SYBASE®

An SAP® Company

New Features

Sybase Unwired Platform 2.1 ESD #3

DOCUMENT ID: DC01203-01-0213-02

LAST REVISED: October 2012

Copyright © 2012 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.

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. ® 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 Oracle and/or its affiliates in the U.S. and other countries.

Unicode and the Unicode Logo are registered trademarks of Unicode, Inc.

All other company and product names mentioned may be 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

New Platform Features

Sybase® Unwired Platform 2.1 ESD #3 includes new features that affect Sybase Mobile SDK and Unwired Platform Runtime components. Key features that affect the entire platform include security and support enhancements. Review these platform features in addition to those described in Mobile SDK and Runtime sections.

Security Enhancements

Unwired Platform security has been enhanced with these new features.

- **Encrypted or unencrypted HTTP application connection support –** In earlier versions, the messaging transport in Sybase Unwired Platform used a proprietary end-to-end encryption over HTTP for secure communication. This new version of Unwired Platform adds support of standard HTTPS protocol for secure communication to both Sybase Mobile SDK and Unwired Platform Runtime. To make use of this new feature, applications must be rebuilt with this latest SDK version, and connected to this new version of Runtime.

  Note: HTTPS support is available for Hybrid Web SDK (except Hybrid Web Container apps on Windows Mobile platforms), Object API, and OData SDK.

  Documented in:

  - *Developer Guide: Mobile Workflow Packages*:
    - *Configuring Android Connection Settings*
    - *Configuring BlackBerry Connection Settings*
  - *Developer Guide: OData SDK*. Search for these topics in the Android, BlackBerry, and iOS sections:
    - *Enabling HTTPS as a Transport Protocol*
    - *Enabling a Listener for HTTPS Support with Server Certificate Validation*
- **Expanded SSO support –** expanded single sign-on support (SSO) is available to Android, BlackBerry, iOS, and Windows Mobile platforms for Object API, and Hybrid Web Container apps. This feature allows a mobile application to provide an SSO token as credentials for synchronization, which enables you to use your existing SSO solution with Unwired Platform.

  Note: This feature is not applicable to Hybrid Web SDK applications on Windows Mobile. The OData SDK does support this feature.

  Documented in the corresponding *Developer Guide* for your application type:

  - *Basic Authentication*
  - *Single Sign-on*
- **Network edge SSO authentication for user name and password authentication providers –** Sybase Unwired Platform applications can now integrate with HTTP-based

SSO authentication providers. In earlier versions, only SSO token authentication from SAP SSO2 token providers were supported. Now, Hybrid Web SDK and Object API applications can connect to reverse proxy servers (agents) at the network edge. These agents perform authentication and return authenticated tokens on behalf of those authentication providers to either Unwired Server or HTTP-base enterprise information system (EIS) systems via session personalization values delivered as HTTP cookies, or HTTP headers.

An example of an HTTP-based SSO provider is SiteMinder running inside the enterprise and its SiteMinder agent running at the network edge inside an Apache or IIS reverse proxy server.

Note: This feature is not applicable to Hybrid Web SDK applications on Windows Mobile. The OData SDK does support this feature.

Documented in:

- *Security*:
  - *HTTP Authentication Security Provider*
  - *SSO Integration Across Client Applications*
- *Developer Guide: Mobile Workflow Packages*:
  - *Single Sign-on*

- **Enhanced LDAP support –** LDAP support now includes nested groups for role computation

  Note: This feature is not applicable to OData SDK.

  Documented in:

  - *Security*:
    - *Using LDAP Nested Groups and Roles*
    - *LDAP Role Computation*
- **Special character support for user names –** You can now use special characters as user names during authentication. This enhancement means that e-mail addresses can legitimately be used for user name values.

  Note: This feature is available for Hybrid Web SDK, Object API, and OData SDK.

  Documented in:

  - *Security*:
    - *Supported Providers and Credential Types*
    - *Considerations for Using E-mail Addresses as User Names*
- **Password Policy for Data Vaults –** A password policy can now be added to application connection templates. By default a password policy is enabled. When the correct enforcement code has been added to an application's login code, a device user must supply a password that conforms to the requirement defined in the password policy. For details,

see *Enabling and Configuring a Password Policy* and *Creating a Data Vault that Enforce Password Policy* in the *Release Bulletin*.

Note: This feature is not applicable to OData SDK.

Extended Device and API Support
Unwired Platform supports the newest devices, operating systems, APIs, and tools. See *Supported Hardware and Software* for specific details.

New Features for Sybase Mobile SDK

In addition to the new platform features, changes to Sybase Mobile SDK now offers better support for the development of mobile business objects, Object API applications, Hybrid Web Container apps, and OData SDK applications.

Note: Deprecated items currently remain available, but will be removed in a future release.

See also

- *New Platform Features* on page 1

Mobile Business Object Development

Once you are familiar with the documented platform features, review these new or changed features for mobile business object (MBO) development.

Operation Cache Policy Enhancements
Additional and enhanced cache policies provide more control over the way enterprise information system (EIS)-affecting operation results are applied to the Unwired Server cache, especially for composite graph MBOs (MBOs in a composite relationship).

Documented in:

- EntityRead Mobile Business Object Project (2.1 ESD#3) - an Unwired WorkSpace example project that illustrates operation cache policy enhancements, Entity Read operations, and output mapping features using a REST Web service. Download the EntityRead example project from the SAP® Community Network: *http://scn.sap.com/docs/DOC-8803*.
- *Sybase Unwired WorkSpace - Mobile Business Object Development*: *Setting an Operation Cache Policy*
- *Mobile Data Models: Using Mobile Business Objects*: *Operation Cache Policies*

Entity Read Operation
A new MBO operation type enables you to identify a specific entity in the cache. Use the operation with the "Immediately update the cache" operation cache policy, and "Apply output

of ENTITY READ operation" option. This operation then refreshes the Unwired Server cache for a single instance of an MBO, or composite graph (MBOs in a composite relationship) for Create and Update operations based on the definition of the Entity Read operation.

Documented in *Sybase Unwired WorkSpace - Mobile Business Object Development*, *Entity Read Operations*

Output Mapping

Provides a graphical editor and view of remote operations to MBOs, and attribute mappings, including mappings for MBO graphs (MBOs in a relationship).

Documented in *Sybase Unwired WorkSpace - Mobile Business Object Development*, search for:

- *Mapping Multiple Results to Multiple Mobile Business Objects*
- *Mobile Business Object Operation Properties*

Enhanced MBO Modeling Validation Rules

Additional validation rules including primary key requirements and maintaining primary key/foreign key affinity in composite object graphs warn or prevent you from defining an invalid MBO model. This may require MBO developers to update their MBO data models and regenerate object API code. Warning and error messages during MBO development help you avoid runtime errors, such as system exceptions in the client log, and various errors in the Unwired Server log.

Documented in:

- *Troubleshooting*:
  - *Relationship Guidelines and Restrictions*
  - *Operation Validation Rules and Error Messages*
- *Sybase Unwired WorkSpace - Mobile Business Object Development*: *Relationship Guidelines and Restrictions*

See also

- *New Platform Features* on page 1

Object API Development

Once you are familiar with the documented platform features, review these new or changed features for native client Object API development.

iOS Support Changed to Replication-Based Synchronization

The iOS default device support has changed from messaging-based to replication-based synchronization. Replication-based applications use the synchronization channel to keep data synchronized between Unwired Server and the client. This puts iOS synchronization on a par with Android, BlackBerry, Windows, and Windows Mobile. In 2.1 ESD #3, iOS messaging-based synchronization support is deprecated.

The Code Generation wizard now uses replication-based synchronization by default; the messaging-based option is still available. The messaging channel is now mainly used for device-side notifications in DOE-based applications.

Existing message-based iOS applications will continue to be supported after updating to Sybase Unwired Platform 2.1 ESD #3, but new features will not be available. Sybase recommends that you migrate existing message-based iOS applications to replication-based synchronization to take full advantage of new features.

Documented in:

- *Developer Guide: iOS Object API Applications*: *Transitioning Existing Object API Applications to SDK Version 2.1 ESD #3* (also in the *Release Bulletin* and *Installation Guide for Sybase Mobile SDK*).
- *Developer Guide: iOS Object API Applications*: *Message-Based Synchronization Applications in SDK Version 2.1 ESD #3*

DataVault

Additional password policy control has been added to the DataVault, making it easier to populate the password policy and enforce enterprise password policies in device applications. A new DataVault API enables you to work with password policy settings, check for default passwords, change password, delete data from the datavault, and iterate through data.

Documented in:

- *Developer Guide: iOS Object API Applications*, search for *SUPDatavault*.
- *Developer Guide: Android Object API Applications*, *Developer Guide: BlackBerry Object API Applications*, and *Developer Guide: Windows and Windows Mobile Object API Applications*, search for *Datavault*.

Object API Changes in SDK Version 2.1 ESD #3

Changes in the Object API for SDK 2.1 ESD #3.

iOS Transition to Replication-Based Synchronization

iOS applications built with earlier versions of the SDK use messaging-based synchronization (MBS) for data delivery. Applications built using SDK version 2.1 ESD #3 now use replication-based synchronization (RBS) for data delivery, to reduce synchronization time to iOS applications. Consequently, messaging-based synchronization has been removed from the 2.1 ESD #3 SDK. You can maintain your messaging-based synchronization applications in an earlier version of the SDK, while deploying the applications to a 2.1 ESD #3 Unwired Server.

API changes related to the application transition include:

- An RBS application use either a synchronous or asynchronous synchronization process. By default, asynchronous replay is enabled.
- In an MBS application, when an operation replay record is generated from a call to `submitPending`, the generated operation is automatically sent to Unwired Server. In an RBS application, a `synchronize` method is required to send the record to Unwired Server.
- In an MBS application, a subscription event caused data to be pushed to the client from the server. In an RBS application, a call to `synchronize` (synchronous) or `beginSynchronize` (asynchronous) is required.
- RBS applications do not support MBS callbacks.

Documented in:

- *Release Bulletin*: *Transitioning an Existing Object API Application to 2.1 ESD#3*

Datavault

Table 1. New Datavault Methods

Methods	Platform
New methods in the `Datavault` class: • The `setPasswordPolicy` and `getPasswordPolicy` methods allow you to configure or retrieve password policy settings for a data vault. When you call the `createVault` or `changePassword` APIs, the data vault checks the password for compliance to the password policy. • The `isDefaultPasswordUsed` method checks whether the default password is used by the data vault. • The `changePassword (string, string, string, string)` is an overloaded method that validates that a new password is compatible with the password policy, uses the current password to unlock the vault, and changes the password of the vault to a new password. • The `getDataNames` method provides support for iterating through data. The method returns an array of dataName objects. • The `deleteValue` method provides an intuitive way to delete data from the data vault. Previously, you had to set a value to null to delete it.	Android, BlackBerry, iOS, Windows, and Windows Mobile

Table 2. Changed Datavault Methods

Method, Class, or Property	Platform
Changed methods in the `Datavault` class: • The `createVault` and `unlock` methods now automatically compute a salt value when you pass a salt parameter with a null value, or with an empty string. • The `createVault` and `changePassword` methods now provide an option to automatically generate a vault password, by passing a null or empty string for the `password` or `newPassword` parameters. A default password is computed only if the `defaultPasswordAllowedSetting` in the password policy is set to true (the default is false).	Android, BlackBerry, iOS, Windows, and Windows Mobile

Table 3. Removed Datavault Methods

Methods	Platform
Methods removed from the `Datavault` class: • The `setLockTimeout` and `getLockTimeout` methods for setting and retrieving the length of time a vault remains unlocked have been removed. The control of this setting is now specified by the password policy. • The `setRetryLimit` and `getRetryLimit` methods for setting and retrieving the retry limit of the vault have been removed. The control of this setting is now specified by the password policy.	Android, BlackBerry, iOS, Windows, and Windows Mobile

Documented in:

- *Developer Guide: Android Object API Applications*:
  - *Datavault*
  - *SUPDatavault*
- *Developer Guide: BlackBerry Object API Applications*, and *Developer Guide: Windows and Windows Mobile Object API Applications*: *Datavault*
- *Security*:
  - *Encrypting Device Data*
  - *Securing Sensitive Data On-Device with Data Vault*

Authentication

Table 4. Deprecated Authentication Methods

Methods	Platform
Deprecated methods from the generated package database class: • `OnlineLogin` • `OfflineLogin` • `LoginToSync`	Android, BlackBerry, Windows Mobile, and Win32

Documented in:

- *Developer Guide: Android Object API Applications*, *Developer Guide: BlackBerry Object API Applications*, and *Developer Guide: Windows and Windows Mobile Object API Applications*, search for:
  - *Connecting to Unwired Server with a Certificate*
  - *Single Sign-On With X.509 Certificate Related Object API*
  - *Logging In*
  - *Check Network Connection Before Login*
  - *Synchronization APIs*
  - *subscribe*
- *Troubleshooting*, search for: *iOS Device Cannot Sync*

Mobile Workflow (Hybrid Web Container) Development

In addition to the platform features, review these new or changed features for Hybrid Web Container development.

Integration with PhoneGap

Integration with PhoneGap allows you to link your own custom native code to the Hybrid Web Container and call this native code from JavaScript, as well as access native device functionality using the PhoneGap framework

Note: This feature is only applicable to Android and iOS applications in this release.

.

Documented in *Developer Guide: Mobile Workflow Packages*:

- *PhoneGap Support*
- *Custom Plug-ins for the iOS Hybrid Web Container*
- *Custom Plug-ins for the Android Hybrid Web Container*

Customization Support for Android and iOS Hybrid Web Container

Template source code is provided for the Android and iOS Hybrid Web Container, which enables you to build your own Hybrid Web Container and customize it in different ways.

Documented in *Developer Guide: Mobile Workflow Packages*:

- *Android Hybrid Web Container Customization*
- *iOS Hybrid Web Container Customization*

OData SDK Development

Once you are familiar with the documented platform features, review these new or changed features for OData SDK development.

Private DataVault

A private DataVault class is available for Android, with these advantages:

- You can securely store data that is specific to an application.
- You need not install `SybaseDataProvider.apk` to use the private DataVault.

Documented in: *Developer Guide: OData SDK*: *Data Vault API References* (for Android development).

SSL Support over SUPMessagingChannel with NetworkEdge

For enabling secure communication, all OData client applications can use the HTTPS protocol. These applications can optionally connect to a Relay Server via HTTPS.

Documented in: *Developer Guide: OData SDK*:

- *Enabling HTTPS as a Transport Protocol*
- *Enabling a Listener for HTTPS Support with Server Certificate Validation*

Basic Authentication with NetworkEdge

For enabling basic authentication, all OData client applications can use the HTTP protocol.

Documented in *Developer Guide: OData SDK*: *Enabling a Listener for HTTP Support with Basic Auth Challenge*.

Inline Feeds

BlackBerry clients can retrieve frequently updated data in the form of inline feeds. The feeds retrieved can be serialized into a suitable format.

Documented in *Developer Guide: OData SDK*: *Inline Feeds*.

Customization Resource Bundles

(Applies only to OData SDK, Android and iOS clients) OData SDK-based applications can leverage the customization resource bundle feature to provision resources to client applications.

This feature lets you build content to customize and configure application on the device. The server provisions the customization resource bundle to the application instance, and then the application parses and customizes the end-user application.

Documented in:

- *Developer Guide: OData SDK*: *Downloading Customization Resource Bundles* (Android and iOS)
- *Developer Guide: Unwired Server Management API*:
  - Managing Customization Resource Bundles
  - Application Settings Properties
- *Sybase Control Center* online help: *Modifying Application Properties*
- *System Administration*: *Customization Resource Bundles*

See also

- *New Platform Features* on page 1

OData SDK API Changes in Version 2.1 ESD #3

Learn about changes in the OData SDK API for SDK 2.1 ESD #3.

Afaria

Various Afaria certificate APIs have been deprecated in this release.

Table 5. Deprecated Afaria Methods

Methods	Platform
Deprecated methods in the `LiteSUPCertificateStore` class: • The `getSignedCertificateFromAfariaForURLScheme` method returns the certificate as an encoded string if the URL Scheme is registered with Afaria. • The `getSignedCertificateFromAfariaForURL` method returns the certificate as an encoded string.	iOS

Methods	Platform
Deprecated method in the `LiteCertificateStore` class: • The `getSignedCertificateFromAfaria` method returns the certificate as an encoded string.	Android
Deprecated method in the `CertificateStore` class: • The `getSignedCertificateFromAfaria` method returns the certificate as an encoded string.	BlackBerry

Documented in *Developer Guide: OData SDK*, search for:

- *Provisioning Certificates Using URLScheme with Afaria*
- *Provisioning Certificates Using URL with Afaria*
- *Provisioning Certificates Using Afaria*

.

New Features for Runtime

Once you are familiar with the documented platform features, review these new or changed features for the Unwired Platform Runtime.

Diagnostic Tool

The diagnostic tool enables the system administrator to verify the configuration and report failures with specific messages. You can install and run the tool on any machine.

Documented in:

- *System Administration*, search for *Diagnostic Tool Command Line Utility*

System Landscape Directory (SLD) Automation

Administrators no longer need to manually start the Data Supplier every time data has to be sent to the SLD. You can now configure Data Supplier in the SCC console to start, generate payload, and automatically upload to SLD as scheduled.

Documented in:

- *Sybase Control Center* online help
- *System Administration*

SAP License Audit Data Generation

The SAP License Audit data generation feature enables an Unwired Platform administrator to generate audit measurements, and manually upload the resulting data to SAP License Audit.

Documented in:

- *Sybase Control Center* online help
- *System Administration*
- *Developer Guide: Unwired Server Management API*, search for *SAP License Audit*