SalesForce SSO with Active Directory Federated Services (ADFS) v2.0

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Tony Davis	tdavis@securenvoy.com	

SalesForce SSO with Active Directory Federated Services (ADFS) v2.0

This document describes how to integrate SalesForce configured for SSO to a local ADFS 2.0 service with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

SalesForce is a customer relationship management tool (CRM) that can be configured to use a local Active Directory Federation Service (ADFS) to enable local users to sign on with their existing AD credentials.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as SalesForce), without the complication of deploying hardware tokens or smartcards.
Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilizing the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seamless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilizes a web GUI for configuration. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

SalesForce

SalesForce Cloud Account

Microsoft

Microsoft Server 2008 R2 with ADFS 2.0 Installed

SecurEnvoy

Microsoft Server (any version)
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v7.2.504

© 2014 SecurEnvoy Ltd. All rights reserved

Index

1.0 Prerequisites 3
1.1 Configure ADFS and SalesForce 6
1.2 Testing ADFS and SalesForce 7
2.0 Configure IIS Agent for Default Website 6
2.1 Configure IIS Agent for ADFS 7
2.2 Configure logout URL 8
2.3 Configure Basic Authentication 8
3.0 Test the Two Factor Authentication 9
3.1 Successful Logon with 2FA 10
4.0 Notes 11

1.0 Prerequisites

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and the ADFS server(s), additional open ports will be required.

IIS Agent has been installed as per the SecurEnvoy IIS Agent Installation and Admin Guide: https://www.securenvoy.com/integrationguides/iis%20agent%20installation%20guide.pdf

The following table shows what token types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✓

© 2014 SecurEnvoy Ltd. All rights reserved

1.1 Configure ADFS and SalesForce

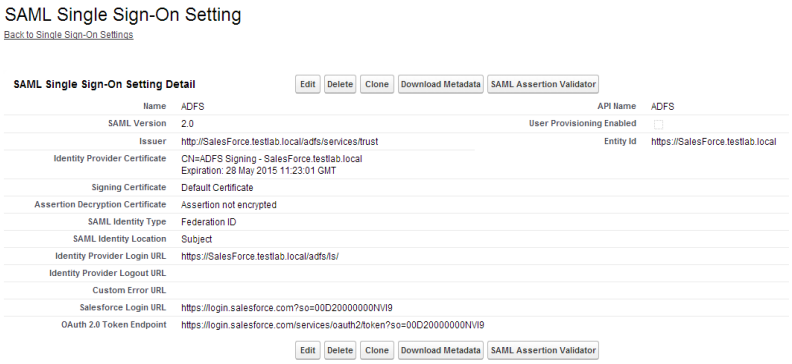
Install and configure ADFS using the following guide:

http://technet.microsoft.com/en-us/library/dd807092(v=ws.10).aspx

Go to SalesForce and navigate to the following:
Setup>Security Controls>Single Sign-On Settings

Provide the following:

Name
Issuer
Identity Provider Certificate
SAML Identiy Type
SAML Identity Location
Identity Provider Login URL
API Name
Entity Id



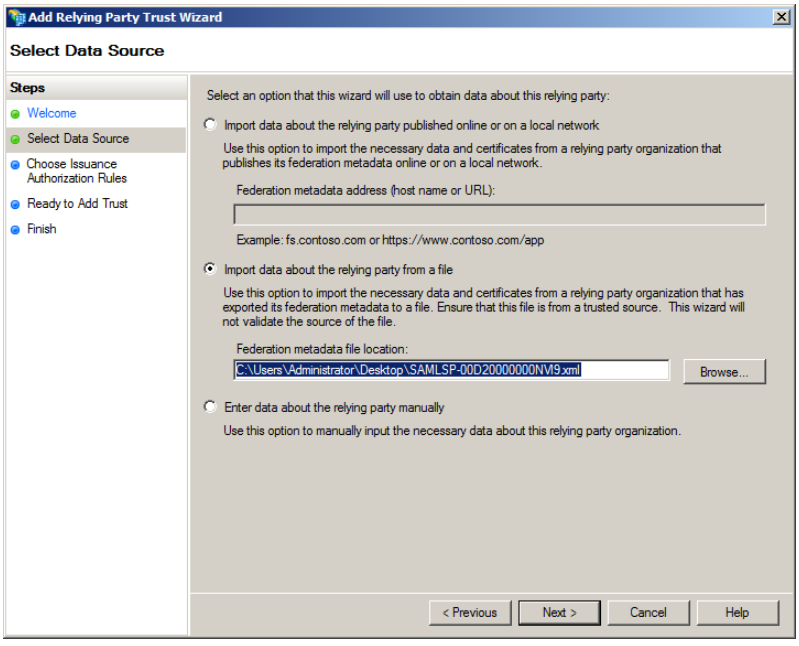
Save the settings and download the Metadata xml file

Open AD FS 2.0 Management and add a new "Relying Party Trust":

Select Data Source and select "Import data about the relying party from file"

Browse and select the Metadata xml file we exported from SalesForce previously.

Work through the wizard, entering "Display Name" and "Permit all users to access this relying party.



Note

Ensure you have "Open Edit Claims Rules Dialog" ticked within the final dialog

© 2014 SecurEnvoy Ltd. All rights reserved

Within the "Edit Claim Rules Dialog select "Add Rule" Enter the following:

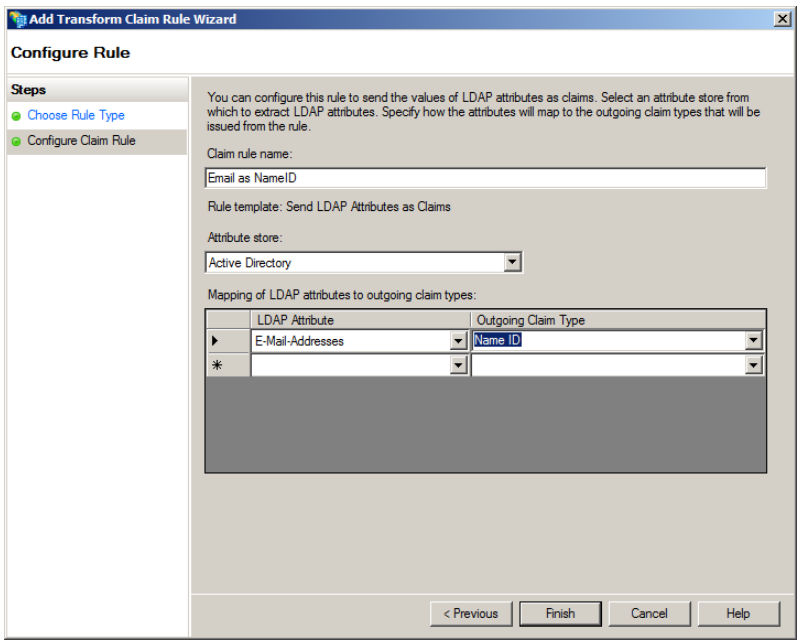
"Claim rule name"
Email as NameID

"Attribute store"
Active Directory

"LDAP Attribute"
E-Mail-Addresses

"Outgoing Claim Type"
Name ID

Click "Finish"

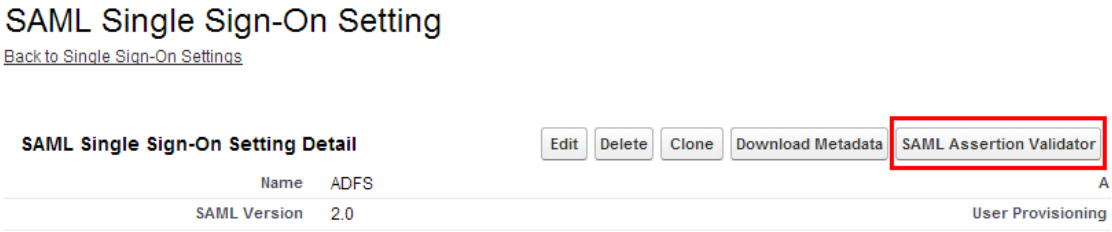


1.2 Testing ADFS and SalesForce

Point your browser to your ADFS ldp-initiated logon URL and specify the loginToRp parameter as the Salesforce SAML entity ID:

E.g.https://salesforce.testlab.local/adfs/ls/idpinitiatedsignon.aspx?loginToRp=https://salesforce.testlab.local

This should redirect you and sign you into SalesForce. If you get a SalesForce login error, use the SAML assertion validator tool on the SalesForce single sign-on configuration page. It will display the results of the last failed SAML login.



Note

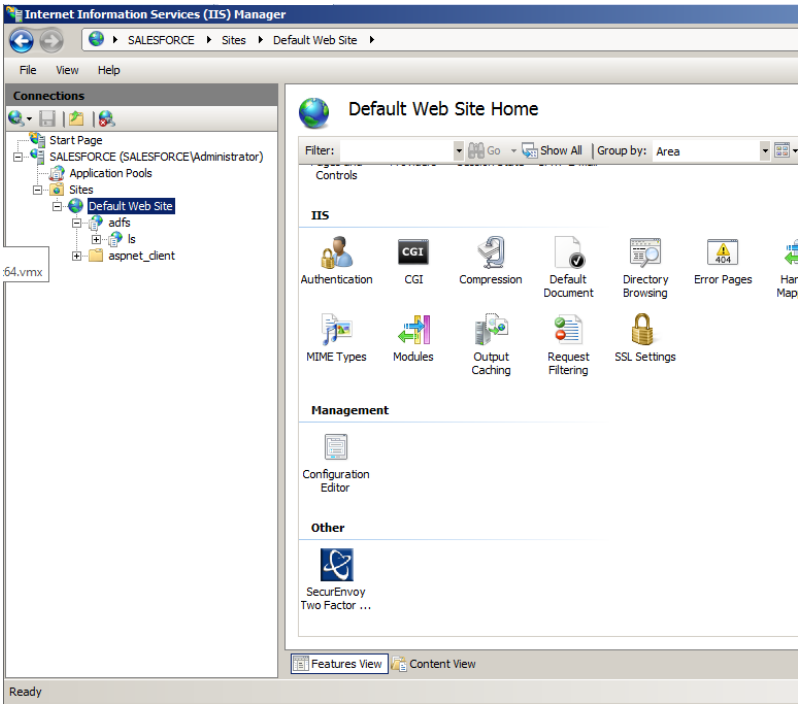
If you get an error from ADFS, check the ADFS logs:
Server Manager\Diagnostics\Applications and Services Logs\ADFS 2.0\Admin.

© 2014 SecurEnvoy Ltd. All rights reserved

2.0 Configure IIS Agent for Default Website

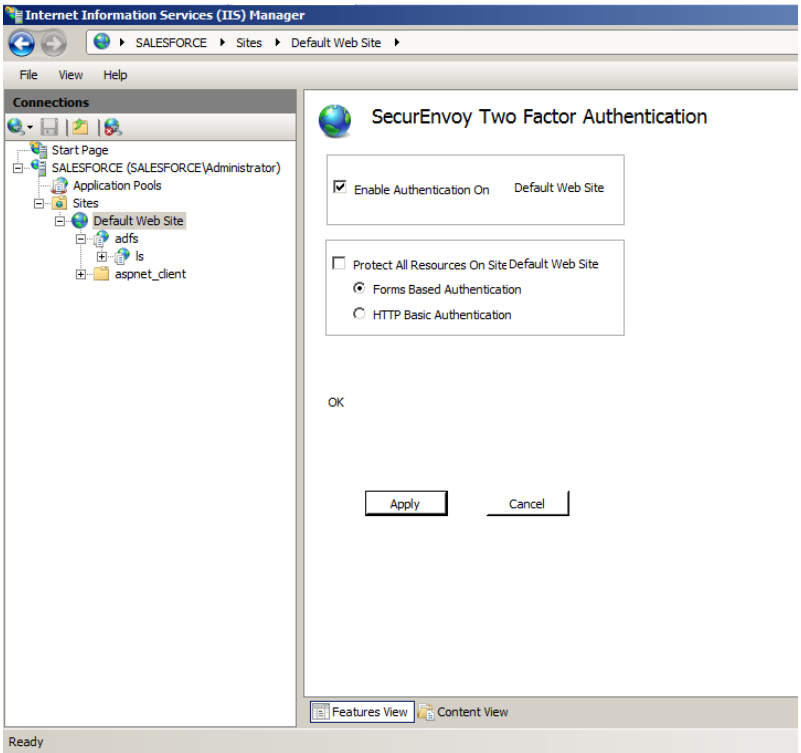
Launch the IIS management interface, either from "Start", "Administration Tools" or from the Server Manager

Expand the sites list on the navigation pane and select "Default Web Site", then scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.



Enable the tick box to "Enable Authentication On Site Default Web Site"

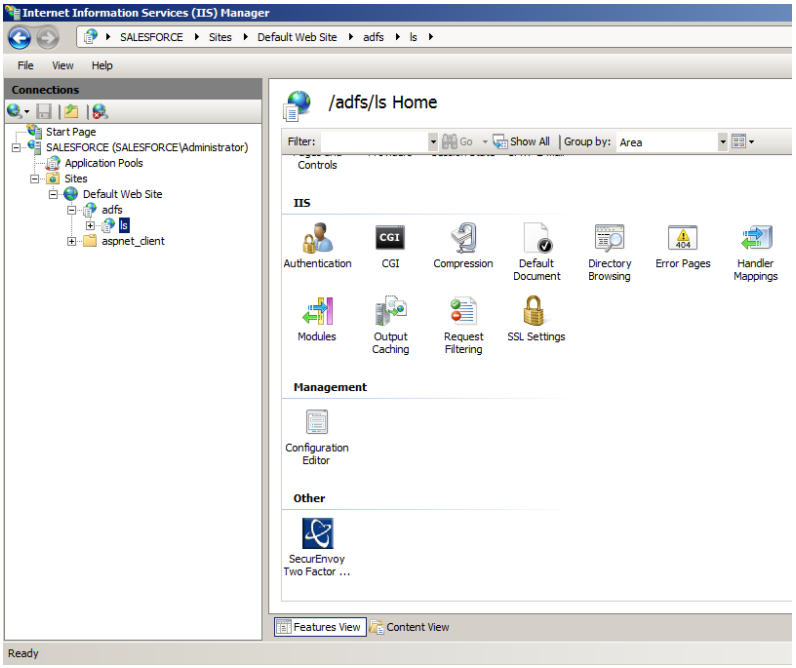
Click "Apply" when complete.



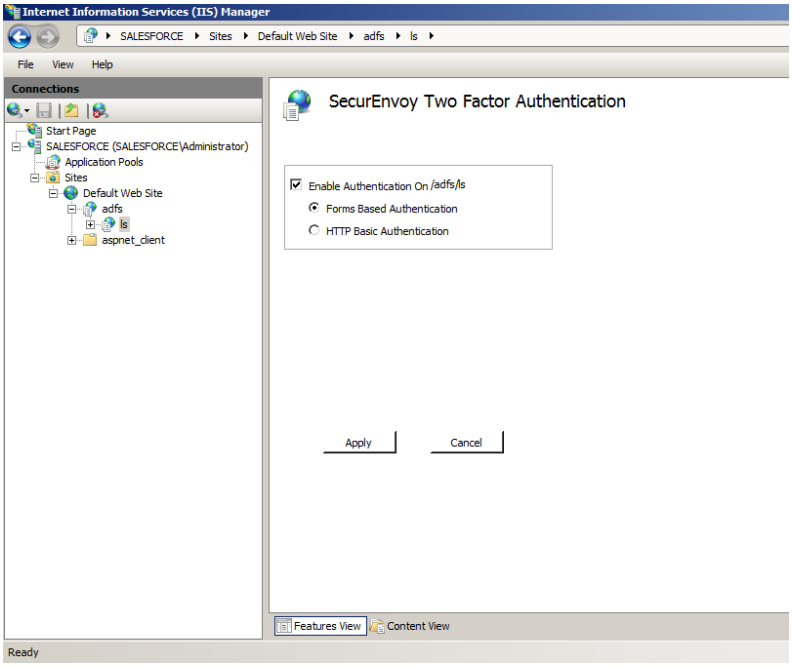
© 2014 SecurEnvoy Ltd. All rights reserved

2.1 Configure IIS Agent for ADFS

Under Default Web Site, expand adfs and select ls, scroll down the centre panel and select "SecurEnvoy Two Factor"



Select the check box "Enable Authentication On /adfs/ls"
Select "Form Based Authentication" (The Default)
Click "Apply" to finish
Cancel restart IIS when prompted.



Note

The virtual directory SecurEnvoyAuth MUST be a member of the ADFSAppPool

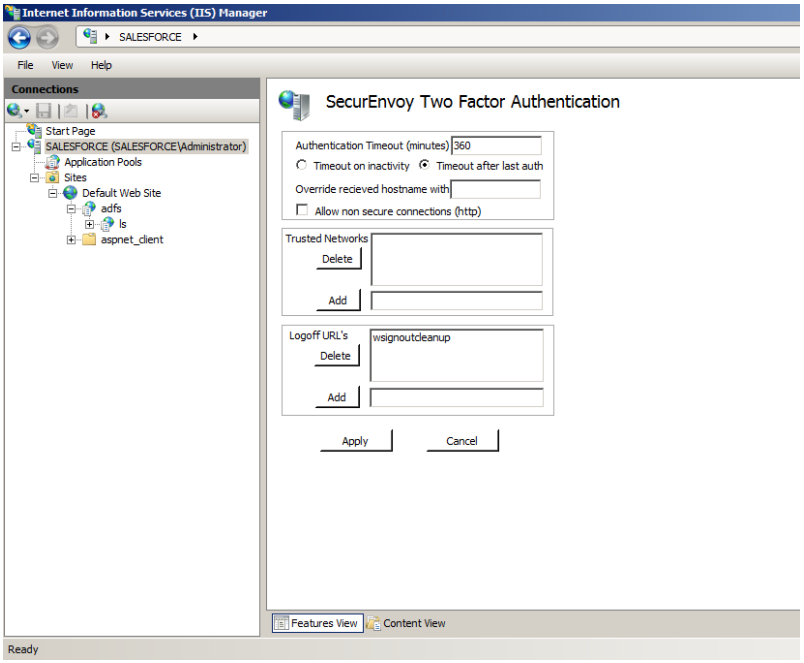
© 2014 SecurEnvoy Ltd. All rights reserved

2.2 Configure logout URL

In the Navigation pane, select top level host name (the 2nd line down).
Scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.
Setup your required inactivity timeout.

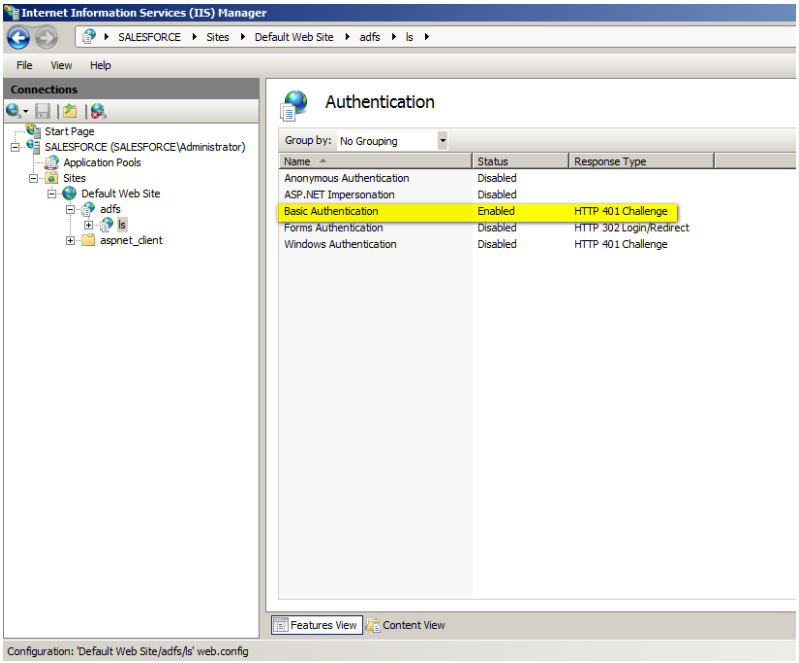
Add the logout URL **wsignoutcleanup**

Restart IIS when prompted.



2.3 Configure Basic Authentication

Navigate back to Default Web Site > adfs > ls and select the Authentication icon
Make sure that **only** Basic Authentication is Enabled



© 2014 SecurEnvoy Ltd. All rights reserved

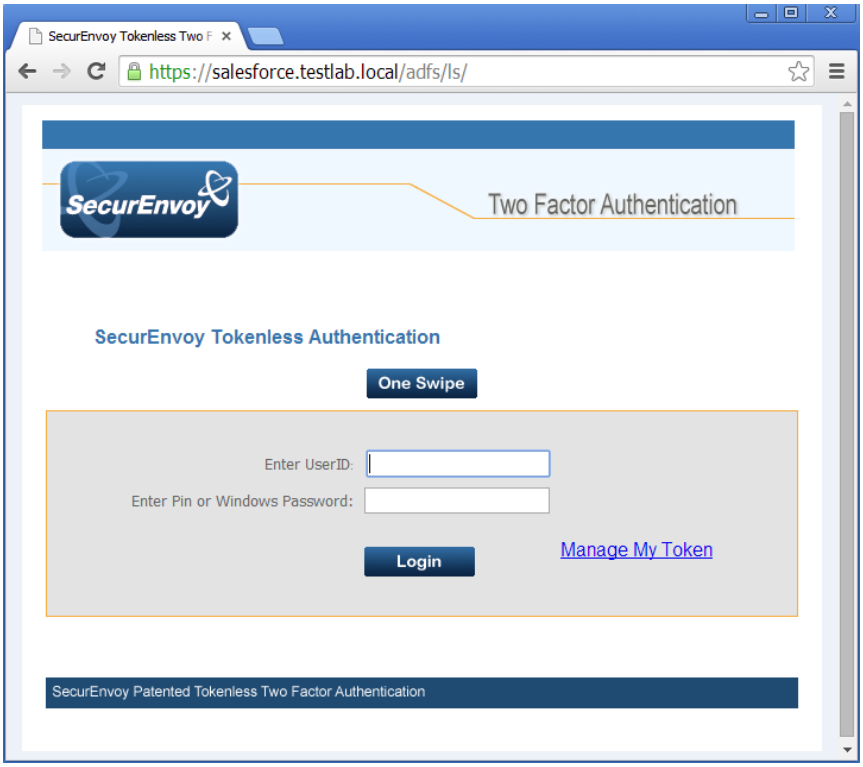
3.0 Test the Two Factor Authentication

Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

https://your_server_name/adfs/ls (Don't forget the https)

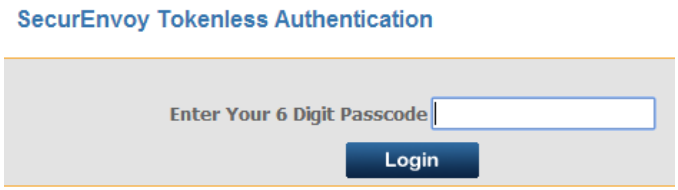
User logon screen is shown.

Enter your UsedID and Password:

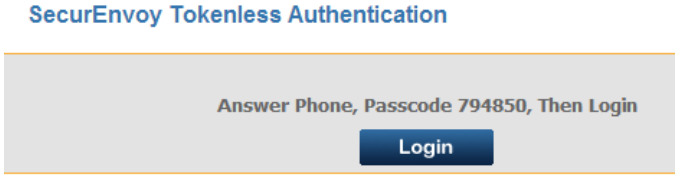


User is then presented with their two factor authentication type:

- Pre load, Realtime and Soft tokens:



- VOICE tokens:



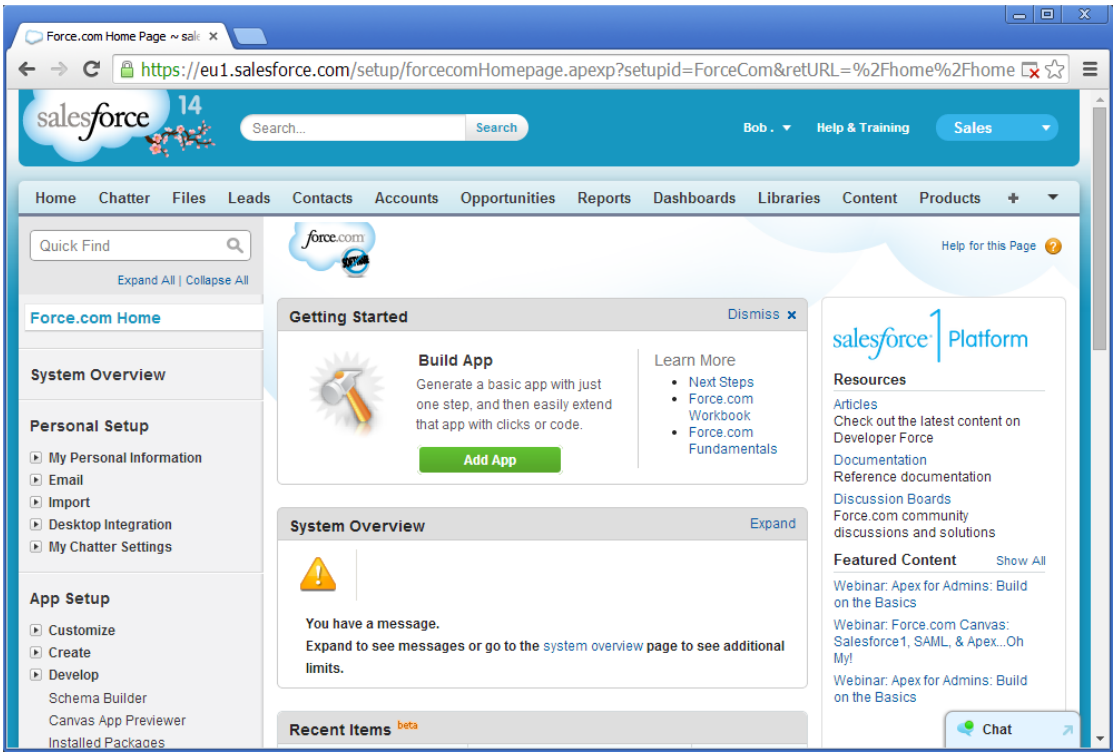
- One Swipe:



© 2014 SecurEnvoy Ltd. All rights reserved

3.1 Successful Logon with 2FA

User authenticates successfully and is presented with SalesForce:



Note

Configure your domain name within seiis.ini (C:\Windows):

# Default Domain Name to use if no domain information is included in this UserID (leave blank if not required)
DefaultDomain="yourdomain"

This will allow your users to logon to SalesForce without specifying the domain name:
domain\UserID

© 2014 SecurEnvoy Ltd. All rights reserved

4.0 Notes

© 2014 SecurEnvoy Ltd. All rights reserved