Introduction
SalesDesktop developed by InvisibleCRM is leading software for integration of Microsoft Outlook and Salesforce.com. SalesDesktop provides access to sales data and relationships directly in Outlook, highly configurable features, rich user experience, and usability.

SalesDesktop relies on SOAP Web Services APIs for communicating with Salesforce.com that allows using Partner Web Services WSDL to support various customizations out of the box.

Support of Single Sign-On (SSO) becomes more important as many organizations deploy various SSO solutions for their enterprises focusing on better manageability, higher security, and usability. There is a strong demand from SalesDesktop customers to see a solid, reliable, and intuitive SSO support in SalesDesktop product.

Addressing this demand, InvisibleCRM provides SSO Support for SalesDesktop designed to enable the same abilities for Outlook users as during working with web applications that provide support of a wide range of SSO implementations available on the market without additional tuning.

Salesforce.com SSO Support
Salesforce.com provides several custom and standards-based scenarios to implement Single Sign-On, including custom Delegated SSO and standards-compliant Federated SSO based on SAML 1.1/2.0, OAUTH, etc.

Delegated Single Sign-On
Delegated SSO support is a legacy technology, please refer to Salesforce.com web site for more information. Delegated authentication does not affect the way of SOAP Web Service clients operation, so SalesDesktop natively supports delegated authentication configurations.

Federated Single Sign-On
Federated Single Sign-On represents secure, reliable, and standards-based approach for enabling Single Sign-On support in the enterprises. Please refer to the Salesforce.com web site for more information about SSO support.

Federated SSO is based on a model where separate entity (known as Identity Provider) establishes user identity and passes that information in form of a SAML assertion to another party in a trusted relationship (Salesforce.com, acting as a Service Provider). Salesforce.com supports SAML 1.1 and SAML 2.0 to define mechanism and requirements for such conversation.
While requirements for Identity Provider and Service Provider are quite complex and highly vendor-specific, the requirements for the Client are simple. In order to participate in federated authentication scenarios and to support OAuth flows, the client must support basic actions available in web browsers: ability to handle POST and GET requests, follow redirects, support JavaScript to define custom logic on the page, show web pages to user to enter necessary information for authentication and authorization.

The above-mentioned requirement allows to enable SSO support for web-based applications.

Supporting the same scenarios in the desktop application is typically more challengeable due to the following reasons:

1. During an authentication process, application must act as web browser, provides the user with the similar experience as during logging into web-based SSO-protected apps.
2. In order to provide more secure and manageable access to Salesforce.com accounts, several SSO scenarios rely on OAuth flows which define logic for retrieving AccessToken after successful login or using RefreshToken to require user log in only once and enable re-establishing AccessToken from RefreshToken on demand.

SalesDesktop SSO Support

Support of SalesDesktop SSO fits for the SSO infrastructure provided by Salesforce.com. This includes:

- Web-based user interface that allows user to complete sign-on operation from Microsoft Outlook.
- Various logon user interface for web-based Identity Providers is supported by delegating login flow to the web windows (Identity Provider logon UI must support Microsoft Internet Explorer 7 or higher).
- Support of SAML configuration and version used by Salesforce.com (1.1 or 2.0 versions are supported with POST profile).
- Support of two login modes: initiated by Service Provider and initiated by Identity Provider.
- Equal support of API sessions established via SSO and normal sessions with login/password specified.
- Support of multiple OAUTH flows and SAML assertion flow.

Users can select required authentication mode in the SalesDesktop - Login dialog box either during initial installation or later. Supported authentication modes are listed below:

- Direct
  - User should specify login and password in the Login dialog.
  - Non-SSO configurations and Delegated SSO work in this mode.
- SAML
  - SAML Assertion flow is used to authenticate a user.
  - Identity provider URL should be specified.
  - Authentication information is entered in a separate web window.
- OAuth2
  - OAuth 2.0 flows are used to authenticate a user (for more information refer to the following topics in Salesforce help: “OAuth 2.0 user-agent” and “OAuth 2.0 refresh token flow”).
  - Login URL and OAuth Consumer Key must be specified in the Login dialog box.
  - Authentication information is entered in a separate web window.
In the **SalesDesktop – Login** dialog box user can select one of the supported authentication modes. These options are illustrated on images below:

During authentication, SalesDesktop can require user to allow an access to user’s details. These details are needed in order to allow a user authentication for the Identity Provider and to perform all necessary steps at the Service Provider. The image is shown below:
Description of authentication modes available in the SalesDesktop - Login dialog box are given below:

1. **Direct** mode:
   - If user decides to save the password in the Login dialog, the Login dialog will not appear again, unless the user’s password expired or changed.
   - If user decides NOT to save the password in the Login dialog box, user will be asked to enter the password each time after Outlook restart and when the network operation is initiated (data synchronization, opening of the Synchronization Control Panel, etc.).

2. **SAML** mode:
   - Users are required to authenticate when the network operation is initiated and it’s either first time after Outlook restart, or previous session (AccessToken) received recently expires.
   - The Salesforce.com logic for determining lifetime of session is described here, see Timeout value field for more details.

3. **OAuth 2.0** mode:
   - When in OAuth 2.0, the refresh token flow is fully supported – that is, when user is successfully authenticated, SalesDesktop requests Refresh Token from Salesforce.com. Once user grants access token allocation to application, RefreshToken is stored in encrypted form to registry and then reused every time when new session (AccessToken) is necessary
   - User will be asked to re-authenticate whenever Refresh token expires or becomes corrupted.
   - The Salesforce.com logic for determining lifetime of session is described here, see Timeout value field for more details.

**Enabling SalesDesktop SSO support**

In order to enable SalesDesktop SSO support for your Salesforce.com account, make sure that:

1. Federated SSO is enabled and working, and users can log into Salesforce.com with SSO from web browser:
   a. SAML Assertion flow, for more details refer to the “SAML Assertion Flow” topic in the Salesforce help.
   b. OAuth 2.0 flows, for more details refer to the “OAuth 2.0 Refresh Token Flow” and “OAuth 2.0 User-Agent Flow” topics in Salesforce help.

2. Make sure your Salesforce.com users have access to SOAP WS API.

3. Make sure **My Domain** feature is enabled for your Salsforce.com account (Setup -> Company Profile -> My Domain).

4. For OAuth 2.0 only:
   a. In Salesforce, open Setup -> App Setup -> Create -> Apps, and click New button in the Connected Apps section on the Apps page. to create a record for OAuth authorization for SalesDesktop (for more details refer to the “Connected Apps View” topic in Salesforce help).
   b. Add a new application.
   c. Specify an application name (users will see this name when granting access to SalesDesktop).
   d. Specify contact details (Email, Phone).
   e. Specify callback URL (must be set to “salesdesktop://oauthcallback”).
   f. Save your changes.
g. Copy the value of **Consumer Key** field and send it to SalesDesktop users.

For SalesDesktop, make sure following is done:

1. Users know the URL for “My Domain” and use it as Login URL in **Sales Desktop – Login** dialog box.
2. **For OAuth 2.0 only**: In the **Login** dialog box, users specify value of **Consumer Key** for SalesDesktop remote application.
3. When SalesDesktop runs on Sandbox accounts, make sure the following settings are configured in the Windows Registry:
   a. **HKEY_CURRENT_USER\Software\InvisibleCRM\SalesDesktop3\OAuthTokenUrl** (string type) must be set to [https://test.salesforce.com/services/oauth2/token](https://test.salesforce.com/services/oauth2/token)
   b. **HKEY_CURRENT_USER\Software\InvisibleCRM\SalesDesktop3\LoginServerUrl** (string type) must be set to [https://test.salesforce.com/services/Soap/u/16.0](https://test.salesforce.com/services/Soap/u/16.0)
4. When SalesDesktop runs on production accounts, make sure both above-mentioned keys are not available in the Windows Registry.