

HOTPin

celestix

# Quick Start Guide

Celestix HOTPin Standalone Application

**Celestix HOTPin Standalone Application Quick Start Guide**  
Document Number: HPN0030-948-002  
Part Number: (CCD) 1005-0000015

Updated: June 28, 2013

Celestix HOTPin 2FA standalone application software version 3.7

© 2013 Celestix Networks, Inc. All rights reserved.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

HOTPin, Celestix and Celestix logo are registered trademarks or trademarks of Celestix Networks, Inc.

Microsoft, Microsoft logo, Microsoft Windows Server, Microsoft Forefront, Threat Management Gateway, Unified Access Gateway, Active Directory, Windows, Windows NT, ActiveX, Internet Explorer, Windows Phone, and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mac, iOS, iPhone, iPod touch, iPad and Safari are either registered trademarks or trademarks of Apple Inc., registered in the U.S. and other countries.

Google Play is a registered trademark of Google, Inc. in the United States and/or other countries. Android is a trademark of Google Inc.

The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Celestix Networks is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited.

Juniper Networks is a registered trademark of Juniper Networks, Inc. in the United States and other countries.

Oracle and JavaScript are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

---

## Contents

Introduction .....	1
Install Celestix HOTPin Server 3.7 .....	3
Prerequisites .....	3
Install HOTPin .....	3
Access the HOTPin Administration Site .....	4
Register.....	5
Configure .....	6
License.....	6
Quick Setup .....	7
System Settings.....	8
Add Users.....	8
Additional Features.....	10
API Extensions.....	11
Support .....	12
Reference: Web User Interface Content Overview.....	13

---

# Introduction

Celestix HOTPin Server® delivers highly secure two-factor authentication (2FA) with one-time passwords (OTPs) that can be generated on or delivered to end user mobile devices and computers. Generation is through client software; delivery is via SMS or email. OTPs can also be generated through hard tokens available from Celestix, or use your own that generates six-digit HOTP digital codes and supports OATH-compliant Portable Symmetric Key Container (PSKC) definition files. The HOTPin system enables organizations to provide market leading levels of authentication to remote users while at the same time reducing costs.

HOTPin can integrate with all leading access gateway solutions including Microsoft® UAG and Juniper Networks® SA series.

The 3.7 update to the HOTPin system adds the following functionality:

- NPS RADIUS client import/export
- QR Code authentication
- API SDK
- HOTPin Agent 1.1 update

NPS RADIUS client configurations can now be transferred to and from HOTPin server for backup or batch configuration. QR code authentication offers simplicity and security because scanning a code is easier and reduces exposure when using public, untrusted computers to access resources. The API SDK allows organizations to customize authentication communication. HOTPin Agent provides API extensions to allow authentication from any website login page.

This document provides brief instructions for the basic steps to set up the HOTPin Server system. It covers:

- [Software Installation](#)
- [Product Registration](#)
- [System Configuration](#)
- [Additional Features](#)

Information is presented sequentially, in the order best completed.

For your reference, there is a **diagram** of the web user interface at the end of this document provided as a navigation overview.

---

# Install Celestix HOTPin Server 3.7

The following topics first review prerequisites, then explain the steps to install the application, and lastly discuss how to access the administrative web user interface.

## Prerequisites

- Microsoft Windows Server® 2008 R2
- Install through an account that is a member of the local Administrator group

## Install HOTPin

1. Navigate to the top folder on the product CD.
2. Right-click the file *CelestixHSAInstallation* and select **Run as administrator**.
  - a. The installation wizard will guide you through the process
  - b. You will be required to accept the license agreement to proceed.
  - c. The wizard will inform when the process is complete.
3. Right-click the file *CelestixHSAConfiguration* and select **Run as administrator**.
  - a. The installation wizard will guide you through the process.
  - b. The wizard will inform when the process is complete.

A shortcut to HOTPin Administration will be placed on the desktop when installation is complete. Next you need to access the administration site to configure the application.

# Access the HOTPin Administration Site

The following explains the two options for launching the web user interface (web UI), which is the administration site for HOTPin.

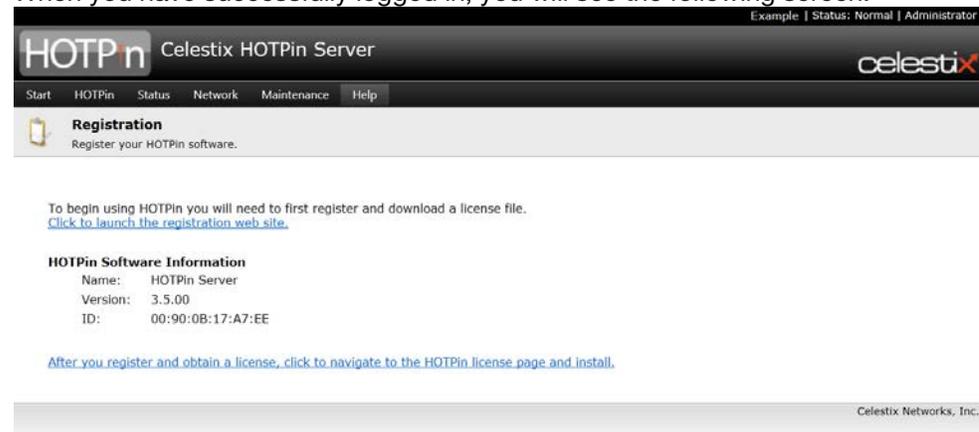
## Please Note:

- › Some web UI functionality requires ActiveX® controls in the Internet Explorer® browser.
- › The web UI uses a self-signed certificate; you must accept the certificate to access the site.

To open the administration site:

1. Launch HOTPin administration. You have two options:
  - Double-click the HOTPin Administration icon on the desktop to launch the web user interface (web UI) in the default browser.
  - From a web browser session, navigate to: `https://ServerName|IP address:8098`.
  - For example, if your server IP address is 192.168.30.4, the web UI URL would be: `https://192.168.30.4:8098`
2. Enter your administrative credentials when prompted.

When you have successfully logged in, you will see the following screen:



Next get information about registering your product.

---

# Register

You can register HOTPin to get a user license for evaluation purposes, but if you have a license skip to [Configure](#). The Registration page is the default web UI page until you upload a user license, but it can also be accessed at **Help|Registration**.

To register your product:

3. If you do not have the web UI open in a browser (Internet Explorer is recommended for full functionality), access it now.
4. Click the link to the registration website (navigate to **Help|Registration** if you don't see the link).
5. Complete and submit the form.
6. Click the link to download the evaluation license.

Keep track of the location as you will need to navigate to it in the license upload procedure.

**Caution:** Do not change the name of the license file; files of a different name will cause an error during upload.

Next you will need to configure the application.

---

# Configure

The following topics briefly cover the basics steps to set up HOTPin Server.

**Please Note:** For a glossary of HOTPin terms, see online help ([Help](#)|[Contents](#)|[HOTPin](#)|[Glossary](#)).

## License

Once you have either [downloaded an evaluation license](#) or purchased a user license, you will need to upload it to HOTPin Server.

To upload and configure your HOTPin license:

1. Navigate to **HOTPin|License**.
2. Under **Upload new license**, click the **Browse** button to navigate to the license file.
3. Click **OK** to install the license.

A message displays when the license import has successfully completed.

4. Click **Cancel** to return to the main HOTPin screen.

**Important:**

- › Only valid license files will be allowed to upload.
- › An invalid file will produce an error message on the License screen.

5. Click **OK** to return to the HOTPin screen.

**Please Note:** The license covers the total number of users. If you have a license for 500 users, and have 490 accounts (either enabled/disabled), deleting 10 accounts would then mean you have 20 available accounts.

Next you need to complete the initial configuration.

# Quick Setup

Access the Quick Setup menu to complete initial configuration for the HOTPin application.

1. Open the HOTPin web UI.
2. Navigate to **Start|Quick Setup**.
3. Complete the following; use the links for additional information:
  - a. **Administrator Password** – change the administrator password from the factory default which is public knowledge.
  - b. **Alert Email** – enable the type of alerts you want to receive through email.

## Administrator Password

1. Enter and confirm a new password.

**Note:** Password complexity requirements are noted on the Administrator Password screen.
2. Click **OK** to complete updating the password.

An error message will inform if the change was not successful.

## Alert Email

**Please Note:** Alert Email requires SMTP.

1. Select Enable alert email.
2. Select the check boxes to enable your appliance to send email for corresponding alert types:
  - Send error alert email
  - Send warning alert email
  - Send informational alert email
3. Complete the following:
  - **To** – indicate one or multiple recipients. Use a comma to separate multiple addresses.
  - **From** – indicate an address that a recipient will recognize.
  - **With** – enter your network SMTP server name or IP address.
  - **Test Settings** – click to send a test email using the settings you entered.

**Note:** The alert email function will indicate whether a test email was sent. If the test email is not received after the alert email feature indicates that one was sent, the error is most likely due to SMTP server settings. An error will occur if the SMTP service is not running or if your appliance is not correctly configured to see the SMTP server. Confirm your SMTP server and network settings before trying to test again.

4. Click **OK** to complete.

You have completed the initial setup. You can next adjust HOTPin settings as needed for your deployment.

## System Settings

There are several options available for your HOTPin deployment. On the Settings page you can configure:

- **General** – features include Authentication, Provider, Client Software, and PIN options.
- **Event Log** – manage HOTPin database size with event trimming and archiving.
- **Backup** – enable backup for HOTPin configuration.

Each of the options are discussed in the online help ([Help|Contents|HOTPin|Settings](#)).

Next you need to add user accounts.

## Add Users

You can add user accounts in multiple ways, and the merits or limits of each option are discussed in the online help, as are instructions for configuration. Navigation to information is indicated after the feature description below.

- You can enable the HOTPin User Website to allow users to provision their own accounts and or to allow users to download token keys for client software.

**Important:** Requires Active Directory® for authorization.

**[Help|Contents|HOTPin|User Website](#)**

- You can synchronize HOTPin with Active Directory to automatically add and delete accounts.

**Help|Contents|HOTPin|AD Synchronization**

- You can add accounts manually.

**Help|Contents|HOTPin|Users|Add New**

---

# Additional Features

HOTPin provides a great deal of flexibility to deploy two-factor authentication, allowing you choose from several options to suit your organization's preferences and security profile. See the HOTPin online help for information about the following features; navigation to information is indicated after the feature description.

- Token Providers  
Send token codes to end users who will not use client software or external token keys.  
**Help|Contents|HOTPin|Providers**
- External Token Keys  
Use token devices (also referred to as hard tokens) to generate token codes for end users who will not use client software or token providers.  
**Help|Contents|HOTPin|Token Keys**
- High Availability  
Deploy a primary and backup server for authentication redundancy.  
**Help|Contents|HOTPin|High Availability**
- NPS RADIUS  
Use Microsoft's Network Policy Server to provide RADIUS authentication services.  
**Help|Contents|HOTPin|NPS RADIUS**
- Agent Software  
Connect HOTPin to a UAG environment.  
**Help|Contents|HOTPin|Agent Software**

Some additional features will be necessary. For example, you will need to select an authentication mechanism based on the environment in which you deploy HOTPin. If you have a Juniper SSL VPN appliance, you will configure NPS RADIUS. If your organization uses a Celestix WSA appliance, you will need to download the install the HOTPin Agent to work with UAG.

As an example of optional configuration, if you will not provide client software for your end users, you will need to configure token providers or external token keys.

More information can be found in the online help (**Help|Contents**).

---

# API Extensions

The following features have sample code libraries in the HOTPin SDK.

- Agent 1.1 – extends agent functionality to allow authentication to any website login page.
- Authentication API for .NET/Java – creates an authentication communication channel for ASP .NET and Java-based websites and applications.
- QR Code Authentication for .Net/Java – allows authentication through a web page using client software.

Contact your sales representative for more information:

[sales@celestix.com](mailto:sales@celestix.com)

---

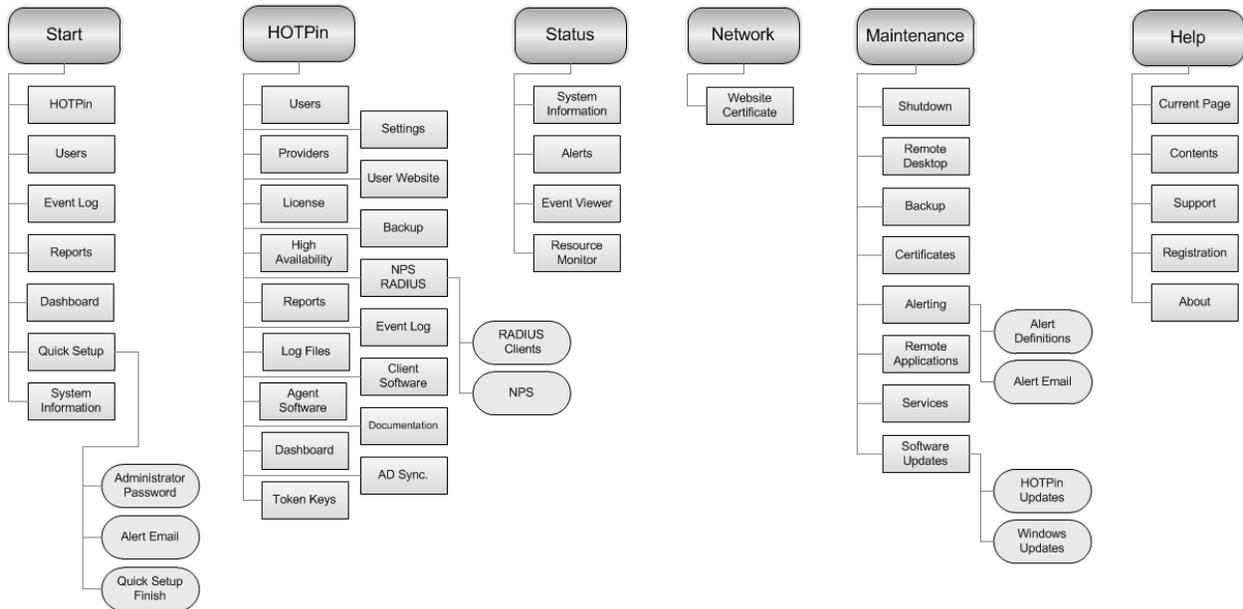
# Support

Email questions to [support@celestix.com](mailto:support@celestix.com)

Thank you for choosing Celestix HOTPin Server for your two-factor authentication solution.

# Reference: Web User Interface Content Overview

HOTPin Standalone Application Web User Interface Menu Diagram



The HOTPin User Website structure is outlined below.

HOTPin User Website Menu Diagram

