SYBASE®
An SAP® Company

New Features

Sybase Mobile Sales for SAP CRM 1.2.1

Document ID: DC01665-01-0121-01
Last revised: May 18, 2011

DOCUMENT ID: DC01665-01-0121-01
LAST REVISED: May 2011
Copyright © 2011 by Sybase, Inc. All rights reserved.
This publication pertains to Sybase software and to any subsequent release until otherwise indicated in new editions or technical notes. Information in this document is subject to change without notice. The software described herein is furnished under a license agreement, and it may be used or copied only in accordance with the terms of that agreement. To order additional documents, U.S. and Canadian customers should call Customer Fulfillment at (800) 685-8225, fax (617) 229-9845.
Customers in other countries with a U.S. license agreement may contact Customer Fulfillment via the above fax number. All other international customers should contact their Sybase subsidiary or local distributor. Upgrades are provided only at regularly scheduled software release dates. No part of this publication may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without the prior written permission of Sybase, Inc.
Sybase trademarks can be viewed at the Sybase trademarks page at http://www.sybase.com/detail?id=1011207. Sybase and the marks listed are trademarks of Sybase, Inc. A ® indicates registration in the United States of America. SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.
Unicode and the Unicode Logo are registered trademarks of Unicode, Inc.
All other company and product names used herein may be trademarks or registered trademarks of the respective companies with which they are associated. Use, duplication, or disclosure by the government is subject to the restrictions set forth in subparagraph (c)(1)(ii) of DFARS 52.227-7013 for the DOD and as set forth in FAR 52.227-19(a)-(d) for civilian agencies. Sybase, Inc., One Sybase Drive, Dublin, CA 94568

Contents

Introduction 1
Multiple Domain Support 2
Domains on SUP Server 2
How To Specify A Domain On A Mobile Client 2
BlackBerry 2
iPhone/iPad 3
Windows Mobile 5
Single Sign On 6
BlackBerry Single Sign On using X.509 Certificates 6
Windows Mobile Single Sign On using X.509 Certificates 8
iOS Single Sign On using X.509 Certificates 8
Sign On using SS02 Token 14

Introduction

This document details the new features available in the 1.2.1 release of Mobile Sales for SAP® CRM version 1.2.1. There are two key areas of new functionality these are

- The ability to support Multiple SUP Domains
- The ability to authenticate using Single Sign On

The new functionality in this release provides the ability for mobile clients to authenticate users using a single sign on (SSO) on methodology. Standard user name and password authentication also remains supported.

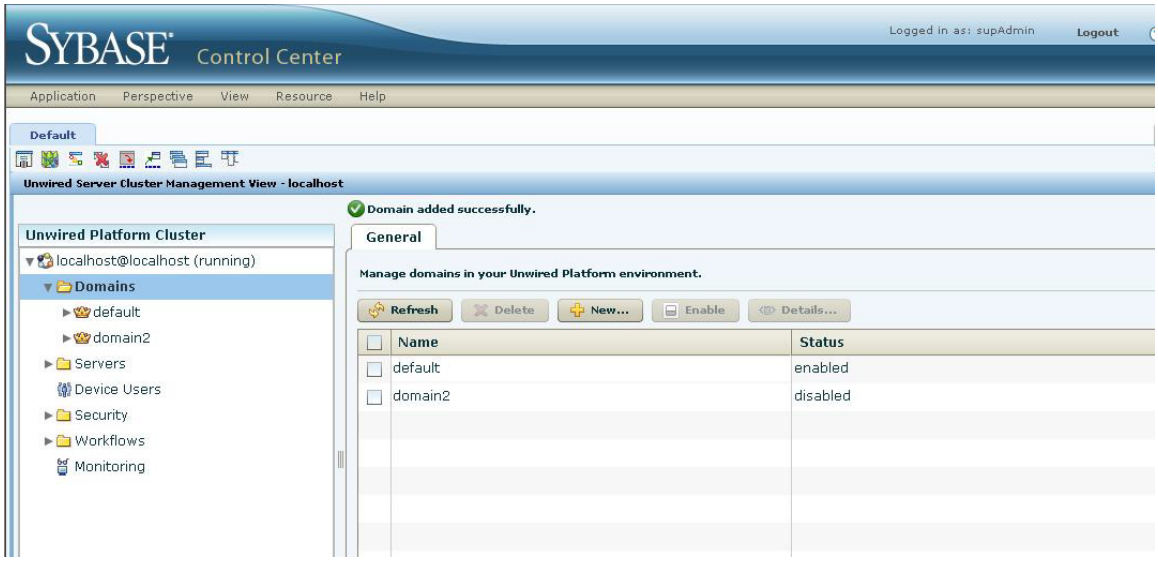
Multiple Domain Support

The Sybase® Unwired Platform (SUP) server supports multiple domains. In the previous Mobile Sales clients, it was only possible to support a single default domain. With multiple domain support on the Mobile Sales clients, the users have the ability to select a specific SUP domain. For more information about domains, please refer the document in the reference section below.

Domains on SUP Server

Domains enable the management of application metadata within a partition, including server connections, packages, role mappings, domain logs, and security, changes are visible to a specific domain.
In order to select an alternative SUP domain, the SUP server must be configured with a new domain name and associated properties, this can be done via the Sybase Control Center (SCC). Please refer to the SUP documentation located at the following URL:
http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.infocenter.dc01092.0155/doc/html/title.html

To access SCC, use the following URL https://<<<SUPSERVER>>:8283/scc/, where <<<SUPSERVER>> should be replaced with you SUP server address in order to access your SCC instance. The image below shows a screen shot of the domain configuration area of within the SCC. Two domains exist, one named “default” and the other “domain2”.



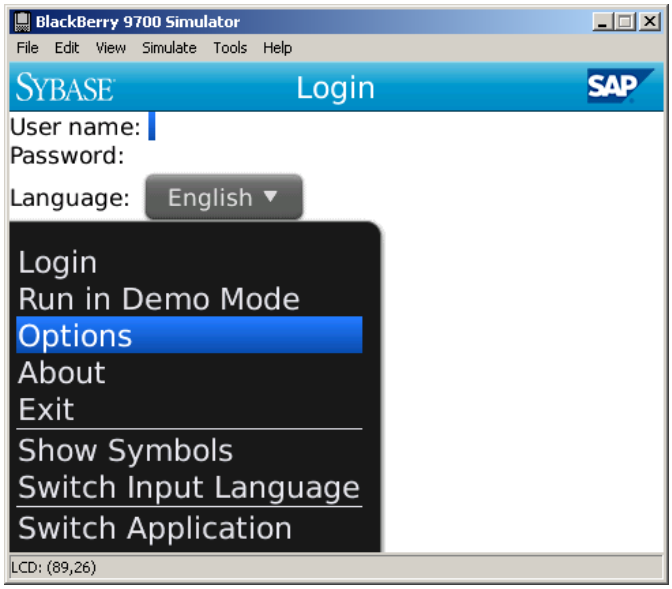
How To Specify A Domain On A Mobile Client

BlackBerry

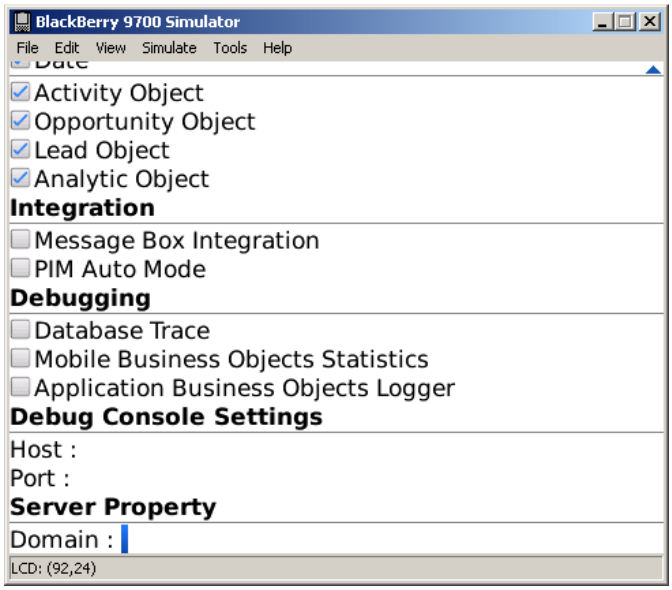
The domain configuration property on the BlackBerry CRM client may be changed by going to the options screen before logging in. The domain can only be set before the attempting to login. Once the device is successfully subscribed to the SAP backend, the domain cannot be changed without first un-subscribing.

The following screen shots show the steps required to select a specific domain.

From the login screen, go to the menu and select “Options”.



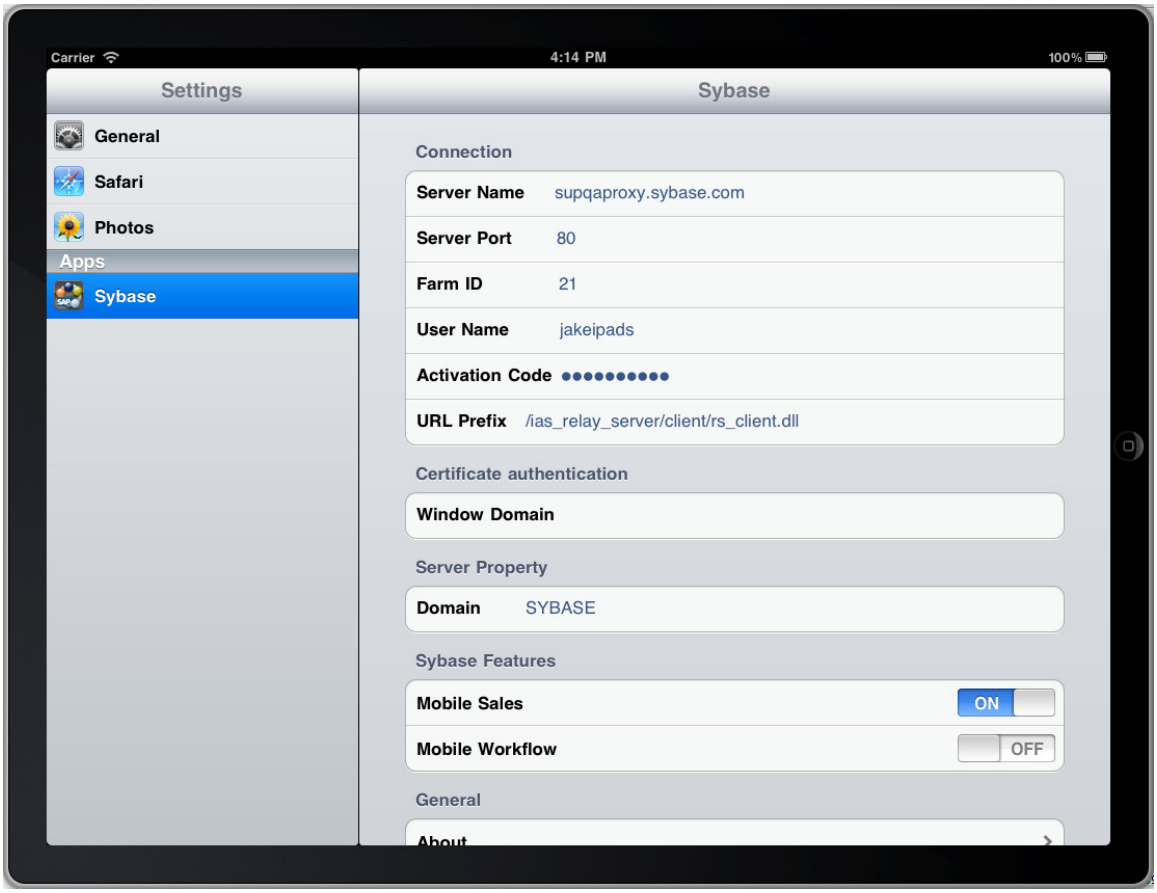
From the options screen, scroll all the way down to the page where the domain property may be viewed/modified. A domain value may be entered in the domain field and saved by selecting Save from the menu.



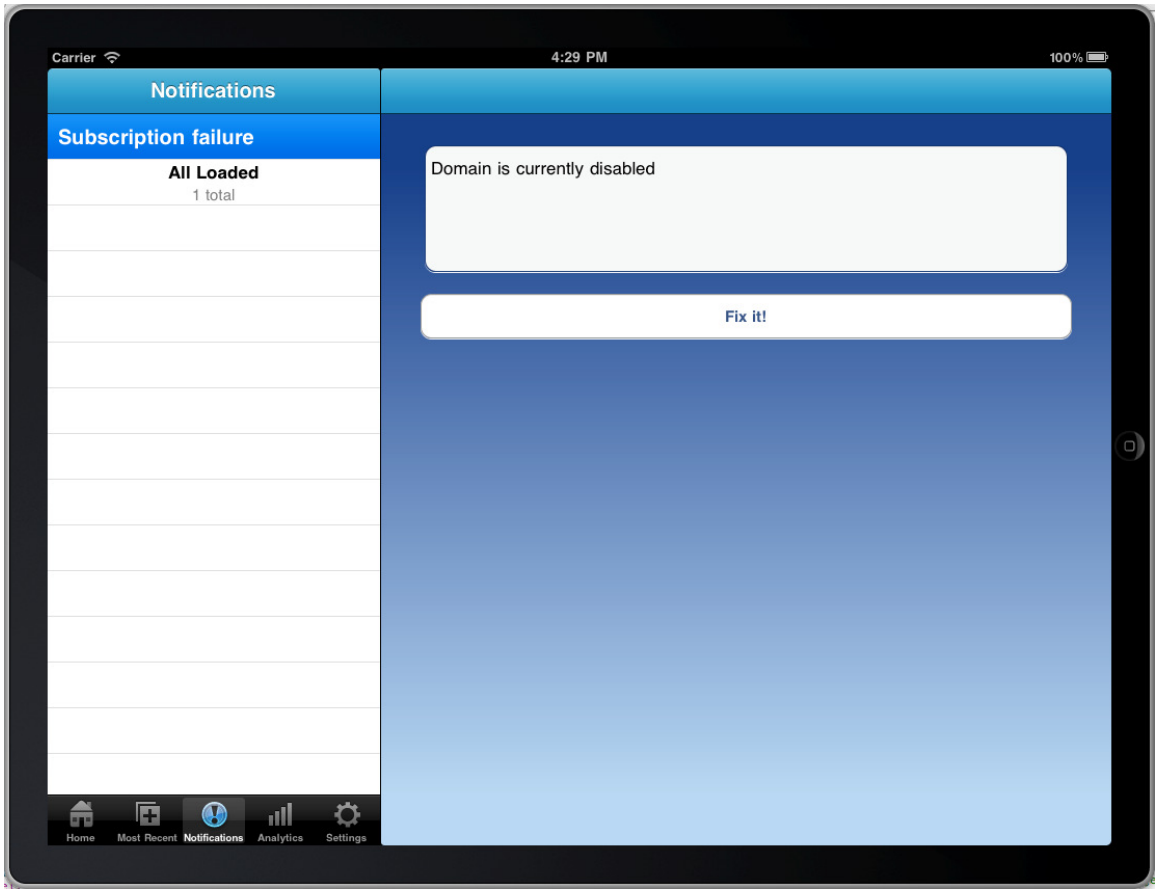
It should be noted the SUP Domain value cannot be validated on the device and is validated by the SUP server during subscription process. If the domain is entered incorrectly the SUP server will reject the subscription and show the following error message, “Subscription Failed”.

iPhone/iPad

The domain configuration property on the iOS Mobile Sales clients can be set by going to the settings screen before launching Mobile Sales application. Users can only set the domain before the login. Once the device is successfully subscribed to the SAP backend, the domain cannot be changed without first un-subscribing.



If the Domain property is set incorrectly or mismatched to the actually domain name configured on the SUP server, the iOS CRM client will receive the following error message, “Domain is currently disabled”. In order to correct the erroneous domain property, click the “Fix it” button and enter a valid Domain value.



Windows Mobile

The domain configuration on the Windows Mobile CRM client is set by a system parameter value in the SybaseCRM.Configuration_template.xml file. The Domain configuration parameter "SYS_ABO_Domain" appears in the SybaseCRM.Configuration_template.xml file as follows;

```
<SYS_ABO_Domain>default</SYS_ABO_Domain>
```

The predefined configuration is set to the "default" domain, this may be edited using any suitable text editor and then configuration file deployed to the Windows Mobile devices before an initial subscribe takes place. See below for an example of a different domain configuration;

```
<SYS_ABO_Domain>client600</SYS_ABO_Domain>
```

If the SUP Domain property is set incorrectly or mismatched to the actually SUP Domain name configured on the SUP server, the WM CRM client will receive the following error message, "Domain is currently disabled".

Single Sign On

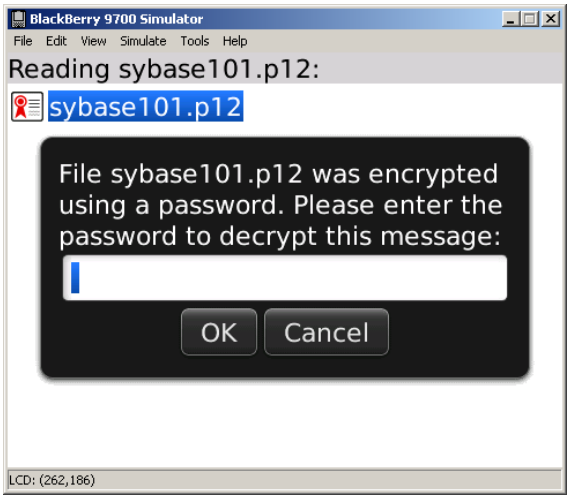
Single Sign On (SSO) allows a Mobile Sales user to connect to the SAP CRM system using an alternative means of authentication from the usual user/password authentication approach. The new SSO capability is supported on all the current Mobile Sales platforms, BlackBerry, Windows Mobile and iPhone/iPad.

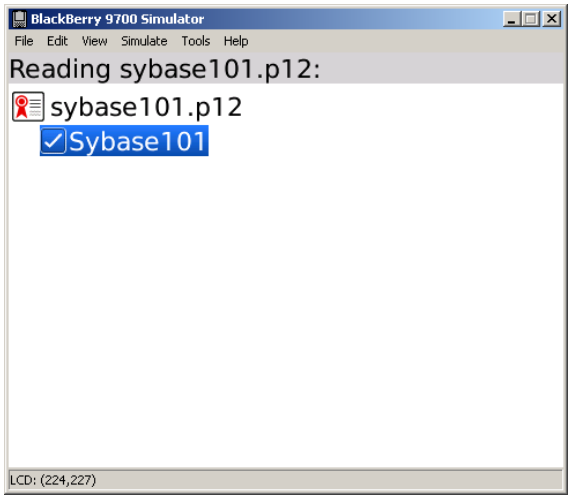
All three device platforms now handle both SSO2 Token and X.509 certificates as a means of authentication.

BlackBerry Single Sign On using X.509 Certificates

Before attempting to authenticate using an X.509 certificate the user must install their certificate onto the BlackBerry device. The certificate may either be emailed or transferred via USB to the devices memory card using the BlackBerry desktop manager. Once on the device, the certificate must be located and imported. All certificates require a password to unlock and import into the devices certificate store.

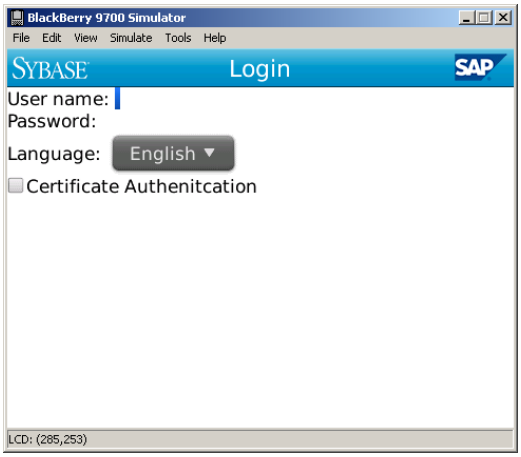
When opening the certificate, the RIM OS will prompt for the certificate password. After entering the correct password, the user must select the user name from the certificate and then go to the menu and select the import certificate menu option.





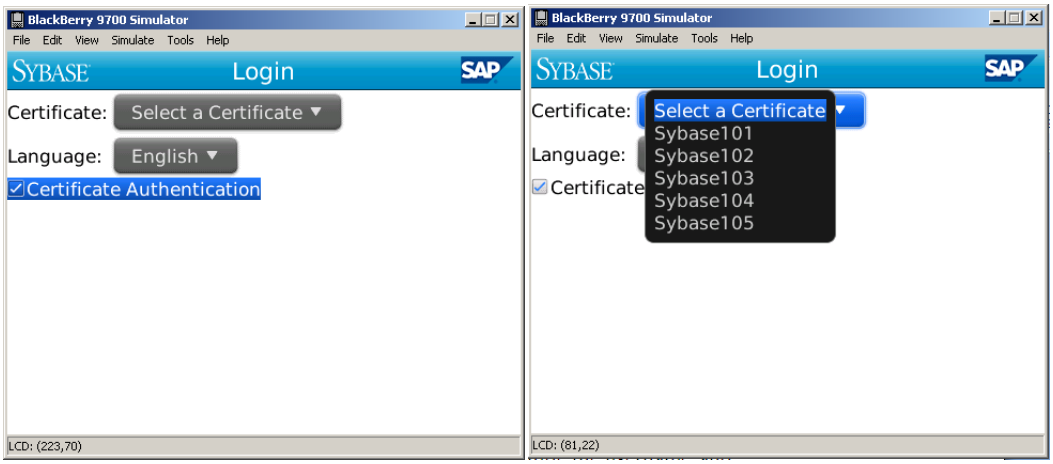
The BlackBerry Mobile Sales application by default continues to show the original login screen, as in previous versions of Mobile Sales, where the username and password for the SAP CRM system may be entered. An additional checkbox below the language drop down call “Certificate Authentication” has been added. This checkbox must be “checked” if the user wishes to authenticate using an X.509 certificate installed on their BlackBerry device.

See below for images of the updated login screen with the new checkbox for “Certificate Authentication” is shown.



When "Certificate Authentication" checkbox is checked, the login screen hides the Username and Password input fields and replace them with a dropdown list of the available certificates installed on the user's BlackBerry device. By default no certificate is selected.

See below for images of the login screen with the certificate dropdown shown.



To authenticate via certificate, the user must select a specific certificate from the dropdown.

Once a certificate is selected in the login initiated, the RIM OS will automatically prompt for the password for the certificate selected.

See below for an example of the RIM OS certificate password dialogue box.

Windows Mobile Single Sign On using X.509 Certificates

Before attempting to authenticate using an X.509 certificate the user must install their certificate onto the Windows Mobile device. To install an X.509 Certificate on to a Windows Mobile device complete the following steps

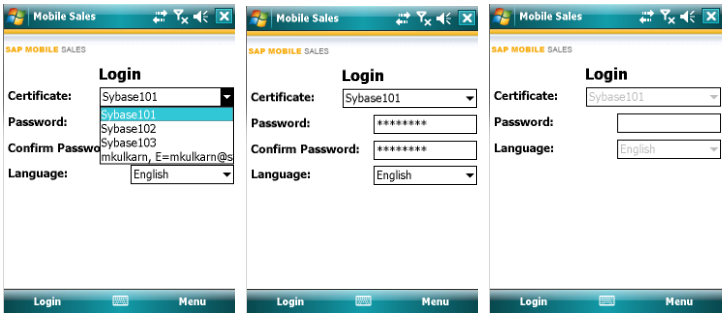
- Connect the device to a PC using ActiveSync and copy the certificate file with Explorer to the device.
- On the device, navigate to the folder containing the certificate file and tap on it to install to the device. Then enter the password at the prompt and then click "Done" menu option to complete the process.

The Mobile Sales application now supports new enterprise configuration options in the `SybaseCRM.Configuration_template.xml` file which are used to select the various sign methods. A new configuration property called "`SYS_SignOnMethod`", may be set to one of 3 values, "Password", "Certificate" or "Token", to select the desired sign in method.

By default the "`SYS_SignOnMethod`" is set to "Password", and therefore the Mobile Sales application continues to show the standard login screen requesting the user to enter their username and password for the SAP CRM system.

When the "`SYS_UseSingleSignOn`" is set to true and the, "`SYS_SignOnMethod`" is set to "Certificate" the login screen displays a drop download list of available certificates one the device from which the user may select. By default no certificate is selected.

See below for images of the login screen when the "`SYS_SignOnMethod`" `configuration parameter` is set to "Certificate".



An additional text box also appears for certificate password confirmation.

Initially the certificate drop down is enabled and the "Confirm password" textbox is present. Subsequent logins only require the password to be provided.

iOS Single Sign On using X.509 Certificates

Before attempting to authenticate using an x.509 certificate, the Mobile Sales application must retrieve the certificate file from the SUP server by providing a windows password, and certificate password. A new setting field has been added called "Window-Domain" to facilitate the file transfer, this must occur before login/subscribing using an x.509 certificate can take place. There will be a short delay before the user can actually login while the certificate is transferred to the

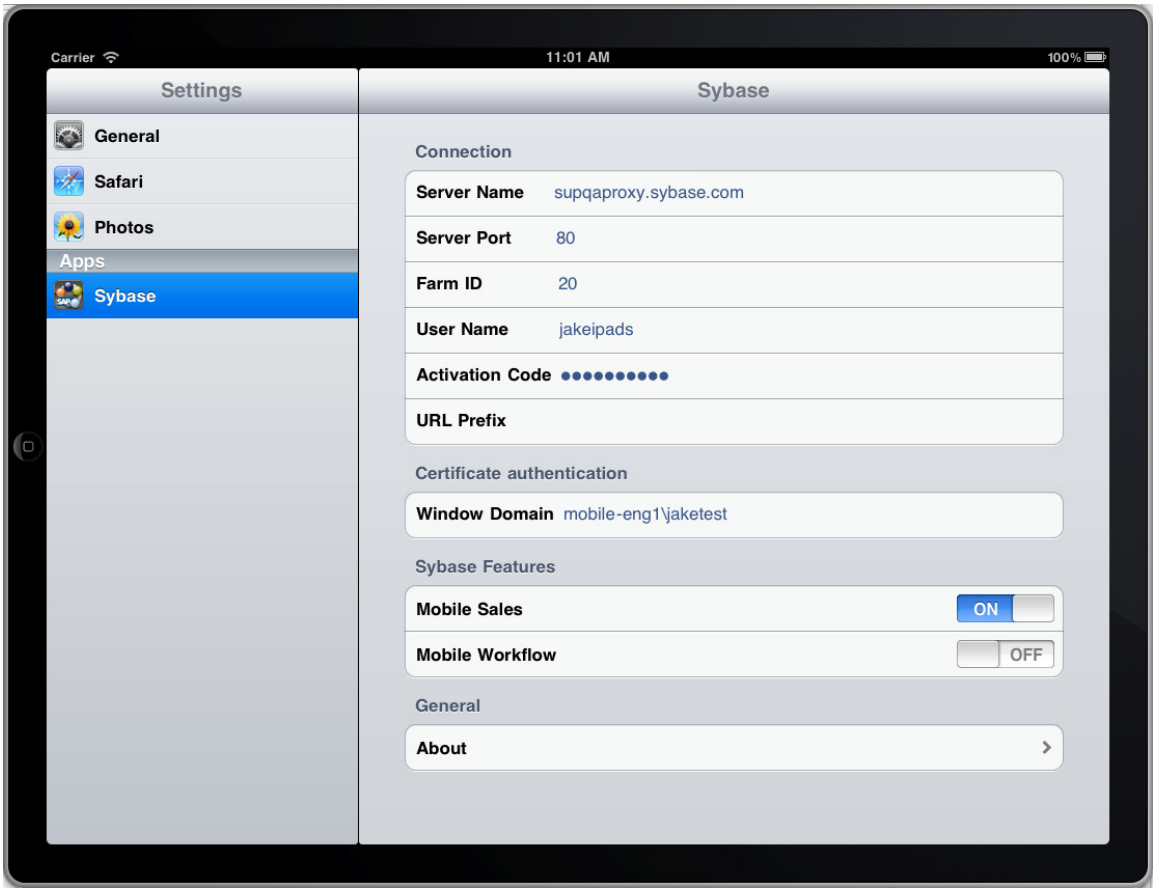
device. Once the certificate file is received by the application, this certificate is used to make an initial subscription (login) to the server. The subscription process continues as normal.

On the SUP server, in order to allow the device to obtain the x.509 certificate file, the administrator must have configured a certificate for the user on a specific domain and the certificate file must named in the following format *windowsdomain_username.p12*. For example, *SYBASE_JOHNDOE.p12*. The user must have "read" permissions for the domain_user.p12 certificate file so it may be copied to the iOS device.

Please see more detail about how to setup this domain_user.p12 from "How to Setup SUP for Single Sign On " document.

The iOS Mobile Sales application, by default, continues to show the original login screen where it requests the user to enter their username and password for the SAP CRM system.

The Sybase Mobile Sales connection settings provide an additional field to allow domain and user to be entered, see below.

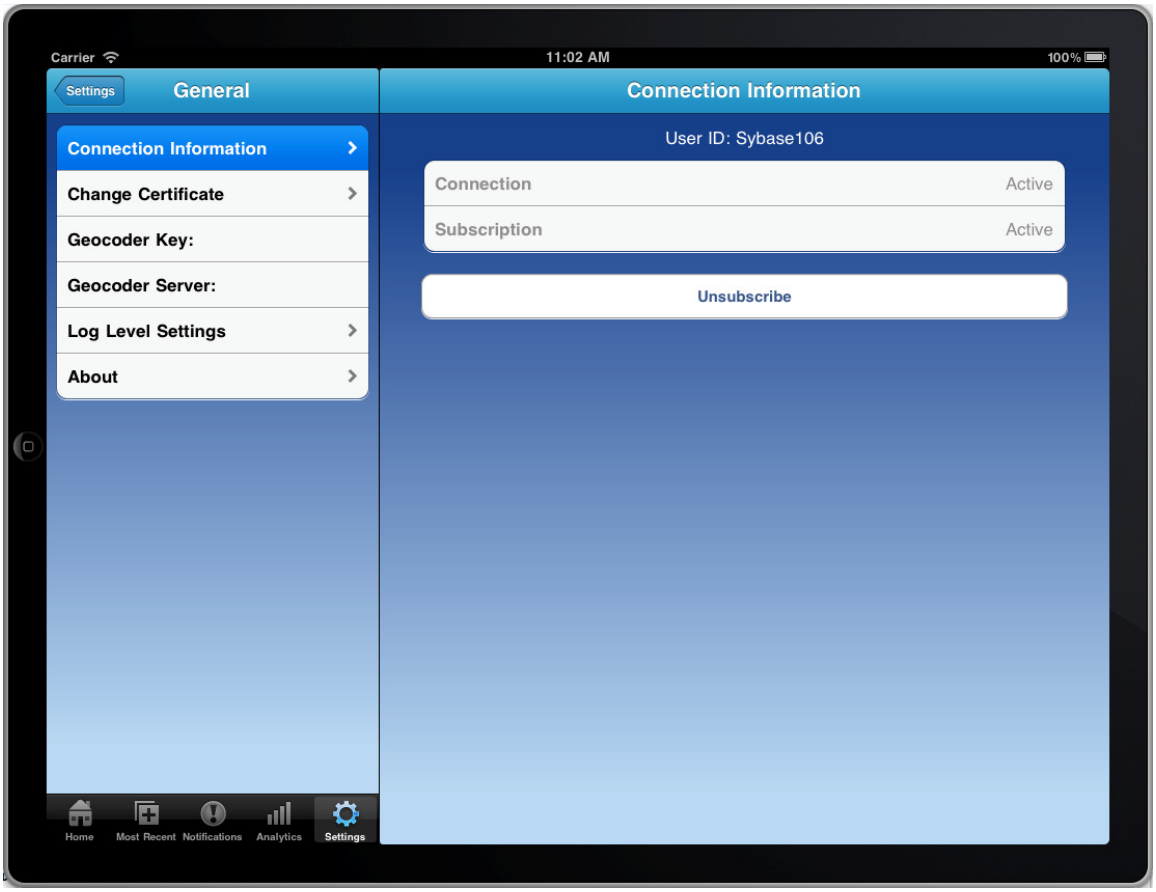


A new On/Off property switch is available on the logon screen to enable SSO authentication. It is an On/Off switch option labeled “Single Sign On”. See screen shot below where the Certificate authentication is set to “ON”:

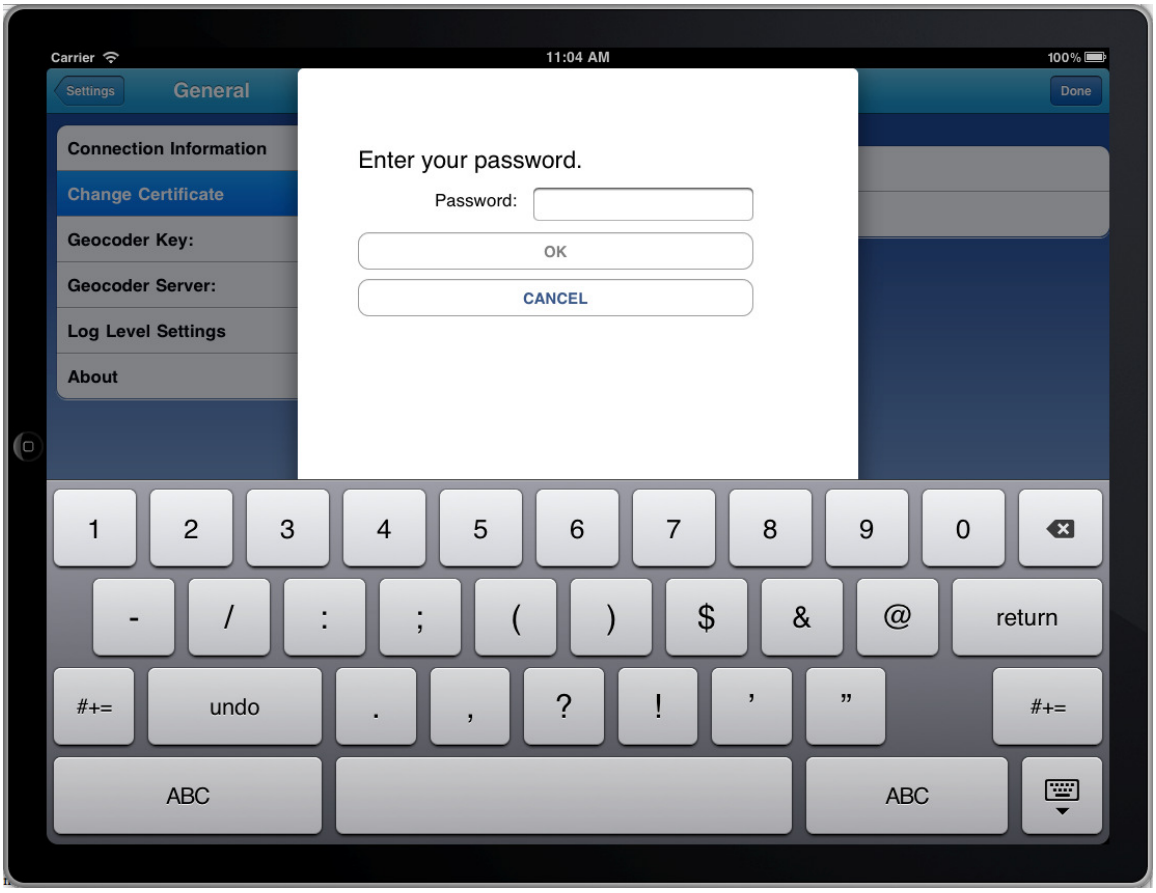
With certificate authentication enabled, the user name and password fields are replaced with Window password and certificate password fields. The certificate password is used when loading the certificate into the local certificate store.

The screen shot below demonstrates where the Certificate authentication switch is set to “OFF”:

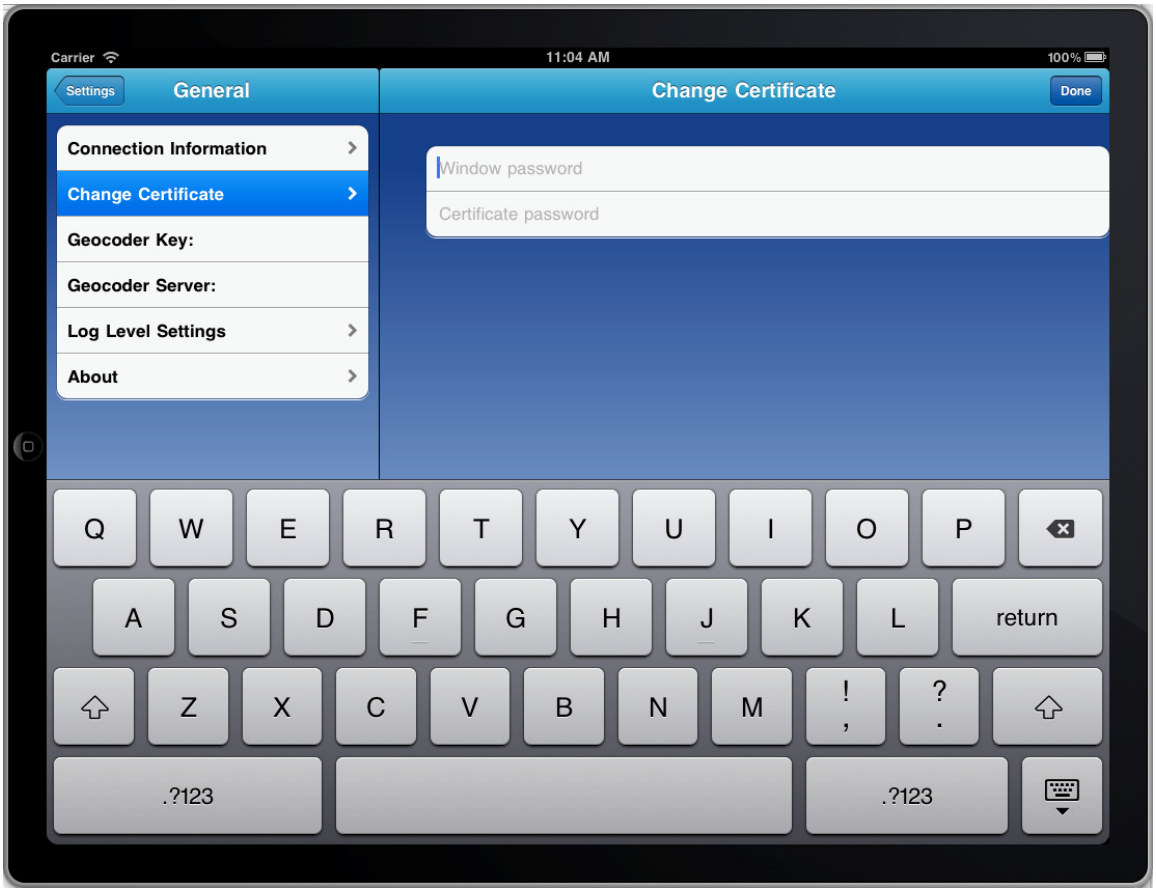
After Login by x.509 Certificate, the User Information is defined under the Connection Information, see the image below.


Carrier
11:02 AM
100%
Settings
General
Connection Information
Change Certificate
Geocoder Key:
Geocoder Server:
Log Level Settings
About
Connection Information
User ID: Sybase106
Connection
Active
Subscription
Active
Unsubscribe
Home
Most Recent
Notifications
Analytics
Settings

After Login by x509 Certificate, there is a “Change Certificate” option on the General Setting list, which will prompts for the Application PIN before allowing the certificate to be changed.



Once the Pin has been entered a new certificate may be requested using Window Password and the Certificate Password, see below.



Sign On using SS02 Token

SSO2Token authentication operates in the same way as previous versions of Mobile Sales requiring a username and password to be entered in order to authenticate a user.

If SUP server is setup for SSO2 Token authentication, then it will route the token username and password to the authentication server to validate they are correct. If there is no matching SSO token, the SUP server will route the SAP CRM username and password to the SAP CRM system in order to validate the username and password.