Security, Simplified.

HOTPin Integration Guide: Microsoft Office 365 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

Copyright

1 Introduction

This document describes how to integrate HOTPin® with Microsoft's Office 365™Online Services configured for single sign-on (SSO) to a local AD FS 2.0 server.

Microsoft Office 365 (O365) is a cloud-based service that can use Active Directory® Federation Service (AD FS) to enable user's locally entered AD credentials to sign on to various Microsoft online services such as Office, SharePoint and Lync.

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

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.

1.1 Overview

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

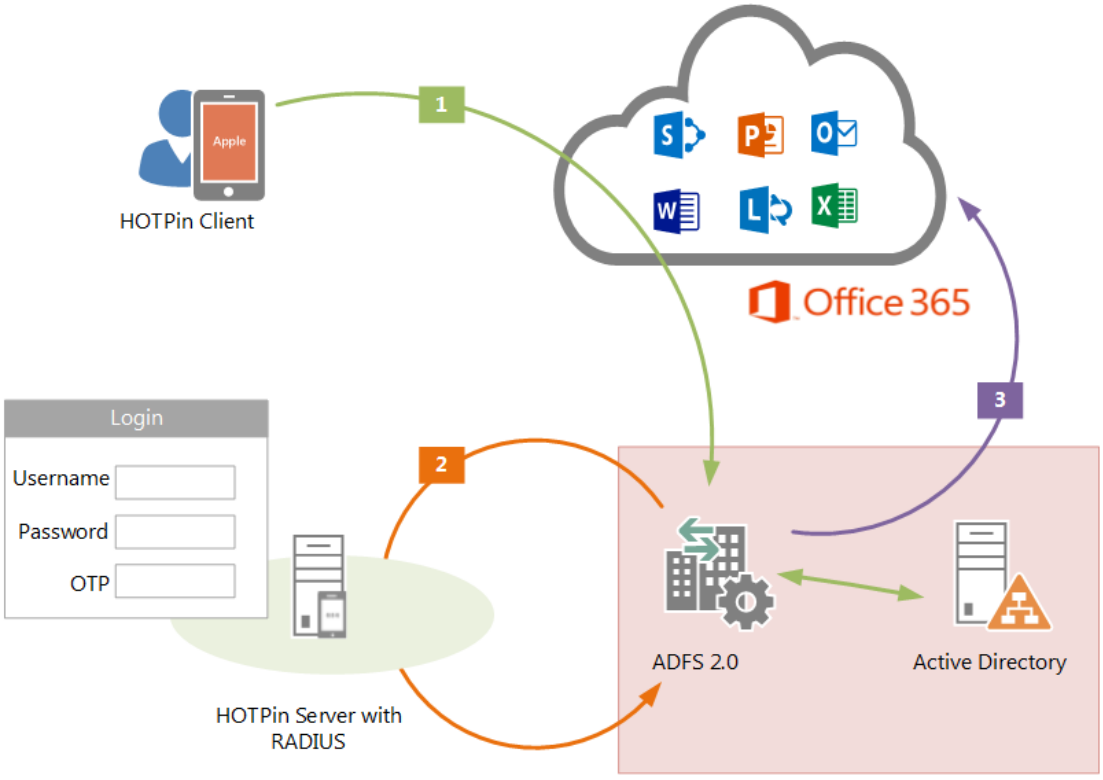


Illustration 1

1.2 Summary

This integration guide covers the set up for a basic installation in which HOTPin provides 2FA for O365 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.

1.3 Prerequisites

The integration covered in this document requires the following components:

- Microsoft
    - Office365 Cloud Account
    - 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:

- HOTPin Server has been provisioned and user accounts align with AD.
- Readers are familiar with AD FS administration.
- Readers are familiar with AD management.
- Office365 has already been setup for SSO to an on-premise AD FS server that uses existing AD user passwords. Illustration 2 provides an example.

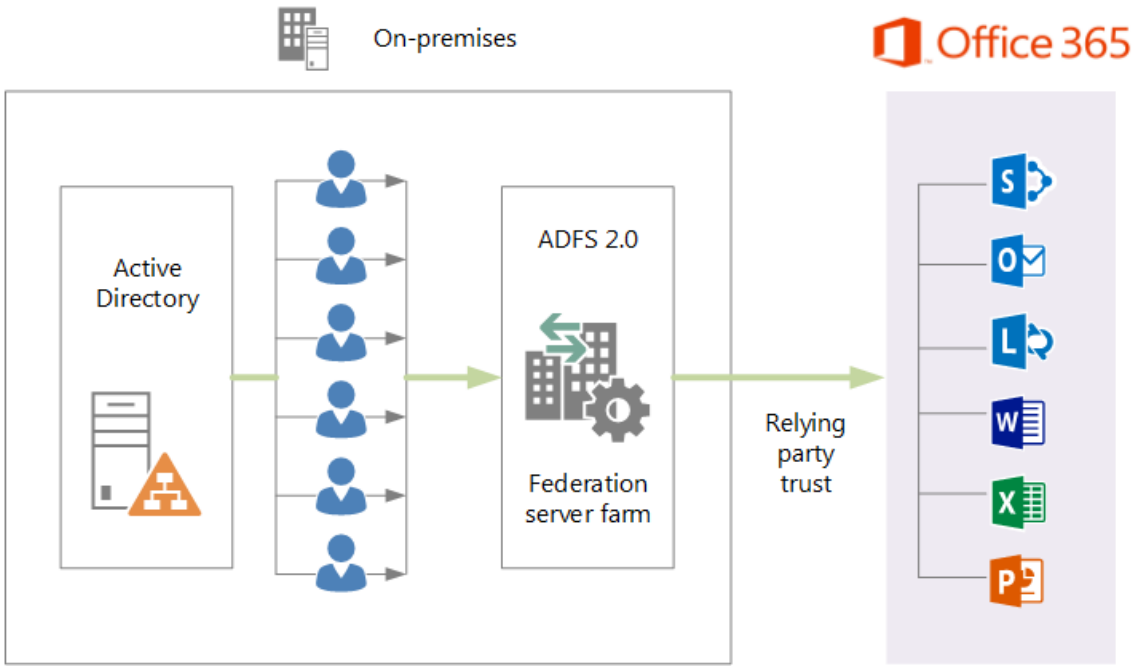


Illustration 2

For reference on how to setup ADFS Server and SSO, refer to the Microsoft article "Setting up ADFS Proxy Server – Part 1" (http://office365support.ca/setting-up-adfs-proxy-server-part-1/).

2 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:

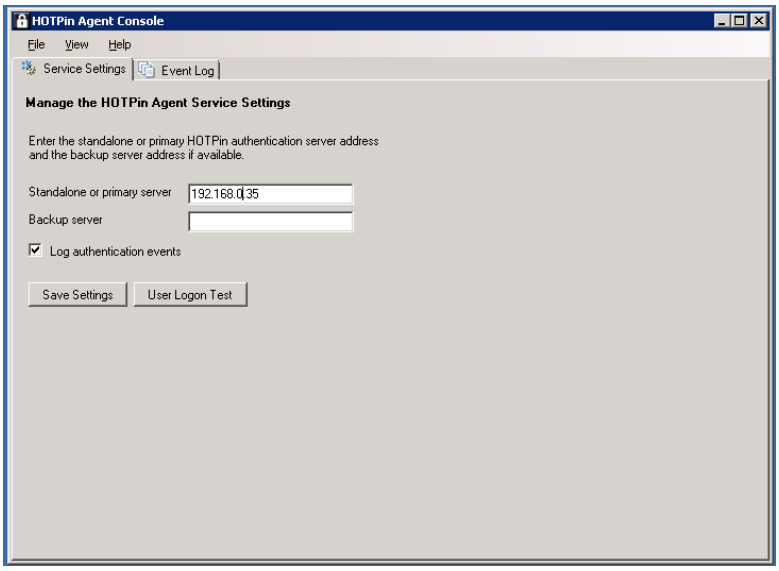
HOTPin installation guides: http://www.celestix.com/products-services/#select_1-7

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

2.1 HOTPin Agent Configuration

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

1. Open the HOTPin Agent Console installed on the ADFS server or ADFS 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.

2.2 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.

2.2.1 ADFS Tab

AD FS uses multiple options to authenticate an O365 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.

Illustration 3 shows the HOTPin ADFS client for your reference.

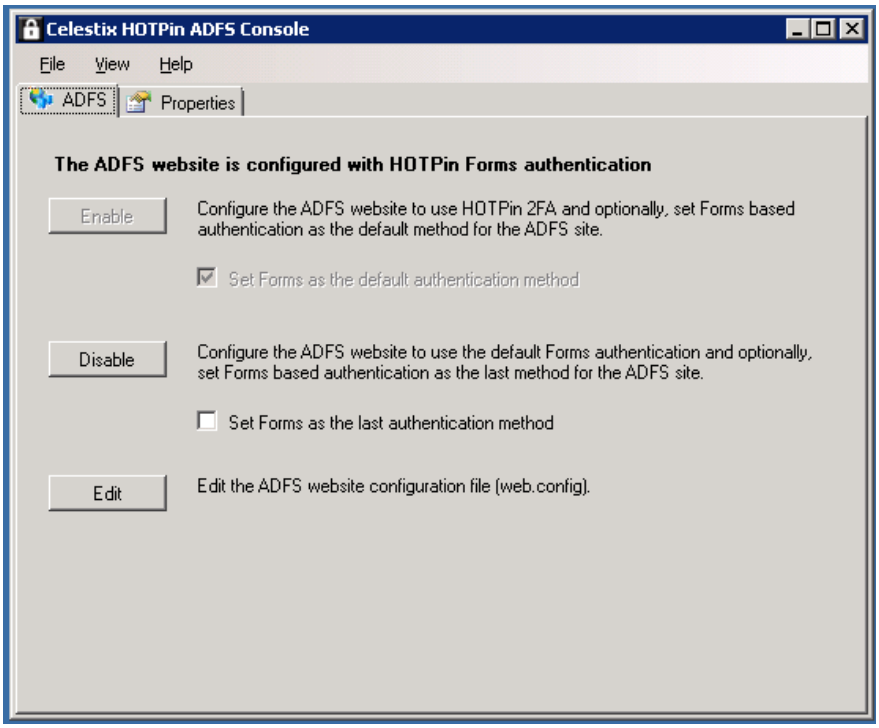


Illustration 3

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.

2.2.2 Properties Tab

Additional configuration options are discussed in the next sections.

Illustration 4 shows the HOTPin ADFS client for your reference.

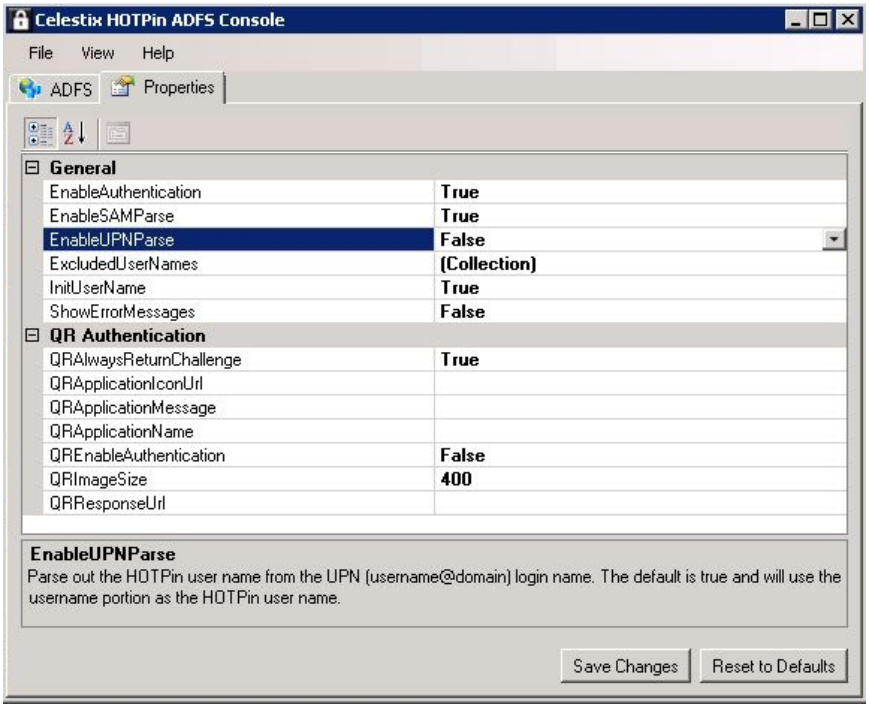


Illustration 4

2.2.2.1 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 – When SAM names are the authentication property configured in AD and HOTPin, “True” enables parsing the HOTPin user name from SAM (domain\username) login name.
- EnableUPNParse – When UPNs are the authentication property configured in AD and HOTPin, “True” enables parsing the HOTPin user name from the UPN (username@domain.com) login name.
- ExcludedUserNames – Create a list of users to exclude from HOTPin 2FA when they log in to Salesforce.
- InitUserName – Designate the O365 login name to auto populate the ADFS 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 Notes.

Illustration 5 shows the HOTPin ADFS login screen shot for your reference.

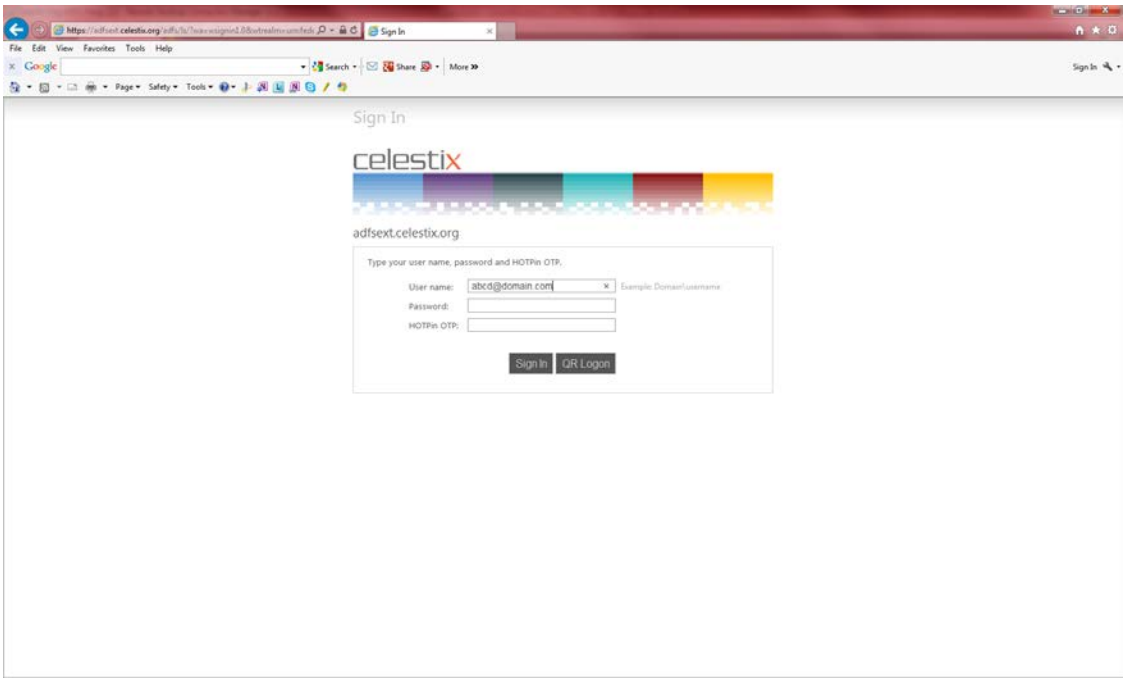


Illustration 5

2.2.2.2 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 AD FS and HOTPin for two-factor authentication.

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

3 Configuration Notes

The following information is included for your reference.

3.1 HOTPin User Names

HOTPin user names can use four AD-compatible options:

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

Important: HOTPin user names should match the AD authentication property to facilitate SSO functionality.

Once an AD authentication property is designated to use as the HOTPin account name, that same property must be used for all HOTPin accounts. To facilitate account management, AD can be used with the following features:

- AD users can create their own accounts through the HOTPin User Website.
- The AD Synchronization feature creates HOTPin accounts automatically from designated AD OU's or groups. The user import feature can add accounts from AD.