Security, Simplified.

HOTPin Integration Guide: Google Apps with Active Directory Federated Services

celestix

Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; Celestix assumes no responsibility for its accuracy and/or completeness.

In no event will Celestix be liable for damages arising directly or indirectly from any use of the information contained in this document.

Updated: November 7, 2013

1 Introduction

This document describes how to integrate HOTPin with Google Apps™ configured for single sign-on (SSO) to a local AD FS 2.0 service.

Google Apps is a software-as-a-service (SaaS) productivity suite. It can be used to replace traditional hardware/software IT models with cloud-based tools. Applications are accessed by a web browser and are available anytime, anywhere with an internet connection, to any web-enabled device.

Celestix HOTPin® provides two-factor authentication (2FA) for remote access and cloud solutions (like SSL VPN, IPSec VPN and Web authentication). Our 2FA solution uses a PIN and one-time-password (OTP). OTP generation has multiple options: client software, hard token devices, or token providers that use email, SMS, or web technologies. Thus HOTPin OTPs can support a variety of devices for strong authentication. Configure the device options that best suit your environment:

- Client software leverages already deployed smart devices
- Token providers use any email/SMS-enabled device
- Hard token devices are available from Celestix, or bring your own OATH-compliant PSKC option

HOTPin is designed to be an easy to deploy, easy to use technology. It integrates directly with Microsoft's Active Directory® and negates the need for additional user security databases. HOTPin consists of two core elements: a RADIUS Server and authentication server. The authentication server directly integrates with LDAP or Active Directory (AD) in real time.

When these three technologies are combined, Google Apps trust AD FS to authenticate users, and AD FS uses HOTPin to apply 2FA before granting access. You can thus increase both login security and convenience.

1.1 Overview

Illustration 1 provides an overview of SSO functionality for AD FS using HOTPin 2FA.

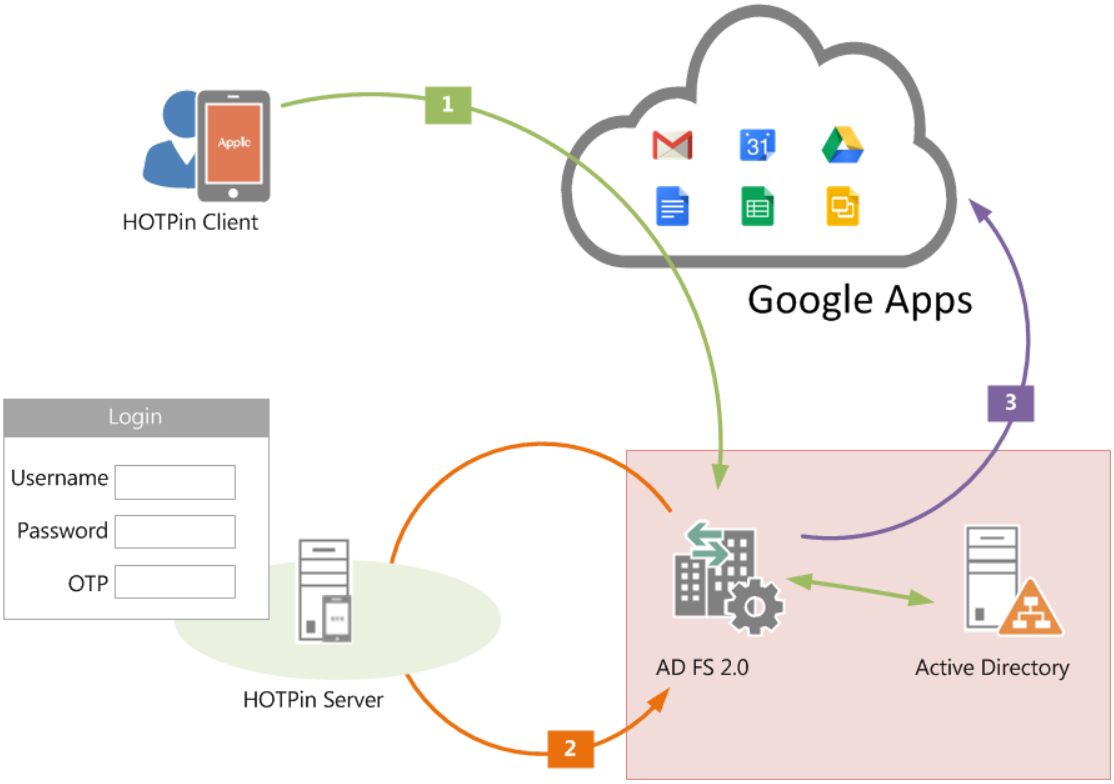


Illustration 1

1.2 Summary

This integration guide covers the set up for a basic installation in which HOTPin provides 2FA for Google SSO through AD FS. It may be helpful to set up a test environment before rolling out to production; as such, some of the example settings suggest test information.

The content is based on information from the website articles noted below; it is revised for your convenience to aid in setting up HOTPin 2FA. You can access the full, original articles at:

- Google Apps Documentation & Support: SSO (Single Sign-On)
  https://support.google.com/a/answer/60224?hl=en
- Ryan Finger – Trials and Tribulations: ADFS 2.0 and Google Apps SAML Integration – Achieve SSO
  http://ryanfinger.wordpress.com/2010/08/10/adfs-2-0-and-google-apps-saml-integration-achieve-sso/

1.3 Prerequisites

The integration covered in this document requires the following components:

- Google Apps
  Admin account to configure SSO
- Microsoft
  - Microsoft Server 2008R2 with ADFS 2.0 installed
    - Or -
    Microsoft Server 2008R2 with ADFS 2.0 installed as a proxy
  - Active Directory installed
  - HOTPin Agent installed
  - HOTPin ADFS Client installed
- HOTPin
  - Windows server 2008 R2 64-bit (Standard or Enterprise)
  - IIS installed with SSL certificate (required for management and remote administration)
  - HOTPin 3.7 server software

1.4 Assumptions

This document assumes the following are true:

- Google Apps are already configured for production with existing AD users.
- Readers are familiar with both Google Apps management and AD FS administration.
- Readers are familiar with AD management.
- HOTPin Server has been provisioned and user accounts align with AD.

2 Google Apps SSO Configuration

To configure Google Apps SSO, you will first need to access your AD FS server to get a signing certificate. Then you will log in to Google to configure SSO settings.

2.1 Get the AD FS Signing Certificate

Open the AD FS 2.0 Console (MMC snap-in) to access AD FS configuration.

Complete the following steps to get the certificate you will need to upload to Google Apps:

1. Select the “Certificates” node under “Service”.
2. Double-click the certificate under “Token-signing”.
3. Navigate to the “Details” tab.
4. Click “Copy to File”.
5. Complete the wizard to save the certificate.
   Important: The signing certificate must be exported in DER format (.cer).

Next, you are ready to set up Google SSO settings.

2.2 Configure Google Apps SSO Settings

Complete the following for SSO configuration with AD FS.

1. Log into your Google Admin console.
2. Navigate to More controls|Security|Advanced settings|Set up single sign-on (SSO).
3. Complete the following:

   Note: Items below reflect the settings you need to configure. Items not listed can use the default settings.

   - Enable Single Sign-on – Select.
   - Sign-in page URL – Use the example below, but replace *(yourdomain.com)* with the domain name you are using for SSO.

     Example:

     https://adfs.(yourdomain.com)/adfs/ls/
   - Sign-out page URL – Use the example below, but replace *(yourdomain.com)* with the domain name you are using for SSO.

     Example:

     https://adfs. (yourdomain.com)/adfs/ls/?wa=wsignout1.0
   - Change password URL – Not available; AD FS does not support this feature.
   - Verification certificate – Upload the signing certificate you downloaded from the AD FS server.
   - Use a domain specific issuer – Select.
4. Click “Save changes”.

Next you will need to configure AD FS for Google Apps SSO.

3 AD FS 2.0 Configuration

The steps below explain how to create the AD FS side of the trust relationship.

1. Open the AD FS 2.0 Console (MMC snap-in).
2. Add a new “Relying Party Trust”.
3. Click “Start”.
4. Select “Enter data about the relying party trust manually” and click “Next”.
5. Enter a “Display name” and click “Next”.
6. Select AD FS 2.0 and click “Next”.
7. Click “Next”; you have used the default signing certificate.
8. Enable SAML WebSSO Protocol support, then add the path: “https://www.google.com/a/*(yourdomain.com)*/acs”

Important: Replace *(yourdomain.com)* with the domain name you are using for SSO. Click "Next".

9. Under "Configure Identifiers", enter "google.com/a/(yourdomain.com)" and click "Add" and then click "Next".
   Important: Replace *(yourdomain.com)* with the domain name you are using for SSO.
10. Designate a permission level; the default is to "Permit all".
11. Validate settings and then click "Next". This will create the relying party.
12. Open the relying party trust and confirm that "POST" is the designated binding and that the URL is "https://www.google.com/a/*(yourdomain.com)*/acs", where *(yourdomain.com)* reflects the domain name you are using for SSO.
13. Right-click the relying party trust and select "Edit Claim Rules".
14. Click "Add Rule".
15. In the wizard, select "Send LDAP Attributes as Claims" and click "Next".
16. Enter a name to distinguish the claim rule.
17. Select "Active Directory" as the attribute store.
18. In the "LDAP Attribute" tab select "Email Address".
19. In the "Outgoing Claim Type" select "Name ID".
20. Click "Finish".

Now that you have configured Google Apps and AD FS, it's time to add 2FA.

4 HOTPin Agent and AD FS Client Setup

HOTPin authentication can be added to AD FS or AD FS proxy deployments. In either case, two packages need to be installed:

- Standalone server
  Install the HOTPin Agent and HOTPin ADFS client on the ADFS server.
- Proxy server
  Install the HOTPin Agent and HOTPin ADFS client on the ADFS proxy server(s) only.

Important: For proxy server setup, all user requests should go to the proxy server and not the ADFS server, even if the client is on the intranet.

Note: Before you configure the HOTPin AD FS client, HOTPin Server should have been provisioned, including all user accounts. Enabling AD Sync in the HOTPin web UI will automatically add designated accounts. For more information, please refer to:

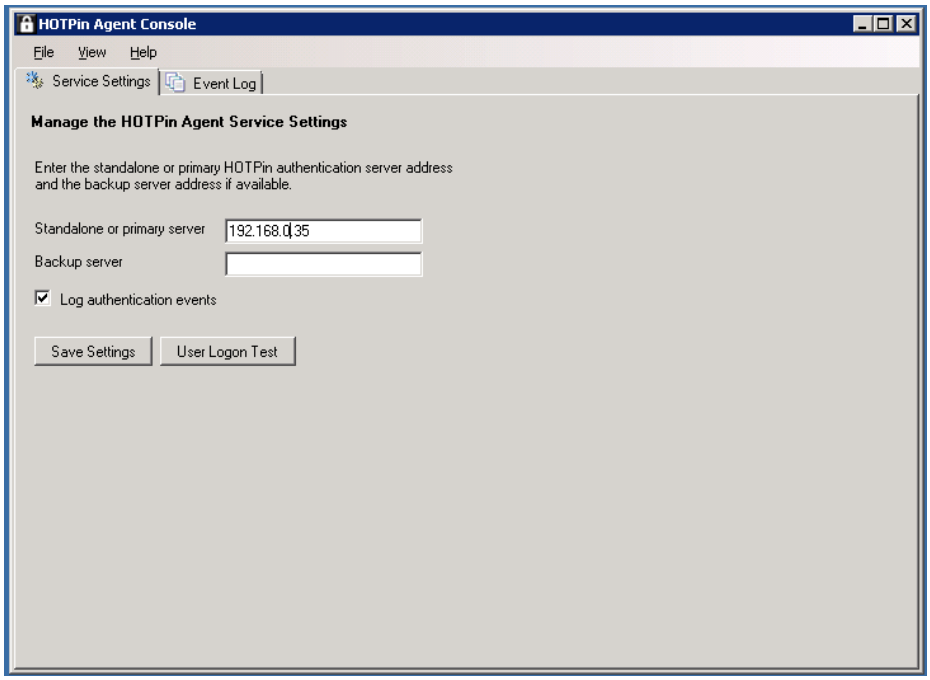
HOTPin installation guides: http://www.celestix.com/products-services/#select_1-7

AD Sync information: http://kb.celestix.com/knowledge-base/412/

4.1 HOTPin Agent Configuration

HOTPin Agent configuration will facilitate communication between HOTPin and AD FS.

1. Open the HOTPin Agent Console installed on the AD FS server or AD FS proxy server:



2. Enter the HOTPin server IP address. If two HOTPin servers are deployed, enter backup server details.
3. Select “Log authentication events” only when you need to debug the integration.

4.2 HOTPin ADFS Client Configuration

Next you will enable HOTPin authentication in AD FS and configure settings.

1. Open the HOTPin ADFS Agent Console installed on the AD FS server or AD FS proxy server.
2. Click the ADFS tab to access enable/disable functions.
   See ADFS Tab for more information.
3. Click the Properties tab to manage settings.
   See Properties Tab for more information.

4.2.1 ADFS Tab

AD FS uses multiple options to authenticate a Google Apps user profile. Forms based authentication is necessary for HOTPin 2FA.Users will be required to enter their federated user name, AD password and HOTPin passcode.

The following screen shot is for your reference.

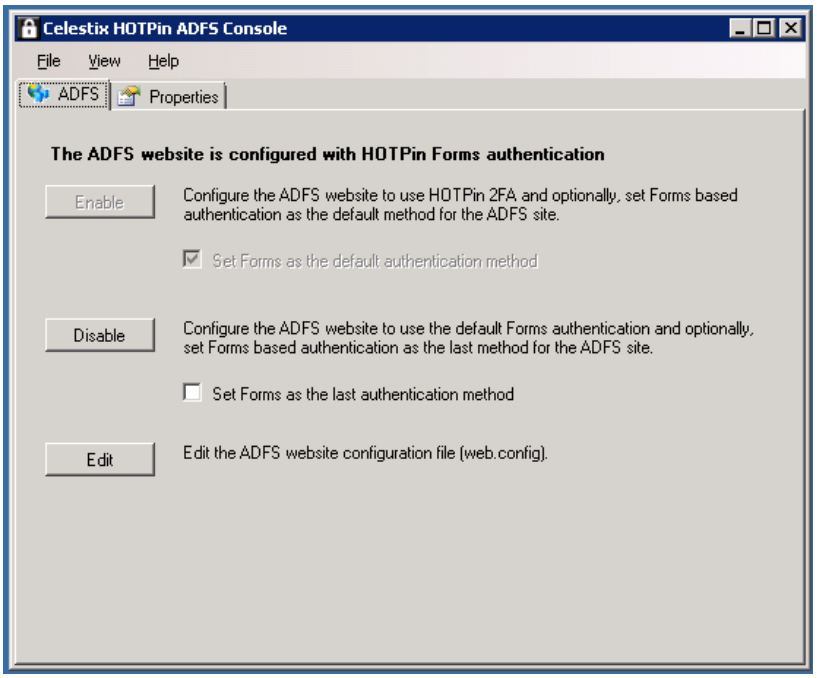


Illustration 2

Complete the following steps:

1. Select “Enable” to activate Forms based authentication.
2. Check “Set Forms as the default authentication method”; this will designate HOTPin as the first authentication method.

Notes:

- The Disable button can be used to erase HOTPin ADFS Console configuration in the event you need to start over.
- The Edit feature is for advanced configuration, and is outside the scope of this document.

4.2.2 Properties Tab

Additional configuration options are discussed in the next sections.

The following screen shot is for your reference.

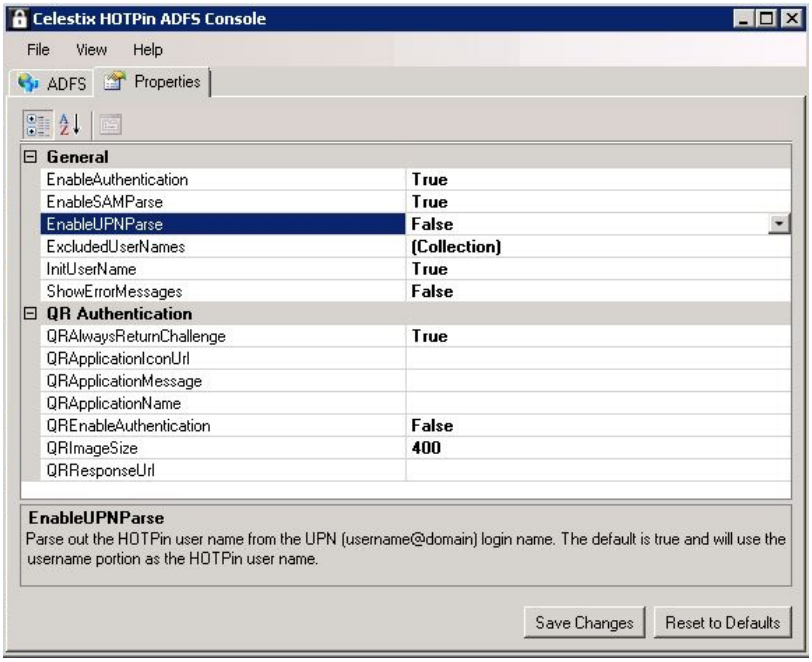


Illustration 3

4.2.2.1 General Options

Adjust the following properties as needed:

- Enable Authentication – “True” indicates HOTPin authentication is enabled on the login form. “False” disables authentication, but does not delete the information configured on the Properties tab.
- EnableSAMParse – Set to “False”; SAM names should not be used for Google SSO.
- EnableUPNParse – Set to “False”; UPNs should not be used for Google SSO.
- ExcludedUserNames – Create a list of users to exclude from HOTPin 2FA when they log in to Google Apps.
- InitUserName – Use the AD user name to autopopulate the login form.
- ShowErrorMessages – The default setting is “False” to avoid showing API-related errors in the front end. Set it to “True” only when you need to troubleshoot.

Note: For more information about user names, see the section Configuration and Notes.

The following HOTPin ADFS login screen shot is for your reference.

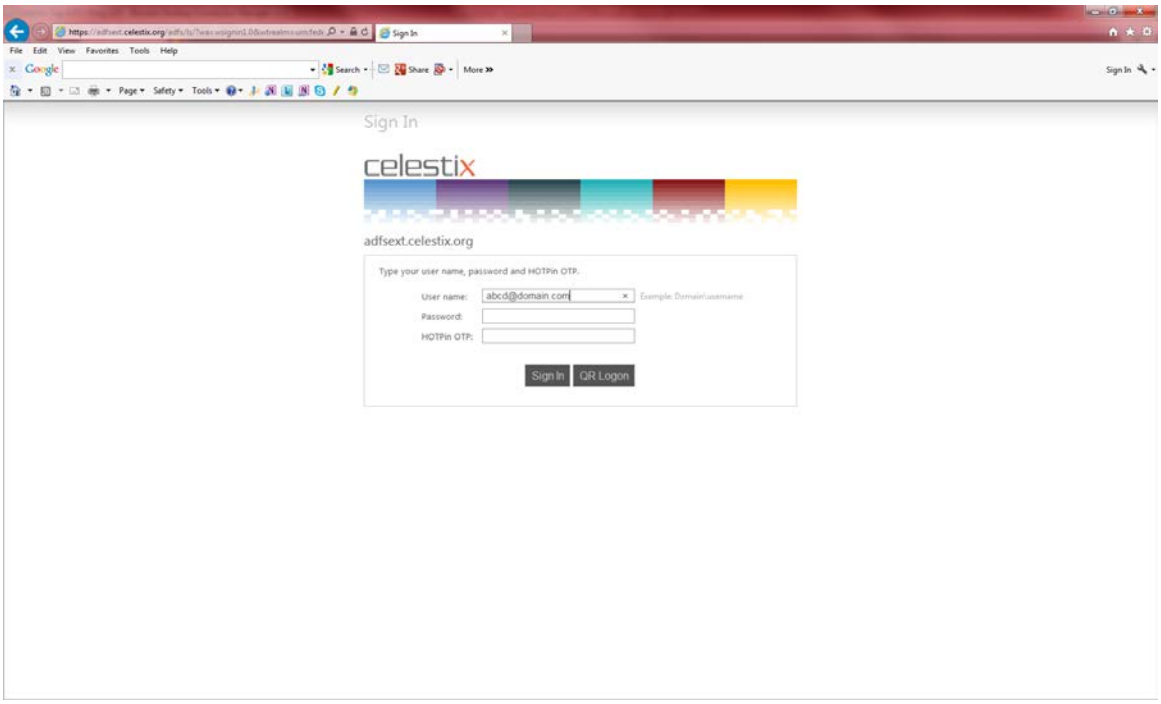


Illustration 4

4.2.2.2 QR Authentication Options

The configuration discussed below applies to QR code authentication for client software. QR code authentication can be made available to client software users who have devices with a camera to scan codes. The settings below allow you to customize both functionality and the items displayed on the QR code authentication screen.

- QRAlwaysReturnChallenge – "True" enables the system to offer a QR code when users enter a wrong user name.
  Note: QR authentication requires an internet connection for the challenge/response authentication mechanism.
- QRApplicationIconUrl – Add an icon to the display.
- QRApplicationMessage – Add a message to the display.
- QRApplicationName – Add an application name to the display.
- QREnableAuthentication – "True" enables QR authentication.
- QRimageSize – Set the QR image display size; guidelines are listed in the description at the bottom of the screen.
- QRResponseUrl – Designate a customized URL to display instead of the default (the host name).

You have completed all the steps necessary to set up a basic trust relationship between Google Apps and AD FS that uses HOTPin for two-factor authentication.

The following section provides some additional information that may be relevant for your organization's deployment.

5 Configuration and Notes

The following information is included for your reference.

5.1 HOTPin User Names

HOTPin user names can use four AD-compatible options:

- SAM Account Name
- Principal Name
- Email Address
- Domain and SAM Account Name

In Google Apps, the user name is generally an email address. This means that the AD authentication property and HOTPin user name should be the email address to facilitate SSO.