



PureConnect®

2018 R5

Generated:

12-November-2018

Content last updated:

8-February-2018

See [Change Log](#) for summary of changes.



# Using Active Directory Accounts with SQL Server in CIC

## Technical Reference

### Abstract

This technical reference describes how to use Windows Active Directory accounts in place of Microsoft SQL accounts in CIC.

For the latest version of this document, see the PureConnect Documentation Library at: <http://help.genesys.com/cic>.

For copyright and trademark information, see [https://help.genesys.com/cic/desktop/copyright\\_and\\_trademark\\_information.htm](https://help.genesys.com/cic/desktop/copyright_and_trademark_information.htm).

# Table of Contents

Table of Contents	2
Introduction	3
Create domain user accounts	4
Create domain group accounts	5
Install the SQL Database	6
Run IC Setup Assistant	8
Report Test 1	9
Run SQL Server script to add AD accounts	10
Run the script:	10
Allow Execute right	15
Verify the CIC reporting configuration settings	16
Reboot the CIC Server	18
Post installation considerations	19
Enable C2 audit tracing	19
Disable the named pipes protocol	20
Set SQL database to use Windows Authentication	20
Report test 2	20
Change Log	21

# Introduction

An organization can use Windows Active Directory (AD) accounts in place of the default SQL accounts that Customer Interaction Center (CIC) creates. This document explains how to use Corporate Windows Domain or Active Directory group and user accounts in CIC reporting and client applications.

IC Setup Assistant uses SQL SA Admin accounts to generate SQL user accounts and passwords, establish permissions for those accounts, and create the CIC database tables. You can create the AD group and AD user accounts defined in this document after you run IC Setup Assistant.

You run a SQL script to use those AD accounts after you complete the database portion of the IC Setup Assistant. The SQL script makes most of the required modification after you complete the IC Setup Assistant.

If you already completed the IC Setup Assistant, you can use this document to create the AD accounts in your AD domain and in you SQL Server. Run the SQL script to make the necessary changes to the SQL Server. For more information about IC Setup Assistant, see the IC Setup Assistant Help.

IC Setup Assistant creates database tables to store information for the Call Detail Report and other reports. CIC collects this information during a call, chat, or other ACD/Non ACD Group or user activity. The SQL Server that CIC uses does not contain any private personal information or CIC configuration settings. CIC can just as easily run without the SQL Server database component or just collect the information as Comma Separated Value (CSV) information.

To use AD accounts in place of the default SQL accounts in CIC, complete the following:

1. Create domain user accounts.
2. Create domain group accounts.
3. Install the SQL Server database.
4. Run IC Setup Assistant.
5. Report test 1.
6. Run the SQL script to add AD users and groups.
7. Allow Execute right.
8. Change the CIC reporting configuration settings
9. Reboot CIC server.
10. Post Installation considerations.

## Create domain user accounts

For the solution to work properly within your AD domain, you must segment the administrator, supervisor, and user accounts into definable roles to establish the correct access controls and system permissions for CIC and the operating system. Create the following AD user accounts by using the Active Directory Add Users and Computers tool on your domain controller.

Domain User	Description	Original Use
Domain\ICAdmin	A domain user that is the IC master admin for CIC. This account acts as a member of the administrator group for the local servers on CIC, Interaction Media Server, and Interaction SIP Proxy servers if the ICService account becomes compromised or locked.	Predesignated administrator account for CIC. This account is automatically created in Interaction Administrator. Link this account to the AD domain user account.
Domain\ICService	CIC, the Interaction Media server, and Interaction SIP Proxy servers use this account as the install and service account for installation and updates. Make the ICService account a member of the administrator group for each local server.	None. This account is used to segregate the IC Admin account that manages Interaction Administrator from the service account that runs CIC as a service on a Windows server.
Domain\ICDatabase	The database server uses this service account to run, install, and update and as part of the local administrator group on the database server. This account acts as the DBO for the CIC database.	None. This account is used as the SQL service account on the Database server account that runs and manages the SQ application.
Domain\DB_IC_Admin	CIC uses this account as part of the IC Report Logging and IC Tracker user ID in the IC Data source container. CIC uses the account to log the Call Detail Report data to the CIC database. CIC uses this database to generate reports in IC Business Manager.	The original predesignated non-domain, SQL server account was IC_Admin.
Domain\DB_IC_ReadOnly	CIC uses this account as part of the IC Report Logs user ID in the IC data source container. CIC uses this account to read and generate Call Detail Report data for reports in IC Business Manager.	The original predesignated non-domain, SQL server account was IC_ReadOnly.
Domain\DB_IC_User	CIC uses this account as part of the IC Contacts user ID in the IC Data Source container. CIC uses this account to read and write ODBC data source for speed dial entries in the CIC Client and IC Business Manager.	The original predesignated non-domain, SQL server account was IC_IC_User.

### Note:

- This document uses the term domain to refer to the name of the onsite domain.
- The system uses these domain\IC User accounts for functionality checks after you install CIC 2015 R1 or later and complete IC Setup Assistant. Once you complete the initial functionality checks and CIC sends and receives calls, you can disable these accounts. You create and use the normal domain user (Windows) accounts for the IC user accounts.

## Create domain group accounts

The following groups provide user and security rights for application access. Create the following domain group accounts and add the appropriate AD domain users to the group.

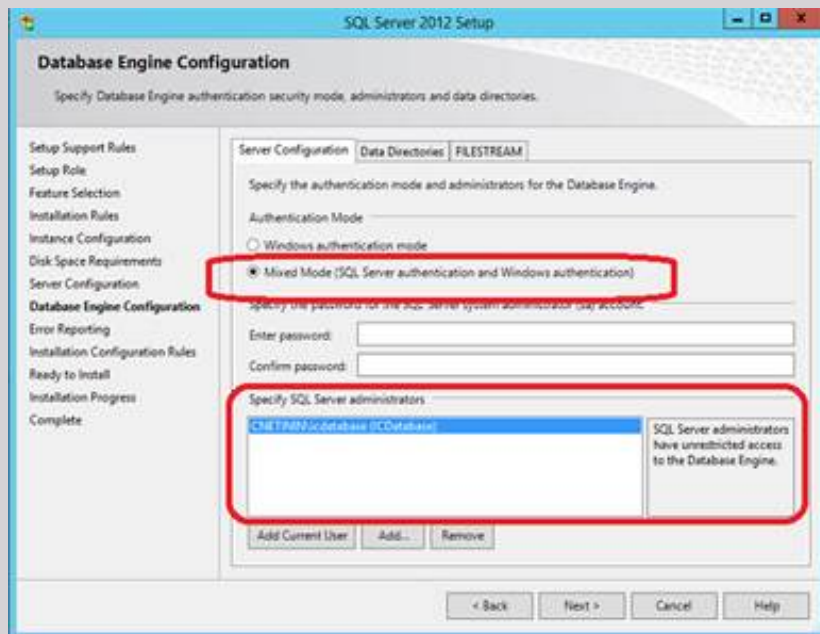
Domain Group	Description
Domain\ICDataOwner	This account group is a DBA for the I3_IC database tables. To this domain group, add CIC domain users that require DBA access to this database. The members of this group include the DB_IC_Admin, ICDatabase, and the ICService users.
Domain\ICDataReader	This account group is a Database Reader group for the I3_IC database. To this domain group, add IC domain users that require report access in IC Business Manager, Interaction Recorder client, or other report generating applications. The members of this group can include administrators, supervisors, managers, and other users that run and access reports.
Domain\ICDataWriter	This account group is a Database Writer group for the I3_IC database. To this domain group, add users that require write access to the database. This group includes users that need to write to the CIC database and Interaction Tracker tables. The members of this group can include the DB_IC_Admin, ICDatabase, and the ICService users.
Domain\ICDBAdmins	This account group is a Database Admin group for the I3_IC database. To this domain group, add users that require administrator, read, and write access to the database. The members of this group can include the DB_IC_Admin, ICDatabase, and the ICService users.
Domain\ICAdmins	This CIC Administrator group is for read and write ACL rights and permissions on the application directory shares on the CIC server. Default members: ICAdmin and ICService.
Domain\ICUsers	This group is used to allow the CIC user the appropriate ACL rights and permissions on the application directory shares on the CIC server. Default members: Any user that needs read access to the application shared directories on the CIC server.
Domain\ICAudit	This domain group is for auditing purposes. Default member: ICAuditor1.
Domain\CICAdminGrp	This account group includes the individuals that are members of the CIC Administrators role in Interaction Administrator. Add these AD users to this group so that when they use their CAC/Smart Card to log on to the server they have the appropriate CIC permissions.

## Install the SQL Database

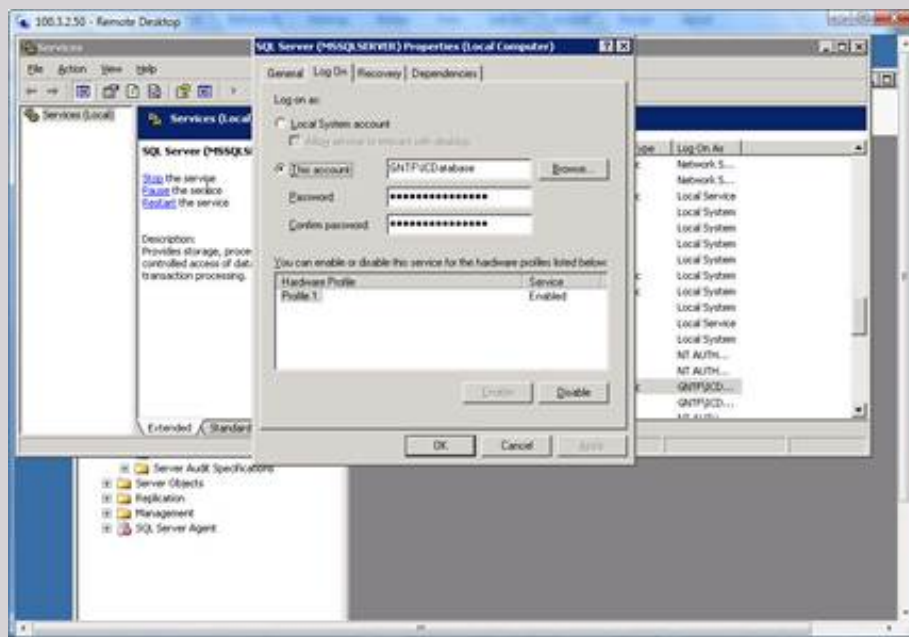
Follow the standard installation instructions for the Microsoft SQL Server 2008 R2 and later. The installation wizard guides you through the process. You can use an existing SQL Server in your environment as long as your database server meets the minimum requirements for the SQL Server for CIC. Refer to <http://testlab.genesys.com/> for information about requirements for SQL Server.

**Note:**

- When the wizard asks you to provide account information to use for the service account, enter the *Domain\ICDatabase* account.



- For a standard SQL installation, locate the SQL Server application and the related files on the first or Operating System partition (C:) with the database files on the second partition (D:).
- During the initial database setup, verify that the installation allows both SQL and Windows Authentication. In a later stage, you can disable SQL Authentication.
- After you complete the database install, verify the database service account by using the Services Control Panel in Windows. To determine that SQL Server is running under the *Domain\ICDatabase* account, display the properties for the MSSQLServer process as shown in the following example:



# Run IC Setup Assistant

Run IC Setup Assistant by using the default options in the wizard for the database configuration. IC Setup Assistant creates database tables to store information for the Call Detail report and other reports. CIC collects this information during a call, chat, or other ACD/Non ACD Group or user activity.

The IC Setup Assistant creates a CIC database that uses the default SQL accounts to create the database and appropriate tables. For more information about IC Setup Assistant, see the IC Setup Assistant Help.





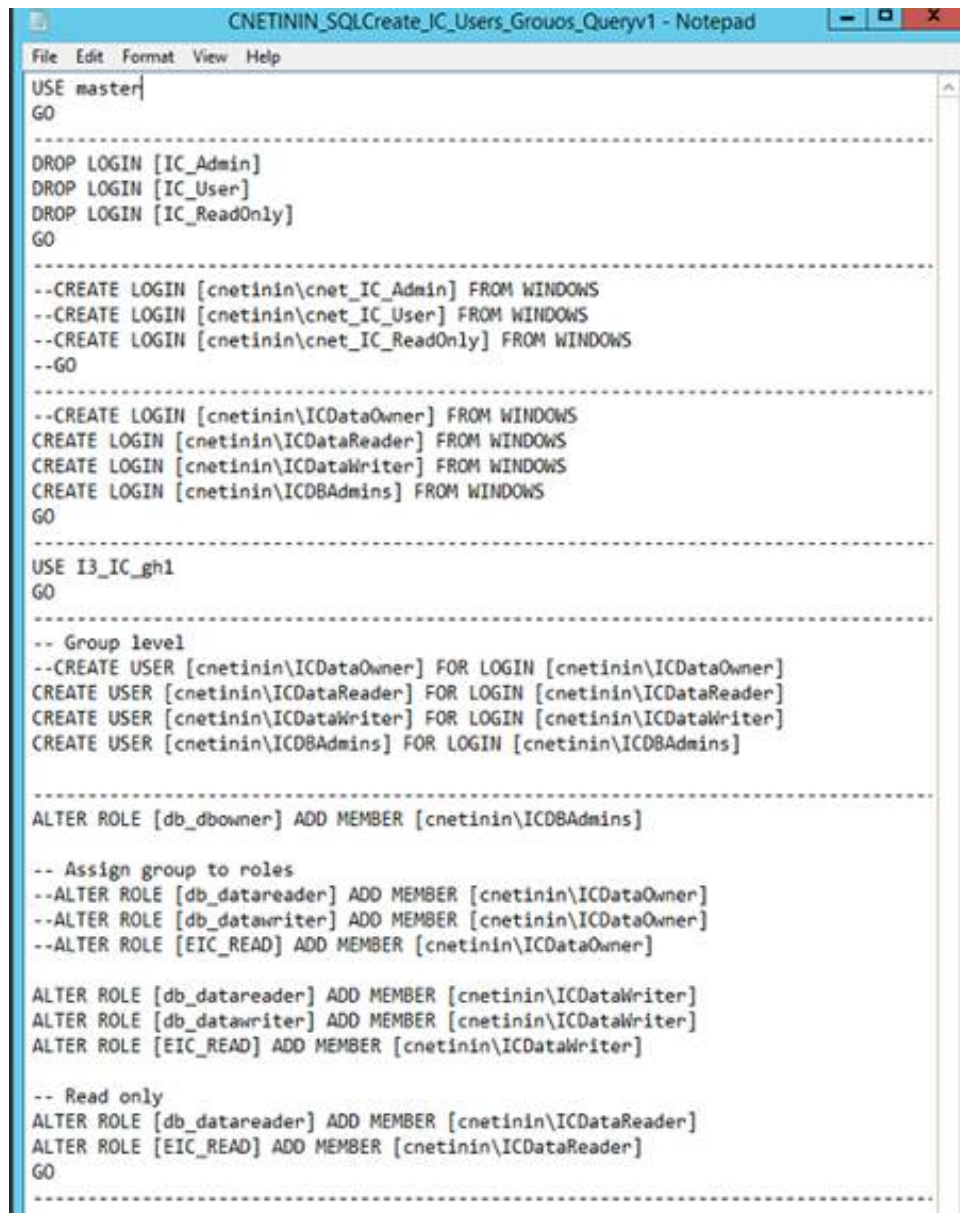
# Report Test 1

To test the CIC to SQL connection, use IC Business Manager to run a report.

1. Select a user account (for example, a supervisor) with the appropriate IC report privileges and an active Client Access license.
2. Using an account with CIC and Windows report privileges, log on to a client workstation and open IC Business manager. Run a report. If the report generates and appears with or without data, the test is successful.

## Run SQL Server script to add AD accounts

Previously, you created the domain user and group accounts that use specific permissions in SQL Server. Next, you run a set of SQL scripts to add the AD accounts to SQL Server by using the SQL Server Admin Console. The SQL scripts add the AD accounts and the SQL roles in the SQL Server application. This step allows the appropriate AD accounts access to the CIC database to perform read, write, and management operations. The following illustration shows an example script.



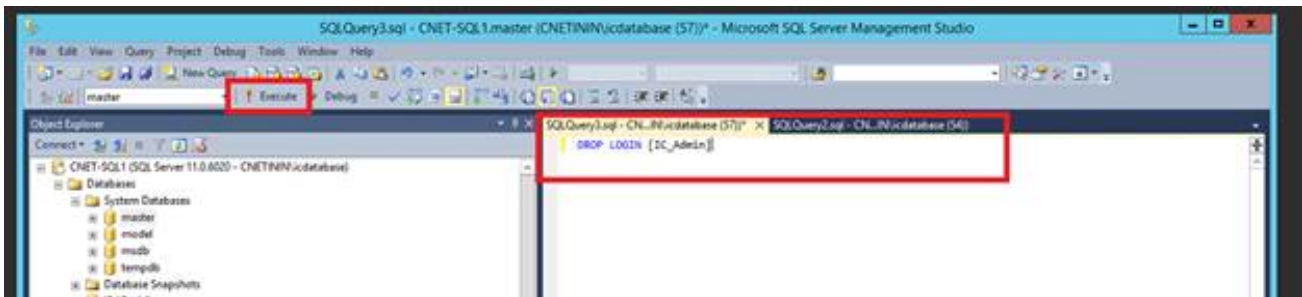
```
CNETININ_SQLCreate_IC_Users_Groups_Queryv1 - Notepad
File Edit Format View Help
USE master
GO
-----
DROP LOGIN [IC_Admin]
DROP LOGIN [IC_User]
DROP LOGIN [IC_ReadOnly]
GO
-----
--CREATE LOGIN [cnetinin\cnet_IC_Admin] FROM WINDOWS
--CREATE LOGIN [cnetinin\cnet_IC_User] FROM WINDOWS
--CREATE LOGIN [cnetinin\cnet_IC_ReadOnly] FROM WINDOWS
--GO
-----
--CREATE LOGIN [cnetinin\ICDataOwner] FROM WINDOWS
CREATE LOGIN [cnetinin\ICDataReader] FROM WINDOWS
CREATE LOGIN [cnetinin\ICDataWriter] FROM WINDOWS
CREATE LOGIN [cnetinin\ICDBAdmins] FROM WINDOWS
GO
-----
USE I3_IC_gh1
GO
-----
-- Group level
--CREATE USER [cnetinin\ICDataOwner] FOR LOGIN [cnetinin\ICDataOwner]
CREATE USER [cnetinin\ICDataReader] FOR LOGIN [cnetinin\ICDataReader]
CREATE USER [cnetinin\ICDataWriter] FOR LOGIN [cnetinin\ICDataWriter]
CREATE USER [cnetinin\ICDBAdmins] FOR LOGIN [cnetinin\ICDBAdmins]
-----
ALTER ROLE [db_downer] ADD MEMBER [cnetinin\ICDBAdmins]
-----
-- Assign group to roles
--ALTER ROLE [db_datareader] ADD MEMBER [cnetinin\ICDataOwner]
--ALTER ROLE [db_datawriter] ADD MEMBER [cnetinin\ICDataOwner]
--ALTER ROLE [EIC_READ] ADD MEMBER [cnetinin\ICDataOwner]
-----
ALTER ROLE [db_datareader] ADD MEMBER [cnetinin\ICDataWriter]
ALTER ROLE [db_datawriter] ADD MEMBER [cnetinin\ICDataWriter]
ALTER ROLE [EIC_READ] ADD MEMBER [cnetinin\ICDataWriter]
-----
-- Read only
ALTER ROLE [db_datareader] ADD MEMBER [cnetinin\ICDataReader]
ALTER ROLE [EIC_READ] ADD MEMBER [cnetinin\ICDataReader]
GO
-----
```

### Run the script:

1. Log on to the Microsoft SQL Server Management Studio console by using the local domain ICDatabase user account or local equivalent.
2. Select **New Query** from the toolbar.
3. Set the focus to the master database so that the actions are replicated in the master database and other databases on this SQL server.



- Drop login accounts. This part of the script removes the SA created SQL accounts on the SQL Server. To drop login accounts, you copy and paste a line of the script (for example, DROP LOGIN [IC\_Admin]) into the right pane of the Query window and select **Execute** from the toolbar to execute the line.



Copy, paste, and execute each of the following lines of the script:

```
DROP LOGIN [IC_Admin]
DROP LOGIN [IC_User]
DROP LOGIN [IC_ReadOnly]
```

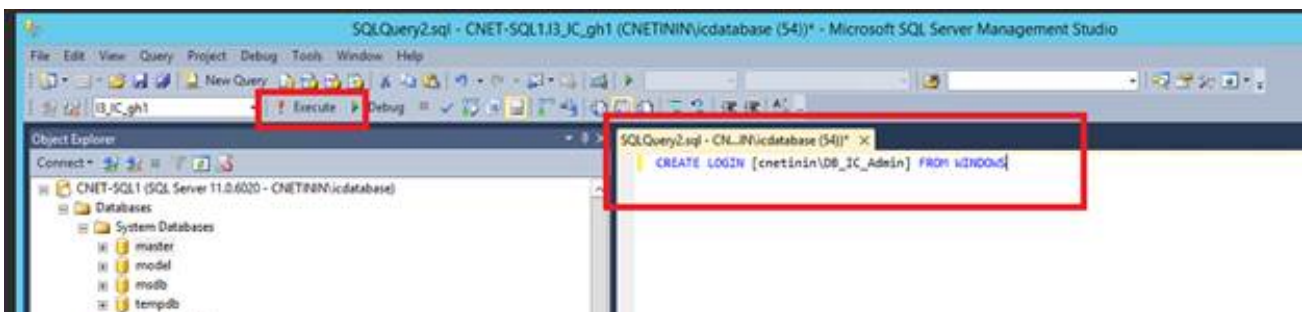
**Note:**

When you execute these lines, you may receive a warning or error that the user is connected. This is expected behavior. You can continue with the next step.

- Add domain users to the database. This part of the script adds the following domain users that you created earlier. Refer to the “Create domain user accounts” section in this document for more information about these accounts.

```
Domain\DB_IC_Admin
Domain\DB_IC_ReadOnly
Domain\DB_IC_User
```

To add domain users to the database, copy and paste a line of the script (for example, CREATE LOGIN [cnetinin\DB\_IC\_Admin] FROM WINDOWS) into the right pane of the Query window and select **Execute** from the toolbar to execute the line.



Copy, paste, and execute each of following lines of the example script. The lines from the example script use the domain name of cnetinin. Replace cnetinin with your domain user name before you execute the line.

```
CREATE LOGIN [cnetinin\DB_IC_Admin]

FROM WINDOWS
CREATE LOGIN [cnetinin\DB_IC_User]
```

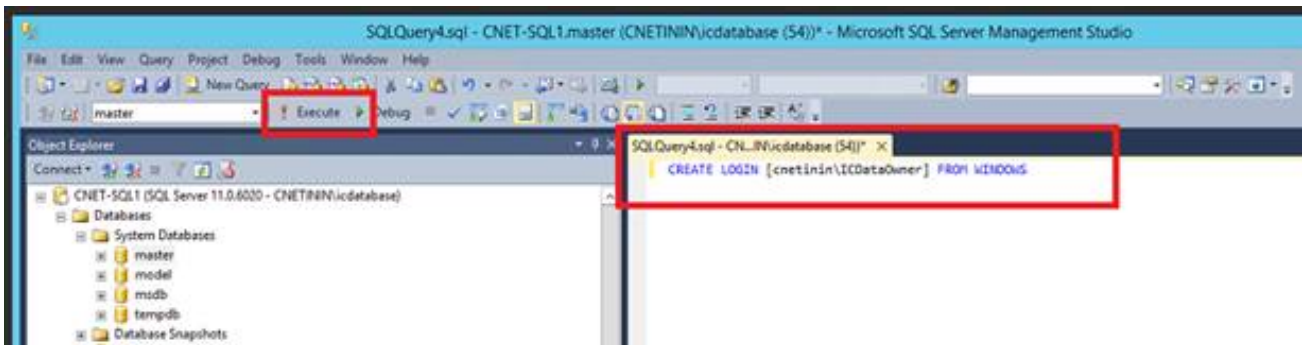
```
FROM WINDOWS
CREATE LOGIN [cnetinin\DB_IC_ReadOnly]
```

```
FROM WINDOWS
```

6. Add domain groups to the database. This part of the script adds the following domain groups that you created earlier. Refer to the "Create domain group accounts" section in this document for more information about these accounts.

```
Domain\ICDataOwner
Domain\ICDataReader
Domain\ICDataWriter
Domain\ICDBAdmins
```

To add domain groups to the database, copy and paste a line of the script (for example, CREATE LOGIN [cnetinin\ICDataOwner] FROM WINDOWS) into the right pane of the Query window and select **Execute** from the toolbar to execute the line.

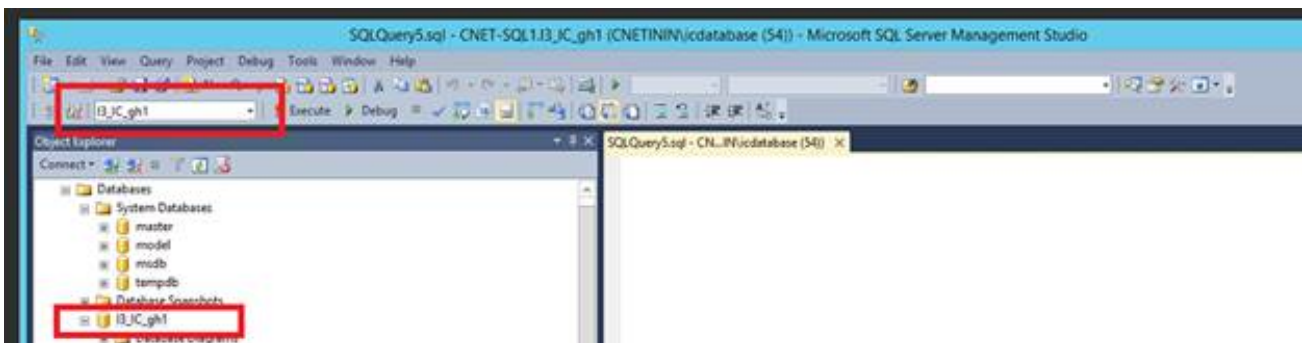


Copy, paste, and execute the following lines from the example script. The lines from the example script use the domain name of cnetinin. Replace cnetinin with your domain group name before you execute the line.

```
CREATE LOGIN [cnetinin\ICDataOwner]

FROM WINDOWS
CREATE LOGIN [cnetinin\
ICDataReader] FROM WINDOWS
CREATE LOGIN [cnetinin\
ICDataWriter] FROM WINDOWS
CREATE LOGIN [cnetinin\
ICDBAdmins] FROM WINDOWS
```

7. Set the focus to the CIC database. The example script uses the I3\_IC\_gh1 database. Set the focus to your CIC database name.



8. Create user logins for domain groups. This part of the script creates user logins for the following domain groups that you created earlier. Refer to the "Create domain group accounts" section in this document for more information about these

accounts.

```
Domain\ICDataOwner  
Domain\  

```

```
ICDataReader  
Domain\  

```

```
ICDataWriter  
Domain\  

```

```
ICDBAdmins
```

To create user logins for domain groups, copy and paste a line of the script (for example, `CREATE USER [cnetinin\ICDataOwner] FOR LOGIN [cnetinin\ICDataOwner]`) into the right pane of the Query window and select **Execute** from the toolbar to execute the line.



Copy, paste, and execute the following lines from the example script. The lines from the example script use the domain name of `cnetinin`. Replace `cnetinin` with your domain group name before you execute the line.

```
CREATE USER [cnetinin\ICDataOwner]
```

```
FOR LOGIN [cnetinin\ICDataOwner]  
CREATE USER [cnetinin\ICDataReader]
```

```
FOR LOGIN [cnetinin\ICDataReader]  
CREATE USER [cnetinin\ICDataWriter]
```

```
FOR LOGIN [cnetinin\ICDataWriter]  
CREATE USER [cnetinin\ICDBAdmins]
```

```
FOR LOGIN [cnetinin\ ICDBAdmins]
```

- Alter roles and assign groups to roles. This part of the script alters SQL roles and assigns groups to roles for the following domain groups that you created earlier. Refer to the "Create domain group accounts" section in this document for more information about these accounts.

```
Domain\ICDataOwner  
Domain\  

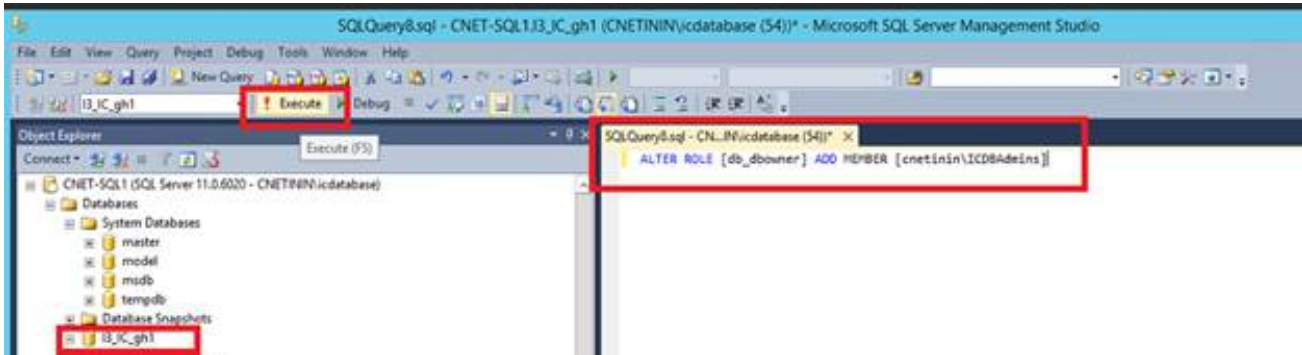
```

```
ICDataReader  
Domain\  

```

```
ICDataWriter
```

To alter roles and assign groups to roles, copy and paste a line of the script (for example, `ALTER ROLE [db_datareader] ADD MEMBER [cnetinin\ICDataOwner]`) into the right pane of the Query window and select **Execute** from the toolbar to execute the line.



Copy, paste, and execute the following lines from the example script. The lines from the example script use the domain name of `cnetinin`. Replace `cnetinin` with your domain group name before you execute the line.

```
ALTER ROLE [db_datareader]

ADD MEMBER [cnetinin\ICDataOwner]
ALTER ROLE [db_datawriter]

ADD MEMBER [cnetinin\ICDataOwner]
ALTER ROLE [EIC_READ]

ADD MEMBER [cnetinin\ICDataOwner]
ALTER ROLE [db_datareader]

ADD MEMBER [cnetinin\ICDataWriter]
ALTER ROLE [db_datawriter]

ADD MEMBER [cnetinin\ICDataWriter]
ALTER ROLE [EIC_READ]

ADD MEMBER [cnetinin\ICDataWriter]
ALTER ROLE [db_datareader]

ADD MEMBER [cnetinin\ICDataReader]
ALTER ROLE [EIC_READ]

ADD MEMBER [cnetinin\ICDataReader]
```

## Allow Execute right

Interaction Recorder uses stored procedures to insert records in the database. For the CIC server to execute these stored procedures, execute the following command against the I3\_IC Database. Use the name you used to create the CIC database.

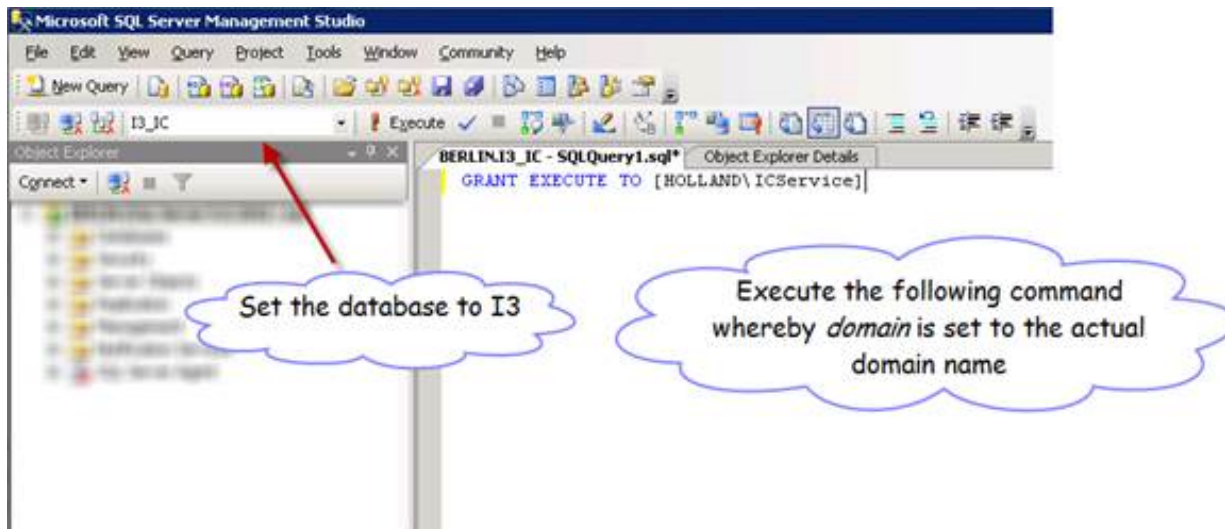
Use the following format for the command and replace *DOMAIN* with the actual domain name:

```
GRANT EXECUTE TO [DOMAIN\ICService]
```

For example:

```
Grant EXECUTE TO [Holland\ICService]
```

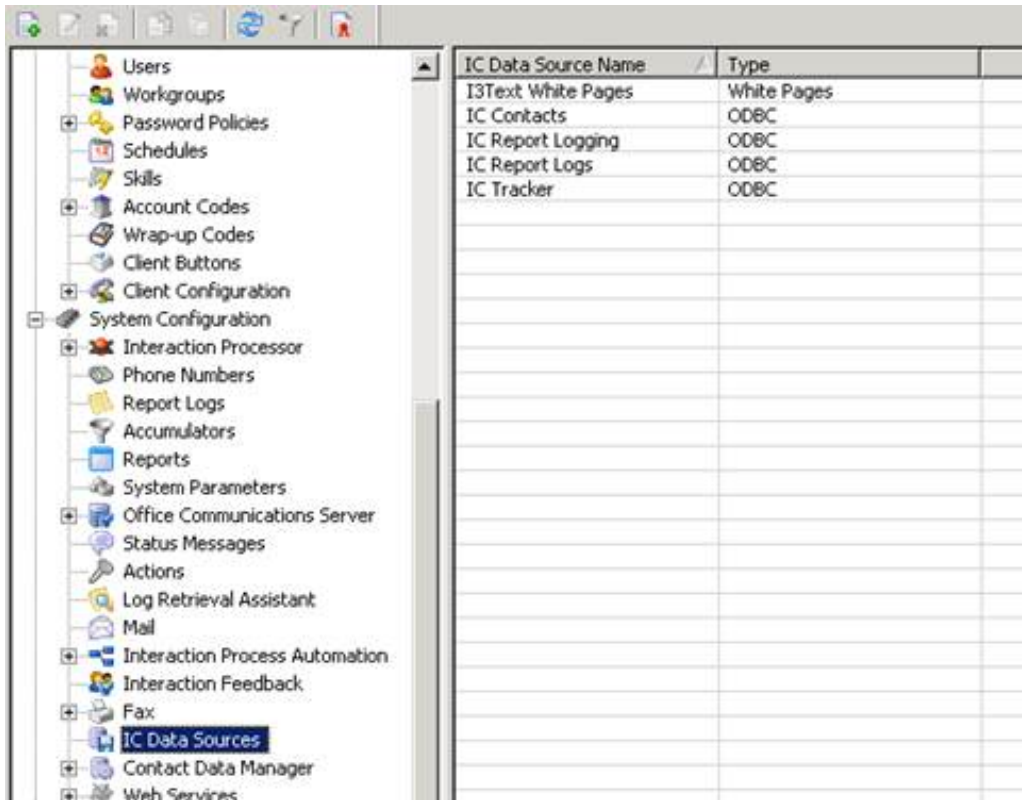
The following illustration shows the command to execute against the I3\_IC database:



# Verify the CIC reporting configuration settings

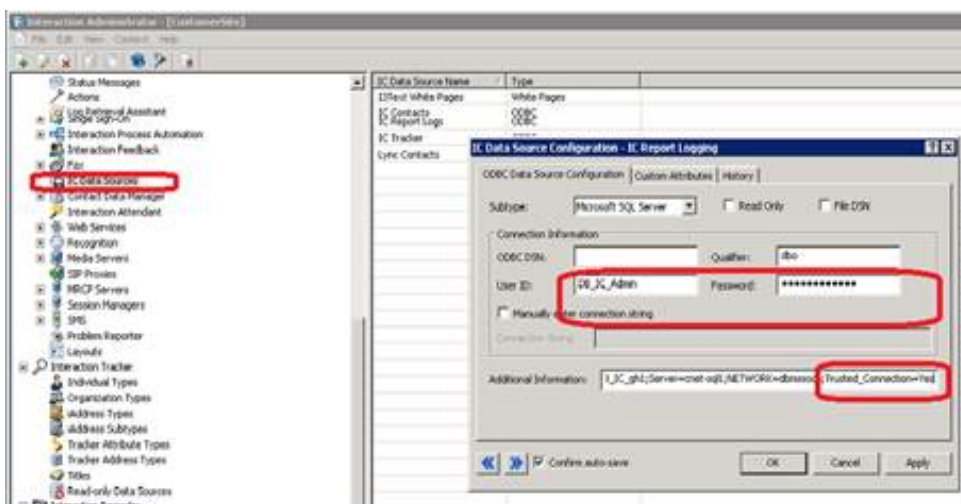
There are several settings in Interaction Administrator to verify in order to make sure that the system and users use Windows Authentication to authenticate with the database.

Open Interaction Administrator and select **IC Data Sources** under **System Configuration**. The following illustration shows the data sources:



Verify that the following data sources use the new domain user accounts (Windows Authentication) to connect with the database:

- IC Contacts
- IC Report Logging
- IC Report Logs
- IC Tracker



Verify or update the connection information in the **Additional Information** field to contain the following connection string:

```
Driver={SQLServer};Database=I3_IC;Server='SERVERNAME';NETWORK=dbmssocn;Trusted_Connection=Yes
```

Replace *SERVERNAME* with the actual server name of the database server.



The system uses the `DomainIC\Service` account to connect to the database. Each user that runs a report from their workstation uses their own account to connect to the database. You can grant access for a user by making their domain account a member of the `DomainIC\DataReader` group.

# Reboot the CIC Server

To run reports, you must reboot the CIC server to adopt the new SQL settings.

**Note:**

Add the appropriate users to the appropriate IC permissions and domain groups so they have Windows permissions to run the IC reports.

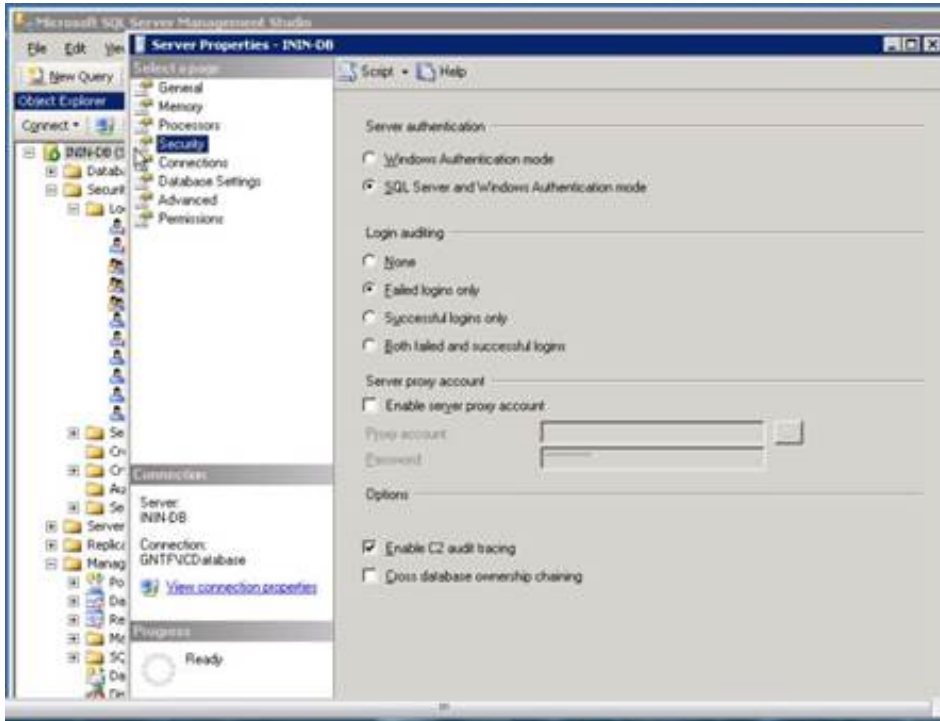
# Post installation considerations

## Enable C2 audit tracing

Enable C2 auditing tracing to configure SQL Server to record both failed and successful statements and objects access attempts. This information can help you identify and profile system activity and track possible security policy violations. C2 auditing saves a large amount of event information to the log file. If the data directory that includes the log file runs out of space, SQL Server shuts down. If your company requires the use of C2 audit tracing, you can enable C2 audit tracing.

To enable C2 Audit tracing:

1. Open the Microsoft SQL Server Management Studio, and open the properties dialog of the server object.
2. Select the **Security** page.
3. Select **Enable C2 auditing tracing** under **Options**.

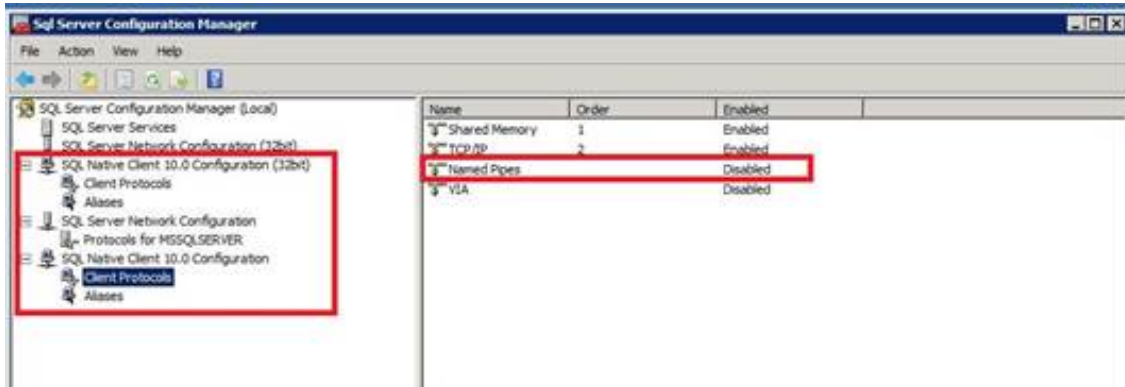


## Disable the named pipes protocol

If your company does not require the use of named pipes protocol, you can disable named pipes on SQL Server.

To disable the named pipes protocol on SQL Server:

1. Log on to SQL Server and start the SQL Server Configuration Manager.
2. Select **SQL Server Configuration manager > SQL Server Network Configuration**.
3. Disable the named pipe protocol in the following configuration containers:
  - SQL Native Client 10.0 Configuration (32bit)
  - SQL Server Network Configuration
  - SQL Native Client 10.0 Configuration



4. Double-click **Named Pipes**.  
The **Named Pipes Properties** screen appears.
5. From **Enabled**, select **No**.
6. Click **OK**.

## Set SQL database to use Windows Authentication

1. Move to the top of the Database and right-click the database server name. Select **Properties**.
2. Double click the **Security** container.
3. Change the server authentication to **Windows authentication**.
4. Click **OK**.

## Report test 2

Using an account with CIC and Windows report privileges, log on to a client workstation and open the IC Business Manager to verify that the user can still run a report.

# Change Log

Date	Change
11-November-2015	New document.
21-April-2016	Added new information received from SME. Updated copyright and trademark information.
11-January-2018	Conversion to HTML
8-February-2018	Rebranding terminology and cover page.