SYBASE®

Release Bulletin - Update 2

Sybase Unwired Platform 1.2

Windows

DOCUMENT ID: DC01253-01-0120-02
LAST REVISED: February 2010

Sybase, Inc., One Sybase Drive, Dublin, CA 94568

Contents

Product Summary

Sybase® Unwired Platform enables you to develop mobile applications with the Unwired WorkSpace development environment and to manage the production environment with Sybase Control Center. Unwired Platform takes your enterprise data and applications into the field to mobile workers quickly and without programming. Unwired Platform allows you to create dynamic, secure mobile applications, which you can deploy, manage, and monitor from the Web-based administrative console.

For information about accessibility, see *Accessibility Features* on page 34.

About this Update

This document is an addendum to the Sybase Unwired Platform 1.2 Release Bulletin. For a complete set of updates for Sybase Unwired Platform 1.2, ensure you read all versions of these Release Bulletin documents.

This document contains new documentation updates as well as new known issues that have been identified since Update 1.

Known Issues

Provides known issues for Sybase Unwired Platform 1.2 Release Bulletin since Update 1. As indicated for each issue below, new or updated documentation may be included.

Table 1. Known Issues

CR#	Description
None	No issues are included.

Documentation Updates

Provides known documentation issues for Sybase Unwired Platform 1.2 since Update 1. As indicated for each issue below, new or updated documentation may be included.

Table 2. Sybase Control Center for Unwired Server

CR#	Description
610611 System Administration	**Problem:**Need backup and restore information to plan disaster recovery. Also need related information for mobile device users. **Solution:** Back up the installation directory routinely as part of normal operations. Back up the consolidated database and transaction logs periodically, especially when major changes are made. **Documentation:** Backup and recovery information, guidelines, and procedures are now documented. • *Backup and Restore Overview* on page 9 (new)
607923 System Administration	**Problem:**Need information to set up Microsoft Active Directory authentication with Sybase Unwired Platform. **Solution:** You can configure Microsoft Active Directory Server as the LDAP security provider for your Sybase Unwired Platform production environment. **Documentation:** Microsoft Active Directory LDAP setup information and procedures are now documented. • *Setting Up Active Directory as an LDAP Security Provider* on page 15 (new)
None System Administration	**Description:** Need information for setting up Lightweight Directory Access Protocol (LDAP) and ActiveDirectory (AD) authentication with Sybase Unwired Platform. **Documentation:** LDAP procedures have been updated with more information. • *LDAP Authentication in Unwired Platform* on page 27 • *Configuring an LDAP Authentication Module* on page 27 (updated) • *LDAP Configuration Properties* on page 20 (updated)

CR#	Description
607528 System Administration	**Problem:** There is no documentation for configuring the lightweight polling configuration, specifically the polling interval, while using Push. **Solution:** You can change lightweight polling configuration on Unwired Server using **dbisql**, and in the client-side program. **Documentation:** **Note:** Lightweight polling documentation was introduced in the Sybase Unwired Platform 1.2 Release Bulletin – Update 1 (CR #584183). Additional topics are provided in this Release Bulletin – Update 2. • *Light Weight Poller in Unwired Platform* on page 30 (new) • *Configuring Lightweight Polling Interval* on page 30 (new) • *Troubleshooting Device Tracking in a Cluster* on page 31 (new)

Table 3. Troubleshooting

CR#	Description
None	**Problem:** Encountered an SQLE_PRIMARY_KEY_NOT_UNIQUE error. **Solution:** Possible causes: • The Primary Key generated in the client is not unique. In this case, try using a better Primary Key generation method, such as GUID. • Multiple clients use only one Sybase Unwired Platform account to connect to Unwired Server. In this case, be sure to use different Sybase Unwired Platform client accounts to connect to Unwired Server. **Documentation:** • *Troubleshooting SQLE_PRIMARY_KEY_NOT_UNIQUE Error* on page 31
None	**Problem:** The server logs for primary and secondary servers list several -10117 stream errors **Solution:** The Unwired Server consolidated database has issues with tracking devices and light weight polling (LWP) in a clustered environment. You must disable device tracking when LWP is used by reconfiguring all servers in your cluster. **Documentation:** • *Troubleshooting Device Tracking in a Cluster* on page 31

Backup and Restore Overview

Learn how to plan Sybase Unwired Platform backup schedules to support disaster recovery planning. Provides information for backing up and restoring the installation file system, consolidated database, and transaction logs; and related information for mobile device client users.

Backup of the Installation File System

Make sure to create regular and complete backups of the Sybase Unwired Platform installation files and directories, which are modified as part of regular operation and with configuration changes.

Examples of these Sybase Unwired Platform installation files and directories include:

- `<`*`SUP_HOME`*`>\Servers\UnwiredServer\Repository`
- `<`*`SUP_HOME`*`>\Servers\UnwiredServer\config`
- `<`*`SUP_HOME`*`>\Servers\UnwiredServer\bin`
- `<`*`SUP_HOME`*`>\ Servers\UnwiredServer\SQLAnywhere11`
- `<`*`SUP_HOME`*`>\ Servers\UnwiredServer\logs`
- `<`*`SUP_HOME`*`>\Servers\UnwiredServer\tomcat\webapps\onepage\config`
- `<`*`SUP_HOME`*`>\Servers\UnwiredServer\tomcat\conf`

Additionally, batch scripts (for example, `<`*`SUP_HOME`*`>\Servers\UnwiredServer\bin`) may be automatically modified by the Sybase Unwired Platform installer, or manually modified later by a Sybase Unwired Platform administrative user. Make sure these files are also backed up.

Instead of backing up these individual artifacts, Sybase recommends that you perform regular backups of the entire Sybase Unwired Platform installation folder. Ideally, include the Sybase Unwired Platform installation directory in your disk backup schedule. At the same time the folder and disk backup is performed, update the Windows registry so it matches the state of the backup.

Plan the frequency of the file system backups to coincide with any changes made to the system, including metadata changes (such as deployment of new Mobile Business Object packages to the server), or configuration changes (such as new enterprise information system connection). To maintain a consistent backup state, Sybase recommends you back up the consolidated database at these times as well.

Backup of the Consolidated Database

Create regular and complete backups of the Sybase Unwired Platform consolidated database (CDB) and its transaction logs. These instructions assume you are using SQL Anywhere as your Sybase Unwired Platform database server.

SQL Anywhere provides backup and recovery tools. Determine your tolerance for data loss, and your expectations for recovery time, then design a backup and recovery plan for your specific enterprise needs.

Following are basic instructions for making your databases recoverable in case of a disk crash or catastrophic computer failure. If you require more comprehensive recovery policies, Sybase offers professional services specifically related to this topic.

The Sybase Unwired Platform consolidated database contains the metadata of deployed applications, and transient and cached data that is sent to mobile devices.

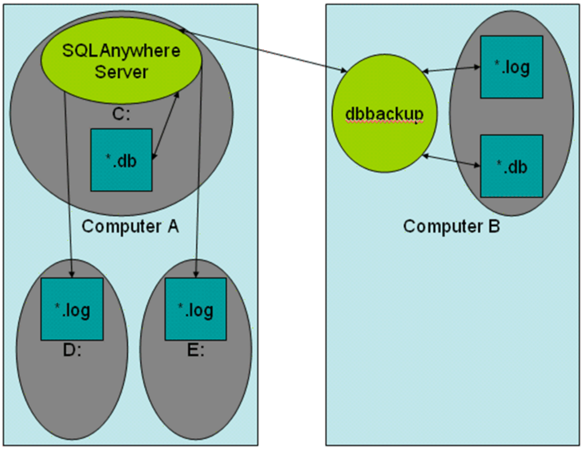
Frequent backups of the consolidated database are required to maintain the deployed applications metadata. The backups may also help restore the transient and cached data (to a large degree) in case of crashes or corruption, and may help mobile device clients from having to perform a full refresh.

Sample Backup and Recovery Plan

Provides a basic backup and recovery plan.

This diagram shows the architecture for a reasonably reliable backup and recovery strategy. Only Sybase Unwired Platform components related to database recovery are included.

Figure 1: Sample backup and recovery plan



Shown in the diagram:

- Computer A is where the SQL Anywhere database server is installed and runs under Sybase Unwired Platform. There are three physical disks on this computer:
  - The C: drive has the SQL Anywhere server and the database files (`uaml.db`, `clusterdb.db`), which hold critical data that Sybase Unwired Platform requires to function.
  - The D: and E: drives hold identical copies of the transaction log files (`uaml.log`, and `clusterdb.log`). Using SQL Anywhere terminology, the D: drive holds the regular transaction log, and the E: drive holds the mirrored transaction log.
- Computer B is for long term backup, and requires only one drive (or backup tapes). Run the **dbbackup** utility from this computer periodically to obtain a full backup of the `*.db` and `*.log` files from Computer A.

Failure and Recovery Scenarios

Describes several failure scenarios (using the Sample Backup and Recovery Plan setup), how recovery works, and implications for Sybase Unwired Platform operation.

Disk C has an unrecoverable error. The *.db files have been lost.

Recovery: Install a replacement disk, and use standard file restore procedures to reinstall the SQL Anywhere software, and whatever else is needed. If the restore returns the `*.db` files, there is no harm, but do not rely on these files to be valid. Instead, copy the last backup version of the `*.db` files across from Computer B.

Next, start the SQL Anywhere server, which detects that the `*.db` files are not up-to-date with the checkpoints in the `*.log` files on drives D: and E: (which are unaffected by the C: drive failure). The server automatically replays transactions recorded in the transaction log to bring the database back to the state of all committed transactions at the time of the C: drive failure.

Sybase Unwired Platform can then start up and run normally. Sybase Unwired Platform mobile device clients are not affected except by the inability to sync between the time of the failure, and the time at which the recovery process has completed.

Disk D: or E: failure. One of the *.log files has been lost.

Recovery: Install a replacement disk and restore from backups.

Once the disk has been restored, copy the `*.log` files from the drive that did not fail to the one that failed. Restart the failed drive.

Complete failure of Computer A, and disks lost.

Recovery: See Restore the Consolidate Database for instructions. This should be a very infrequent event.

In this scenario, the database has lost all transactions since the previous backup to Computer B. Any Sybase Unwired Platform mobile device clients that synchronized between the time of the previous backup and the time of the failure cannot now sync. Clients must delete their

UltraLite database and start fresh. Any pending operations on these clients are lost. Clients that have not synchronized since the previous backup are unaffected.

Configuring Your Databases for Transaction Logs on Separate Drives

Use SQL Anywhere tools to configure and manage your consolidated databases for transaction logs and mirrored transaction logs on separate drives.

These tools are located in the `<SUP_HOME>\Servers\UnwiredServer\SQLAnywhere11\BIN32` directory. Add this directory to your PATH.

1. Shut down the SQL Anywhere server.
2. From the `SQLAnywhere11` directory, run:

   ```
   dblog -t D:\logs\uaml.log -m E:\logs\uaml.log uaml.db
   ```

   Output from a successful run of this command will look similar to:

   ```
   SQL Anywhere Transaction Log Utility Version 11.0.1.2250
   "uaml.db" was using log file "uaml.log"
   "uaml.db" was using no log mirror file
   "uaml.db" is now using log file "D:\logs\uaml.log"
   "uaml.db" is now using log mirror file "E:\logs\uaml.log"
   Transaction log starting offset is 0000746294
   Transaction log current relative offset is 0001015441
   ```
3. Repeat this command for the `clusterdb` database:

   ```
   dblog -t D:\logs\clusterdb.log -m E:\logs\clusterdb.log
   clusterdb.db
   ```
4. Restart SQL Anywhere server to start using these logs on other disks.

Performing a Remote Backup

Perform a remote backup using the sample recovery plan as an example.

Once your database is properly mirrored with transaction logs on separate disks, perform an initial backup of the consolidated database. Use the tools in the `<SUP_HOME>\Servers\UnwiredServer\SQLAnywhere11\BIN32` directory. Add this directory to your PATH.

Note: In some configurations, the **dbvalid** and **dbbackup** commands do not work remotely.

1. Use the **dbvalid** utility to validate the integrity of the database. The validation must be performed when there are no active connections to the server. Use the **dblocate** utility to locate the actual name of the database server in a particular installation. Typical names take the form of `<clustername>_primary`. The `clusterdb` is present if Unwired Server has been configured to run as a cluster.

   ```
   dbvalid.exe -c "DBF=uaml.db;UID=dba;PWD=SQL"
   ```

   ```
   dbvalid.exe -c "DBF=clusterdb.db;UID=dba;PWD=SQL"
   ```
2. On Computer B, verify that SQL Anywhere software is installed, and the PATH is set. If you are running Sybase Unwired Platform as a cluster, you already have that software

installed under the Sybase Unwired Platform installation directory. Otherwise, install another copy of Sybase Unwired Platform there. You need not add this installation to your cluster; you can even use a Developer Edition installation if you like.

3. Once Computer B is set up with the SQL Anywhere tools, run:

```
dbbackup -c "ENG=<clusterName>_primary;DBN=uaml;UID=dba;PWD=SQL"
\SQLAnybackup
```

```
dbbackup -c
"ENG=<clusterName>_primary;DBN=clusterdb;UID=dba;PWD=SQL"
\SQLAnybackup
```

   This creates `uaml.db`, `uaml.log`, `clusterdb.db`, and `clusterdb.log` in the `\SQLAnybackup` directory on Computer B.

4. As a precaution, validate the backups are suitable for recovery:

   a) On Computer B, create a temporary working directory (such as `\tmp`).

   b) Under the temporary directory, create an identical directory structure for the two log locations. You may need to use the **subst** command to map local directories to drive letters used on Computer A.

   c) Copy `*.log` to these locations.

   d) Run **dbvalid** on the `\tmp` copy of the `.db` file.

   WARNING: Do not run **dbvalid** on the backup copy itself (in the `\SQLAnybackup` directory of this example). The command runs, but corrupts your `.db` file so it cannot be used in recovery.

   e) If validation succeeds, you are assured that your backup in `\SQLAnybackup` can be used for recovery. You can delete the files in the `\tmp` and log directories.

   If validation fails, the backup is not usable for recovery and you should try again.

Next

Sybase makes these recommendations for setting up your backup schedule:

- Schedule backups from Computer B for some reasonable frequency so that, in the worst-case failure of a complete failure of Computer A, you do not lose too many transactions.
- Perform adhoc backups when there has been some major deployment of new Mobile Business Object packages to Sybase Unwired Platform. Otherwise you may lose those packages and have to redeploy them.

Restoration of the Installation File System

Restore the Sybase Unwired Platform installation file system from a backup.

To perform a normal restoration, use the file or disk backup utilities used to perform the backup. Sybase recommends that you save the current installation directory before you restore from backup.

Note: You may also need to restore the Windows registry from the backup done at the same time.

Restoration of the Consolidated Database

Restore the Sybase Unwired Platform consolidated database and transaction logs from backup after complete failure.

As discussed in *Failure and Recovery Scenarios*, if only one of C:, D:, or E: drives fail, recovery should be automatic once you have completed the appropriate tasks.

These steps are required in case of complete failure of all three drives:

1. Restore the computer's C:, D:, and E: drives from backup.
2. Delete the `*.db`, `*.log` files from their normal places after you have restored the file system.
3. Copy the `*.db` and `*.log` files from Computer B's backup directory to the normal locations on Computer A.

   Note: Copy the *.log files twice—once to the normal transaction logs directory, and once to the mirrored transaction logs directory.
4. Restart Sybase Unwired Platform.
5. If there have been package deployments or other cluster-affecting operations since the last database backups, the file-system data corresponding to the packages may be out-of-sync with the database contents related to these packages. If this has occurred, the Sybase Unwired Platform servers cannot fully start. The `ml.log` file indicates a mismatch between the local cluster version and that of the current cluster. To recover from this:
   a. Choose one of the Unwired Servers.
   b. Shut down that server.
   c. Edit the `sup.properties` file (`UnwiredServer` directory), and change the `cluster.version` property value to match that of the current cluster as reported in the logs.
   d. Run `updateProps -r` from the same directory to apply the change into the `clusterdb.`
   e. Restart that Unwired Server.

   Note: This server should be able to take over as the Sybase Unwired Platform primary. Sybase recommends you redeploy all your packages (using the **UPDATE** option) to make sure all the packages you expect to be available really are. All of your Sybase Unwired Platform clients should delete their UltraLite databases, and perform full synchronizations.

Setting Up Active Directory as an LDAP Security Provider

If you already have Microsoft Active Directory Server (ADS) on your network you can use this as the LDAP security provider for your production environment.

Active Directory consists of the server and the LDAP data repository. To use an existing installtion of Active Direcory with Uniwred Platform, perform these setup tasks:

Active Directory Considerations

When extending Active Directory to Unwired Platform, understand the following design implications.

Factors that impact the implementation of Active Directory as and LDAP provider in a production environment include:

- Shared identities among Sybase components – If you are using Active Directory for all authentication requests (that is, administration logins to access Sybase Control Center and application logins to access data), you must set up both Sybase Control Center and Unwired Server to use this Active Directory installation. This configuration allows users to have a shared user identity in both components. However, the user identity must be already configured both as an Unwired Platform user as well as an administrator.
- LDAP data structure and administrative control – Depending on how much control your organization wants remote administrators to have, the LDAP structure may vary. For example, an organization with 100 employees that scattered among three different offices in three different parts of world:
  - To grant remote administrators privilege for resetting passwords, unlocking user accounts, and so one, the organization may use organizational units (OUs) for each remote office and then place the user accounts from each office into the appropriate organizational unit. In this case control can still be maintained for the entire directory by a super administrator.
  - To completely delegate control of the remote offices to the remote administrator, separate domain for each office may be created.

  Because Unwired Platform requires that roles be added to the repository in specific locations, you must be sure that these roles are added in the organizational structure correctly or authentication may be problematic. In this case you may need to coordinate the implementation with one or more LDAP administrators.
- Resource and availability requirements – resource and availability plans may dictate that your organization may also maintain separate Active Directory sites for some offices. For example, the same organization with 100 distributed employees may use two physical server nodes in each remote office. One server would act as a domain controller, global catalog, DHCP, and DNS server. The other would act as a file server (possibly a DFS

server). In this case, ensure that ADS server locations are configured appropriately when you configure LDAP providers in Unwired Platform.

Adding Unwired Platform LDAP Entities

Active Directory setup for Unwired Platform use requires that you add the correct combination of users, roles, and groups.

Prerequisites

Ensure you have read the Active Directory considerations documented for this LDAP server.

1. Create a user entries for the super administrator in Active Directory in the required organizational unit (OU). If these credentials do not exactly match, authentication fails.

   Depending on the directory structure, you may need to add this users to one or more OUs:

   - If all user entries are part of the same OU, then add `supAdmin` in the common OU.
   - If users are distributed among multiple OUs, add `supAdmin` to the parent OU.

   By default, the super administrator user ID is`supAdmin` and the default password is `s3pAdmin`. However, you can change these credentials to those belonging to a real user.

   Repeat this step if you are using multiple domains or multiple Active Directory sites.
2. Create a group called `SUP Administrator` and ensure it is added at the same level as administrator user entries.
3. Assign all administration user entries to the `SUP Administrator` group.

   Only users in the SUP administration group can log into Sybase Control Center with their LDAP user entry credentials.
4. Ensure all other SUP users are added to the directory in the appropriate OU and replicate these additions to other domains or sites as required.

For example, say user01, user02, and user03 are members of the Sales OU in a domain called Europe.Mycompany.com, and user04, user05, user06, and user07 are members of the Support OU in a domain called NA.Mycompany.com. The directory would then look something like this:

```
Europe.Mycompany.com (Domain)
  Sales (OU)
    Region1 (OU)
      user01 (User)
    Region2 (OU)
      user02 (User)
    Region3 (OU)
      user03 (User)
```

```
NA.Mycompany.com (Domain)
  Support (OU)
    Toronto (OU)
      user04 (User)
    NewYork (OU)
      user05 (User)
      user06 (User)
      user07 (User)
```

When you are finished, the directory would appear something like this, with Unwired Platform entities bolded:

```
Europe.Mycompany.com (Domain)
  Sales (OU)
    supAdmin (User)
    SUP Administrator (Group)
    Region1 (OU)
      user01 (User)
    Region2 (OU)
      user02 (User)
    Region3 (OU)
      user03 (User)
```

```
NA.Mycompany.com (Domain)
  Support (OU)
    supAdmin (User)
    SUP Administrator (Group)
    Toronto (OU)
      user04 (User)
    NewYork (OU)
      user05 (User)
      user06 (User)
      user07 (User)
```

Configuring Active Directory as an LDAP Provider for Sybase Control Center

Once you have added required users to Active Directory, you can use the directory to authenticate administration login requests for Sybase Control Center.

For Sybase Control Center, you define an LDAP providers by manually editing a configuration file. Sybase recommends that you back up this file before making any changes to it.

1. Exit Sybase Control Center.
2. From a text editor, open `<SUP_installdir>\UAF-2_6\conf\csi.properties`.
3. Define an LDAP module in this file by configuring these properties.

Property	Syntax	Description or value
`Authentication-SearchBase`	`ou=<ou name>, dc=<domain name>`	The Active Directory search base for the Unwired Platform admin account. For example, `ou=Sales,dc=sybase,dc=com`.

Property	Syntax	Description or value
BindDN		The Unwired Platform admin account. For example, cn=supAdmin,ou=Sales,dc=sybase,dc=com.
BindPassword		The Password for Unwired Platform admin account.
DefaultSearchBase	ou=<ou name>, dc=<domain name>	The Active Directory search base for the Unwired Platform admin account. For example, ou=Sales,dc=sybase,dc=com.
AuthenticationFilter		Use (&(sAMAccountName={uid})(objectclass=user)).
ProviderURL	ldap://<LDAP hostname>:<LDAP port>	The Active Directory server name or IP address, and port number.
AuthenticationScope		subtree
ServerType		msad2k

Each line of the LDAP server module of the properties file must begin with "CSI.loginModule." followed by a module number. The module number in this sample is 5. The module number you assign must be unique in the properties file, and you must use the same module number in every line of the module.

When you are finished, your module definition is similar to this example:

```
===================================================
## LDAP login module for SCC
CSI.loginModule.
5.options.AuthenticationSearchBase=ou=Sales,dc=sybase,dc=com
CSI.loginModule.
5.options.BindDN=cn=supAdmin,ou=Sales,dc=sybase,dc=com
CSI.loginModule.5.options.BindPassword=mysecret
CSI.loginModule.
5.options.DefaultSearchBase=ou=Sales,dc=sybase,dc=com
CSI.loginModule.5.options.ProviderURL=ldap://mylocalhost:389
CSI.loginModule.
```

```
5.options.RoleSearchBase=ou=groups,dc=example,dc=com
CSI.loginModule.5.options.AuthenticationScope=subtree
CSI.loginModule.5.options.ServerType=msad2k
CSI.loginModule.5.options.moduleName=LDAP Login Module
CSI.loginModule.
5.provider=com.sybase.ua.services.security.ldap.LDAPWithRoleLogin
Module
CSI.loginModule.5.controlFlag=sufficient
=====================================================
```

This example specifies that Active Directory is used as the LDAP server for Sybase Control Center authentication requests.

For a complete list of available LDAP properties and values you can configure for Active Directory, see *System Administration>System Reference>Security Provider Configuration Properties>LDAP Configuration Properties*.

4. Save the file.
5. If your LDAP server's SSL certificate is signed by a nonstandard certificate authority (for example, if it is a self-signed certificate), use the **keytool** utility to configure your JVM or JDK to trust the certificate. Execute a command similar to this:

```
keytool -import -keystore <SUP_installdir>\shared\JRE-<version>
\bin\keytool\lib\security\cacerts -file
<your cert file and path> -alias ldapcert -storepass changeit
```

6. Restart Sybase Unified Agent.
7. Open Sybase Control Center and login. Active Directory now authenticates these login requests.

Configuring an Active Directory LDAP Provider for Unwired Server

Once you have added required users to Active Directory, you can use the directory to authenticate device user login requests for Unwired Server.

For Unwired Server, you define an LDAP provider by manually editing an XML configuration file. Sybase recommends that you back up this file before making any changes to it.

1. From a text editor, open `<SUP_installdir>\servers\UnwiredServer\tomcat\conf\csi\default.xml`.
2. Define an LDAP module in this file, similar to the sample below. This example specifies that Active Directory is used as the LDAP server for Unwired Server authentication requests from device users.

```
<config:authenticationProvider controlFlag="sufficient"
name="com.sybase.security.ldap.LDAPLoginModule">
<config:options name="BindDN"
value="cn=supAdmin,ou=Sales,dc=sybase,dc=com"/>
<config:options encrypted="false" name="BindPassword"
value="s3pAdmin"/>
<config:options name="AuthenticationSearchBase"
value="ou=Sales,dc=sybase,dc=com"/>
<config:options name="AuthenticationFilter"
```

```
value="(&(sAMAccountName={uid})(objectclass=user))"/>
<config:options name="DefaultSearchBase"
value="ou=Sales,dc=sybase,dc=com"/>
<config:options name="ProviderURL" value="ldap://
192.168.1.2:389"/>
<config:options name="RoleSearchBase"
value="ou=Sales,dc=sybase,dc=com"/>
<config:options name="AuthenticationScope" value="subtree"/>
<config:options name="ServerType" value="msad2k"/>
</config:authenticationProvider>
```

3. If your LDAP server's SSL certificate is signed by a nonstandard certificate authority (for example, if it is a self-signed certificate), use the **keytool** utility to configure your JVM or JDK to trust the certificate. Execute a command similar to this:

```

keytool -import -keystore <SUP_installdir>\shared\JRE-<version>
\bin\keytool\lib\security\cacerts -file
<your cert file and path> -alias ldapcert -storepass changeit
```

4. Restart all Unwired Servers in your cluster and any dependent services like Sybase Unified Agent and Relay Server as required.

LDAP Configuration Properties

Use these properties in your `csi.properties` file to control your LDAP service.

Unwired Server implements a Java LDAP provider through a common security interface used by other Sybase products like Sybase Control Center.

The Java LDAP provider consists of three provider modules, each of which is in the `com.sybase.security.ldap` Java package. This is why the syntax used between Sybase Control Center provider and Unwired Server varies.

- The LDAPLoginModule class provides the authentication services.
- LDAP role-based authorization is accomplished using the core RoleCheckAuthorizer or LDAPAuthorizer. LDAP-specific authorization provider is not necessary if LDAP authentication is employed. One can use LDAPAuthorizer for LDAP role-based authorization when non-LDAP authentication is used.
- The LDAPAttributer class provides attribution services.

When configuring modules or general server properties in Sybase Control Center, note that properties and values can vary, depending on which module or server type you configure.

Property	Default Value	Description
ServerType	None	Optional. The type of LDAP server you are connecting to: • `sunone5` -- SunOne 5.x OR iPlanet 5.x • `msad2k` -- Microsoft ActiveDirectory, Windows 2000 • `nsds4` -- Netscape Directory Server 4.x • `openldap` -- OpenLDAP Directory Server 2.x The value you choose establishes default values for these other authentication properties: • RoleFilter • UserRoleMembership • RoleMemberAttributes • AuthenticationFilter • DigestMD5Authentication • UseUserAccountControl
ProviderURL	`ldap://localhost:389`	The URL used to connect to the LDAP server. Without this URL configured, Unwired Server cannot contact your server. Use the default value if the server is: • Located on the same machine as your product that is enabled with the common security infrastructure. • Configured to use the default port (389). Note that development editions of Unwired Platform include an OpenDS LDAP server that runs on a nonstandard port of 10389. However, most LDAP servers use the standard port of 389. Otherwise, use this syntax for setting the value: `ldap://<hostname>:<port>`

Property	Default Value	Description
DefaultSearchBase	None	Tthe LDAP search base that is used if no other search base is specified for authentication, roles, attribution and self registration: 1. `dc=<domainname>,dc=<tld>` For example, a machine in sybase.com domain would have a search base of dc=sybase,dc=com. 2. `o=<company name>,c=<country code>` For example, this might be o=Sybase,c=us for a machine within the Sybase organization.
SecurityProtocol	None	The protocol to be used when connecting to the LDAP server. To use an encrypted protocol, use "ssl" instead "ldaps" in the url. **Note:** ActiveDirectory requires the SSL protocol when setting the value for the password attribute. This occurs when creating a user or updating the password of an existing user.
AuthenticationMethod	simple	The authentication method to use for all authentication requests into LDAP. Legal values are generally the same as those of the java.naming.security.authentication JNDI property. Choose one of: • simple — For clear-text password authentication. • DIGEST-MD5 — For more secure hashed password authentication. This method requires that the server use plain text password storage and only works with JRE 1.4 or later. See the*Java Sun* Web site for more information.

Property	Default Value	Description
AuthenticationFilter	For most LDAP servers: `(&(uid={uid})(objectclass=person))` or For Active Directory email lookups: `(&(userPrincipalName={uid})(objectclass=user))` `[ActiveDirectory]` For Active Directory Windows username lookups: `(&(sAMAccountName={uid})(objectclass=user))`	The filter to use when looking up the user. When performing a username based lookup, this filter is used to determine the LDAP entry that matches the supplied username. The string "{uid}" in the filter is replaced with the supplied username.
AuthenticationScope	onelevel	The authentication search scope. The supported values for this are: • `onelevel` • `subtree` If you do not specify a value or if you specify an invalid value, the default value is used.
AuthenticationSearchBase	none	The search base used to authenticate users. If this value is not specified, the LDAP DefaultSearchBase is used.

Property	Default Value	Description
BindDN	none	The user DN to bind against when building the initial LDAP connection. In many cases, this user may need read permissions on all user records. If you do not set a value, anonymous binding is used. Anonymous binding works on most servers without additional configuration. However, the LDAP attributer may also use this DN to create the users in the LDAP server. When the self-registration feature is used, this user may also need the requisite permissions to create a user record. This behavior can occur if you do not set useUserCredentialsToBind to `true`. In this case, the LDAP attributer uses this DN to update the user attributes.
BindPassword	none	BindPassword is the password for BindDN, which is used to authenticate any user. BindDN and BindPassword are used to separate the LDAP connection into units. The AuthenticationMethod property determines the bind method used for this initial connection. If you encrypt the password, append .e to the property name. For example: `CSI.loginModule.7.options.BindPassword.e=1-AAAAEgQQOLL+LpXJO8fO9T4SrQYRC9lRT1w5ePfdczQTDsP8iACk9mDAbm3F3p5a1wXWKK8+NdJuknc7w2nw5aGJlyG3xQ==`
RoleSearchBase	none	The search base used to retrieve lists of roles. If this value is not specified, the LDAP DefaultSearchBase is used.

Property	Default Value	Description
RoleFilter	For SunONE/iPlanet: `(&(objectclass=ldapsubentry) (objectclass=nsroledefinition))` For Netscape Directory Server: (`objectclass=groupofnames) (objectclass=groupofuniquename`s)) For ActiveDirectory: `(objectclass=groupofnames) (objectclass=group))`	The role search filter. This filter should, when combined with the role search base and role scope, return a complete list of roles within the LDAP server. There are several default values depending on the chosen server type. If the server type is not chosen or this property is not initialized, no roles are available.
RoleMemberAttributes	For Netsape Directory Server: member,uniquemember	The role's member attributes defines a comma-delimited list of attributes that roles may have that define a list of DN's of people who are in the role. These values are cross referenced with the active user to determine the user's role list. One example of the use of this property is when using LDAP groups as placeholders for roles. This property only has a default value when the Netscape server type is chosen.
RoleNameAttribute	cn	The attribute for retrieved roles that is the common name of the role. If this value is "dn" it is interpreted specially as the entire dn of the role as the role name.
RoleScope	onelevel	The role search scope. The supported values for this are: • `onelevel` • `subtree` If you do not specify a value or if you specify an invalid value, the default value is used.

Property	Default Value	Description
UserRoleMembershipAttributes	For iPlanet/SunONE: nsRoleDN For ActiveDirectory: memberOf For all others: none	The user's role membership attributes property is used to define an attribute that a user has that contains the DN's of all of the roles as user is a member of. These comma-delimited values are then cross-referenced with the roles retrieved in the role search base and search filter to come up with a list of user's roles.
UserFreeformRoleMembershipAttributes	None	The "freeform" role membership attribute list. Users who have attributes in this comma-delimited list are automatically granted access to roles whose names are equal to the attribute value. For example, if the value of this property is "department" and user's LDAP record has the following values for the department attribute, { "sales", "consulting" }, then the user will be granted roles whose names are "sales" and "consulting".
Referral	ignore	The behavior when a referral is encountered. The valid values are those dictated by LdapContext, for example, "follow", "ignore", "throw".
DigestMD5Authentication-Format	DN For OpenLDAP: User-name	The DIGEST-MD5 bind authentication identity format.
UseUserAccountControlAttribute	For most LDAP servers: false For ActiveDirectory: true	The UserAccountControl attribute to be used for detecting disabled user accounts, account expirations, password expirations and so on. ActiveDirectory also uses this attribute to store the above information.
controlFlag	optional	Indicates whether authentication with this login module is sufficient to allow the user to log in, or whether the user must also be authenticated with another login module. Rarely set to anything other than "sufficient" for any login module. **Note:** controlFlag is a generic login module option rather than an LDAP configuration property.

LDAP Authentication in Unwired Platform

LDAP authentication must be enabled for both Unwired Server, and Sybase Control Center.

Configuring an LDAP Provider for Unwired Server

Configure an LDAP Provider for Unwired Server to configure security features that include authentication, attribution, and authorization capabilities. Use Sybase Control Center to configure these properties.

1. Log into the Unwired Server in Sybase Control Center and click **Security** > **Configuration** .
2. Select **Authentication**, and modify the appropriate security options.

Configuring an LDAP Authentication Module

Configure an LDAP authentication module for Sybase Control Center by editing the security properties file to point to the correct LDAP server.

1. Open the `<SCC-install-dir>\conf\csi.properties` file.

   The location of this file indicates that the provider you are editing is intended for use with Sybase Control Center only.
2. Uncomment the LDAP module in the properties file by removing the # symbol at the beginning of each line (or, if necessary, add an LDAP module to the file). The sample module below specifies the LDAP server that will provide user authentication.

   The sample module shows the properties used for an OpenDS LDAP server. See the example at the end for values that work for ActiveDirectory. Configuration properties you can use in the LDAP module are described in a subtopic.

   Each line of the LDAP server module of the properties file must begin with "CSI.loginModule." followed by a module number. (The module number in this sample is 7.) The module number you assign must be unique in the properties file, and you must use the same module number in every line of the module.

   ```
   CSI.loginModule.
   7.options.AuthenticationSearchBase=ou=users,dc=example,dc=com
   CSI.loginModule.7.options.BindDN=cn=Directory Manager
   CSI.loginModule.7.options.BindPassword=secret
   CSI.loginModule.7.options.DefaultSearchBase=dc=example,dc=com
   CSI.loginModule.7.options.ProviderURL=ldap://localhost:10389
   CSI.loginModule.
   7.options.RoleSearchBase=ou=groups,dc=example,dc=com
   CSI.loginModule.7.options.ServerType=openldap
   CSI.loginModule.7.options.moduleName=LDAP Login Module
   CSI.loginModule.7.controlFlag=sufficient
   ```

```
CSI.loginModule.
7.provider=com.sybase.ua.services.security.ldap.LDAPLoginModule
```

Note: Change the values of bolded lines only.

3. Save the file.
4. If your LDAP server's SSL certificate is signed by a nonstandard certificate authority (for example, if it is a self-signed certificate), use the **keytool** utility to configure your JVM or JDK to trust the certificate. Execute a command similar to this:

```
keytool -import -keystore <sybase-dir>/shared/JRE-6_0_6/bin/
keytool/lib/security/cacerts -file
<your cert file and path> -alias ldapcert -storepass changeit
```

LDAP configuration values for ActiveDirectory

For an ActiveDirectory server, use these values for configuration properties in your LDAP login module:

```
ServerType: msad2K
DefaultSearchBase: dc=<domainname>,dc=<tld> or o=<company
name>,c=<country code>
                E.g. dc=sybase,dc=com or o=Sybase,c=us
ProviderUrl: ldaps://<hostname>:<port>
                E.g.:  ldaps://myserver:636
AuthenticationFilter: (&(userPrincipalName={uid})
(objectclass=user))
BindDN: <User with read capability for all users>
BindPassword: <Password for BindDN user>
RoleFilter: (|(objectclass=groupofnames) (objectclass=group))
controlFlag: sufficient
```

Next

There are two additional steps:

- Set up roles and passwords for LDAP
- Map Sybase Control Center role to LDAP groups

Setting Up Roles and Passwords

Set the initial user roles and passwords required for Sybase Control Center to authenticate through an LDAP server.

Prerequisites

Configure an LDAP authentication module.

1. Open the `<SCC-install-dir>\conf\roles-map.xml` file and add an LDAP login module.

   Insert an LDAP login module similar to this at the end of the security-modules portion of the file, just before `</security-modules>`:

```
    <module name="LDAP Login Module">
      <role-mapping modRole="sybase"
uafRole="uaAnonymous,uaPluginAdmin,sccUserRole" />
      <role-mapping modRole="administrators"
uafRole="uaAnonymous,sccAdminRole" />
    </module>
```

2. Ensure that the roles defined in the LDAP repository match the roles defined in `roles-map.xml`.
3. In the `<SCC-install-dir>\conf\csi.properties` file, set the BindPassword and ProviderURL properties with values used in your deployment.

   Sybase recommends that you encrypt sensitive values before saving them in `csi.properties`.

Next

Map Sybase Control Center roles to LDAP groups.

Encrypting a Password

Use the **passencrypt** utility to encrypt passwords and other values that must be kept secure while stored in text files.

You can safely store an encrypted password in a properties file. Enter the password in clear text (unencrypted) when you execute **passencrypt** and when you use the password to log in.

passencrypt, which is located in the Sybase Control Center `bin` directory, uses the DES encryption algorithm.

1. Open a command window and change to the `bin` directory:

   Windows: `cd <SCC-install-directory>\bin`

   UNIX: `cd <SCC-install-directory>/bin`
2. Encrypt a password:

   ```
   passencrypt -text <new_password>
   ```

   The passencrypt utility encrypts the password you enter and displays the password in encrypted form.
3. Copy the encrypted password.
4. Paste the encrypted password where needed.
5. When you have encrypted all the passwords you need, immediately close the command window—it displays passwords in clear text.

Lightweight Poller in Unwired Platform

You can configure lightweight polling intervals for multiple client programs in Unwired Server, or for a single client in the client side program.

Configuring Lightweight Polling Interval

You can change the lightweight polling configuration on Unwired Server for multiple device clients, or in the client-side program for a single client.

1. To change the lightweight polling interval for multiple clients using **dbisql** on Unwired Server:

   a) Navigate to `%SUP%\Servers\UnwiredServer\SQLAnywhere11\BIN32\`, and start the **dbisql** application.

   b) Choose ODBC Data Source Name for the connection, and supply the data source name `uaml_<servername>`.

   c) Call `ml_add_property('SIS', 'NOTIFIER(UALIGHTWEIGHT)', 'poll_every", 180)` and execute it.

   This command example specifies that the server initiated synchronization polling occurs every 180 seconds. You can set the **poll_every** interval to S, M, and H for units of seconds, minutes, and hours. You can also combine units, as in 1H 30M 10S. If no unit is specified, the interval is in seconds. The **poll_every** parameter default is 30 seconds.

   Note: This approach applies the polling interval to all the clients that have not specified this interval.

2. To set the polling interval in the client side program for a single client:

   a) In your program, look for where you specify the polling option right after: `...;poll_notifier=UALIGHTWEIGHT;poll_key....`

   b) Change the polling option, for example: `....;poll_notifier=UALIGHTWEIGHT;poll_every=180;poll_key=.....`

   Note:

   - This approach applies the polling interval only to this client.
   - For clients, the **poll_every** property unit should typically be set to seconds (not minutes or hours or a combination).
   - Do not set the client **poll_every** value to a shorter time interval than the server value. This does not result in receiving push notifications any faster, and can cause the client to see the same notification multiple times, causing multiple useless synchronizations. Only set this value on the client if for some reason (trying to save battery life?) you do

not want to see notifications as frequently as the server checks for pending notifications.

- The Lightweight Poller listener on the client can be turned on/off if you do not want to receive notifications during a specific period; changing the polling interval is typically not what a customer would want.

Troubleshooting

Provides new or updated troubleshooting topics.

Troubleshooting SQLE_PRIMARY_KEY_NOT_UNIQUE Error

Problem: Encountered an SQLE_PRIMARY_KEY_NOT_UNIQUE error.

Solution: Possible causes:

- The Primary Key generated in the client is not unique.

  In this case, try using a better Primary Key generation method, such as GUID.
- Multiple clients use only one Sybase Unwired Platform account to connect to Unwired Server.

  In this case, be sure to use different Sybase Unwired Platform client accounts to connect to Unwired Server.

Troubleshooting Device Tracking in a Cluster

Problem: The server logs for primary and secondary servers list several -10117 stream errors.

Solution: The Unwired Server consolidated database has issues with tracking devices and light weight polling (LWP) in a clustered environment. You must disable device tracking when LWP is used by reconfiguring all servers in your cluster.

Obtaining Help and Additional Information

Use the Sybase Getting Started CD, SyBooks™ Online or CD or download, and online help, to learn more about this product release.

- The Getting Started CD (or download) – contains release bulletins and installation guides in PDF format, and also contains other documents or updated information not included on the SyBooks CD.
- The SyBooks CD (or download) – contains product manuals. The Eclipse-based SyBooks browser allows you to access the manuals in an HTML-based format. Some documentation is provided in PDF format, which you can access through the PDF directory on the SyBooks CD. See the *SyBooks Installation Guide* on the Getting Started CD, or the *README.txt* file on the SyBooks CD for instructions about installing and starting SyBooks.
- SyBooks Online at *http://sybooks.sybase.com/* – is an online version of SyBooks that you can access using a standard Web browser. You can browse documents online, or download them as PDFs. In addition to product manuals, the Web site also has links to EBFs/ Maintenance, Technical Documents, Case Management, Solved Cases, newsgroups, and other resources.
- Online help in the product, if available.

To read or print PDF documents, you need Adobe Acrobat Reader, which is available as a free download from the *Adobe* Web site.

Note: A more recent release bulletin, with critical product or document information added after the product release, may be available from SyBooks Online.

Technical Support

Get support for Sybase products.

If your organization has purchased a support contract for this product, then one or more of your colleagues is designated as an authorized support contact. If you have any questions, or if you need assistance during the installation process, ask a designated person to contact Sybase Technical Support or the Sybase subsidiary in your area.

Sybase Product and Component Certifications

Certification reports verify Sybase product performance on a particular platform.

To find the latest information about certifications:

- For partner product certifications, go to *http://www.sybase.com/detail_list?id=9784*
- For platform certifications, go to *http://certification.sybase.com/ucr/search.do*

Creating a MySybase Profile

MySybase is a free service that allows you to create a personalized view of Sybase Web pages.

1. Go to *http://www.sybase.com/mysybase*.
2. Click **Register Now**.

Accessibility Features

Accessibility ensures access to electronic information for all users, including those with disabilities.

Documentation for Sybase products is available in an HTML version that is designed for accessibility.

Vision impaired users can navigate through the online document with an adaptive technology such as a screen reader, or view it with a screen enlarger.

Sybase HTML documentation has been tested for compliance with accessibility requirements of Section 508 of the U.S Rehabilitation Act. Documents that comply with Section 508 generally also meet non-U.S. accessibility guidelines, such as the World Wide Web Consortium (W3C) guidelines for Web sites.

Note: You may need to configure your accessibility tool for optimal use. Some screen readers pronounce text based on its case; for example, they pronounce ALL UPPERCASE TEXT as initials, and MixedCase Text as words. You might find it helpful to configure your tool to announce syntax conventions. Consult the documentation for your tool.

For information about how Sybase supports accessibility, see the Sybase Accessibility site: *http://www.sybase.com/products/accessibility*. The site includes links to information about Section 508 and W3C standards.

You may find additional information about accessibility features in the product documentation.

Index