

IBM i
7.4

Connecting to IBM i
IBM i Access Client Solutions - Windows
Application Package: Administration



Note

Before using this information and the product it supports, read the information in [“Notices” on page 39.](#)

This document may contain references to Licensed Internal Code. Licensed Internal Code is Machine Code and is licensed to you under the terms of the IBM License Agreement for Machine Code.

© **Copyright International Business Machines Corporation 2013, 2021.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Administration.....	1
What's new.....	1
PDF file for Windows Application Package: Administration.....	1
ODBC administration.....	2
Overview of the IBM i Access ODBC driver.....	2
Set up your system for the IBM i Access ODBC driver.....	3
Adding the local system to the RDB directory.....	3
Specify the ODBC data source.....	4
Use independent ASPs through ODBC.....	4
IBM i Access ODBC security.....	5
Common ODBC strategies that are not secure.....	5
ODBC program security strategies.....	6
Related information for ODBC security.....	7
Troubleshoot ODBC.....	7
ODBC diagnostic and performance tools.....	7
Client-side ODBC diagnostic and performance tools.....	8
Server-side ODBC diagnostic and performance tools.....	8
Collecting an ODBC Trace (SQL.LOG).....	10
IBM i Access ODBC error messages.....	10
Troubleshoot the IBM i connection.....	11
Checking the server status.....	12
Verifying that subsystems are active.....	12
Verifying that prestart jobs are running.....	12
Additional TCP/IP considerations.....	13
Common ODBC errors.....	13
SQL errors.....	14
Stored procedure errors.....	16
ODBC incorrect output and unpredictable errors.....	17
Gather information for IBM Support.....	17
Restrict users with policies and application administration.....	18
Overview of IBM i Access policies.....	19
Types and scopes of policies.....	20
Set up your system to use policies.....	21
Configure a system for using IBM i Access Client Solutions policies.....	21
Create policy files.....	21
Microsoft System Policy Editor.....	21
Create IBM i Access policy templates.....	22
Create and update policy files.....	22
IBM i Access policy list.....	23
Policies by function.....	23
Policies by function: .NET Data provider.....	24
Policies by function: ActiveX automation objects.....	24
Policies by function: Communication.....	25
Policies by function: License management.....	29
Policies by function: National Language Support.....	29
Policies by function: ODBC.....	31
Policies by function: OLE DB.....	32
Policies by function: Passwords.....	33
Policies by function: PC Commands.....	33
Policies by template.....	35
Introducing Caecfg.adm.....	35

Caerestr.adm: IBM i Access Runtime Restrictions.....	36
Config.adm: IBM i Access mandated connections.....	36
SYSNAME.adm: Per-system policies.....	37
Transport Layer Security (TLS) administration.....	37

Notices.....39

Programming interface information.....	40
Trademarks.....	40
Terms and conditions.....	41

Windows Application Package: Administration

Use this topic to administer Windows Application Package in your client/server environment.

This information assumes that you are familiar with the Windows Application Package, and have installed it on your system.

Note: By using the code examples, you agree to the terms of the [“Code license and disclaimer information”](#) on page 37.

What's new

Read about new or significantly changed information relating to the administration of Windows Application Package for this release.

Windows Application Package is an optional package that is part of IBM® i Access Client Solutions. It contains the middleware, database providers, and programming APIs that were previously part of the 7.1 version of the IBM i Access for Windows product.



Other information

After installing Windows Application Package, use this path from the IBM i Access Client Solutions folder to access the User's Guide: **Start > Programs > IBM i Access Client Solutions > User's Guide**.

See the Programmer's Toolkit for technologies that you can use for database access.

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

To find other information about what's new or changed this release, see the [Memo to Users](#).

Related information

[.NET programming](#)

[OLE DB programming](#)

PDF file for Windows Application Package: Administration

You can view and print a PDF file of this information.

To view or download the PDF version of this document, select [IBM i Access Client Solutions - Windows Application Package: Administration](#).

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click **Save Target As** if you are using Internet Explorer. Click **Save Link As** if you are using Netscape Communicator.
3. Navigate to the directory in which you would like to save the PDF.
4. Click **Save**.

ODBC administration

Windows Application Package includes an ODBC driver that allows your applications convenient access to Db2® for IBM i databases in your network. This topic provides an overview of ODBC, instructions for setting up the driver, and a troubleshooting guide.

Note: For information and considerations when working with the ODBC APIs, refer to ODBC programming.

Open Database Connectivity (ODBC) is a Microsoft standard for providing access to databases. It has a well-defined set of application programming interfaces (APIs) that use Structured Query Language (SQL) to access databases.

For help with integrating ODBC support into your applications, refer to the IBM i Access ODBC programming, where you can get information on the following subtopics:

- ODBC API list
- ODBC API implementation
- Programming examples
- ODBC performance

Related information

[IBM i Access ODBC](#)

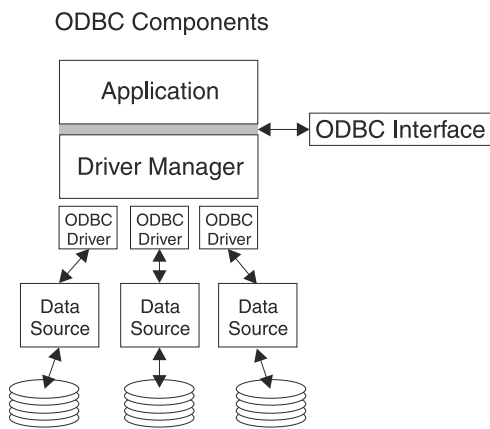
Overview of the IBM i Access ODBC driver

Provides a general description of ODBC, and how you can use it with IBM i Access Client Solutions.

The IBM i Access ODBC driver is a collection of application programming interfaces (APIs) for accessing database information using Structured Query Language (SQL). Using the IBM i Access ODBC driver allows applications to access different databases using the same source code, and to handle data in the format most convenient for those applications. ODBC provides an application developer a relatively simple model for creating portable applications or components that must deal with multiple DBMSs.

The ODBC architecture involves an application, driver manager, ODBC driver, and a data source. IBM i Access provides both a 32-bit and a 64-bit ODBC driver. ODBC applications will automatically use the appropriate driver that corresponds to the bit version the application was compiled for.

For an application to use ODBC you must set up a data source. You can use the ODBC Administrator to set up a data source. There are two versions of the ODBC Administrator, 32-bit and 64-bit, that can be accessed from the IBM i Access Client Solutions folder. When using ODBC Administrator, you have the option to setup three different types of data sources: User, System, and File data sources. For more information about how data sources are configured, see 64-bit ODBC Support, in the IBM i Access Client Solutions' User's Guide.



RV3W364-1

Application. Performs processing and calls ODBC functions to run SQL statements.

Driver manager. Processes ODBC function calls and forwards the requests to the driver.

Driver. Processes ODBC function calls, submits SQL requests to a specific data source, and returns results to the application.

Data source. To use a data source you have to create a Data Source Name (DSN). A DSN contains information about how to access the DBMS. You can specify any of the following DSNs:

- **User DSN:** These data sources are local to a computer and may only be available to the user who created them. This information is stored in the registry.
- **System DSN:** These data sources are local to a computer, rather than dedicated to a user. The system, or any user having privileges, can use a data source set up with a system DSN. This information is stored in the registry.

Note: On Windows, System DSNs are split between 32-bit and 64-bit applications. System DSNs configured using the 32-bit ODBC Administrator are available only to 32-bit applications, and those configured using the 64-bit ODBC Administrator are available only to 64-bit applications.

- **File DSN:** These are file-based data sources that may be shared between all users that have the same drivers installed so that they have access to the database. These data sources do not need to be dedicated to a user, or to be local to a computer.

For more information about ODBC, refer to the Microsoft Web site.

Related tasks

[Specify the ODBC data source](#)

You must specify the IBM i Access ODBC data source for your application to access and manipulate data.

Set up your system for the IBM i Access ODBC driver

Presents procedures for setting up your environment to support the ODBC driver. For help configuring the ODBC driver, start the ODBC administration program from the IBM i Access Client Solutions program group, and refer to the online help.

See the ODBC data source topic to configure your ODBC driver. Complete your configuration by following the steps identified by the topic adding the local system to the RDB directory.

Using independent ASPs through ODBC is optional. See independent ASPs for more information about configuring this support.

For help configuring options for a specific data source, start the ODBC Administrator from the IBM i Access Client Solutions program group, select the data source to configure, and refer to the online help.

Related information

[MDAC](#)

Adding the local system to the RDB directory

To use IBM i Access ODBC, OLE DB, or the .NET Data Provider, the local system name must appear in the RDB directory.

To add the local system to the RDB directory:

1. From the command prompt run the CL command, Add Relational Database Directory Entry (ADDRDBDIRE).
2. When the ADDRDBDIRE screen prompts you for values, enter the name of the system as the Relational Database parameter.
3. Enter *LOCAL as the Remote Location parameter.

There may be additional steps to get the database (RDB) name set if your application accesses data residing in an independent ASPs. The RDB name corresponds with a namespace that consists of the system ASP and any user ASPs or linked ASP group associated with the system ASP. For more information about independent ASPs, see Disk management.

Note: ODBC allows the use of fully qualified names in the format of [catalog name].[schema name].identifier (for example, where identifier is the name of a table, view, or procedure). In the Db2 for IBM i implementation of SQL this corresponds to [RDB name].[collection name].identifier.

Related information

[Disk management](#)

Specify the ODBC data source

You must specify the IBM i Access ODBC data source for your application to access and manipulate data.

To specify the data source:

1. Start the ODBC Administration program from the IBM i Access Client Solutions program group.
2. Select the appropriate tab for the type of data source. See Overview of the IBM i Access ODBC driver for more information.
3. Select an existing data source from the list, or select **Add** to create new one. If you are using an existing data source, click **Configure** and proceed to step “5” on page 4.
4. Select the IBM i Access ODBC driver for your data source, and click **Finish**.

Note: You might notice the Client Access ODBC Driver (32-bit) or iSeries Access ODBC Driver names in the list of drivers. These names are listed so that data sources created with previous releases of Client Access will continue to work. All names point you to the same ODBC driver. Although you can use the previous names, in future releases the previous names will be removed.

5. Specify desired options using the IBM i Access ODBC setup dialog. For a description of the controls, refer to the data source's online help by using the F1 key or the Help button.

Note: The data source name can include up to 32 characters, must start with an alphabetic character, and cannot include the following characters:

Unallowed data-source characters	
Left bracket ([)	Question mark (?)
Right bracket (])	Asterisk (*)
Left brace ({)	Equal sign (=)
Right brace (})	Exclamation point (!)
Left parenthesis ((At sign (@)
Right parenthesis ())	Semicolon (;)

Related concepts

[Overview of the IBM i Access ODBC driver](#)

Provides a general description of ODBC, and how you can use it with IBM i Access Client Solutions.

Related tasks

[Use independent ASPs through ODBC](#)

Find steps to use when connecting to an independent ASP through IBM i Access ODBC.

Related information

[Disk management](#)

Use independent ASPs through ODBC

Find steps to use when connecting to an independent ASP through IBM i Access ODBC.

To use **independent ASPs** through ODBC, configure your ODBC DSN and do the following:

1. Select the **Server** tab.
2. Click on "Override default database with the following:".

3. Specify the **RDB name** that corresponds with the **Independent ASP** to connect.
4. If no RDB name is specified, the default RDB name is determined from the job description of the user profile that is making the ODBC connection. By default, the driver uses the setting of the user profile for the user making the ODBC connection.

For more information about **independent ASPs**, see Disk management content topics.

Related tasks

[Specify the ODBC data source](#)

You must specify the IBM i Access ODBC data source for your application to access and manipulate data.

Related information

[Disk management](#)

IBM i Access ODBC security

Highlights a few security considerations when working with IBM i Access ODBC and provides references to more detailed security instructions.

The following information is not intended to be a comprehensive guide to security strategies on the IBM i platform or with IBM i Access Client Solutions. It simply provides an overview of security strategies that impact IBM i Access Client Solutions and ODBC users. For more in-depth information, see the IBM Security - Reference.

Related information

[Security reference](#)

Common ODBC strategies that are not secure

Avoid some common IBM i Access ODBC security techniques to ensure your environment is secure.

Sometimes system administrators attempt to secure access to the data, rather than securing the data itself. This is extremely risky, as it requires that administrators understand ALL of the methods by which users can access data. Some common ODBC security techniques to avoid are:

Command line security

This may be useful for a character-based interface or for 5250 emulation-based applications. However, this method assumes that if you prevent users from entering commands in a 5250 emulation session, they can access data only through the programs and menus that the system administrator provides to them. Therefore, command line security is never truly secure. The use of IBM i Access policies and Application Administration improve security, and the use of object level authority improves it even more.

Potentially, IBM i Access policies can restrict ODBC access to a particular data source that might be read only. Application Administration in IBM Navigator for i can prevent ODBC access.

For additional information, see the IBM Security - Reference.

User exit programs

A user exit program allows the system administrator to secure an IBM-supplied host server program. The IBM i Access ODBC driver uses the Database host server: exit points QIBM_QZDA_INIT; QIBM_QZDA_NDBx; and QIBM_QZDA_SQLx. Some ODBC drivers and IBM i Access data access methods (such as OLE DB) may use other host servers.

Journals

Journaling often is used with client/server applications to provide commitment control. The journals contain detailed information on every update made to a file that is being journaled. The journal information can be formatted and queried to return specific information, including:

- The user profiles that updated the file

- The records that were updated
- The type of update

Journaling also allows user-defined journal entries. When used with a user exit program or trigger, this offers a relatively low-overhead method of maintaining user-defined audits. For further information, see the Backup and Recovery.

Data Source Name (DSN) restrictions

The IBM i Access ODBC driver supports a DSN setting to give read-only access to the database. The IBM i Access ODBC driver supports a read-only and a read-call data source setting. Although not secure, these settings can assist in preventing inadvertent delete and update operations.

Related information

[Security reference](#)

[Backup and recovery](#)

ODBC program security strategies

Consider the following IBM i Access ODBC program security strategies.

Restricting program access to the database

System administrators often need to limit access to particular files, to a certain program, or to sets of programs. A programmer using the character-based interface would set restrictions by using program-adopted authority. A similar method can be used with ODBC.

Stored procedures allow ODBC programmers to implement program-adopted authority. The programmer may not want users to be able to manipulate database files by using desktop applications such as Microsoft Access or Lotus® 1-2-3. Instead, the programmer may want to limit database updates to only the programmer's application. To implement this, user access to the database must be restricted with object-level security or with user exit programs. The application must be written to send data requests to the stored procedure and have the stored procedure update the database.

Restrict CPU utilization by user

ODBC has greatly eased the accessibility of Db2 for i data. One negative impact has been that users may accidentally create very CPU-intensive queries without realizing it. ODBC runs at an interactive job priority and this can severely affect system performance. The system supports a **query governor**. ODBC can invoke the query governor (for example, through the PC application) in a stored procedure call. Or the ODBC APIs can invoke the governor by way of the query time-out parameter. Also, a user exit program can force the query governor on the ODBC job. The time limit is specified on the QRYTIMLMT parameter of the CHGQRYA CL command. The query options file (QAQQINI) can also be used to set the value.

The *SQL Reference* book contains additional information. View an HTML online version of the book, or print a PDF version, from the Db2 for i SQL Reference.

Also see Host server administration for more information.

Audit logs (monitoring security)

Several logs can be used to monitor security. QHST, the History Log, contains messages that relate to security changes that are made to the system. For detailed monitoring of security-related functions, QAUDJRN can be enabled. The *SECURITY value logs the following functions:

- Changes to object authority
- Create, change, delete, display, and restore operations of user profiles
- Changes to object ownership
- Changes to programs (CHGPGM) that adopt the owner's profile

- Changes to system values and network attributes
- Changes to subsystem routing
- When the QSECOFR password is reset to the shipped value by DST
- When the DST security officer password is requested to be defaulted
- Changes to the auditing attribute of an object

For additional information, see the IBM Security - Reference.

Related information

[DB2 for i SQL Reference](#)

[Host server administration](#)

[Security reference](#)

Related information for ODBC security

Locate additional information on IBM i Access ODBC security.

Choose from the related links for in-depth information on specific topics.

You can also contact your IBM i technical support or search the technical support web page at <https://www.ibm.com/mysupport> for additional information.

Related information

[Host server administration](#)

[Security reference](#)

[Backup and recovery](#)

[DB2 for i SQL Reference](#)

Troubleshoot ODBC

Helps you solve a few of the more commonly encountered difficulties with IBM i Access Client Solutions and ODBC. It also identifies several tools that can help you remove performance bottlenecks. You should review this information before contacting technical support.

For help with integrating ODBC support into your applications, refer to IBM i Access Client Solutions ODBC programming, where you can get information on the following subtopics:

- ODBC API list
- ODBC API implementation
- Programming examples
- ODBC performance

The following topics provide general guidelines for finding and resolving IBM i Access Client Solutions ODBC errors:

Related information

[ODBC programming](#)

ODBC diagnostic and performance tools

Use tools to help diagnose IBM i Access ODBC problems.

Choose from the following for information on ODBC client or server-side diagnostic and performance tools:

Related concepts

[Checking the server status](#)

Use the IBM i Access Client Solutions CWBPING command.

[Gather information for IBM Support](#)

The IBM Support staff can offer you better service, if you have certain information available when you open a problem record to IBM Support for IBM i Access Windows Application Package troubleshooting.

Client-side ODBC diagnostic and performance tools

Use client-side tools to help diagnose IBM i ODBC problems.

The following table contains ODBC client-side diagnostic and performance tools:

Client Tool	Description
ODBC Trace (SQL.LOG)	Microsoft's ODBC Administrator provides its own trace utility to trace ODBC API calls from applications. See Collecting an ODBC Trace (SQL.LOG) for more information.
ODBC trace utilities	There are other ODBC trace utilities available that can be more robust than the ODBC Trace (SQL.LOG). These retail utilities can provide detailed entry and exit point tracing of ODBC API calls. Two tracing utilities are Trace Tools (Dr. DeeBee) and SST Trace Plus (Systems Software Technology).
CWBPING	To use CWBPING, type <code>cwbping (your system name or IP address)</code> at a command prompt. For example: <code>cwbping testsys1</code> or <code>cwbping 10.42.126.4</code> CWBPING responds with a list of servers, and their status. Run CWBPING without any parameters for help with using CWBPING. For more information about CWBPING, see Checking the server status.
CWBCOTRC	To use CWBCOTRC, type CWBCOTRC ON at a command prompt while located in the \Program Files\IBM\Client Access directory. After turning on the trace, you can start your application. Typing CWBCOTRC OFF stops tracing. CWBCOTRC gathers information about data that is being transmitted to and from the server. Run CWBCOTRC without any parameters for help with using CWBCOTRC.

Server-side ODBC diagnostic and performance tools

Use server-side tools to help diagnose IBM i Access ODBC problems.

The following tables contain ODBC diagnostic and performance tools the server side:

Server-side tools

Server Tool	Description
Communications trace	The communications trace facility will trace and format any communications type that has a line description (token ring and Ethernet). This is a tool for isolating many problems. It also is a useful aid for diagnosing where a performance delay is occurring. Use the timestamp and eye-catcher fields to measure how long it takes to process a request.

Server Tool	Description
Job traces	<p>The job trace can help isolate most host problems and many performance issues. A service job must first be started on the job to be traced. Locate the fully qualified job name of the ODBC job. From any 5250 emulation session, start a service job on this QZDASOINIT job by using the STRSRVJOB command. Then choose one of two traces, depending on the information needed:</p> <p>Trace job Traces the internal calls made by the host server. Run the TRCJOB *ON command.</p> <p>Debug trace Used to review the performance of your application and to determine the cause of a particular problem.</p> <p>The STRDBG command runs against an active service job. This command logs the decisions made by the query Optimizer to the job log of the debug session. For example, it records estimated query times, access paths used, and cursor errors.</p> <p>An easy way to enable STRDBG is to configure the ODBC DSN you are using through ODBC Administrator by selecting the Enable the Start Debug (STRDBG) command option on the Diagnostic tab. Alternatively, you can run the following command:</p> <pre style="background-color: #f0f0f0; padding: 5px; text-align: center;">STRDBG UPDPROD(*YES)</pre> <p>The ODBC job log can record all errors that occur for the IBM i database. When the job is in debug mode, the job log also will contain performance-related information.</p>
Performance tools	<p>Performance toolkit provides reports and utilities that can be used to create an in-depth analysis of your application performance. The toolkit provides information about CPU utilization, disk arm utilization, memory paging and much more. Although the base operating system includes the ability to collect performance data, you will need the separately licensed program IBM Performance Tools for i to analyze the results.</p> <p>You can also use the tools Database Monitor and Visual Explain. Refer to the IBM i Access Client Solutions help for more information.</p>
QZDASOINIT job log	<p>To receive optimal support, generate, locate and retrieve the QZDASOINIT job log. The job log may contain messages that can help you to determine and resolve errors that are returned through ODBC.</p> <p>An easy way to access the job log is to configure the ODBC DSN you are using through ODBC Administrator by selecting the Print job log at disconnect option on the Diagnostic tab. To find the job log, open a PC5250 emulation session and run the WRKSPLF command. Specify the IBM i user profile that was used on the ODBC connection as the user parameter for the WRKSPLF command.</p>
QAQQINI (Query options file)	<p>You can set the library for Query options file, by configuring the ODBC DSN you are using through ODBC Administrator and selecting the Diagnostic tab. Enter the name of the library you want to use in the Query options file library box.</p>

Collecting an ODBC Trace (SQL.LOG)

Steps for collecting IBM i Access ODBC API calls

Follow these steps to collect an SQL.LOG:

1. Start **ODBC Data Source Administrator**.
2. Select the **Tracing** tab
3. Select the **Start Tracing Now** button.
4. Select **Apply** or **OK**.
5. Recreate the error
6. Return to **ODBC Administrator**.
7. Select the **Tracing** tab.
8. Select the **Stop Tracing Now** button.
9. The trace can be viewed in the location that you initially specified in the **Log file Path** box.

Note: This procedure applies when you are using MDAC version 2.5. If you are using a different version of MDAC, then you may need to follow different steps.

IBM i Access ODBC error messages

When an error occurs, the IBM i Access ODBC driver returns the SQLSTATE (an ODBC error code) and an error message. The driver obtains this information both from errors that are detected by the driver and from errors that are returned by the DBMS.

For errors that occur in the data source, the IBM i Access ODBC Driver maps the returned native error to the appropriate SQLSTATE. When both the IBM i Access ODBC driver and the Microsoft Driver Manager detect an error, they generate the appropriate SQLSTATE. The IBM i Access ODBC driver returns an error message based on the message returned by the DBMS.

For errors that occur in the IBM i Access ODBC driver or the Microsoft Driver Manager, the IBM i Access ODBC driver returns an error message based on the text associated with the SQLSTATE.

Error message format

Error messages have the following format:

```
[vendor][ODBC-component][data-source]error-message
```

The prefixes in brackets ([]) identify the source of the error. The following table shows the values of these prefixes returned by the IBM i Access ODBC driver.

When the error occurs in the data source, the [vendor] and [ODBC-component] prefixes identify the vendor and name of the ODBC component that received the error from the data source.

Error source	Value
Driver Manager	[Microsoft] [ODBC driver Manager] [N/A]
IBM i Access ODBC driver	[IBM] [System i Access ODBC driver] N/A
NLS messages	[IBM] [System i Access ODBC driver] Column #: NLS error message number NLS error message text

Error source	Value
Communication layer	<p>[IBM] [System i Access ODBC driver]</p> <p>Communications link failure. Comm RC=xxxx - (message text) Where xxxx is the error number in decimal, not hexadecimal, format. Message text describing the nature of your error appears with the error number.</p> <p>Note: For more information about error message ids, see IBM i Access return codes or the IBM i Access Client Solutions online User's Guide.</p>
Db2 for i	<p>[IBM] [System i Access ODBC driver] [DB2] Server error message</p>

Viewing Db2 for i error message text:

For errors that begin with:	Use this CL command
SQL	DSPMSGD RANGE(SQLxxxx) MSGF(QSQLMSG)
IWS or PWS	DSPMSGD RANGE(ZZZxxxx) MSGF(QIWS/QIWSMSG) where ZZZ is IWS or PWS

Refer to Common ODBC errors for help with other ODBC error messages.

You can search and view NLS or communication error messages in the Service, Error and Trace message help topic in the IBM i Access Client Solutions online User's Guide.

Related concepts

[Common ODBC errors](#)

Find and resolve IBM i Access ODBC errors.

Related information

[IBM i Access return codes](#)

Troubleshoot the IBM i connection

Each ODBC connection communicates with one IBM i database program. This program is referred to as the **host server program**.

The name of the Database Server program used with TCP/IP is **QZDASOINIT**. It is normally located in subsystem QUSRWRK, however it can be set up differently by the system administrator.

Under normal conditions, the program is evoked transparently, and the user is not required to take action except to verify that the proper subsystems and communication protocols are running. See the Host server administration for details on administration of host server jobs.

The most common indication of a connection failure is an error message from the ODBC driver mentioning a communications link failure.

If ODBC is unable to connect to the IBM i host, perform the following troubleshooting tasks:

Related information

[Host server administration](#)

Checking the server status

Use the IBM i Access Client Solutions CWBPING command.

The IBM i Access Client Solutions product has a special command to verify status of host servers:

```
CWBPING systemname
```

where systemname is the name of the system.

The command should return something like the following:

```
To cancel the CWBPING request, press CTRL-C or CTRL=BREAK
I - Verifying connection to system MYSYSTEM..
I - Successfully connected to server application: Central Client
I - Successfully connected to server application: Network File
I - Successfully connected to server application: Network Print
I - Successfully connected to server application: Data Access
I - Successfully connected to server application: Data Queues
I - Successfully connected to server application: Remote Command
I - Successfully connected to server application: Security
I - Successfully connected to server application: DDM
I - Successfully connected to server application: Telnet
I - Successfully connected to server application: Management Central
I - Connection verified to system MYSYSTEM
```

Related concepts

[ODBC diagnostic and performance tools](#)

Use tools to help diagnose IBM i Access ODBC problems.

Verifying that subsystems are active

TCP/IP-connected IBM i Access ODBC jobs (QZDASOINIT) will run in the QUSRWRK subsystem. Verify that this subsystem is running.

The QSERVER subsystem may need to be manually started. To do this, simply issue the following command:

```
STRSBS QSERVER
```

To have the subsystem start automatically at IPL, modify the IPL Start up procedure (the default is QSYS/QSTRUP) to include the STRSBS QSERVER command.

In addition to subsystem QSERVER, subsystem QSYSWRK, and QUSRWRK must be running.

Verifying that prestart jobs are running

IBM ships the QSERVER/QUSRWRK subsystems to use prestart jobs to improve performance at job initialization and startup. If not active, these prestart jobs can impact a IBM i connection.

When prestart jobs are configured in the subsystem, the job **MUST** be active to connect. The prestart job used for a TCP/IP connection is:

- QZDASOINIT - Server program
- QZDASSINIT - Server program used when using SSL

To verify a prestart job is running use one of the following:

```
WRKACTJOB SBS(QUSRWRK)
WRKACTJOB SBS('user-defined-subsystem')
```

The appropriate prestart job should be active:

```
Job      User      Type      -----Status-----
QZDASOINIT  QUSER    PJ        ACTIVE                (socket connection)
```

Prestart jobs do not display in WRKACTJOB unless a connection is already active. You must use F14 - Include from the WRKACTJOB panel.

Additional TCP/IP considerations

Use NETSTAT, STRTCP, and STRHOSTSVR to verify and start TCP/IP functions when troubleshooting a IBM i connection.

Verify that TCP/IP is started with the following command:

```
NETSTAT *CNN
```

Note: To verify that TCP/IP is started with System i® Navigator, you must already have configured your server with TCP/IP, then do the following:

1. In System i Navigator, select your **server > Network**.
2. Right-click TCP/IP Configuration, and select Utilities.
3. Select Ping.
4. Specify a host name or TCP/IP address, and click Ping Now.

Use the command STRTCP to start the desired protocol if it is not running.

Verify the necessary daemons are running by browsing the information returned from the NETSTAT *CNN command:

Remote Address	Remote Port	Local Port	Idle Time	State
*	*	as-cent >	000:09:31	Listen
*	*	as-signon	000:09:41	Listen
*	*	as-svmap	002:57:45	Listen
*	*	as-data >	002:57:45	Listen

Use the command STRHOSTSVR SERVER(*ALL) to start them if necessary.

- Verify QZDASRVSD, the database host server socket daemon, is running in the QSERVER subsystem.
 - as-database should be in the Listen State
 - WRKJOB QZDASRVSD should be used to check the job log of the daemon for any error messages.
- Verify that socket daemon QZSOSMAPD is running in QSYSWRK subsystem.
 - as-svmap should be in the Listen State as shown by NETSTAT *CNN.
 - WRKJOB QZSOSMAPD should be used to check the job log of the daemon for any error messages.

The PC locates the port used by the database server by connecting to the server mapper port. It retrieves the port used by as-database. It then connects to the proper port which is being monitored by the database server daemon, QZDASRVSD. The server daemon will attach the client's connection to a QZDASOINIT prestart job in QUSRWRK. If this is the first connection made to the server from this PC, then two other servers are used: Central server for licensing and signon server for userid/password validation.

For more information about verifying that TCP/IP is started, see General TCP/IP problems.

Related information

[Configure your server with TCP/IP](#)

[General TCP/IP problems](#)

Common ODBC errors

Find and resolve IBM i Access ODBC errors.

The following topics provide general guidelines for finding and resolving common IBM i Access ODBC errors:

Related concepts

[IBM i Access ODBC error messages](#)

When an error occurs, the IBM i Access ODBC driver returns the SQLSTATE (an ODBC error code) and an error message. The driver obtains this information both from errors that are detected by the driver and from errors that are returned by the DBMS.

SQL errors

List of common SQL IBM i Access ODBC errors that are encountered by applications

Note: For more information on SQL errors, see SQL messages and codes.

Related information

[SQL messages and codes](#)

SQL0104 - Token &1 was not valid. Valid tokens: &2

Invalid IBM i Access ODBC SQL Syntax message

Probable cause:

- The application generated an SQL statement with incorrect syntax. For help with problem determination, use the ODBC trace tool, provided with the ODBC Administrator, to look at the SQL.LOG.
- See SQL0114 - Relational database &1 not the same as current &2 server if "*" is the token.
- The SQL statement is using a literal that exceeds the 32K size limitation. Consider using a parameter marker instead of a literal. This reduces the size of the statement while allowing you to pass the maximum field size worth of data.
- The application is using incorrect syntax for left outer join. Some applications default to a proprietary left outer join syntax of *= in the WHERE clause (PowerBuilder 3.0 & 4.0, Crystal Reports). Check with your application vendor. Most provide an ini setting or a configuration value to use ODBC left outer join syntax.

Related concepts

[SQL0114 - Relational database &1 not the same as current &2 server](#)

Update the IBM i Access ODBC Relational Database Directory Entry.

SQL0113 - Name &1 not allowed.

Update the IBM i Access ODBC Relational Database Directory

Probable cause:

It is likely that the system name is not in the Relational Database Directory. Run the Add Relational Database Directory Entry command:

```
ADDRDBDIRE RDB(SYSNAME) RMTLOCNAME(*LOCAL)
```

In the above example, SYSNAME is the name of your system's Default Local Location name (as specified in the DSPNETA command).

Another common cause for this error is a period (.) in a table or library name. Although the period is valid in IBM i file naming conventions the name must be enclosed in double quotes to be used in a SQL statement. A short-term circumvention may be to build a logical file over the desired physical file, using the SQL naming syntax. Another possible solution is to create an SQL Alias over the desired file and then access the file indirectly through the alias.

SQL0114 - Relational database &1 not the same as current &2 server

Update the IBM i Access ODBC Relational Database Directory Entry.

Probable cause:

It is likely that the system name is not in the Remote Database Directory. Run the Add Relational Database Directory Entry command:

```
ADDRDBDIRE RDB(SYSNAME) RMTLOCNAME(*LOCAL)
```

In this above example, SYSNAME is the name of your system's Default Local Location name (as specified in the DSPNETA command).

Another common cause for this error is a period (.) in a table or library name. Although valid in naming conventions, in order to use it within an SQL statement, enclose the name within double quotes. A short-term circumvention may be to build a logical file over the desired physical file, using the SQL naming syntax.

Related concepts

SQL0104 - Token &1 was not valid. Valid tokens: &2
Invalid IBM i Access ODBC SQL Syntax message

SQL0204 - MYSYSCONF not found
For IBM i Access ODBC: Optional table on the server.

Probable cause:

Usually only job logs for jobs using the Microsoft Jet Engine (Microsoft ACCESS or Microsoft Visual Basic applications) contain this message. The MS Jet Engine always checks for an optional table on the server that is called MYSYSCONF. The applications ignore this warning. For further information, see the Microsoft Jet Database Engine Connectivity white paper or contact Microsoft.

SQL0208 - ORDER BY column not in result table
For IBM i Access ODBC: Problem with ORDER BY clause

Probable cause:

The IBM i Access ODBC driver reports "Y" to the property SQL_ORDER_BY_COLUMNS_IN_SELECT (ODBC 2.0). A character string of "Y" implies that the columns in the ORDER BY clause must be in the select list. Some common desktop reporting applications either ignore or do not check this value and attempt to use an order by field which is not in the select list.

SQL0900 - Application process not in a connected state
Update the IBM i Access ODBC Relational Database Directory Entry.

Probable cause:

It is likely that the system name is not in the Remote Database Directory. Run the Add Relational Database Directory Entry command:

```
ADDRDBDIRE RDB(SYSNAME) RMTLOCNAME(*LOCAL)
```

In the above example, SYSNAME represents the name of your system's Default Local Location name (as specified in the DSPNETA command).

Another common cause for this error is a period (.) in a table or library name. Although valid in naming conventions, in order to use it within an SQL statement, enclose the name within double quotes. A short-term circumvention may be to build a logical file over the desired physical file, using the SQL naming syntax.

Your ODBC Data Source Name (DSN) configuration uses the wrong naming convention. Use the ODBC Administrator to change your DSN to use the proper (*SQL or *SYS) naming convention. Always use *SQL unless your application design specifically expects *SYS.

SQL0901 - SQL System Error
For IBM i Access ODBC: Server machine (function) check error

Probable cause:

Another, previously reported error has prevented the processing of a SQL statement. The previous error is logged only in the IBM i job log and is not returned to the ODBC application. You must locate and retrieve the job log to identify and resolve the problem.

To find the job log, open a PC5250 emulation session and issue a **WRKSPLF** where user is the IBM i user profile used on the ODBC connection. However, in some cases the joblog is found using **WRKSPLF QUSER**.

For example, it is necessary to use **WRKSPLF QUSER** to find the associated joblog when the prestart jobs fail to start.

SQL5001 - Column qualifier or table &2 undefined.

Change your naming convention in your IBM i Access ODBC DSN.

Probable cause:

Your ODBC Data Source Name (DSN) configuration uses the wrong naming convention. Use the ODBC Administrator to change your DSN to use the proper (*SQL or *SYS) naming convention. Always use *SQL unless your application design specifically expects *SYS.

SQL5016 - Object name &1 not valid for naming convention

Change your naming convention in your IBM i Access ODBC DSN.

Probable cause:

Your ODBC Data Source Name (DSN) configuration uses the wrong naming convention. Use the ODBC Administrator to change your DSN to use the proper (*SQL or *SYS) naming convention. Always use *SQL unless your application design specifically expects *SYS.

SQL7008 - &1 in &2 not valid for operation. The reason code is 3

For IBM i Access ODBC: Error related to files not journaled

Probable cause:

The database performs commitment control by journaling. Any ODBC application that takes advantage of commitment control will require journaling the files that are used.

Stored procedure errors

There are common IBM i Access ODBC errors returned to applications from stored procedure.

SQL0444 - External program &A in &B not found (Db2 for i SQL)

The SQL0444 is generated on an execute or execute direct when the Db2 for i database server is able to locate the procedure declaration but is unable to locate the program object.

The external program must be in the location specified in the system catalog tables. Note that this location is defined by the naming convention and default collection in affect when the procedure is defined (using CREATE PROCEDURE) and not when the procedure is called. To check the location defined for the external program name of a stored procedure run a query over QSYS2.SYSPROCS and note the value for the "EXTERNAL_NAME" name field.

No data returned on OUTPUT and INPUT_OUTPUT parameters

For IBM i Access ODBC: SQLBindParameter problem when no data returned

This problem could be caused by any of the following:

- The ODBC **SQLBindParameter** API incorrectly specified **fParamType** as SQL_PARAM_INPUT.
- DECLARE PROCEDURE was used instead of CREATE PROCEDURE, and extended dynamic support is disabled.
- The programmer incorrectly declared a parameter as IN on the CREATE or DECLARE PROCEDURE.
- The stored procedure program incorrectly returned the parameter.

SQL0501 - Cursor CRSR000x not open

For IBM i Access ODBC: To return data when using embedded SQL in ILE programs, you must specify the compile option ACTGRP(*CALLER) and not the default of *NEW.

Verify that the program executes a return instead of an exit.

When the stored procedure program executes an exit instead of a return, you must set the **Close SQL Cursor** option to *ENDACTGRP. If the Close SQL Cursor option is set to *ENDMOD, the cursor will be closed before data is retrieved.

Also, verify that the CREATE PROCEDURE specifies the correct number of result sets. This is especially important when using array result sets.

ODBC incorrect output and unpredictable errors

Ensure that the IBM i Access ODBC driver and the database server program are at matching code levels.

Check for PTF corequisite requirements on any PTF that you order or in the readme.txt file of the Service Pack.

Note that *result set cursors* from stored procedures are read only.

Note: Binary or hexadecimal data instead of ASCII characters

The default value of the Translation parameter is set to not convert binary data (CCSID 65535) to text. A CCSID is attached to files, tables, and even fields (columns) to identify the conversion table that is used to convert the data. A CCSID of 65535 often identifies raw data (binary or hexadecimal), such as bitmapped graphics, that is language independent. Not selecting *Convert binary data (CCSID 65535) to text* ensures that the raw data is not damaged.

Setting the Translation parameter to *Convert binary data (CCSID 65535) to text*, changes the CCSID that is attached to the data to the CCSID that is attached to the job. **This parameter setting can cause damage to the data if the data is truly binary.**

Gather information for IBM Support

The IBM Support staff can offer you better service, if you have certain information available when you open a problem record to IBM Support for IBM i Access Windows Application Package troubleshooting.

To gather this information, complete the following tasks:

Support Task	Task Description
Run cwbsvget.exe to gather information.	<p>The cwbsvget.exe tool can help collect all traces run plus other information that may be helpful in diagnosing a problem. cwbsvget produces a zip file to send to IBM Service for analysis. Note that cwbsvget does NOT turn traces on and off -- it simply gathers traces and other data into one file for convenience and completeness. If you use the cwbsvget.exe tool you will not need to complete the steps below for gathering the version of the ODBC driver and for locating the trace files. Make sure to run cwbsvget.exe after the traces are stopped so that the trace files get packaged into the zip file that cwbsvget generates. To use cwbsvget.exe complete the following steps:</p> <ol style="list-style-type: none">1. Open a Command prompt.2. Navigate to the Client Access folder typically located in the \Program Files\IBM\Client Access directory and run the following command: <pre>cd \Program Files\IBM\Client Access</pre>3. Run the command: cwbsvget.exe <p>Note: cwbsvget.exe generates a .zip file for you. The output on the Command window indicates where that .zip file was created.</p>

Support Task	Task Description
Record the IBM i version and cumulative PTF level.	<ol style="list-style-type: none"> 1. Issue the display PTF command on an terminal emulation command line: <pre>DSPPTF</pre> 2. Record the IBM i release information that has the format VxRxMx. 3. Verify that the IPL source is ##MACH#B. 4. Press F5 to display the PTF details. 5. Record the first PTF ID in the list. It will have the format Tzxyyy where xx is the year, yyy the Julian date and z is either L or C.
Record the version of the ODBC driver.	<ol style="list-style-type: none"> 1. From the Task bar select Start > Programs > IBM i Access Client Solutions > ODBC Administration (64-bit). 2. Select the Drivers tab. 3. Record the version of the IBM i Access ODBC Driver.
Record the version of the ODBC driver manager.	<ol style="list-style-type: none"> 1. From the Task bar select Start > Programs > IBM i Access Client Solutions > ODBC Administration (64-bit). 2. Select the About tab. 3. Record the version of the Driver Manager.
Gather traces	The traces you will most likely be asked to gather for support are: an ODBC trace (SQL.LOG), CWBCOTRC or Communication Trace, and a Detail Trace. See ODBC diagnostic and performance tools, for more information about traces.
Record additional information	Such as the PC application, the error description, and what ODBC driver (32-bit or 64-bit) you are using.

Related concepts

ODBC diagnostic and performance tools

Use tools to help diagnose IBM i Access ODBC problems.

Restrict users with policies and application administration

IBM i Access policies provide multiple methods of setting up restrictions and profiles.

The policies use either Microsoft's policy editor or the Application Administration function of IBM Navigator for i.

The two primary methods for implementing administrative control over your network are Application Administration and policies. Application Administration bases restrictions on the IBM i user profile, and is administered through IBM Navigator for i. Policies mandate configuration settings and restrictions, and can apply to both specific PCs and individual Windows user profiles. As such, they offer greater granularity than Application Administration, but are significantly more difficult to set up and administer. In order to use policies, you must download the Microsoft System Policy Editor and configure your PCs and system for storage, retrieval, and application of the policies you set. Generally, Application Administration is

preferable if all of the functions you want to restrict are Application Administration-enabled, and if the version of the IBM i server being used supports Application Administration.

For more information about Application Administration, refer to Application Administration.

To learn about policies, refer to the following topics:

Related information

[Application Administration](#)

Overview of IBM i Access policies

Use system policies to restrict users from certain actions, and to suggest or require certain configuration features.

IBM i Access policies can apply to individual Windows user profiles, and specific PCs. However, these IBM i Access policies do not offer control over the system resources and thus are not a substitute for system security. For a description of what you can do with these policies, refer to Types and scopes of policies.

Use of Group Policy to control use and configuration of IBM i Access Client Solutions had limited testing and can therefore provide unpredictable results. For additional information about Group Policy, see Microsoft documentation. The remainder of this topic discusses the tested, supported use of IBM i Access Client Solutions policies.

Policy support in your network

Policies can reside on a file server. When configured on a file server, each time users sign-on to their Windows workstation, their workstation downloads all the policies that apply to that Windows user profile. The user's PC applies the policies to the registry before the user does anything on the workstation. Each Windows operating system comes with the code needed to download policies.

To use the full capability of policies, you need the following:

- A primary logon server
- A policy server

You can use IBM i Support for Windows Network Neighborhood (IBM i NetServer) as the policy server.

See [Set up your system to use policies](#) for more information.

Policy files

Policy definitions are contained in policy templates, which organize the policies into categories. Following are the IBM i Access five policy templates for each function.

- Restricting functions for a given system (sysname.adm)
- Restricting specific function at runtime (caerestr.adm)
- Restricts checking the service pack level (caeinrst.adm)
- Mandate or suggest configuration settings for specific environments, the systems within those environments, and some configurable values for those systems (config.adm)
- Suggest or mandate global configurable values (caecfg.adm)

You must generate the policy templates with the CWBADGEN utility before creating or modifying specific policies. Then use the Microsoft System Policy Editor or the Microsoft Management Console Group Policy snap-in, gpedit.msc, to activate the templates and set their constituent policies. If using the Microsoft System Policy Editor, save the changes to a policy file. If using gpedit.msc, the policy settings are stored in a Group Policy Object automatically. See Microsoft documentation for details.

See [Create policies](#) for more information.

Types and scopes of policies

Each IBM i Access policy varies in scope and provides either a restriction or a configuration.

Restriction policies

Restriction policies can usually be set to any scope and may have the following uses:

- Restrict or allow use of a function or action.
- Include restrictions for checking service pack levels.
- Include several other restrictions. For example, you can restrict a certain type of data transfer upload, or you can restrict all types of data transfer uploads at once using the Prevent All Data Transfer policy.
- Cause controls or options normally selectable to be hidden or "greyed-out".
- Notify the user when a restriction policy prevents a function they attempt from completing, usually by a message displayed in a console or a window.

Configuration policies

Configuration policies can only be set to a user scope, and may have the following uses:

- Pre-configure settings that the end user could normally configure themselves.
- Configure values, features that the user may normally enable or disable, lists of environments and connections.
- "Grey-out" a mandated value. When a configuration policy mandates a value, the input field for that value will not accept changes.

Configuration policies may be either suggested or mandated.

- Suggested: The value provided is used unless explicitly configured by the user or set by an application program. This effectively overrides the normal IBM i Access default value but does not force use of the value -- a new value may be specified, overriding the suggested value.
- Mandated: The value provided will be used -- neither the user nor application programs may change it.

Policy scopes

There are three scopes at which each policy is set: machine scope, user scope and IBM i connection scope. Some policies are set at more than one scope, while others are not.

Scope	Description
Machine scope	A policy set at this scope applies to all users of the PC. The only exception is when the same policy is set for a specific user to override the machine scope setting.
User Scope	A policy set at this scope can be applied on a per-user basis. It may be set for some users, but not others. It may be set for the "Default User" (any user without an individual policy configuration) as well. Some user scope policies provide a setting that allows a function regardless of the machine scope setting. When this setting is used, the machine scope setting is ignored.

Scope	Description
IBM i Connection (or "Per-System") Scope	<p>Some policies that are set at user or machine scope are more narrowly set at system connection scope within the user or machine scope. When set at system connection scope, the policy setting is applied only when working with the named system. For example, if a restriction policy is set at system connection scope inside of user scope, where the system is named SYS1 and the user is USER1, the function is restricted only when USER1 works with SYS1.</p> <p>Note: If a policy is set at system connection scope, this setting takes precedence over the user or machine scope setting. For example, if default user mode is mandated for user USER1 to be "Use default user id", but set for system SYS1 to be "Use Windows user id and password", when USER1 connects to SYS1, his Windows user id and password are used. When USER1 connects to any other system, the specified default user id is used</p> <p>Note: To enable setting policies at this scope, you must generate and use one or both of the following policy templates:</p> <ul style="list-style-type: none"> • config.adm -- Configured environments and connections template • sysname.adm -- Per-system (by IBM i name) template

Set up your system to use policies

Download a IBM i Access policy file.

Complete the following steps to use policies by downloading a saved policy file across a network.

1. Configure a IBM i environment for policies
2. Create policy files

Configure a system for using IBM i Access Client Solutions policies

Use the following steps to configure your system for serving policies. These steps assume that you have Windows PCs in your network.

- Configure your system as a IBM i NetServer, if this has not already been done.
- Create an integrated file system folder to hold your policy files.

Related information

[IBM i NetServer](#)

[Integrated file system](#)

Create policy files

Create or modify policies and store them in a IBM i Access policy file.

To create or modify specific policies and store them in a policy file, follow these steps:

1. Download the Microsoft System Policy Editor.
2. Create the IBM i Access policy templates.
3. Create and update the policy file.

Note: A policy file is not needed if the Microsoft Management Console Group Policy snap-in, gpedit.msc, is used to set policies. See Microsoft documentation for more information.

Microsoft System Policy Editor

To create your own IBM i Access policy files, you need the Microsoft policy editor.

Use the Microsoft Web site to obtain the version of the policy editor that is supported on the Windows operating system that you are using. Search for **policy editor** at www.microsoft.com.

Follow the directions that come with the editor to extract the file and install the policy editor and templates.

Related information

[Microsoft Corporation](#)

Create IBM i Access policy templates

An IBM i Access program creates the policy templates you need to control policies.

1. Open a command prompt window.
2. Go to the IBM i Access Client Solutions directory, usually located at:
 [C:]\Program Files\IBM\Client Access\
 3. Type the command and parameter to give you the templates for the policies that you want to set.

Policy template commands

Command cwbadgen with parameters	Description
cwbadgen /ps S1034345 (Where s1034345 is the system name.)	Generates the template for setting system specific policies, S1034345.adm.
cwbadgen /std	Generates caecfg.adm (covers global configuration), caeinrst.adm (covers checking service pack level restriction), & caerestr.adm (covers run time restrictions).
cwbadgen /cfg config.adm	Generates the config.adm (configuration policy based on system configurations that exist on the PC from which this command is run). Specify the name of the file after the /cfg argument. In this example the template file is config.adm.

Create and update policy files

Create IBM i Access policy files to control default computer or default user actions.

Note: The following instructions do not cover the use of Group Policy or the Microsoft Management Console Group Policy snap-in, although the instructions are similar. To administer IBM i Access functions using Group Policy, see the Microsoft documentation on Group Policy use.

1. Start the policy editor by double-clicking **poledit.exe**.
2. Go to **Options > Policy Template > Add**.
3. Go to the location where you stored the .adm files that you created in creating policy templates.
4. Select the .adm files that you want to add and click **Add**. Keep doing this until you have added all the .adm files that you want to use. Then click **OK**.
5. Go to **File > New Policy**.
6. Set your policies and save the policy file:

 \\QYOURSYS\POLICIES\ntconfig.pol

Where:

- QYOURSYS is the name of your IBM i NetServer.
- POLICIES is the name of the shared file folder on your IBM i NetServer.
- config.pol is the name of your policies file.

To update the policy file, open your policy file with the policy editor, make your changes and save the file back to the above location.

Note: You must create and maintain individual policies for the different Windows operating systems. See Microsoft documentation for details.

IBM i Access policy list

Administrators can use Microsoft system policies to control which IBM i Access functions and settings are available to each user.

This topic lists all the IBM i Access policies that are provided and describes the effects and scope of each.

Sets of policies are defined by template files. You can generate IBM i Access policy templates (.adm files) on a PC with IBM i Access installed using the **cwbadgen** command. See [Create policy templates for IBM i Access](#) for details.

Choose different topic collections, from the links below, for more information. For a general description of policies, choose [Overview of IBM i Access policies](#). Choose [Policies by function](#) to see a list of existing policies by the function they affect or choose [Policies by template](#) for a set of templates to assist you in creating policies.

Policies by function

Set these policies to control IBM i Access functions.

The following table lists policies by the function they affect.

Function	Related policies
.NET Data provider	Prevent .NET Data provider usage
ActiveX Automation Objects	Prevent data queue automation object
Communications	<ul style="list-style-type: none">• Default user mode• TCP/IP Lookup• Port lookup mode• Require secure sockets• Prevent changes to active environment• Prevent changes to environment list• Prevent connections to systems not previously defined• Prevent use of non-mandated environments• Connection timeout
License management	Time to delay before license is released
National Language Support	<ul style="list-style-type: none">• ANSI code page• OEM code page• EBCDIC code page• Bi-directional transformation of data
ODBC	<ul style="list-style-type: none">• Named data sources• Prevent program generated data sources
OLE DB	Prevent OLE DB provider usage
Passwords	<ul style="list-style-type: none">• Warn user before IBM i password expires• Prevent IBM i Access Client Solutions password changes

Function	Related policies
PC Commands	<ul style="list-style-type: none"> • Cwblogon • Cwbcfg • Cwbback • Cwbrest • Cwbenv

Policies by function: .NET Data provider

Control IBM i Access .NET provider by policies.

.NET Data Provider policy: Prevent .NET Data Provider usage

Use this policy to prevent use of the IBM i Access .NET Data Provider. When not restricted by this policy, the .NET Data Provider allows applications using Microsoft 's .NET framework to access Db2 for i Databases.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	X

Policies by function: ActiveX automation objects

Control IBM i Access ActiveX by policies.

ActiveX policy: Prevent data queue automation object

Use this policy to prevent users from using the IBM i Access data queue automation object.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X		

Policies by function: Communication

Control IBM i Access communication functions by policies.

Communication policy: Default user mode

Use this IBM i Access policy to configure the default user connection mode.

You can configure the default user mode to:

- Always prompt for user ID and password.
- Use a default user ID, which you must specify with this policy.
- Use the Windows user ID and password of the logged-on user.
- Use the Kerberos principal name, no prompting.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection.
	X		X

Communications policy: TCP/IP Address Lookup Mode

Use this policy to suggest or mandate the frequency of IBM i IP address lookups.

You can use this policy to set the TCP/IP address lookup mode to:

- Lookup always (do not cache the address)
- Lookup once per hour
- Lookup once per day
- Lookup once per week
- Lookup after Windows has been re-started
- Never look it up

Note: If you select Never look it up, you must also specify an IP address to use.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
	X		X

Communication policy: Port lookup mode

Use this policy to suggest or mandate the method used, or the search location to obtain the TCP/IP port number for a specific IBM i program.

A per-system (IBM i connection scope) mandate will always override a global (machine scope) mandate, or a user-configured value, for port lookup mode.

You can use this policy to set the port lookup mode to:

- Lookup locally
- Lookup on server
- Use standard port

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (may override machine setting)	Per IBM i connection
	X		X

Communication policy: Require Secure Sockets

Use this policy to require secure sockets layer (SSL) for a IBM i Access user.

To use this policy, SSL must be installed and configured on both the system and the client PC. It is not possible to mandate that SSL is turned off. It is always possible for a user to elect to use SSL, assuming that it is installed and configured on both the system and the client PC.

If this policy mandates the use of SSL, any connection attempt that cannot use SSL fails. This means that if the user does not have SSL installed, or if the system is incapable of using SSL or does not have the SSL-capable versions of the host servers started, no connections to the system is made.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
	X		X

Communication policy: Prevent changes to active environment

Use this policy to prevent switching the active environment. Use it to force IBM i Access users to use a specific environment.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

Communication policy: Prevent environment list changes

Use this policy to prevent an IBM i Access user, or users of a PC, from making changes to the list of connection environments. Specifically, the user is not allowed to add new environments, rename existing environments, or delete existing environments.

This policy only prevents manipulation of the environment list. The user is still permitted to manipulate the contents of an environment, i.e. add, rename, or remove systems in the environment.

This policy is of interest to administrators who want to tightly control their IBM i Access Client Solutions user connections.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

Communication policy: Prevent connections to systems not previously defined

Use this policy to prevent IBM i Access users from connecting to or configuring systems not yet defined.

This policy does not mandate systems or environments. Mandating these is done by creating and using the policy template config.adm. See Create policy templates for IBM i Access to read about how to do this.

When this policy is used:

- Systems not yet defined may not be used for any IBM i Access function.
- New systems may not be defined.
- Systems may still be deleted but cannot then be re-defined.
- Environments may still be added, deleted, or renamed.

When environments and systems are mandated:

- Systems not yet defined are used for IBM i Access Client Solutions functions.

- New systems and environments are defined.
- Systems and environments already defined are not deleted.

To force a user to use, and not modify, a set of environments and systems, use this policy along with mandating environments and systems.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

Communication policy: Prevent use of non-mandated environments

Use this policy to restrict IBM i Access users to using only connection environments mandated by the administrator. This policy is helpful for administrators who want to tightly control user connections.

To mandate use of a collection of environments, and systems within those environments, create a policy template using cwbadgen.exe and the /cfg option. Then include this template when building the policy file. The creation of this template should be done only when the environments and systems configured on the PC are exactly those the users should use.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

Communication policy: Timeout value

Use this policy to enforce a timeout value. However, the IBM i Access user can overwrite the policy programmatically, or by manually configuring the value for the specific system connection.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X			

Policies by function: License management

Control IBM i Access license by policies.

You can use these policies to control the amount of time to delay before license is released.

License policy: Time to delay before releasing IBM i Access license

Use this policy to control IBM i Access wait time for giving up a license, after licensed programs have ended.

This setting is usually configured by the user on the Other tab of IBM i Access Client Solutions Properties, to set the number of minutes the product waits. If a value is not set by this policy, and the user has not configured a value, the default is to wait 10 minutes before giving up the license.

Even though the policy setting allows only minutes to be specified, the value on the IBM i Access Client Solutions Properties Other tab is shown in both hours and minutes.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X			

Policies by function: National Language Support

Control National Language Support function for IBM i Access by policies.

National Language Support policy: ANSI code page

Use this policy to control which ANSI code page should be used for specific users for IBM i Access functions.

This setting is normally configured on the Language tab of IBM i Access Client Solutions Properties. If no value is set using this policy, and no value has been configured by the user, the PC's default ANSI code page will be used.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i Access connection
	X		

National Language Support policy: OEM code page

Use this policy to control which OEM code page is used when for IBM i Access functions.

This setting is normally configured on the Language tab of IBM i Access Client Solutions Properties. If no value is set using this policy, and no value has been configured by the user, the PC's default OEM code page will be used.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
	X		

National Language Support policy: EBCDIC code page

Use this policy to control which EBCDIC CCSID is used by IBM i Access functions.

This setting is normally configured on the Language tab of IBM i Access Client Solutions Properties. If no value is set using this policy, and no value has been configured by the user, the EBCDIC CCSID is taken from the job serving the client.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
	X		

Language policy: BiDi Transform

Suggests or mandates the value for the BiDi Transform setting on the IBM i Access Client Solutions Properties Panel.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate

Policy Type		
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
	X		

Policies by function: ODBC

Control IBM i Access ODBC functions by policies.

ODBC policy: Prevent use of named data sources

Use this policy to restrict the use of named data sources when using IBM i Access ODBC support.

A "named data source" is one that:

- has been created by the user or a program and given a specific name, and
- is specified using the **DSN** option when connecting.

A user may create a named data source using the IBM i Access ODBC Administration program. A program may create a named data source too -- by calling, for example, SQLCreateDataSource.

A program may create an ODBC connection by calling SQLDriverConnect. If the DSN option is used, it specifies a named data source to use. If the FILEDSN option is used, it specifies the name of a file that contains connection options. The file name is not a data source name, hence use of FILEDSN does not constitute use of a named data source.

The restriction options for this policy are the following:

- **Allow all:** All named data sources may be used.
- **Allow listed sources:** Only those sources specifically listed in this policy may be used. To view or change the list, click the Show button.
- **Prevent using named data sources:** No named data sources may be used.

If when connecting no named data source is specified, the data source used will be a temporary one, called a "program generated data source." The use of program generated data sources can be restricted using the Prevent use of program generated data sources policy.

This policy is an override of **machine setting enabled**.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X		X

Related concepts

[ODBC policy: Prevent use of program generated data sources](#)

Use this policy to restrict the use of program generated data sources when using IBM i Access ODBC support.

ODBC policy: Prevent use of program generated data sources

Use this policy to restrict the use of program generated data sources when using IBM i Access ODBC support.

A "program generated data source" is one that is created temporarily when an ODBC connection is made without using the DSN option to specify the name of the data source. Note that use of the FILEDSN option does not mean the data source used is named. FILEDSN simply specifies the name of a file containing connection options, not the name of a data source.

If a program first creates a data source (using SQLCreateDataSource, for example) and then connects using the DSN option, the data source is not considered a program generated data source, but a named data source. To restrict the use of named data sources, use the Prevent use of named data sources policy.

This policy is an override of **machine setting enabled**.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X		X

Related concepts

ODBC policy: Prevent use of named data sources

Use this policy to restrict the use of named data sources when using IBM i Access ODBC support.

Policies by function: OLE DB

Control usage of the OLE DB provider, using IBM i Access policies.

OLE DB Provider policy: Prevent OLE DB Provider usage

Use this policy to prevent use of the IBM i Access OLE DB providers.

When not restricted by this policy, the OLE DB Provider is used to access IBM i database files, stored procedures, data queues, CL commands, and programs.

Note: A single policy covers all OLE DB providers so, if this prevent policy is set, none of the OLE DB providers will work.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection

Policy Scope			
X	X	X	X

Policies by function: Passwords

Control passwords, using IBM i Access policies.

Password policy: Warn user before IBM i password expires

Use this policy to control IBM i Access warnings that a system password is near expiration.

If the policy is set, the number of days before expiration at which point the user is to be warned must be specified as well. Normally these can be configured by the user using the Passwords tab of IBM i Access Client Solutions Properties. If no value is set by policy and the user has not configured a value, the default action is to warn the user when a password is within 14 days of expiring.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
	X	X

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
	X		

Password policy: Prevent IBM i Access password changes

Use this policy to prevent PC users from changing system passwords through the Passwords tab of IBM i Access Client Solutions Properties.

Note: If this policy is not in effect, the user is still prevented from changing his system password by restrictions placed on his account by the system administrator.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

Policies by function: PC Commands

Restrict use of PC commands using IBM i Access policies.

PC command policy: Prevent use of Cwblogon.exe

Use this IBM i Access policy to prevent use of the Cwblogon utility.

For more information about this PC command, refer to the IBM i Access Client Solutions online User's Guide.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

PC command policy: Prevent use of Cwbcfg.exe

Use this IBM i Access policy to prevent use of the Cwbcfg utility.

For more information about this PC command, refer to the IBM i Access Client Solutions online User's Guide.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

PC command policy: Prevent use of Cwback.exe

Use this IBM i Access policy to prevent use of the cwback utility.

For more information about this PC command, refer to the IBM i Access Client Solutions online User's Guide.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

PC command policy: Prevent use of Cwbrest.exe

Use this IBM i Access policy to prevent use of the Cwbrest utility.

For more information about this PC command, refer to the IBM i Access Client Solutions online User's Guide.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

PC command policy: Prevent use of Cwbenv.exe

Use this IBM i Access policy to prevent use of the Cwbenv utility.

For more information about this PC command, refer to the IBM i Access Client Solutions online User's Guide.

Policy Type		
Restriction	Configuration	
	Suggestion	Mandate
X		

Policy Scope			
Per PC (all users)	Per user	Per user setting (May override machine setting)	Per IBM i connection
X	X	X	

Policies by template

Use these IBM i Access template files to control policies.

Choose from the following templates. See Create policy templates for more information.

Introducing Caecfg.adm

Use these policies to suggest or mandate specific IBM i Access configurable values.

Function	Policies
Communications	<ul style="list-style-type: none"> • Default user mode • TCP/IP address lookup • Port lookup mode • Require secure sockets • Connection timeout • Active Environment

Function	Policies
Passwords	<ul style="list-style-type: none"> • Warn users before IBM i password expires
National language support	<ul style="list-style-type: none"> • ANSI code page • OEM code page • EBCDIC code page • Enable BiDi transformation of data
License management	Time to delay before IBM i Access Client Solutions license is released

Caerestr.adm: IBM i Access Runtime Restrictions

Use these policies to restrict specific IBM i Access functions.

Function	Related policies
.NET Data provider	Prevent .NET Data provider usage
ActiveX Automation Objects	Prevent data queue automation object
Passwords	Prevent IBM i Access Client Solutions password changes
Communications	<ul style="list-style-type: none"> • Prevent changes to active environment • Prevent changes to active environment list • Prevent connections to systems not previously defined • Prevent use of non-mandated environments
ODBC	<ul style="list-style-type: none"> • Named data sources • Prevent program generated data sources
OLE DB provider	Prevent OLE DB provider usage
PC commands	<ul style="list-style-type: none"> • Cwblogon • Cwbcfg • Cwbback • Cwbrest • Cwbenv

Config.adm: IBM i Access mandated connections

Use these policies to mandate configuration settings for specific environments, the systems within those environments, and some configurable values for those systems.

This template only stores the environments and systems that are configured on your PC when you generate the template. If you want to add or remove environments and systems from the template, re-run cwbadgen with the /cfg option. Using the /cfg option also lets you specify a filename for the configuration template. This allows you to keep several different versions of the file, reflecting various configurations.

Function	Related policies
Environment1: system1: Communications	<ul style="list-style-type: none"> • Default user mode • TCP/IP Lookup • Port lookup mode • Require secure sockets
Environment1: system2:	
Environment2: system1:	

SYSNAME.adm: Per-system policies

Use these policies to restrict specific IBM i Access functions for a given system.

Function	Related policies
ODBC	<ul style="list-style-type: none"> • Named data sources • Prevent program generated data sources
OLE DB provider	Prevent OLE DB provider usage
.NET Data provider	Prevent .NET Data provider usage

Transport Layer Security (TLS) administration

Use IBM i Access TLS support in client/server environments.

Transport Layer Security (TLS), previously referred to as Secure Sockets Layer (SSL), is a popular security scheme that allows the client to authenticate the server and encrypts all data and requests.

Use TLS when transferring sensitive data between clients and servers. The transfer of credit card and bank statement information are examples of client/server transactions that typically take advantage of TLS. There is an increased cost in performance with TLS because of the added encryption and decryption processing.

The optionally-installed IBM i Access support for TLS allows all IBM i Access functions to communicate over TLS. The IBM i Access TLS support allows TLS communications at the 128-bit, or higher, level of encryption.

Related information

[Transport Level Security \(TLS\)](#)

Code license and disclaimer information

IBM grants you a nonexclusive copyright license to use all programming code examples from which you can generate similar function tailored to your own specific needs.

SUBJECT TO ANY STATUTORY WARRANTIES WHICH CANNOT BE EXCLUDED, IBM, ITS PROGRAM DEVELOPERS AND SUPPLIERS MAKE NO WARRANTIES OR CONDITIONS EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, REGARDING THE PROGRAM OR TECHNICAL SUPPORT, IF ANY.

UNDER NO CIRCUMSTANCES IS IBM, ITS PROGRAM DEVELOPERS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY:

1. LOSS OF, OR DAMAGE TO, DATA;
2. DIRECT, SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR

3. LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, SO SOME OR ALL OF THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_.

Programming interface information

This IBM i Access for Windows publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks of Oracle, Inc. in the United States, other countries, or both.

Other product and service names might be trademarks of IBM or other companies.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Product Number: 5770-XJ1