HOTPin Software Instructions

Mac Client

HOTPin

celestix

Celestix HOTPin Mac Client Software Application Instructions

Document No. HPN0030-982-001 Updated: January 4, 2012

Celestix HOTPin Mac Client Software Application version 1.0

Contents

Section 1: Introduction

The HOTPin™ system creates a more secure login process for your organization's network systems by offering two types of authentication. Two-factor authentication uses two pieces of information 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). The PIN and OTP are combined to make a passcode to log in to a protected system. Generating a passcode that is only valid for a single use makes the HOTPin system more secure than traditional password systems.

Your organization may choose to use HOTPin as a one-factor authentication system, in which case you will just use the OTP when you log in. HOTPin one-factor authentication may be used to complement another authentication system, like Active Directory®. If another type of authentication is used, you may also need to provide a password for that system in addition to your HOTPin OTP when you log in.

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

- You can use a client software token application (client software) to generate the token code.
- The HOTPin server can send the token code to you through email or text message.

These instructions cover 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 a key that is in sync with the HOTPin server to generate a token code when you need to log in.

To set up the HOTPin Client, you will need to:

1. Install the client software (installation file will have the .pkg extension).
2. Import your token key configuration.

A HOTPin token key configuration can be obtained from the HOTPin User Website, or as either a file or 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.

Document Notes

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

The HOTPin Mac Client is supported on Mac OS® 10.6.3 and later.

Related Topics
Import a Token Key
Load/Unload a Token Key

Section 2: 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 HOTPin Mac Client Application

The following explains the options for installing the HOTPin Client using the .pkg file. The first topic explains how to download and install the client software token application (client software) from the Mac® App Store. The second topic explains how to install the client software from a file saved to a local or network location. You will only need to use one of the options to set up your HOTPin client software.

To download and install the HOTPin Client from the Mac App Store.

These instructions cover the use of Safari®; if you use another web browser, the steps may vary somewhat from the instructions.

To download the HOTPin Client you will need:

- An Apple® Account to use for downloading HOTPin from the App Store (the HOTPin client application is free).
- An internet connection.

1. Open the App Store on your device.
2. Search for hotpin (from Celestix Networks, Inc.).
3. Click the **Free** screen button.
4. Click the **Install App** screen button.

5. Follow the screen prompts for entering account information and installing the application.

Skip the following installation option instructions and jump to Complete the Installation.

To install the HOTPin client software token application from a file

To run the installation file from a location on or connected to your device:

1. Navigate to the location of the installation file (.pkg extension).
2. Double-click the installation file.
3. The installer will guide you through the installation process.
4. When the installation is complete, click the **Close** button.

Complete the Installation

The client software application is installed as **HOTPin**; the default location is in **Applications/HOTPin**.

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

Related Topics
HOTPin Introduction
Import a Token Key

HOTPin Client First Use Overview

To use the HOTPin Client, you will need to configure the client software token application (client software) with the token key configuration for your user account. The key configuration may be obtained from the HOTPin User Website, your system administrator, or through a local network connection. 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. Generate a token 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).

Related Topics
Token Key
Import a Token Key
Load/Unload a Token Key

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.
- Import it from a token key configuration that you get from your system administrator and save to your device.

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

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 in the client software 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 Token Keys screen (HOTPin Client/**Menu**/**Keys/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.

To import from file

This feature allows you to import a token key from a location on or connected to your device. If provided by your administrator, the token key configuration file may be sent by email or transferred on removable media (for example, a memory card or flash drive).

Important: If the token key configuration was encrypted with a passphrase, make sure you have it.

1. Open the HOTPin Client.
2. Navigate to **Keys|Import File**.
3. The import screen opens; complete the following:
   a. **Token key file** – load the file's location:
      - Click the arrow button.
      - In the **Open** window, navigate to the token key configuration file (a file with a .dat extension) and select it.
      - Click **Open**.
      - The file path is loaded into the **Token key file** text box.
   b. **File passphrase** – if required, a passphrase must be entered in the **File passphrase** text box; otherwise, leave blank.
   c. **Friendly name** – assign a name to the key.
      It is helpful if you choose a name that will identify the key (like USoffice, APIoffice).
      Important: For security, choose a friendly name that is different from your user name.
   d. **Key passphrase** – if a **Key Passphrase** has been required, you must enter and confirm it. If not required, you can elect to add it as an encrypted key is more secure. See Passphrase Requirements for more information.
   e. **Set as default** – if this will be the key you use the most, the **Set as default** box should be checked.
   f. **Load after import** – if you want the token key to load in the client when you complete the set up process, the **Load after import** box should be checked.
      Important: The HOTPin Client must have a token key loaded to generate token codes.
   g. Click **OK**.
4. Click **OK** on the successful import notification.

Please Note: Your system administrator may have set a delete option on the token key configuration file. If so, the .dat file will be deleted after the key is imported to the client software.

Skip the following import option instructions and jump to Complete the Import.

To 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.

1. Open the HOTPin Client.
2. Navigate to **Keys|Import from Network**.
3. The **Import** window opens. Provide the following:
    a. **Host name or 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** – this name will identify the key you download. It is helpful if you choose a name that will identify the key (like USoffice, APIoffice).
        Important: For security, choose a friendly name that is different from your user name.
    e. **Key passphrase** – if a passphrase has been required, you must enter and confirm it. If not required, you can elect to add it as an encrypted key is more secure. See Passphrase Requirements for more information.
    f. **Set as default** – if this will be the key you use the most, the **Set as default** box should be checked.
    g. **Load after import** – if you want the token key to load in the client when you complete the set up process, the **Load after import** box should be checked.
        Important: The HOTPin Client must have a token key loaded to generate token codes.
    h. Once you have entered information in all the fields, click the **OK** button.
4. Click **OK** on the successful import notification.

Skip the following import option instructions and jump to Complete the Import.

To Add New Key

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

1. Open the HOTPin Client.
2. Navigate to **Keys|New Key**.
3. The **New Key** window opens. Provide the following:
    a. **Key string** – either paste or manually enter the string digits in the text field.

b. **Friendly name** – this name will identify the key you download. It is helpful if you choose a name that will identify the key (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 it as an encrypted key is more secure. See Passphrase Requirements for more information.
d. **Set as default** – if this will be the key you use the most, the **Set as Default** box should be checked.
e. **Load after import** – if you want the token key to load in the client when you complete the set up process, the **Load after Import** box should be checked.
   Important: The HOTPin Client must have a token key loaded to generate token codes.
f. Once you have entered information in all the fields, click the **OK** button.

4. Click **OK** on the successful import notification.

Complete the Import

If you loaded the key as part of the import process, the HOTPin Client is now ready to use. If not, see the section Load/Unload a Token Key.

Related Topics
HOTPin Introduction
HOTPin User Website
Load/Unload a Token Key
Passphrase

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.

Please Note: You may be required to enter the key's passphrase.

To load a key

1. Open the HOTPin Client.

2. Navigate to **Keys**|**Load**.
3. Select the key you want to load.
4. Click the **OK** button.

A loaded key's name is displayed in the client title bar and on the **HOTPin**|**About HOTPin** page.

To unload a key

1. Open the HOTPin Client.
2. Navigate to **Keys**|**Unload** and click.

The token key is now unloaded. You can confirm that a key is unloaded by looking at the Keys menu, if the Unload command is grayed out, then no key is loaded in the client software.

Related Topics
Token Key

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 Client Instructions for User Login*).

In addition to items you may have downloaded previously, like the client software application or these instructions, the HOTPin User Website can also provide the login instructions as a downloadable PDF. If the site is not enabled, your system administrator will provide the information you need.

Related Topics
HOTPin Introduction
HOTPin User Website

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 **Keys|Manage** to access HOTPin administration features. The Manage Token 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 to use the key to generate codes.
- **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; deleting a key 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. The **Delete** button will remain disabled if you select a loaded key.

The Token Key section has more information.

Related Topics
HOTPin Introduction
Load/Unload a Token Key
Add or Change Passphrase
Delete a Token Key

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. Navigate to **HOTPin**|**About HOTPin**.
4. The key's friendly name and ID are listed in under **Loaded Key**.

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

The client software Help topic *Having Trouble Logging In* (HOTPin Client|**Help**|**HOTPin Help**|**General Information**) provides information to assist login issues.

Related Topics
Load/Unload a Token Key

Switch Token Keys

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

Related Topics
Token Key
Load/Unload a Token Key
Multiple Keys

Delete a Token Key

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

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 **Keys**|**Manage**.
3. Select the key you want to delete.
4. Click the **Delete** button.

5. Click the **OK** button on the **Delete Confirmation** dialog box.
6. The key is removed from the token keys list.
7. Click **OK** to save the changes and close the Manage Token Keys screen.

Related Topics
Load/Unload a Token Key

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 in the HOTPin Client

1. Open the HOTPin Client.

   Enter your existing passphrase if necessary.
2. Navigate to **Keys**|**Manage**.
3. Select a token key by clicking on it.
4. Click the **Passphrase** button.
5. The **Change Passphrase** dialog box opens.
   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 be inactive.
   b. Enter a new 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. Click **OK** on the confirmation prompt.
6. Click the **OK** button on Manage Token Keys to save the changes.

Related Topics
Passphrase

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.

Please 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 **Keys**|**Manage**.
4. Select a token key by clicking on it.
5. Click the **Passphrase** button.
6. The **Change Passphrase** dialog box opens.
   a. Enter the existing passphrase in the **Old passphrase** text box.
      If the **Old passphrase** is inactive, then the key does not have a passphrase encrypting it.
   b. Leave the **New passphrase** and **Confirm** fields blank.
   c. Click the **OK** button.
7. Click **OK** to confirm saving the key without a passphrase.
8. Click **OK** to save changes and close the Manage Token Keys screen.

The passphrase is removed from your token key.

Related Topics
Passphrase

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 the new key, you will be able to set a new passphrase.

Please Note: You must delete the current key before you can import the new key instance.

Related Topics
Passphrase
Delete a Token Key
Import a Token Key
Load/Unload a Token Key

Uninstall the HOTPin Client

Removing HOTPin from your device follows the standard procedure to uninstall software on a Mac. The following provides brief instructions to assist with the uninstall process.

Please Note: Once the HOTPin Client is deleted from your device, you cannot undo the action.

To uninstall the HOTPin Client

1. Navigate to **Finder**|**Applications**|**HOTPin**.
2. Drag the **HOTPIN Client** to the trash.

To complete removing the HOTPin application from your system, you will need to empty the trash.

Download Documentation

Users can get their own client and login instructions if both the HOTPin User Website and the document download feature are enabled. Your administrator will provide access information if the user site is enabled.

Please 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 client software documentation on the user site

1. Open the HOTPin User Website in a web browser.

   Ask your network administrator for the URL, it should 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).

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

2. Log in to the user site.

   If you do not have an account, you will need to create one. See the site's online help for instructions.

3. Navigate to **Client Software**.

4. Click the link for your user device document to start the download process; follow your device procedure for downloads.

Related Topics

Install the HOTPin Mac Client Application

HOTPin User Website

Section 3: 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 two-factor 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 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.

Related Topics
Install the HOTPin Mac Client Application
Download Documentation

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 system, 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.

Related Topics
Import a Token Key
Load/Unload a Token Key
Passphrase
Multiple Keys

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 HOTPin Client.

One or both passphrase encryption options may be required in your organization's HOTPin deployment. Each option adds a layer of security for network and system resource access.

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.

Related Topics
Forgotten Passphrase
Add or Change Passphrase for a Token Key

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, when you close the client software, a default key will automatically load the next time you open HOTPin (if a default is designated).

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”. See the Name column on the Manage Token Keys screen (accessed by navigating to **Keys**|**Manage**).

Related Topics
Load/Unload a Token Key
Manage Token Keys

HOTPin Navigation Reference

The following reference provides descriptions for menu items in a hierarchical format. The reference list uses the following conventions:

- Main HOTPin menu items are bulleted.
- Menu commands are noted in bold.

- **HOTPin**
  - **About HOTPin** – display includes software version information and loaded key ID.
  - **Quit HOTPin** – close the HOTPin Client application.

- **Keys**
  - **Load** – enter/activate a downloaded token key.
  - **Unload** – deactivate a token key.
  - **Manage** – open the Manage Token Keys window.
    - **Set Default** – set the selected key to load automatically when the HOTPin Client is started. A checkmark denotes the default key.
    - **Passphrase** – change the passphrase that encrypts the token key.
    - **Delete** – remove the selected key.
    - **Rename** – change the friendly name assigned to the selected token key.
  - **Import File** – add a token key to the HOTPin Client from a file stored on or accessed by the user device.
  - **Import from Network** – add a token key to the HOTPin Client from a network location the user device can access.
  - **New Key** – add a token key to the HOTPin Client from a data string key configuration.

- **View**
  - **Always on Top** – forces the HOTPin Client window to remain visible on the desktop.

- **Help**
  - **Search** – access the Mac OS help search.
  - **HOTPin Help** – access the online help contents.