HOTPin Login Instructions

Client Software Users

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 User Login Instructions for Client Software

Document Number: HPN0030-969-001

Updated: June 28, 2013

Product Version:

Celestix HOTPin 2FA system software 3.7

Table of Contents

HOTPin User Login: Client Software

A user name and password are generally referred to as login credentials, or just credentials. They demonstrate who you are so that you can access a protected network or published resource, like an intranet or email. When you log in, that process is referred to as authentication. The HOTPin system creates a more secure login process for your organization's resources by offering two authentication options: one-factor or two-factor authentication.

HOTPin two-factor authentication uses two pieces of information to grant access by requiring both a Personal Identification Number (PIN) and a One-Time Password (OTP). These two factors comprise something a user knows (the PIN) and something a user has (in this case, the OTP generated by client software). The PIN and OTP are combined to make the passcode that is used to log in to a protected system. Depending on your organization's deployment, login screens may refer to either a *passcode* or a *password*; however documentation will generally use the term *passcode* for any field where you will enter your secret identification information.

Your organization may prefer to use HOTPin as a one-factor authentication system, in which case you will use just the OTP as the passcode. HOTPin one-factor authentication may be used to complement another authentication system, like Active Directory. If another authentication method 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. The client software installed on your user device generates the token code. The passcode is dynamic because it includes a token code that changes after each use, which also makes the HOTPin system more secure than traditional password systems.

Document Notes

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

Document Assumptions

These instructions assume that the following are true:

- Your HOTPin account has been configured for client software.
- HOTPin client software is installed and configured on your device.
- A key is loaded in the client software to generate token codes.
  The HOTPin Client software instructions for your user device provide details if you need more information about client usage.
- You have any necessary information, for example the login page address (URL), PIN requirement, or any additional passwords.

Login Overview

The general steps to use client software for logging in to a system protected by HOTPin two-factor authentication include:

1. Generate a token code on your device.
2. Enter the passcode on your organization's login screen or prompt:

Two-factor authentication: PIN + token code
One-factor authentication: token code only

Token Code Generation

You should only use one token method (for example, either client software or a token provider) at a time to maintain synchronization with the server. Synchronization is necessary to generate valid token codes.

You can switch methods, but configuration will need to be adjusted on the server and possibly your device. Switching from either the token provider or hard token device method to client software still requires installing client software and importing the token key configuration. See your HOTPin administrator for more information about changing your token method.

PIN

As mentioned previously, a PIN will be required if your organization uses two-factor authentication. A PIN is string of numbers between 4-8 digits. An example would be 624351. Once created it will be required for subsequent logins, so you will need to remember it.

You may need to create a PIN the first time you use HOTPin to log in to your network. This depends on whether or not the PIN was created at the same time as your account. If PINs are required and your account does not have one, you may be prompted during login to create it; however, some authentication methods do not allow prompting, so you should check the login information provided by your system administrator for PIN requirement information. You only have to create the PIN once.

After a PIN is created, it is combined with token codes from client software to create passcodes for subsequent logins. Your HOTPin administrator determines whether or not PINs are required. If PINs are not required, then you will just need a token code for login (one-factor authentication).

Login Instructions

These instructions cover the following two HOTPin system authentication systems:

- HOTPin with UAG
- HOTPin with RADIUS

Your system administrator will provide login information that specifies which system you should use. Each system has a section that explains the login processes.

The instructions first explain two-factor authentication, meaning the steps for initial and subsequent logins when PINs are required. Then the steps for one-factor authentication, when PINs are not required, are covered. You will only need to follow one set of steps. The information details the standard login procedure. Your organization may have customized the login method to include other items; for example, an Active Directory password may also be necessary. Your administrator will provide the information you need to complete the login process.

Important: If using a mobile device, the first log in is generally easier if you just use the device for the token code, and use another machine (like a desktop or laptop computer) to access the login page. Going back and forth on a mobile device can be cumbersome while you are acclimating to the process.

Note: On some systems, the server may impose a time limit for the login process. If your login attempt times out, go back to the login page and start over. It may be helpful to read through all of the steps in a section before you start the login process.

HOTPin with UAG

If your organization uses Unified Access Gateway (UAG) to authenticate user access to resources like email or an intranet, you will log in through a web browser.

Your login information should indicate that these are the instructions you should use.

Two-Factor Authentication

Use these instructions if PINs are required for your organization.

Instructions for login if you need to create a PIN

This set of instructions covers creating a PIN during initial login.

1. Think of a PIN.
   A PIN must be 4 - 8 numerical digits, for example 654321.
   You will need it later in the instructions.
2. Open the login screen for your network or published resource.
   As mentioned previously, it may be easier to do this on a machine besides the device that generates the token code if that device is a mobile phone.
3. Enter your user name.
4. On a mobile device or a computer, open the HOTPin Client application.
5. In the client, click the **Next Code** button to get a token code.
   - The group of numbers displayed is the token code.
   - A descending timer (a bar that decreases in size) indicates the amount of time the code will be displayed; it must finish before you can generate another code.
6. Go back to the login page; enter the token code in the password/passcode field.
7. Click the button to submit credentials.
   It may say Log On, Submit, or something different.
8. You will see an invalid PIN message prompting you to create a new PIN.
9. Enter your new PIN in the text field and submit.
   If you do not finish adding your PIN before the login screen times out, you will see the message "The login process could not be completed." Return to the login screen and start over.

   > Important: Once your PIN has been acknowledged, you will need to use it for all subsequent logins.
10. When you have successfully entered a new PIN, you will need to use it with a new token code to complete the login process.
11. On the login page, enter your user name.
12. Go back to the HOTPin Client and click the **Next Code** button to generate a new token code.

    > Important: You may have to wait for the descending timer to finish its cycle from the first token code before the Next Code button is available.
13. Switch to the login page; enter your PIN and the new token code in the password/passcode field.
    Example: **654321**890123
    If your **PIN** is 654321 and the generated token code is 890123
14. Click the button to submit credentials.

Your organization's site will display once you have set your PIN and successfully completed the login process. You should close the client once login is complete.

The section Instructions for logging in with a PIN provides guidance for subsequent logins.

Instructions for logging in with a PIN

After you have set a PIN, you are ready to log in to your network as follows:

1. Open your organization's login page.
2. Enter your user name.
3. On a mobile device or a computer, open the HOTPin Client application.
4. In the client, click the **Next Code** button to generate a token code.
5. Go back to the login page; enter your PIN and the token code in the password/passcode field.
   Example: **654321**890123
   If your **PIN** is 654321 and the generated token code is 890123
6. Click the button to submit credentials.
7. Close the HOTPin Client after you successfully authenticate.

Your organization's site will open once you have successfully completed the login process.

One-Factor Authentication

Use these instructions if PINs are not used for your organization.

Instructions for logging in with a token code only

This set of instructions covers logging in just with token codes.

1. Open the login screen for your network or published resource.
2. Enter your user name.
3. On a mobile device or a computer, open the HOTPin Client.
4. In the client, click the **Next Code** button to generate a token code.
5. Go back to the login; enter the token code in the password/passcode field.
   Example: 890123
6. Click the button to submit credentials.
   It may say Log On, Submit, or something different.
7. Close the HOTPin Client after you successfully authenticate.

Your organization's site will open once you have successfully completed the login process.

HOTPin with RADIUS

Depending on how your organization implements RADIUS in the HOTPin authentication system, login might be through either a web browser or a system prompt (for example, a window into which you can enter credentials). These instructions will cover the basic steps to authenticate; see your system administrator if you need more information.

Your login information should indicate that these are the instructions you should use.

Two-Factor Authentication

Use these instructions if PINs are required for your organization.

Instructions for login if you need to create a PIN

This set of instructions covers creating a PIN during initial login.

1. Think of a PIN. You will need it later in the instructions.
   A PIN must be 4 - 8 numerical digits, for example 654321.
2. If necessary, open the login screen for your network or published resource.
   As mentioned previously, it may be easier to do this on a machine besides the device that generates the token code if that device is a mobile phone.
3. Enter your user name.
4. On a mobile device or a computer, open the HOTPin Client application.
5. In the client, click the **Next Code** button to get a token code.
   - The group of numbers displayed is the token code.
   - A descending timer (a bar that decreases in size) indicates the amount of time the code will be displayed; it must finish before you can generate another code.
6. Go back to the login page or prompt; enter the token code plus a comma (,) and then a PIN in the password/passcode field.
   Example: 890123,**654321**
   If the generated token code is 890123 and your **PIN** is 654321
7. Submit your credentials.
8. Close the HOTPin Client after you successfully authenticate.

If using a browser your organization's site will open once you have successfully completed the login process. If authentication is through a system prompt, your connection is established. The PIN you created will be required for subsequent logins. The section Instructions for Logging in with a PIN provides guidance for subsequent logins.

Instructions for logging in with a PIN

After you have set a PIN, you are ready to log in to your network as follows:

1. If necessary, open your organization's login page.
2. Enter your user name.
3. On a mobile device or a computer, open the HOTPin Client application.
4. In the client, click the **Next Code** button to generate a token code.
5. Go back to the login page or prompt; enter your PIN and the token code in the password/passcode field.
   Example: **654321**890123
   If your **PIN** is 654321 and the generated token code is 890123
6. Submit your credentials.
7. Close the HOTPin Client after you successfully authenticate.

If using a browser your organization's site will open once you have successfully completed the login process. If authentication is through a system prompt, your connection is established.

One-Factor Authentication

Use these instructions if PINs are not used for your organization.

Instructions for logging in with a token code only

This set of instructions covers logging in just with token codes.

1. If necessary, open the login screen for your network or published resource.
2. Enter your user name.
3. Open the HOTPin Client.
4. In the client, click the **Next Code** button to generate a token code.

5. Go back to the login page or prompt; enter the token code in the password/passcode field.
6. Submit your credentials.
7. Close the HOTPin Client after you successfully authenticate.

If using a browser your organization's site will open once you have successfully completed the login process. If authentication is through a system prompt, your connection is established.

> Caution: Clicking the Next Code button too many times without successfully logging in to your network will cause your HOTPin Client to become out of sync with the server. If you get a "Failed to authenticate" message, but think that you have a valid user name, PIN and token code, notify your system administrator. You may need to replace the token key in your client to resume using the HOTPin system.

This completes the steps to log in to your network or protected resource. If you have difficulty logging in the future, see the topic Having Trouble Logging In.

HOTPin User Website QR Code Login

The HOTPin® User Website is a provisioning tool for HOTPin accounts. It offers the option to login through a Quick Response (QR) code. QR login codes can be used by devices that have a camera which can scan a code that is displayed as part of a login page. HOTPin Clients combine information from the QR code with your token key to negotiate login to the user website.

Requirements

- HOTPin client software installed on a device with a camera; for example, an Android smart phone.
- A computer to access the HOTPin User Website.
- A connection to the Internet or the organization's network. Both the computer and the smart phone must be connected.

Two-Factor Authentication

Use these instructions if PINs are required for your organization.

Instructions for login if you need to create a PIN

This set of instructions covers creating a PIN during initial login.

1. Think of a PIN.
   A PIN must be 4 - 8 numerical digits, for example 654321.
   You will need to enter it later in the instructions.
2. On a mobile device, open the HOTPin Client application and complete the following:
   a. If necessary, load a token key.
   b. Tap the **QR Login** button.
   c. Leave the scan screen open on your device; you will come back to it shortly.
3. On a laptop or desktop computer, open the HOTPin User Website login screen in a web browser. Complete the following:
   a. Enter your **User name**.
   b. Go to the **Authenticate using** drop menu; select **HOTPin**.

c. Click **Login with QR Code**.
d. Leave the login code up, you will use it shortly.

4. Go back to your mobile device; complete the following:
   a. Scan the QR code presented by the login page.
      Line up the QR code in the viewfinder on your device screen. It will automatically scan the code when it is in focus.

      > Important: Leave the login page QR code screen open after you scan it; it facilitates the login communication between your device and HOTPin Server.

   b. The client screen QR Code Authentication will open; tap the **Login** button to send your information to the user website.
   c. Tap **OK** on the sent confirmation.
5. Go back to the login page; you will be prompted to set a PIN for your account:
   a. Enter and confirm a PIN.

      > You will need your PIN for every login, so keep track of the number you enter.

   b. Click **Save PIN**.
      When you successfully save your PIN, you will be redirected to the login screen; you need to use your PIN with a new code to complete the login.
6. Still on the login screen, complete the following:
   a. Enter your **User name**.
   b. Go to the **Authenticate using** drop menu; select HOTPin.
   c. Click **Login with QR Code**.
      Leave the login code up, you will use it shortly.
7. Go back to the client application; complete the following:
   a. Tap **QR Login**.
   b. Scan the QR code presented by the login page.

      > Important: Leave the login page QR code screen open; it facilitates the login communication between your device and HOTPin Server.

   c. Enter your PIN when prompted on the mobile device.
   d. Tap **Login** on the QR Code Authentication screen.
      The client sends your information to the server.
   e. Tap **OK** on the sent confirmation.
8. The site will open in the web browser on your computer when the login information is received.
9. Close the HOTPin Client after you successfully authenticate.

Login steps are complete. The PIN you created will be required for subsequent logins. The section below, Instructions for Logging in with a PIN, provides details.

Instructions for logging in with a PIN

1. On a mobile device, open the HOTPin Client application.
   a. If necessary, load a token key.
   b. Tap the **QR Login** button.
   c. Leave the scan screen open on your device; you will come back to it shortly.
2. On a laptop or desktop computer, open the HOTPin User Website login screen in a web browser. Complete the following:
   a. Enter your **User name**.
   b. Go to the **Authenticate using** drop menu; select **HOTPin**.
   c. Click **Login with QR Code**.
   d. Leave the login code up, you will use it shortly.

3. Go back to your mobile device; complete the following:
    a. Scan the QR code presented by the login page.
        Line up the QR code in the viewfinder on your device screen. It will automatically scan the code when it is in focus.

        > Important: Leave the login page QR code screen open after you scan it; it facilitates the login communication between your device and HOTPin Server.

    b. Enter your PIN when prompted on the mobile device.
    c. Tap **Login** on the QR Code Authentication screen.
        The client sends your information to the server.
    d. Tap **OK** on the sent confirmation.
4. The site will open in the web browser on your computer when the login information is received.
5. Close the HOTPin Client after you successfully authenticate.

Login steps are complete.

One-Factor Authentication

Use these instructions if PINs are not used for your organization.

Instructions for logging in with a token code only

1. On a mobile device, open the HOTPin Client application.
    a. If necessary, load a token key.
    b. Tap the **QR Login** button.
    c. Leave the scan screen open on your device; you will come back to it shortly.
2. On a laptop or desktop computer, open the HOTPin User Website login screen in a web browser. Complete the following:
    a. Enter your **User name**.
    b. Go to the **Authenticate using** drop menu; select HOTPin.
    c. Click **Login with QR Code**.
        Leave the login code up, you will use it shortly.
3. Go back to your mobile device; complete the following.
    a. Scan the QR code presented by the login page.
        Line up the QR code in the viewfinder on your device screen. It will automatically scan the code when it is in focus.

        > Important: Leave the login page QR code screen open after you scan it; it facilitates the login communication between your device and HOTPin Server.

    b. Tap **Login** on the QR Code Authentication screen.
        The client sends your information to the server.
    c. Tap **OK** on the sent confirmation.
4. The site will open in the web browser on your computer when the login information is received.
5. Close the HOTPin Client after you successfully authenticate.

Login steps are complete.

Reference

The following topics provide information about the HOTPin system and login problems.

HOTPin User Website

The user website is a system feature that administrators may make available to users. It is a provisioning tool that allows users to create and edit HOTPin user accounts and to download token keys for client software. It also provides links to download resources.

If self-provisioning is enabled, your HOTPin administrator will provide information to access the user site.

Having Trouble Logging In?

The troubleshooting tips in this section provide solutions for potential login issues.

Next Code Button Is Dimmed

If the Next Code button is dimmed or won't generate a token code, check to see if a key is loaded in the client software. A token key must be loaded in the client application to generate a token code.

"Failed to authenticate" Message

If you see the message "Failed to authenticate" after you enter login information, try the following steps:

- Make sure that you type your user name and password correctly.
- If a PIN is required, make sure that you are using the correct PIN followed by a valid token code; if a PIN is not required, you should still confirm that you are correctly entering the token code.
- If you have multiple token keys, make sure you have loaded the correct token key for the system you are logging in to.
- If you think you have the correct key, check the Key ID and confirm it with your system administrator.
- If you still get a failed to authenticate message, you will need to delete the current key instance in your client software and import a new one.

Forgotten PIN

If you forget your PIN, you have the following options:

- If it is enabled and you can use Active Directory® credentials, log in to the HOTPin User Website to access your account and reset it.
- Ask your HOTPin administrator to place your user account in New PIN Mode. You can then set a new PIN during login.
- Ask your administrator to reset your PIN for you. The administrator will then need to provide the PIN to you.