HOTPin Software Instructions

iOS Client

HOTPin

celestix

The information contained in this document represents the current view of Celestix Networks on the issues discussed as of the date of publication. Because Celestix Networks must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Celestix Networks, and Celestix Networks cannot guarantee the accuracy of any information presented after the date of publication.

These instructions are for informational purposes only. CELESTIX MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

HOTPin Client Software Instructions for iOS

Document Number: HPN0030-919-002

Updated: June 28, 2013

Product Version:

Celestix HOTPin 2FA system software 3.7

Client Software 3.5

Table of Contents

HOTPin Client Software Instructions: iOS

These instructions will help you set up and use the HOTPin Client for two-factor authentication.

Authentication is the process where users provide credentials that verify who they are to a protected network or resource; it is commonly referred to as logging in. The HOTPin® system creates a more secure login process for your organization's network systems by offering two options: two-factor (2FA) or one-factor authentication.

HOTPin Two-factor authentication uses two pieces of information as a password to grant network or system access by requiring both a Personal Identification Number (PIN) and a One-Time Password (OTP). In the HOTPin system, the two factors are composed of something a user knows (their PIN) and something a user has (in this case, the OTP generated from an application). Combining the PIN and OTP make a passcode to log in to a protected system. However, if your organization chooses to use HOTPin as a one-factor authentication system, you will just use the OTP when you log in. Either way, the passcode is dynamic because it changes after each use, which makes the HOTPin system more secure than traditional password systems.

In the HOTPin system, an OTP is referred to as a token code. There are three ways to get a token code:

- You can use a client software token application (client software) to generate the codes.
- The HOTPin server can send the token codes to you through email or text message.
- Your HOTPin administrator can provide you with a hard token device that generates codes.

These instructions cover setting up the client software method to generate token codes. Client software must be installed on your user device (for example, a laptop or smart phone). It uses an encrypted key that is in sync with the HOTPin server to generate a token code when you need to log in.

To get started with HOTPin you will need to:

1. Install the client software.
   Installation file will have the .ipa extension (if visible).
2. Import your token key configuration.

A HOTPin token key configuration can be obtained from the HOTPin User Website, or as data string from your system administrator (see Import a Token Key). Key configuration import options depend on your device capabilities and the HOTPin features that your administrator has enabled.

Application Requirements

The HOTPin Client supports iOS device versions 3.1.3 and above on iPhone and iPod touch.

Document Notes

Using a PDF viewer besides Adobe® Reader® may disable some functionality (like hyperlinks) and may change how the content displays.

The instructions were written using the standard Home screen layout and the Safari® browser. The steps will generally be the same if you customized your device or use a different browser, but may vary somewhat.

Document Assumptions

These instructions assume that the following are true:

- You have any necessary information, for example the HOTPin User Website address (URL) or any additional passwords. Your administrator may provide you with the document *HOTPin User Login Information Sheet* to convey those items.
- You have access to the Internet.
- You have sufficient permissions to install applications on your device.

Application Installation and Features

This section provides information to help install and configure HOTPin client software on your device and includes an overview of the login process. It also provides information and instructions for application features.

Install the Client Application

These instructions explain how to install the HOTPin client application from Apple's App Store.

> Note: To download HOTPin Client, you will need:
>
> - An Apple account to use for downloading HOTPin from the App Store (the client application is free).
> - An Internet connection.

To install the HOTPin client software token application

1. Open the App Store on your device.
2. Search for hotpin (from Celestix Networks, Inc.).
3. Tap the FREE screen button.
4. Tap the INSTALL screen button.
5. Follow the screen prompts for entering account information.

The client software application is installed as **HOTPin** and placed on the Home screen.

The HOTPin Client is now ready to import your token key. For instructions, see Import Token Key.

The topic HOTPin Client Use Overview provides a general introduction to using HOTPin.

HOTPin Client Use Overview

To use the HOTPin Client, you will need to add the token key configuration for your user account to the client software token application (client software). The key configuration may be obtained from the HOTPin User Website, your system administrator, or through a local network connection (meaning your device is directly connected to the network). These options depend on your device capability and your organization's HOTPin deployment.

The general steps for first use include

1. Import the token key configuration to the HOTPin Client.
2. Load the token key in the HOTPin Client.
3. Either generate a token code or scan a QR code for login.

The token key can be loaded as part of the import process, or you can do it in a separate step. After setting up the token key in the client software, you will be ready to log in to your network. The first time you log in, you may be prompted to set a personal identification number (PIN).

Once configured, the client adds just a few steps to your login process.

The general steps for regular use include

1. Open the HOTPin Client.
2. Load the token key if necessary.

If a default key has been designated, it will load automatically.

3. Either generate a token code or scan a QR code for login.

Configure the Application

First you installed the client software application on your device, now you will configure it for login use.

Import a Token Key

To generate the token codes used in passcodes for network login, you will need to import the token key associated with your user account. There are three potential methods to obtain your token key:

- Download it from the HOTPin User Website.
- Download it through the HOTPin Client **Import from Network** feature.

  > Note: This feature also requires that the HOTPin User Website is enabled.

- Import it from a configuration that you get from your system administrator.

Your options will depend on the features your administrator has enabled and your device capability.

The following topics first discuss features you will need to understand before you import a token key. Then instructions for import options are explained.

Passphrase Encryption

The passphrase feature can be assigned to protect the token key in transit (the key configuration is encrypted when it is created), and/or when it is in the HOTPin Client (the key is encrypted during or after import). Depending on the level of security required for your organization, a passphrase may be required to protect both instances, or one and not the other.

Passphrase Requirements

- 6-16 characters
- Can include letters, numbers, symbols, but not spaces
- Example:
  mykey:4

See Passphrase for more information.

Default Key

HOTPin allows you to set a default key that will load automatically each time the client is opened. For users who require multiple token keys to log in to different systems, the default is convenient for regular log in to one system.

The default key is noted on the Manage Keys screen [**HOTPin**|Settings ()|**Manage**] with a checkmark.

If you do not set a default, you will need to load a key each time you want to generate a token code.

Import Options

The following topics explain each of the methods to add key configuration to the client application. You will only need to use one of these methods.

Import from Network

This feature is only available for networks that use Active Directory®. You must use your Active Directory (AD) network login information to download a token key from the network. Check with your system administrator if you need more information.

To import key from a network connection

1. Open the HOTPin Client.
2. Navigate to Settings (⚙)|**Import from Network**.
   The import screen opens.
3. Provide the following information:
   a. **Host name/IP** – this is the server name or IP address that hosts the HOTPin system. See your system administrator if you don't have this information.
   b. **User name** – this is your AD login name.
   c. **Password** – this is your AD password.
   d. **Friendly name** – assign a name to identify the key.
      It is helpful if you choose a descriptive name like USoffice, APIoffice.

      > Important: For security, choose a friendly name that is different from your user name.

   e. **Key passphrase** – if required, enter and confirm a passphrase. If not required, you can elect to add one as an encrypted key is more secure. See Passphrase Requirements for more information.
   f. **Load after import** – if you want the token key to load in the client when you complete the setup process, toggle the switch to **On**.

      > Important: The HOTPin Client must have a token key loaded to generate token codes.

4. Once you have entered information in all the fields, tap **Import**.
5. Tap **OK** on the success notification.

If you loaded the key as part of the import process, the HOTPin Client is now ready to use. If not, you will need to load it before you can generate a token code.

Import from QR Code

This feature allows you to import token key configuration through the camera on your device by scanning a QR code from the HOTPin User Website.

> Note: QR code access must be enabled on the HOTPin User Website by your administrator.

> Important: QR codes are generally encrypted with a passphrase; make sure you have it.

To import from a QR code

1. Open the HOTPin Client.
2. Navigate to Settings (⚙)|**Import From QR Code**.
   The import screen opens.
3. Tap **Scan QR Code**.
4. Scan the code and tap **OK** on the success notification.
5. Provide the following information:
   - **QR Passphrase** – the QR code will be protected by encryption; you will need to enter the passphrase to continue.
   - **Friendly Name** – assign a name to identify the key.
     It is helpful if you choose a name that will identify the key (e.g. USoffice, APIoffice).

     > Important: For security, choose a friendly name that is different from your user name.
   - **Key Passphrase** – if required, enter and confirm a passphrase. If not required, you can elect to add one as an encrypted key is more secure. See Passphrase Requirements for more information.
   - **Load after Import** – if you want the token key to load in the client when you complete the setup process, toggle the switch to On.

     > Important: The HOTPin Client must have a token key loaded to generate token codes.
6. Once you have entered information in all the fields, tap **Import**.
7. Tap **OK** on the success notification.

If you loaded the key as part of the import process, the HOTPin Client is now ready to use. If not, you will need to load it before you can generate a token code.

Add New Key

This feature is used to import a key configuration data string to the client application.

To import key from a string

1. Open the HOTPin Client.
2. Navigate to Settings (⚙)|**New Key**.
   The New Key screen opens.
3. Provide the following information:
   a. **Key string** – either paste or manually enter the string digits in the text field.
   b. **Friendly name** – assign a name to identify the key.
      It is helpful if you choose a descriptive name like USoffice, APIoffice.

      > Important: For security, choose a friendly name that is different from your user name.
   c. **Key passphrase** – if required, enter and confirm a passphrase. If not required, you can elect to add one as an encrypted key is more secure. See Passphrase Requirements for more information.
   d. **Load after import** – if you want the token key to load in the client when you complete the setup process, toggle the switch to **On**.

      > Important: The HOTPin Client must have a token key loaded to generate token codes.

4. Once you have entered information in all the fields, tap **Import**.
5. Tap **OK** on the success notification.

If you loaded the key as part of the import process, the HOTPin Client is now ready to use. If not, you will need to load it before you can generate a token code.

Load/Unload a Token Key

A token key must be loaded into the client software token application (client software) to generate a token code. You may need the unload feature to delete a key. The following instructions explain how to load and then unload a token key.

To load a key

1. Open the HOTPin Client.
2. Navigate to Settings (🔧)|**Load**.
3. Select the key you want to load.
   You may be prompted to enter a passphrase if one has been assigned to the key.
4. Tap **Load**.
5. Tap **OK** on the success notification.

A loaded key's name is displayed in the client title bar.

To unload a key

1. Open the HOTPin Client.
2. Navigate to Settings (🔧)|**Unload** and tap.
3. Tap **OK** on the success notification.

You can confirm that a key is unloaded by looking at the title bar on the main screen: it will show **Token key not loaded**.

Login Information

Once you have configured the client application on your user device, you are ready to login to your network's protected resources through the HOTPin system. What you will need:

- Your client device configured with the HOTPin application.
- Your user information (the document *User Login Information Sheet* should be provided by your administrator).
- Login instructions (see the document *HOTPin User Login Instructions for Client Software*).

Token Code Authentication

The Next Code button on the main screen will display when a token key is loaded. When the button is tapped, it will display a 6-digit number that must be entered on a login page or prompt.

QR Code Authentication

The HOTPin system can employ Quick Response Codes (QR codes) to facilitate login. The QR code provides information that a HOTPin client installed on a device with a camera will scan and then use to negotiate the login process.

The QR Login button displays when a token key is loaded in the application. To use this feature, however, an administrator must enable the functionality on the server. Your login information should indicate whether QR code authentication is available.

Client Application Features

The following sections provide instructions for the features you may need to manage the HOTPin client application.

Manage Token Keys

Navigate to Settings (🔧)|**Manage** to access HOTPin administration features. The Manage Keys screen is used to complete the following actions:

- Set a key as default – a default key is automatically loaded in the client application when the client is launched (if required, a passphrase will need to be entered).
- Add or change a passphrase – the key passphrase encrypts a key. See Passphrase for information and Add or Change a Passphrase for instructions.
- Delete a key – removing a key is permanent; it is sometimes necessary if you need to import a new instance of the same key to resolve login issues. See Delete a Token Key for more information.
- Rename a key – the key name is used to identify the token key. If you have multiple keys, it can be helpful to use a descriptive name.

You will need to select a key to enable management features (tap a key to select).

The Token Key section has more information about keys.

Locate Token Key ID

If you have trouble logging in to your network, you may need to find the ID of the token key you are using to help resolve the issue.

To find your token key ID

1. Open the HOTPin Client.
2. If necessary, load the token key.
3. Tap the ⓘ button.

The ID is listed after the key name.

> Note: Keys imported from a data string (through the New Key feature) will not display an ID.

Locate HOTPin Software Information

The following instructions explain how to find your software version information.

To access client software version information

1. Open the HOTPin Client.
2. If necessary, load the token key.
3. Tap the ⓘ button.

Version information is listed after the application title.

Switch Token Keys

To switch token keys, use the load feature. The key you select will replace a currently loaded key.

Delete a Token Key

> Caution: Once you delete a key, the action cannot be undone. You will need to import a new key to use HOTPin again.

> Important: You cannot delete a key that is loaded in the HOTPin Client. See Load/Unload a Token Key if you need instructions.

To delete a token key

1. Open the HOTPin Client.
2. Navigate to Settings (🔧)|**Manage**.
3. Select the key you want to delete.
4. Tap **Delete**.
5. Tap **OK** to confirm.
6. Tap **OK** on the success notification.

The key is removed from the token keys list.

Add or Change Passphrase for a Token Key

You can add or change passphrase protection through the HOTPin Client's Change Passphrase feature.

To access passphrase encryption

1. Open the HOTPin Client.
   Enter your existing passphrase if necessary.
2. Navigate to Settings (🔧)|**Manage**.
3. Select a token key by tapping it.
4. Tap the **Passphrase** button.
   The change passphrase screen opens.
5. Complete the following:
   a. If there is an existing passphrase, enter it in the **Old passphrase** text box.
      > Important: If you are adding a new passphrase, the Old passphrase text box will not display.
   b. Enter a passphrase in the **New passphrase** and **Confirm** fields.
      > Important: A passphrase must be a string of characters (letters, numbers, symbols, but no spaces) from 6 to 16 digits long.
   c. Tap **OK**.
   d. Tap **OK** on the success notification.

Passphrase encryption changes are complete.

Delete a Token Key Passphrase

If you added a passphrase to encrypt a token key when it was not required, you have the option to delete it.

> Note: HOTPin will not allow you to remove a passphrase from a token key that requires one.

To delete a passphrase

1. Open the HOTPin Client.
2. Enter your existing passphrase.
3. Navigate to Settings (⚙)|**Manage**.
4. Select the token key by tapping it.
5. Tap the **Passphrase** button.
   The change passphrase screen opens.
6. Complete the following:
   a. Enter the existing passphrase in the **Old passphrase** text box.
      If the Old passphrase is not displayed, then the key does not have a passphrase encrypting it.
   b. Leave the **New passphrase** and **Confirm passphrase** fields blank.
   c. Tap **OK**.
7. Tap **OK** on the success notification.

The passphrase is removed from your token key.

Forgotten Passphrase

A passphrase may be required to access the token key your HOTPin client application uses to generate token codes. If you forget your passphrase, you will need to get a new key instance. See Import a Token Key for instructions.

When you import or add the new key, you will be able to set a new passphrase.

> Important:
>
> - You must delete the current key before you can import the new key instance.
> - If you have forgotten the passphrase for a default key, click **Cancel** on the passphrase prompt when the client opens. You can then access the Manage function to delete the key.

Access the HOTPin User Website

If the user site has been enabled by your system administrator, the following instructions explain how to access it.

> Note:
>
> - You will need to be connected to your company's internal network to access the user site.
> - You may see a message when you navigate to the HOTPin User Website that there is a problem with the website's security certificate. It is common for internal websites to use self-signed certificates, so this is generally not a cause for concern. Check with your system administrator for more information.

To access the user site

1. Open a web browser.
2. Enter the user site address (URL).

Your administrator should provide the URL, which will look something like:

https://111.222.333.444:8098/hotpin/

https://server_name:8098/hotpin/

The IP address or name of your company's HOTPin server will replace the portion of the URL that is highlighted in gray above (if your site administrator deployed the standard site).

Important: The beginning of the address is https, not http.

3. Log in to the user site.

   If you do not have an account, you may be able to create one if self-provisioning has been enabled. Your administrator should provide information. The user site's online help provides instructions.

HOTPin User Website functionality is discussed in the Reference section.

Uninstall the HOTPin Client

Before removing the application, consider that once the HOTPin Client is deleted from your user device, you cannot undo the action.

To uninstall HOTPin Client

1. Navigate to where the HOTPin Client is located.
2. Touch and hold the **HOTPin** icon until the applications start to wiggle on the screen.
3. Tap ⊗ in the corner of the **HOTPin** icon.
4. Tap **Delete** when prompted.
5. Press the Home button to save the change.

HOTPin client software is now removed from your device.

Download Documentation

Users can get their own client and login instructions from the Celestix download site:

http://www.celestix.com/product_content/hotpin/

Reference

The following topics provide additional information about HOTPin system components.

HOTPin User Website

The HOTPin User Website is a provisioning tool that administrators can make available to users. When the site is deployed, your organization's HOTPin administrator can enable the following features:

- Create or edit HOTPin accounts
- Download client software token applications (client software)
- Download key configuration
- Download documentation

HOTPin user accounts are required to log in to a protected system or network through the HOTPin authentication system. Client software generates the token codes that are necessary to log in. Client software requires a key to generate the token code; the key is imported to client software through a key configuration. Documentation includes setup information for client software (this document) and login instructions.

If self-provisioning is enabled, your administrator will provide information to access the user site. Disabled features will not display. See the site's online help for more information.

Token Key

A token key enables the HOTPin Client to generate a token code that is part of the passcode used for login. The key must be imported and then loaded in the client. The import process uses a token key configuration that includes the key along with necessary user information. Configuration formats include a file, a string, and a QR code. The key configuration can be obtained from the HOTPin User Website if it is enabled, or from your system administrator. Additionally, the key configuration can be imported directly through a local network connection to the HOTPin User Website. Your system administrator will make the appropriate options available.

HOTPin client software allows you to import multiple keys. If you have multiple keys, you can select a default key if you will log in to one system most often. The default key is designated by a checkmark.

Because the token key is associated with a user account, it must only be used with one device. If HOTPin client applications on additional user devices try to use the same token key, all devices using that key could lose synchronization with the HOTPin server. This could cause each of the client applications to produce invalid token codes.

The token key may be protected by a passphrase. The passphrase may be optional, or it may be required. The Passphrase section provides more information.

As another security feature for imports through a file, your system administrator may have included a setting to remove the key from the token key configuration during the import process. In some instances, you may still see the key configuration file on your device, but it will not be usable. Removing the key increases system security and prevents later importing the key when it would be out of sync with the HOTPin server.

Multiple Keys

To log in to separate network systems using the same device, you will need a different token key for each system. For example, if you have offices in the U.S. and Asia that use different HOTPin servers to authenticate user logins, you will need to have a separate token key for each system. A key must synchronize with the server to provide a valid token code.

Switching keys in the HOTPin Client is a quick process; using the example above, if you have been logging into the system for your U.S. office but then need to log in to the system for your office in Asia, you just need to load the key for the office in Asia. The key for the office in Asia will replace the key for the U.S. office. However, if a default key is designated it will automatically load the next time you open HOTPin.

When using multiple keys, it is helpful to give them each a name (also referred to as a friendly name) that illustrates the context in which you will use it. “USoffice” and “AsiaOffice” are more illustrative names than “default”, “key1”, or “key2”. The name appears in the key list shown in the Manage feature [Settings (🔧) |**Manage**].

Passphrase

The passphrase is a security feature that encrypts the token key used by the HOTPin Client. Encrypting the token key impedes a malicious user from stealing the key or accessing the HOTPin Client. Passphrase encryption may be used in two ways:

- To protect the key configuration while it is in transit between the server and client application.
- To protect the token key after it has been imported to the client application.

One or both passphrase encryption options may be required in your organization’s HOTPin deployment; each option adds a layer of security.

When importing a key configuration through a file or QR code, make sure you have the passphrase if required.

If a passphrase is required to protect the key once it has been imported to the client, you will be prompted to create a new passphrase during the import. Passphrases are composed of 6-16 characters and can include letters, numbers, symbols, but not spaces (for example, mykey:4).

If your system administrator did not require a passphrase, you can choose to add passphrase encryption to increase the security of the client software deployment on your device.

Navigation

The following diagram can help you to acclimate to the client application.