Security, Simplified.

# HOTPin Integration Guide: Salesforce SSO 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 Salesforce® configured for single sign-on (SSO) to a local AD FS 2.0 service.

Salesforce is a cloud-based CRM service that can be configured to use a local Active Directory Federation Service (AD FS) to enable local users to sign on with AD credentials to gain access to Salesforce services.

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, Salesforce trusts 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.

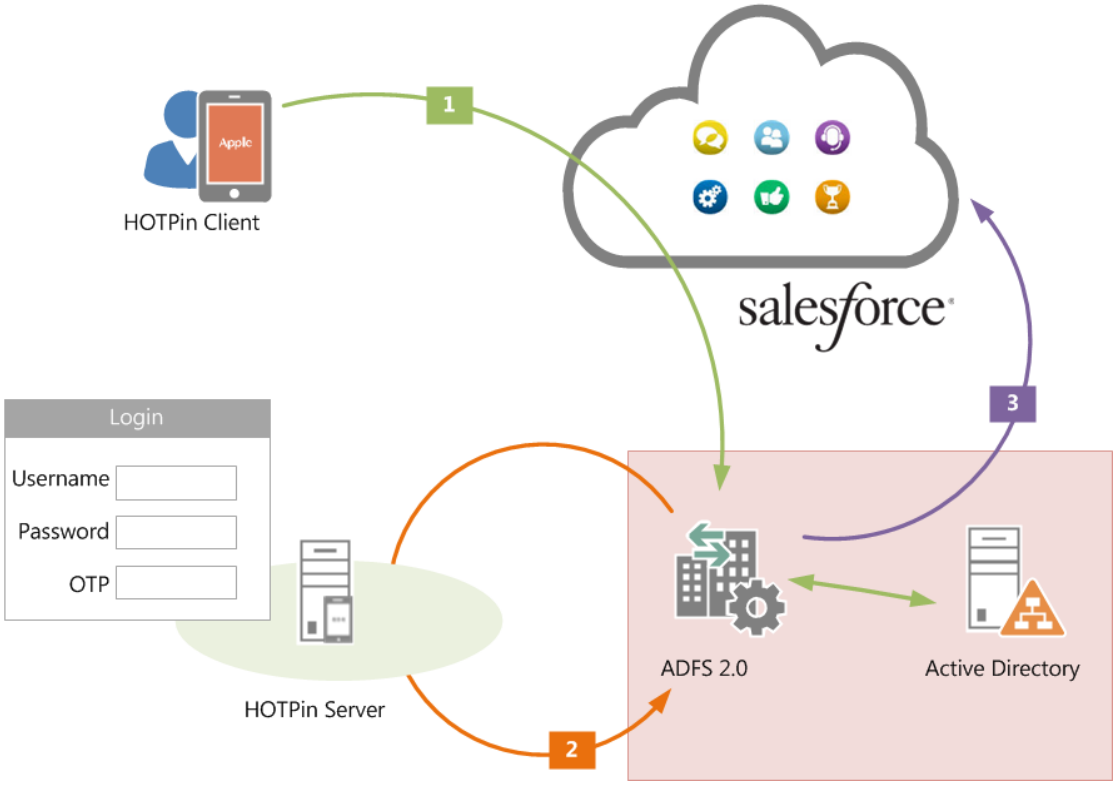



**Illustration 1**

# 1.2 Summary

This integration guide covers the set up for a basic installation in which HOTPin provides 2FA for Salesforce 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 excerpted from the article “Single Sign-On with Force.com and Microsoft Active Directory Federation Services” on the Developer Force website; it is revised for your convenience to aid in setting up HOTPin 2FA. You can access the full, original article at:

http://wiki.developerforce.com/page/Single_Sign-On_with_Force.com_and_Microsoft_Active_Directory_Federation_Services

# 1.3 Prerequisites

The integration covered in this document requires the following components:

- Salesforce

  Enterprise 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:

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

# 2 Salesforce SSO Configuration

To configure Salesforce SSO, you will first need to access your AD FS server to get a signing certificate and the entityID. Then you will log in to Salesforce to configure SSO settings. Once those settings are complete, you will download them as an XML file to use for ADFS configuration.

## 2.1 Get the AD FS Signing Certificate and entityID

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 Salesforce:

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).

Complete the following steps to acquire the AD FS entityID.

1. Select the “Endpoints” node under “Service”.
2. Navigate to “Metadata”.
3. Type “Federation Metadata”.
4. Copy the entityID attribute value and save it to a location from which you can retrieve it later during Saleforce configuration.
   Example: http://adfs.(yourdomain).com/adfs/services/trust

Next, you are ready to set up Salesforce.

## 2.2 Configure Salesforce SSO Settings

Complete the following for SSO configuration with AD FS.

1. Log into your Salesforce.com account.
2. Click “Setup”.
3. Navigate to: Administration Setup|Security Controls|Single Sign-On Settings.
4. Click “Edit” to open the Single Single-On screen. Complete the following:
   - SAML Enabled – Click the checkbox.
   - Click “Save”.
5. Under SAML Single Sign-On Settings, click “New”. Complete the following:
   **Note:** Items below reflect the settings you need to configure. Items not listed can use the default settings.
   - Name – Enter a name to distinguish the SAML instance.
   - SAML Version – 2.0 (listed for reference, you cannot change the version)
   - Issuer – Paste the AD FS entityID that you copied from the AD FS 2.0 Console here.
     Example: http://adfs.(yourdomain).com/adfs/services/trust
   - Identity Provider Certificate – Upload the identity provider certificate you downloaded from the ADFS server.
     **Note:** The signing certificate must have been exported in DER format (.cer).
   - SAML Identity Type – Select “Assertion contains the Federation ID from the User object”.
   - SAML Identity Location – Select “User ID is in the NameIdentifier element of the Subject statement”.
   - Identity Provider Login URL – Use the example below, but replace (yourdomain) with the domain name you are using for SSO.
     Example:
     https://adfs.(yourdomain).com/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=https://saml.salseforce.com
   - Identity Provider Logout URL – Use the example below, but replace (yourdomain) with the domain name you are using for SSO.

https://adfs.(yourdomain).com/adfs/ls/?wa=wsignout1.0

6. Click “Save”.

Now you must download the SSO settings configured above to use in AD FS setup.

## 2.3 Download SAML SSO Settings

The Single Sign-On Settings screen should still be open in your browser. Complete the following:

1. Click the name of the SAML instance you just created.
2. Click the “Download Metadata” button.
3. Save the file to a location you can access when configuring AD FS; you will need to upload it then.

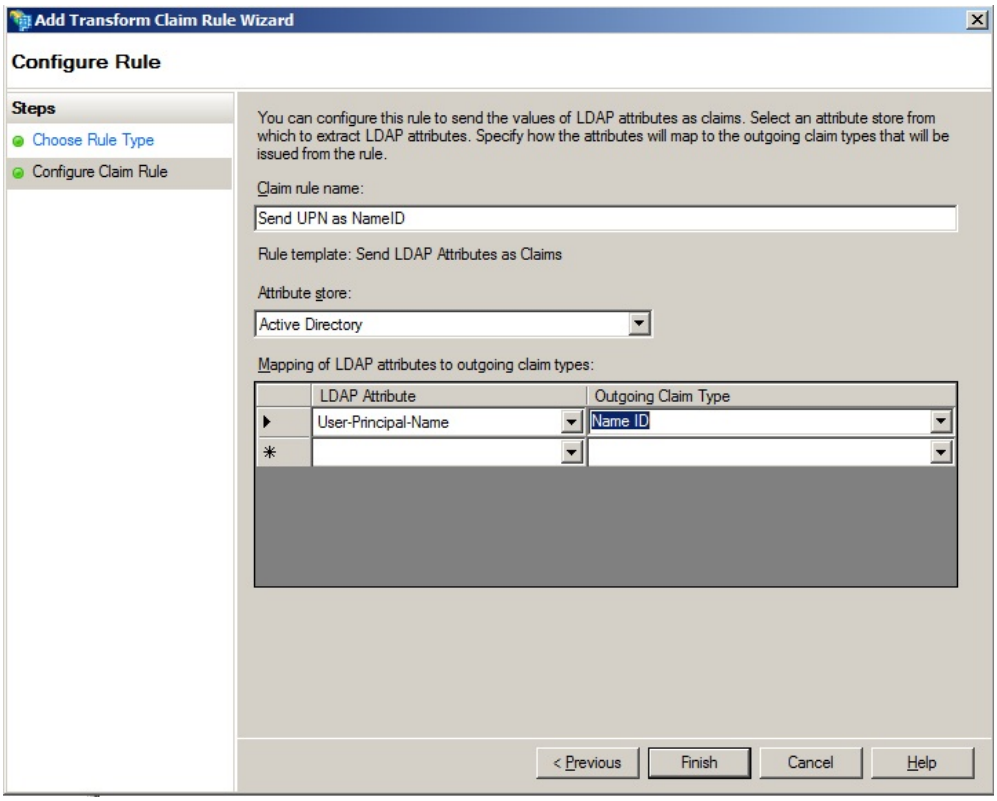
This completes the basic setup for Salesforce SSO. See Optional Configuration for additional feature information that may be relevant for your deployment.

Next you will need to configure AD FS for Salesforce 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. Use the wizard to complete the following:
   - Select Data Source – Import relying party data; navigate to the XML you downloaded from Salesforce.
   - Display Name – Give the trust relationship a display name, like ‘Salesforce Test’.
   - Choose Issuance Authorization Rules – Permit all users to access this relying party.
4. The claim rule wizard opens automatically when a trust relationship has been created. Complete the following:
   - Edit Claim Rules Dialog – Select the checkbox.
   - Select the “Issuance Transform Rules” tab.
   - Claim Rule Template – Select “Send LDAP Attributes as Claims”.
   - Select “Configure Claim Rule”. The screen shot provides a reference for the steps to follow.




5. Configure Rule – There are many options that may work for your organization; this example shows one method. Complete the following:
   - Claim Rule Name – Use the User Principal Name (UPN) as NameID and call the rule: “Send UPN as NameID”.
   - LDAP Attribute – User Principal Name
   - Outgoing Claim Type – Name ID

Now that you have configured Salesforce 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:

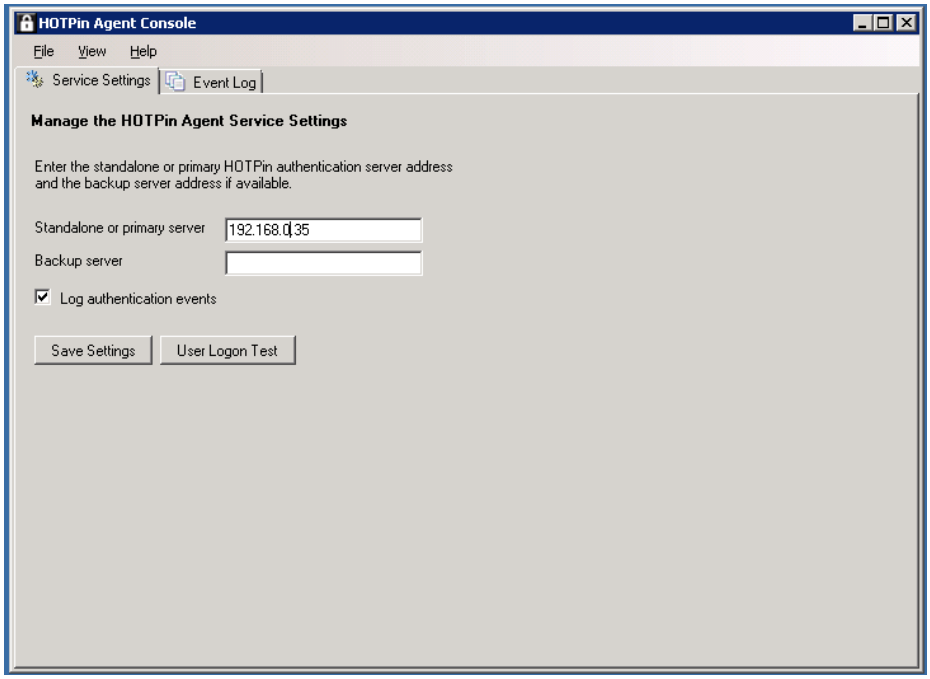
HOTPin installation guides: http://www.celestix.com/products-services/#select_1-7

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

## 4.1 Configure HOTPin Agent

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 Configure HOTPin ADFS Client

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 Salesforce 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.

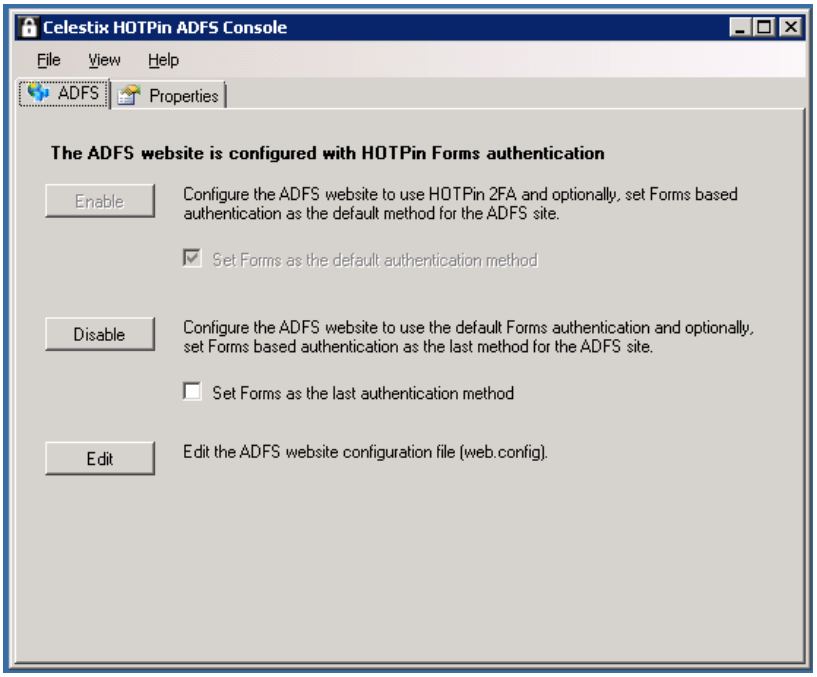



**Illustration 2**

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.

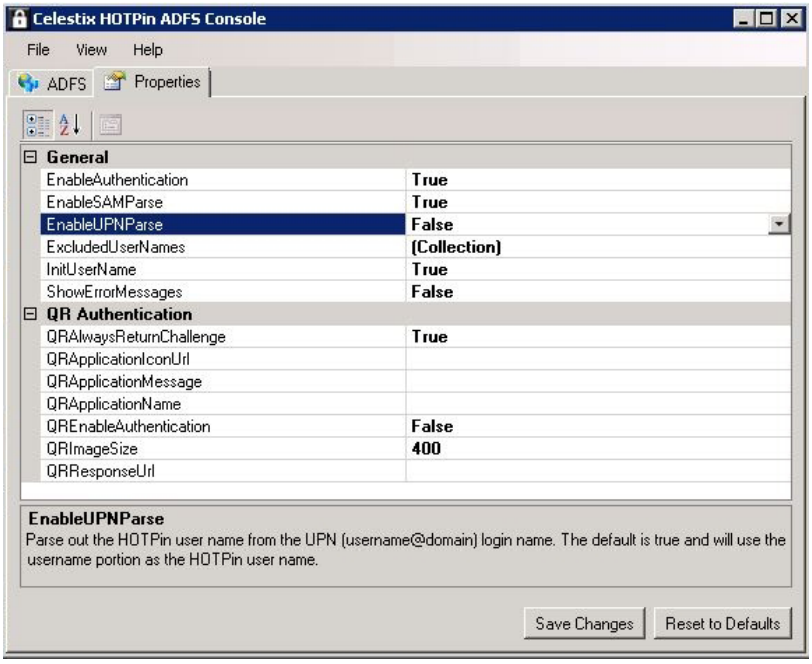



**Illustration 3**

## 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 Salesforce SSO.
- EnableUPNParse – Set to “False”; UPNs should not be used for Salesforce SSO.
- ExcludedUserNames – Create a list of users to exclude from HOTPin 2FA when they log in to Salesforce.
- InitUserName – This feature is unavailable for use with Salesforce.
- 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 Optional Configuration and Notes.

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

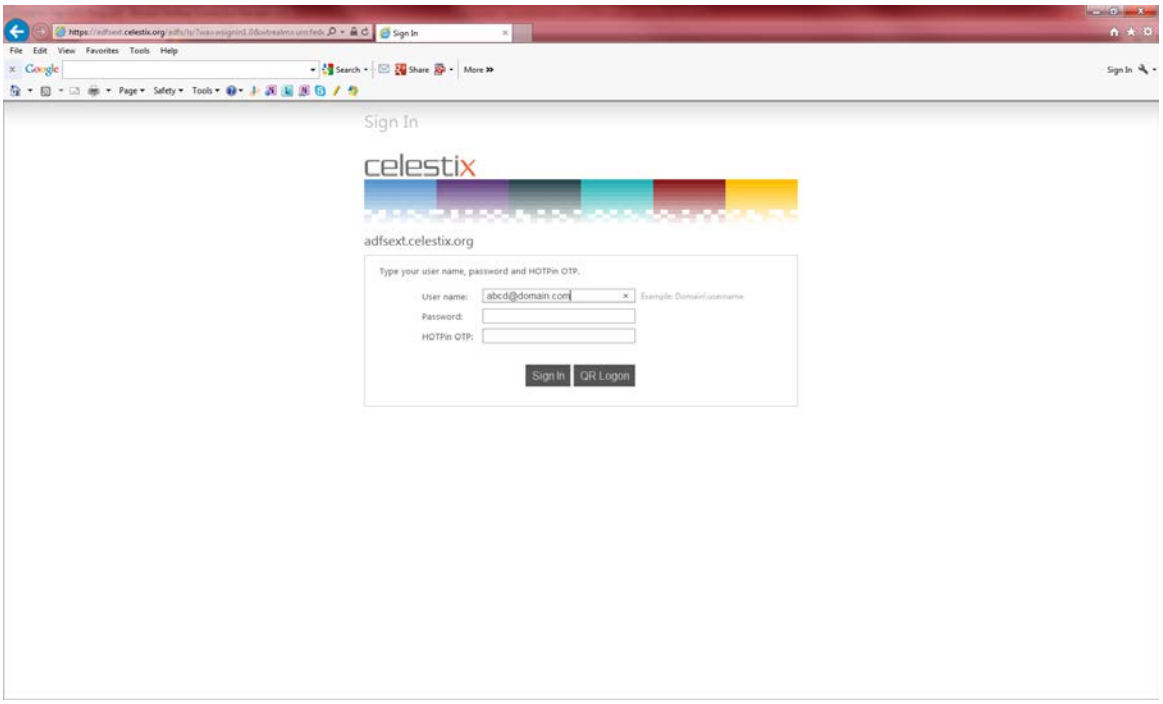



**Illustration 4**

### 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 Salesforce 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 Optional Configuration and Notes

The following information is included for your easy reference, but configuration is outside the scope of this document. Links are included to help you find additional information.

## 5.1 Service Provider Initiated Login and My Domain

In the federated login relationship between Salesforce and AD FS, Salesforce is the service provider (SP) and AD FS is the identity provider (IdP). With IdP-initiated login, you typically set up a link on the company intranet that users click to get access to Salesforce.com. However, SP-initiated login happens when a user clicks a direct link to Salesforce.com.

The Salesforce "My Domain" feature facilitates SP-initiated login. If you configure a My Domain entity ID in the Salesforce.com SAML settings, for example, https://testinfo-developer-edition.my.salesforce.com, users can go to URLs in that domain and will be automatically redirected to AD FS for authentication.

Notes for SP and IdP login:

- SP-initiated login requires that the AD FS Secure Hash Algorithm parameter be set to SHA-1; Force.com uses the SHA-1 algorithm when signing SAML requests, but AD FS defaults to SHA-256. Access the parameter in the AD FS trust properties for the Force.com relying party under "Advanced".
- IdP-initiated login requires that you use the AD FS login URL and specify the loginToRp parameter with the Force.com SAML entity ID as the "Identity Provider Login URL" setting (Setup|Administration Setup|Security Controls|Single Sign-On Settings |(Edit)|SAML Single Sign-On Setting| Identity Provider Login URL).
  Example:
  https://adfs.domain.com/adfs/ls/idpinitiatedsignon.aspx?loginToRp=https://saml.salesforce.com

**Note:** If users log in on the intranet, you could use an internal DNS instead of external DNS.

For more information, see the source article:

http://wiki.developerforce.com/page/Single_Sign-On_with_Force.com_and_Microsoft_Active_Directory_Federation_Services

Search for the Section “My Domain”.

To access My Domain configuration in Salesforce, navigate to Setup|Administration Setup|Domain Management|My Domain.

## 5.2 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 Salesforce, 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.