celestix

celestix.com/hotpin

HOTPin

Strong Authentication. Simplified.

Looking to protect SharePoint portals? remote access via Citrix XenDesktop? Firewall access? HOTPin works in all of these scenarios. HOTPin is a simple and easy to deploy two-factor authentication solution that uses your phone as a token. HOTPin authentication service is available as software, virtual machine or appliance form factor for on premise deployment or as a managed service with pay as you go price model.

Features

- Multiple form-factors – soft token, hard token, YubiKey, SMS, email, and instant messenger.
- Soft tokens for iPhone, Blackberry, Windows Mobile 7, Win32, iPad and Mac
- Clientless mode utilizes SMS, instant messenger or email for unmanaged devices
- Intelligent price model – one price per user per year, regardless of form factor
- Intuitive web portal for user self-provisioning
- Simple to use administration console
- Comprehensive reporting and compliance engine
- Authentication server available as Appliance, Software versions and managed service
- Integration and migration options available
- Authentication API

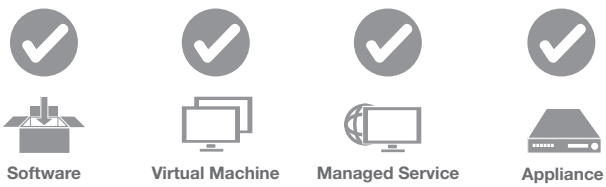
Celestix Networks HOTPin authentication solution allows companies to embrace the use of smart devices in the workplace. By installing a soft token on a mobile device, it is transformed into a token capable of generating a one time password (OTP) that can be used to authenticate the user when working remotely.

Celestix HOTPin can also simplify the authentication of remote users on devices that cannot utilize a soft token and for workers who may not own a corporate smart device such as contractors. HOTPin uses the GSM network to deliver OTPs via SMS and the email system for delivery of OTPs to an inbox.

HOTPin client now supports QR codes. Users can scan the QR code and will be instantly logged in to the application in a secure manner. The integration of this function to any web services is simple. The latest HOTPin 3.7 includes API with the samples that helps to simplify the integration into your existing server architecture.

Celestix believes IT shouldn't be complicated and costly, but it should be secure and controlled. This is why HOTPin uses HOTP, an HMAC-based algorithm for generating OTPs. HOTP is an open standard that continues to receive extensive scrutiny from security industry experts and leading academics.

Some authentication products use time-based OTPs (leveraging a vendor assigned seed with the current time). HOTPin OTPs are event-based (using a key generated on-site by the IT manager in conjunction with a counter). As such, HOTPin OTPs are not susceptible to attacks that compromise the seed or predictable algorithms based on the current time.



celestix

celestix.com/hotpin

HOTPin

Secure your Organization with HOTPin

- Two-Factor Authentication. Simplified.
- Available as software, appliance, managed services and virtual machine.
- Works with all smart phones
- Now supports QR code login
- Cost-effective, secure and reliable

Strong Authentication. Simplified.

HOTPin integrates seamlessly into your VPNs, Firewalls, Microsoft TMG, UAG, Citrix XenDesktop, XenApp and Windows servers, and web applications to provide strong two-factor authentication for your entire organization.

Microsoft Forefront | Remote Desktop | Firewall Access | Web Portal | VPN Access | HOTPin API

Features

HOTPin Features

Client mode – Soft tokens
Supported platforms
- iOS
- Android
- Windows Phone 7
- Blackberry
- Microsoft Windows
- Mac

Clientless mode – Out of Band
One Time Passwords can be delivered without a token for true Out of Band (OOB) authentication.
- SMS and text-messages
- Emails
- Instant Messenger
- QR code via camera

For users who might be out of network coverage, HOTPin can send an additional OTP at time of successful logon. This OTP can be stored on the users' device for subsequent use.

Hardware tokens
HOTPin can be purchased with hard tokens for users as needed.
- OATH compliant
- HOTP (event-based)
- 6 digit OTPs

Third-party hardware tokens
HOTPin supports any HOTP compliant hardware token
- OATH compliant
- HOTP (event-based)
- 6 digit OTPs

This allows interoperability and ease of migration.

Quick Installation
Installation and deployment is designed to be simple.
- Award winning COMET interface
- Embedded RADIUS server
- LCD display and jog dial (for appliances)
- Built-in database
- AD synchronization for user management

Self-service portal
End users can provision themselves, import their own keys and reset their PIN if required, without having to go through IT helpdesk.
- Reduce IT help desk costs
- Enhanced user experience
- Higher adoption and user satisfaction

QR provisioning
HOTPin soft tokens users can import the token keys by scanning a QR code from the self service portal.

Comprehensive Reporting
Comprehensive reporting engine provides complete visibility.
- Provide visibility to management
- Enforce and monitor compliance
- Automated report generation and delivery

Customization
HOTPin server, self-service portal and soft token application can be customized to promote corporate branding.

Celestix Networks, Inc.
3125 Skyway Court
Fremont, California 94539

USA +1 510 668 0700
UK +44 (0) 118 959 6198

Japan +81 03 5210 2991
Singapore +65 6781 0700

info@celestix.com