolment is complete and the device is Enrolled on the iDENprotect SERVER. The mobile device displays an "iDENprotect unlocked" screen.

The "iDENprotect unlocked" may be misleading because the User expects something more to happen even though the enrolment process has been completed. This is an Apple restriction on App controls. However, the next releases will provide a more graceful approach to close the App.

The mobile device is now ready for use as an authentication module in iDENprotect-compliant applications.
Testing Enroled Device

when iDENprotect for BlackBerry has been installed on the device and the User has successfully enroled the device, the User can authenticate in iDENprotect-compliant applications. To test this, the User has to:

1. Download and install an iDENprotect-compliant application. In this walkthrough, BlackBerry Access from App Store is used.
2. Launch BlackBerry Access.
3. Select “Set up using iDENprotect for BlackBerry”

![BlackBerry

Access can be set up using the password for one of the following applications or by using the Access Key provided by an Administrator.

Application for amqcp991:

Set up using iDENprotect for Good

Set up using your Access Key

Figure 13. Selecting an Authentication Option

4. Authenticate in iDENprotect for BlackBerry using Touch ID or PIN.

![Information

When activating BlackBerry apps with iDENprotect, the activation proceeds in the background even though the BlackBerry Access interface gives no indicators of progress. This will be mitigated in later releases with a progress bar.

Please be patient and allow the process to finish.

Using BlackBerry Access application usually requires a separate Access Key from a BlackBerry Administrator. When using iDENprotect authentication, this separate authorization step can be avoided.
Troubleshooting

My iDENprotect Authentication Hangs With no Progress

Due to the design of iOS, the iDENprotect for BlackBerry App remains in background instead of closing completely when it is swiped off screen. This feature can conflict with iDENprotect security controls, making the App hang during an authentication attempt. To solve this, force the App to close:

1. Hit the home button twice to access the iOS app switcher
2. Swipe up the iDENprotect for BlackBerry application to fully close the App

Then retry authenticating.

I get a DRA Error when Enroling

This is most likely caused by multiple enrolment attempts from the same device. The device ID is stored in the iDENprotectSERVER and it is not removed even if iDENprotect for BlackBerry is temporarily uninstalled from the device. The Administrator must first remove the existing device ID from the iDENprotectSERVER:

1. Log in to iDENprotectSERVER Management Console
2. Open Devices tab
3. Locate the correct device by user email and device state
4. Press Delete

Any Devices in the Devices tab that do not have an email associated with them are orphaned and can safely be removed.

Every new install of iDENprotect for BlackBerry generates a new unique serial number. Later iDENprotect releases will improve on the management of new and orphaned serial numbers.