New Features
Mainframe Connect™ 15.0

Document ID: DC00182-01-1500-03

Last revised: August 2008

This document alphabetically lists and describes new features available for Mainframe Connect™ 15.0, including the most current release of features in ESD #2, where noted.

ASE ODBC Driver by Sybase

Note For DirectConnect™ for z/OS Option only.

Sybase® has replaced the third-party client-side DirectConnect ODBC driver with the Adaptive Server® Enterprise (ASE) ODBC Driver by Sybase.

One driver can now be used for connecting to ASE and Mainframe Connect. The Sybase driver is engineered for full, seamless, high-performance support of ASE and Mainframe Connect.

For migration information, see “Appendix C: Migrating to the ODBC Driver by Sybase” in the Mainframe Connect DirectConnect for z/OS *Installation Guide*.

For more information about this driver, see the Adaptive Server Enterprise ODBC Driver by Sybase *Users Guide*, which is part of the Software Developer’s Kit documentation set.

Extended encryption login

Note For all Server Options only.

(ESD #2) The OCS API provides the ability to support the public key encrypted password handshake between the Open Client™ and the Open Server™, making this functionality available for implementation in Enterprise Connect Data Access products.

Following is the process that occurs when any Open Client-based application (such as isql) issues a public key encrypted login request to an Open Server application (such as ECDA and the DirectConnect server):

1 The server sends a public key to the client, and waits for the client to send back the encrypted password.

2 When the DirectConnect server receives the encrypted password, it decrypts the password to plain text.

3 The DirectConnect server sends the plain text password to a remote server or database for authentication.

To request an extended encrypted login, use the isql `-X` command. In the following example, “testsrv” is a DirectConnect service name, “tester” is a user name, “sybase” is a password, and `-X` is the option for the encrypted login request:

```
isql -Stestsrv -Utester -Psybase -X
```

IBM CICS sockets interface implementation

Note For Client Option for CICS and Server Option for CICS only.

The IBM CICS sockets interface is implemented in the Client Option for CICS and the Server Option for CICS. This implementation eliminates compatibility issues and provides these advantages:

- An individual listener can handle a socket pool of up to 1000 sockets.
- A new listener can be added without requiring system intervention.
- An individual listener can be used as both gateway and gateway-less.

For more information, see "Appendix C: Setting Up the CICS Sockets Interface" in these guides:

- Mainframe Connect Client Option for CICS *Installation and Administration Guide*
- Mainframe Connect Server Option for CICS *Installation and Administration Guide*

License keys for multiple CPUs

Note For all Mainframe options except DirectConnect for z/OS Option.

(ESD #2) You can use a single SYGWXCPH customization module to accommodate all of your licensing information across multiple CPUs and Mainframe Connect options.

License management with SySAM 2.0

Note For DirectConnect for z/OS Option only.

Mainframe Connect 15.0 DirectConnect for z/OS Option now provides Sybase Software Asset Manager (SySAM) 2.0. This upgrade performs the following security-related tasks:

- Verifies that a valid license exists for the software being used. If a license is not valid, the service does not start and the DirectConnect server logs the license error message.
- Allows Sybase customers with support contracts to access every Emergency Bug Fix (EBF) published before the end of their contract date.

Note If you download Mainframe Connect DirectConnect for z/OS Option 15.0 software without a license, SySAM 2.0 allows a 30-day grace period for you to obtain a valid license through the Sybase Product Download Center on the Web.

For more information about SySAM 2.0, see:

- Mainframe Connect 15.0 DirectConnect for z/OS Option *Installation Guide*
- Sybase Software Asset Management 2.0 *Users Guide*

Listener options

Note All options in this section are for Server Option for CICS only.

(ESD #2) The following new listener customization options were added to the SYBTPSEC configuration module.

Detecting the non-start of a transaction

The new SYBTPSEC parameter called STRTCHK allows recovering and recycling of unused TCP sockets, thus preventing sockets from "hanging" and causing problems with client applications.

The listener handles an incoming request to start an RPC transaction by first starting a handler transaction designated for a gateway or gateway-less mode. In turn, the handler starts the application transaction.

In some situations, the handler transaction will be unable to start, such as when the RACF "APPL" class is being used. CICS provides no way for the listener to detect the non-start of the transaction. However, when activated, the STRTCHK parameter resolves such situations: It specifies a time interval in seconds that the listener can use to compare to the time elapsed since a socket is made available for a new application transaction. If a socket has not been taken in the specified time, the listener recovers the socket, sends an error message, and closes the socket.

Because the STRTCHK feature decreases the efficiency of the listener, it may be left inactive if not needed. A value of -1 (the default) makes the STRTCHK feature inactive.

Mixed-case passwords

In Mainframe Connect

Versions 1.7 and later of z/OS support mixed-case passwords with the incoming login requests. This feature can be used in both two-tier and three-tier configurations with Mainframe Connect Server Option for CICS and DirectConnect for z/OS Option versions 15.0 ESD #2 or later.

The SYBTPSEC parameter MIXEDCASEPW controls the use of mixed-case passwords on the Server Option side. A value of N (the default) indicates that the listener will convert all incoming passwords to uppercase. A value of Y will leave the passwords in mixed case.

Note Do not set MIXEDCASEPW=Y unless the z/OS Security Manager is set to use mixed-case passwords.

In DirectConnect for z/OS Option

In the three-tier environment, the DirectConnect for z/OS Option uses the UpperCasePassword configuration property to set the case:

- Yes – (the default) converts the password to uppercase.

- No – passes the password as entered—whether uppercase, lowercase, or mixed case. In fact, you must set it to No to allow lowercase or mixed case.

The UpperCasePassword configuration property is found in the Target Interaction section, for DB2 Access Service only.

TCP options

There are three new SYBTPSEC parameters to control data transfer flow: SO_RCVBUF, SO_SNDBUF, and TCP_NODELAY.

- SO_RCVBUF overrides the TCP/IP system default for the maximum size of the *receive* buffer. A value of -1 (the default) indicates that the system default should be used.
- SO_SNDBUF overrides the TCP/IP system default for the maximum size of the *send* buffer. A value of -1 (the default) indicates that the system default should be used.
- TCP_NODELAY overrides the TCP/IP system default for the Nagel Algorithm. A value of 1 disables the feature, and a value of 0 enables it. A value of -1 indicates that the system default should be used.

The SO_RCVBUF and SO_SNDBUF options control the physical packet size for the TCP/IP transmissions. Optimum packet sizes depend on the amount of data received or transmitted by an individual transaction. TCP/IP data transmission can also be controlled by the Nagel Algorithm option, which attempts to reduce the amount of data collisions by adding an arbitrary wait between receives and sends.

SO_RCVBUF, SO_SNDBUF, and TCP_NODELAY settings override the z/OS system defaults for any connections accepted through a particular listener.

Trace parameter

The SYBTPSEC parameter called TRACE can control the trace messages issued by the listener:

- A value of Y turns on the listener trace messages.
- A value of N (the default) turns them off.

Login information conversion

Note For all Server Options only.

(ESD #2) Server Options can now convert the incoming ASCII client login information to either a 037 or 500 EBCDIC code page when USEIBMUNICODE=Y. The login conversion is controlled by the CHARSETSRV parameter of the SYGWMCST macro in the SYGWXCPH customization module.

The following information indicates how the login record is converted.

- If the CHARSETSRV parameter is set to CCSID=037, then the login information is converted to code page (CCSID) 037. For example, you can use CHARSETSRV=ibmebcdic or CHARSETSRV=cp37 to set the server default character set to 037.

  In all other cases, when the CHARSETSRV parameter is set to a value that corresponds to a different CCSID (such as utf8 or iso_1), the login information is converted to the default code page of 500.

- All character set names used as values for the CHARSETSRV parameter must be defined as entries in the SYGWMCXL macro. “System” entries, such as “ibmebcdic” or “utf8,” need no additional definition.

- All ASCII single-byte “system” character sets (ascii_8, iso_1, cp850, cp437, roman8, and mac) are supported for login conversion. For all other login character sets (single-byte, double-byte, or utf8), the client login information is converted as if it were sent in the default iso_1 character set.

- The TDGETUSR API returns the client login information converted to code page 037 or 500, depending on the CHARSETSRV parameter specification.

RPC configuration parameters

Note For all Server Options only.

(ESD #2) Two new parameters, RPCPROGCCSID and RPCDATACCSID, have been added to the SYGWMCST configuration macro in the SYGWXCPH customization module. They can be used only if USEIBMUNICODE=Y. Instead of coding TDPROPS SET APIs in each Remote Procedure Call (RPC) application program, you can set the default Program and Data Coded Character Set Identifiers (CCSIDs) for RPCs across the region.

When using these parameters, consider the following:

- You must use the new SYGWMCST macro to reassemble the customization module SYGWXCPH that will be used with this and later EBFs.
- Set through TDPROPS API, the Program and Data CCSID properties are mainly intended for visualizing mainframe data by the server applications. In this case, they are usually set to an EBCDIC CCSID. However, they can also be useful in some internal data transformations, in which case they are not limited in value to EBCDIC CCSIDs.
- The RPCPROGCCSID and RPCDATACCSID parameters should be set to EBCDIC CCSIDs only. Because the parameter values are not checked against a predefined list of valid CCSIDs, you need to verify that the CCSID is valid.
- RPCPROGCCSID controls the conversion of data between the server and server application and has a default of 500. You should set it to an EBCDIC CCSID—ideally, to the one that is used internally by the z/OS subsystems. (For example, it can be the value of the SCCSID generation parameter in DB2.)
- RPCDATACCSID controls the conversion for metadata and has a default of 500. It is usually set to the value of RPCPROGCCSID.
- The new parameters can be used in place of, or together with, TDPROPS SET APIs. If needed, the TDS_PROG_CCSID and TDS_DATA_CCSID properties can be still used by the server application to dynamically change Program or Data CCSIDs.
- All CCSIDs used to set Program and Data CCSID values must be described through the SYGWMCXL macro in the SYGWXCPH module. For these CCSID entries, there is no requirement to the name specified in the CHARSET parameter of the macro.

Secure Sockets Layer (SSL) implementation

Note For Client Option for CICS and Server Option for CICS only.

Client Option for CICS and Server Option for CICS provide Secure Sockets Layer (SSL) session-based security. They implement the IBM Application Transparent - Transport Layer Security (AT-TLS) option. AT-TLS provides application-transparent, SSL-secured connections for both the client and server. SSL is the standard for securing the transmission of sensitive information (such as credit card numbers, stock trades, and banking transactions) over the Internet.

Note Client Option for CICS and Server Option for CICS work with Secure Sockets Layer (SSL) in gateway-less mode.

SSL provides these features:

- Authentication for clients and servers, with practical emphasis on the server
- Data confidentiality (encryption)
- Verification that a transaction was sent by the client and that the identical transaction was received by the server

To provide efficient authentication and encryption, SSL combines private-key and public-key technologies. For more information, see “Appendix D: Setting Up Secure Sockets Layer Protocol” in these guides:

- Mainframe Connect Client Option for CICS *Installation and Administration Guide*
- Mainframe Connect Server Option for CICS *Installation and Administration Guide*

Unicode On Demand feature from IBM

Note For all Mainframe Connect Server Options and Client Options only.

(ESD #2) Beginning with z/OS 1.7, IBM introduced a new feature called Unicode On Demand for its Unicode Conversion Services. This feature makes creating and maintaining a conversion image easier by automatically adding supported conversion entries when they are needed and not found in the active image. Both IBM default or customized conversion images can be used. For details, see IBM “Support for Unicode: Using Conversion Services” (SA22-7649). You may need to apply some IBM Unicode Services PTFs before using the Unicode on Demand feature. Check with IBM for the list of PTFs to be applied to your z/OS system.

The Unicode On Demand feature significantly reduces the amount of work and errors when you are customizing conversions for Mainframe Connect products. You no longer need to duplicate conversion image entries for use with both DB2 and Mainframe Connect. However, be sure to define all character sets used with your installation in the SYGWMCXL macro in the SYGWXCPH customization module.