Bluink Key User Guide

Version 3.0

TABLE OF CONTENTS

INTRODUCTION

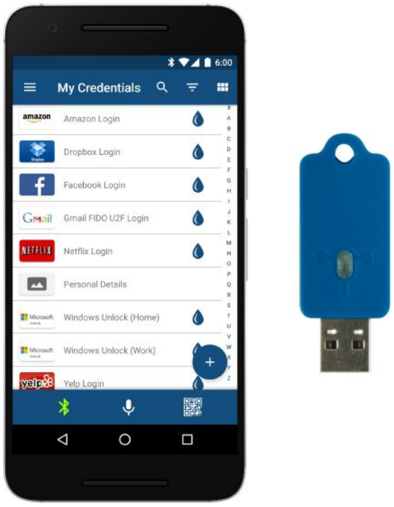
BLUINK KEY OVERVIEW

Bluink Key is a smartphone-based universal authentication solution, with strong authentication and login support for any system. With Bluink Key, users can forget their passwords and use their smartphones to effortlessly log in to anything. The solution supports many types of authentication including static passwords, one time passwords (TOTP or HOTP), and public key authentication via FIDO U2F. Bluink Key is FIDO U2F certified: fidoalliance.org/certification/fido-certified. Bluink Key can provide two-factor and three-factor authentication.

Users only have to remember one password which unlocks their digital login credentials within the Bluink Key app locally on their smartphone. Unlike other password management systems nothing is stored in the cloud. All sensitive information is securely encrypted and carried on the user's smartphone. With a single tap, a scan of a QR code, or a voice command, a user can log in to any system automatically once the app is unlocked.

Bluink Key requires no software installs on any machine. The solution is an app that is installed on the user's smartphone and is available for iOS and Android. Since no software is required, Bluink Key will work with any existing system, whether it is a computer login (Mac, Windows, Linux), a website, remote computer, or even a full-disk encryption system unlock at pre-boot.

Using a Bluink Key USB device, the smartphone makes a direct, wireless connection via Bluetooth with the computer and information is sent over an encrypted, mutually authenticated channel. The key also allows users to control their computer with their smartphone with the keyboard and touchpad function. While not necessary, the Bluink Key provides an enhanced user experience through the automation of logins to any system and is also necessary for FIDO U2F public key authentication.



App User Interface and Bluink Key

KEY CONCEPTS

Bluink Password

In order to use the app, you need to set a Bluink password. Your Bluink password is used to protect your sensitive information in the app and in backups so make sure it is strong. You can change your Bluink password in the `Settings` view.

IMPORTANT: Do not forget your Bluink password or you will not be able to access your protected information.

Credentials

The term ‘credentials’ describes the information you manage with Bluink Key including usernames and passwords. Use the `Credentials` screen to view and edit existing credentials, or add a new ones using the plus icon. Select a predefined credential template from a category to help you get started, or define your own custom credential by choosing an Empty Set.

Within the credentials are credential items. These are the elements that actually hold your information such as account IDs, passwords, and credit card numbers. You access credential items by tapping on the credential.

Automation

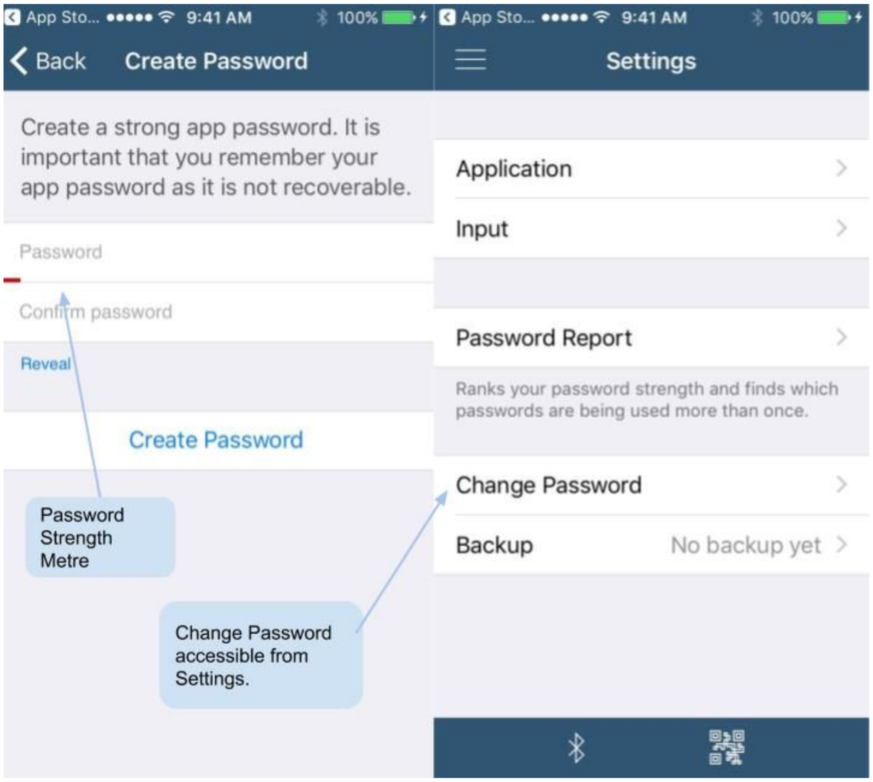
Credentials can be created using templates that automate the use of your credential items. Choose from the latest templates available from the Bluink Key web service when you create a credential to use this feature. Empty Credentials can also be automated so long as they include an account ID, password, and URL.

Bluink Key

If you have a Bluink Key, you should take ownership of it in `Bluink Keys`. Doing so will allow your smartphone to securely connect to your Bluink Key and prevent unauthorized phones from connecting.

SET BLUINK PASSWORD

Create a strong app password. As you type, the strength indicator will indicate the strength of your password; we recommend a password that fills the strength metre. **It is important that you remember this one password as it is not recoverable.** You can change your password in `Settings` at any time.



Create a strong app password. It is important that you remember your app password as it is not recoverable.

Ranks your password strength and finds which passwords are being used more than once.

Password Strength Metre

Change Password accessible from Settings.

CREDENTIALS

This view allows you to create a new credential or modify an existing one. You create a new credential simply by tapping the plus icon. Select a category, then you can choose from a list of predefined credential templates which will have credential items already defined (with no values). You can always add and delete credential items in a credential template. Alternatively, you can create a custom credential by selecting Empty Set, which will create an empty credential that you can then add items to.

You can optionally choose an image to use as a visual cue for the credential, or change the existing one. You can also set tags to organize your credentials. When modifying an existing credential, you can change its name, tags, and optional image, but not the template.

You can delete a credential by pressing `Delete Credential` at the bottom of the credential view. If you delete a credential, all of the items belonging to it will also be deleted.

CREDENTIAL ITEMS

The `Credential Details` view allows you to create and modify credential items. Items have titles and values. The title is a meaningful name to help you identify what the item is while the value is what will be used when the item is activated. For example, an item title could be "Account ID" and its value might be an email address. You can create your own title or use the one set for the item type.

Item Actions

When you are connected to a Bluink Key, tapping on a credential item's inkdrop icon automatically sends it to the computer. If you are not connected, tapping will allow you to edit the item. You can copy the value into the smartphone paste buffer by using the copy icon in the more menu. This will allow you to paste it into other apps on your phone.

Generate Random Password

Use the `Generate Random Password` button from the edit item view to create a random value for a password. A password strength meter will be displayed to show you how strong the value is. Use the gear icon beside the `Generate Random Password` button at the bottom of this view to customize the parameters of the generated password (e.g., uppercase/lowercase characters, contains digits, length).

Secure Display

If you set this attribute, located under `Security Options`, then the credential item will not display itself on your smartphone unless you swipe left on the item and tap on the eye icon.

Require Reauthentication

Turning on reauthentication provides extra protection to see or use this credential item. For example, a very sensitive item, such as your online banking password, can be set so that it cannot be used unless you re-enter your Bluink password or use a biometric (if your phone allows).

Allow Biometric

On smartphones that offer biometric authentication, this switch determines whether or not you can use the biometric for reauthentication instead of your Bluink password.

One Time Passwords

An item with the type One Time Password is a special kind of credential item. This is a secret value used by a Bluink Key code generator for two-factor (sometimes called two-step) authentication. You can create code generator items for web sites that support them by choosing this type for your item. You would then follow the registration instructions for the web site. If the site allows registration of the OTP seed via QR code, you can use the `Scan OTP` button that appears for this item. Alternatively you can type in the secret key value that the web site displays during registration. Tapping on a One Time Password credential item actually generates a code before sending it to the computer or into the paste buffer.

BROWSE CREDENTIALS

Use the top right buttons on `Credentials` view to display the credentials in grid view or list view. By default, all credentials are shown.

Tag & Filter

You can assign tags to credentials to organize them. A tag is automatically assigned based on the category chosen when creating the credential, and can be added/removed in the `Credential Details` view. Credentials can have more than one tag.

The `Filter` button allows you to select tags you would like to display. Selecting multiple tags limits the view to credentials that have all of the selected tags. The `Filter` button will display the number of credentials that meet this criteria.

Search

You can also limit the credentials displayed by using the search bar. This searches credential and item titles, but not item values. This can be combined with `Filter` to narrow down the selection.

AUTOMATION

Credentials can be automated to use the credential items for form filling. For example, a login form might have a username field, a password field, and a submit button. An automated credential for this form can find the correct credential items for the username and password, enter them into the fields, and press the submit button.

CREATE AN AUTOMATED CREDENTIAL

When you create a new credential, you can choose a Bluink Key template. Select an automated template from the list to create your credential. Credential templates are maintained by the Bluink Key team, and new ones are always being added. If you don't see one for your site, you can try the Web Login template. This will work for most logins.

EXECUTE CREDENTIAL

Automation is triggered either by tapping on an inkdrop icon in `Credentials` view, or by scanning a Bluink Key QR code. Before executing a credential, ensure that you have the focus on the form starting field. Bluink Key QR codes can appear in browser extensions on supported web pages or as account pictures for PC and

Mac logins. A recognized Bluink Key QR code will automatically find the correct credential to use. You can activate a scan by tapping the QR code icon in the app.

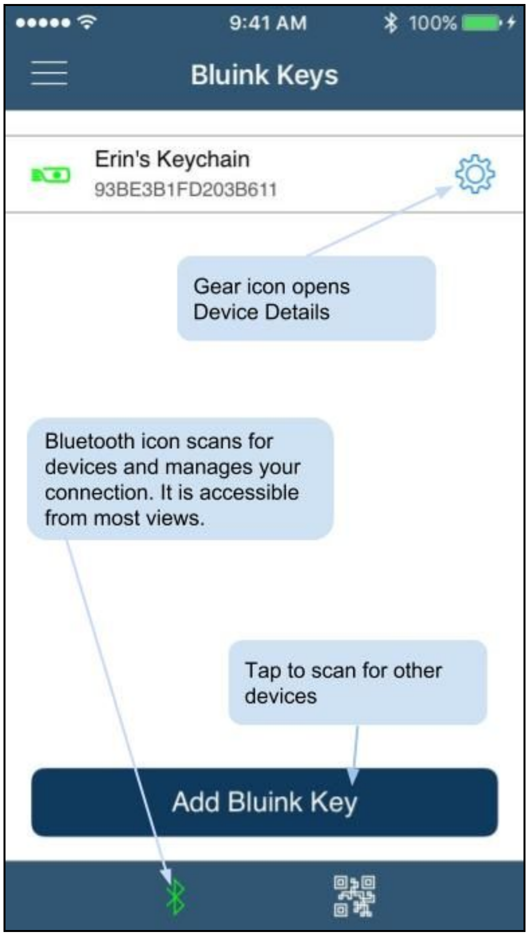
MY BLUINK KEYS

You can take ownership of a Bluink Key or pair with one that is owned by another smartphone. In order to see what Bluink Keys are available to be managed, you must connect using the connection icon. If more than one Bluink Key is found, a list will be presented for you to select one. You can always disconnect and reconnect to refresh the list.

INITIALIZE BLUINK KEY

This allows you to set a friendly name for a new Bluink Key that is in factory state. The name helps you identify it when multiple Bluink Keys are detected within range of your smartphone so you should think of something that is easily recognizable and distinguishable. It also automatically generates a unique identifier and programs it into the key.

This operation also creates a unique pairing key that allows your smartphone to take ownership of the key. This key is used by the smartphone and key to mutually authenticate each other as well as to set up a secure, encrypted communication channel over Bluetooth.



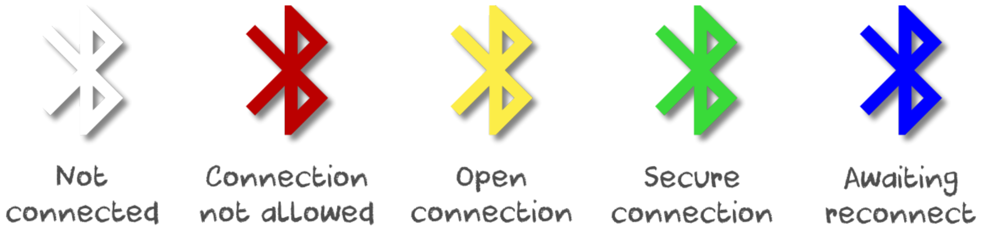
9:41 AM
100%
Bluink Keys
Erin's Keychain
93BE3B1FD203B611
Gear icon opens Device Details
Bluetooth icon scans for devices and manages your connection. It is accessible from most views.
Tap to scan for other devices
Add Bluink Key

PAIR WITH BLUINK KEY

If a key is already owned by another smartphone, this operation allows your smartphone to also use it. You must obtain the pairing key from the key owner in order to pair successfully. The pairing key is listed under Bluink Key Details, accessed by pressing the gear icon next to a listed key.

CONNECT TO YOUR BLUINK KEY

No software is required to connect to your Bluink Key. All you need to do is plug the key into the computer. You can see the connection state with the Bluink Key from the state of the connection icon which appears on several views:



- Not connected - No key is connected with the smartphone
- Connection not allowed - A key was detected but a connection is not allowed. This occurs when the key has a pairing code installed but it is not paired with your smartphone
- Open connection - Key is in a factory state (no pairing code) and may be initialized by a Bluink Key app to take ownership
- Secure connection - A key is connected to your smartphone. A mutually authenticated secure communication channel has also been established. All your messages to the key are encrypted.
- Awaiting reconnect - A secure session has been disconnected and may be re-established if the phone and key are within range.

You can connect with the Bluink Key by tapping on the connection icon. In some cases you may not want to connect; for example, when you want to send credential items to the local phone paste buffer instead of the computer. You can disconnect by toggling the connection icon when you already have a connection. Alternatively you can disconnect simply by removing the Bluink Key from the computer.

GENERATE ONE TIME PASSWORD

One time passwords (OTP) are a form of authentication supported by many web sites for enhanced security. Instead of using a static password, which can be stolen and reused by a hacker, an OTP changes after each use or after a short time period (such as every minute).

To use OTPs you need to have a code generator that is synchronized with the authentication server of the web site. The registration process of Bluink Key as a code generator for Dropbox two-step verification will be shown but you can use Bluink Key as a code generator with as many sites as you would like provided you go through the registration process for each one.

- Make sure the site knows you want to use a mobile app code generator
- Add a new credential item
- Choose One Time Password as the item type
- Scan a QR code to get the secret key if the site offers one, or type in the secret key manually
- Sometimes a site may ask you to generate a code to ensure that it works
- If the site offers a secure backup code, you can create another credential item for this.

Once you have registered your Bluink Key code generator for a site, you can now use it for stronger authentication whenever the site requires it. All you need to do is tap on the OTP item for that site. Unlike other mobile app code generators, the code generated by Bluink Key will automatically be sent to the computer if you have a connection. You can also use OTP codes in automated credentials. Using an OTP code usually goes like this:

- The site prompts for a generated code
- Make sure the code field has the focus (click with the mouse)
- Find the OTP for the site and tap the inkdrop icon

Alternatively, if you have a Bluink Key browser extension and automation set up for the site, you can scan a QR code that the extension pops up.

FIDO U2F

Bluink Key is fully compliant with the FIDO Alliance Universal Second Factor (U2F) authentication standard. This means that you can use your smartphone to perform public key authentication at participating web sites, which eliminates passwords altogether and is much more secure.

You must have the Bluink Key app in the foreground and be connected to your Bluink Key in order to register and authenticate at participating sites. All interaction with Bluink Key is done through a FIDO U2F enabled browser (such as Chrome).

REGISTRATION

Using the FIDO U2F enabled browser, visit any site that supports FIDO authentication and follow their FIDO U2F registration instructions. When the registration process requires the U2F key, you will see a registration dialog appear in Bluink Key. Upon confirmation, Bluink Key will create a FIDO authentication key in the FIDO U2F Authenticator credential. You can then authenticate with this site using your Bluink Key.

AUTHENTICATION

When you authenticate at a FIDO enabled web site that you have registered with, you will see an authentication dialog appear in Bluink Key. Upon confirmation, Bluink Key will perform a private key operation for that specific site to complete the authentication request.

KEYBOARD/TOUCHPAD

This view allows you to control your computer remotely via the Bluink Key by emulating a keyboard and a mouse. You can type on the computer using the built-in soft keyboard of your smartphone. A special keyboard is also available to let you access modifier keys (such as Ctrl and Alt) as well as other useful keys for navigation (such as page up, page down and arrows).

MOUSE CONTROLS

You can move and interact with your computer mouse cursor using the smartphone touchpad as follows:

- Move mouse cursor: single-finger drag on touchpad
- Left button click: single-finger tap
- Right button click: two-finger tap
- Left button drag: single-finger hold (pause for 0.5 seconds) and then drag on touchpad
- Exit drag mode: single-finger tap
- Scroll wheel: two-finger drag up or down

PASTE TO COMPUTER

This option lets you send copied text from your smartphone to the computer. Any text that you have copied into the phone paste buffer (clipboard) will be sent provided you have connected via a Bluink Key.

SPEECH

Bluink Key supports speech on Android. Here are the basic commands:

GOTO: Go to a specific URL based on a template search result. For this command to work properly you must have focus within a browser on the computer. Example: “Go to Dropbox”

LOGIN: Execute a login by name. Example: “Log in to Windows”

WHAT IS: Find credential items by searching through credentials. Example: You may use a Gmail address such as “john.smith@gmail.com” as a username in a Dropbox login. In this case “What is Dropbox identity,”“What is Dropbox username,” and “What is Gmail email address” will all find “john.smith@gmail.com.”

USE: Identical to WHAT IS except that once a credential item is found, take the extra step of sending it to the computer or the local pasteboard (if a Bluink Key is not connected). Example: “Use my Facebook password.”

DICTATE: Send arbitrary speech to the computer or pasteboard. Everything following the DICTATE command in the spoken phrase will be sent. Example: “Dictate ‘it was a dark and stormy night’” sends “it was a dark and stormy night” to the computer.

NEXT, BACK, and GO: Navigate through forms using speech only. NEXT sends a `Tab` key and moves to next field. BACK sends a `Shift Tab` key and moves to previous field. GO sends a `Return` key and executes a button press.

SETTINGS

BACKUP

It is important to create a backup of your Bluink Key items every now and then, especially when you have created or changed some credential items. Bluink Key will show you which credentials and items require a backup. If you lose your smartphone you can recover your items by importing the backup into another key. You may also use backups to synchronize Bluink Key items between multiple keys. During an import any new items will be added and the newest version of an existing item will be preserved.

Backups are created as an email attachment or file and are protected with your Bluink password. When importing a backup you will need to use the Bluink password that was set during the backup creation.

CHANGE PASSWORD

This allows you to change your Bluink app password. Your Bluink password protects your sensitive information, both within the Bluink Key app and in backups, so you should make this password strong. Try to make the password strength meter go full when you are creating your Bluink password.

LOCK BLUINK KEY APP

You can automatically lock the Bluink Key app after a period of inactivity. Choose from 5 min, 10 min, 30 min, or Never.

KEYBOARD TYPE

Bluink Key can emulate a number of different keyboards. This is important if you are on a system that is expecting input from a keyboard layout for a specific language or country since the same keys can map to different characters. For example, a shift-2 will produce an "@" symbol on a United States keyboard and a '"' (double quote) on a British keyboard. If your Bluink Key keyboard type does not match what the computer is expecting, then credentials sent to the system may come out incorrectly. If your desired language is missing, please make a request at bluink.ca/support.

MOUSE SENSITIVITY

When you use the `Keyboard/Touchpad` view to control your computer from the Bluink Key app, this option lets you adjust the responsiveness of the mouse pointer based on your finger movements on the smartphone display.

ENTERPRISE

REGISTER

To register with the Bluink Enterprise server, you must receive a registration email. After connecting to your Bluink Key, open the attachment with the Bluink Key app. You will be prompted for your corporate directory password. This is your system password, not your Bluink password.

ENTERPRISE CREDENTIALS

Once you are registered, you will receive any corporate credentials that have been assigned to you. These credentials cannot be deleted. As well, the credentials and credential items can have restrictions on use. These are called policies.

ENTERPRISE POLICIES

There are a number of different types of policies in Bluink Enterprise. Some policies are applied purely to the credential item while others depend on both the user or group and credential combination.

For example, a password formation rule such as “contains uppercase” is applied just to the credential item while a geofence restriction will be dependent on the user and the credential since it might include your home as a valid location.

Geofences

A geofence consists of a location (latitude and longitude) and a radius (in meters). An administrator defines a geofence by typing in an address and then specifying a radius.

To protect employee privacy, a geofence can be either public or private. A public geofence is available to be applied to any user. For example, “Corporate Headquarters” is likely a public geofence. A private geofence is a location that can only be applied to a particular user and is not available to others. For example, this could be your home location.

Multiple geofences can be applied to a credential. When geofence restrictions are applied, you can use the credentials whenever you are within any geofence in the list for that credential. The location is determined using the location services of your smartphone. Location services must be enabled when geofences are applied; otherwise access to the associated credentials will always be denied.

Bind Credentials to Bluink Keys

In addition to geofences, credential use can be restricted by binding the credential to your registered Bluink Key. When set, you can only use the credential when connected to your registered Bluink Key. Otherwise, the credential can be used with any key you can connect to.

Credential Item Policies

There are several policies that apply to credential items, especially to passwords. You can see the policies when you edit the item; however you cannot change them as you can with your personal credentials.

Some item values will be constant (e.g., the username on a shared account). Some items will require you to reauthenticate (with your Bluink password or a biometric) before you can view or execute them. Passwords have settings for randomization, minimum length, and what characters you can use (e.g., lowercase, uppercase, digits, special characters).

Bluink Enterprise can automatically change passwords for any system for which there exists a connector. For example, if you have an AD Login credential, the Auto-Change password policy may be enabled. This means that your password will automatically be changed after a set time period. Since you can use Bluink Key to log in, you do not even need to be aware that the password has changed.