Proficy CSense

Secure Deployment Guide

Proprietary Notice

The information contained in this publication is believed to be accurate and reliable. However, General Electric Company assumes no responsibilities for any errors, omissions or inaccuracies. Information contained in the publication is subject to change without notice.

No part of this publication may be reproduced in any form, or stored in a database or retrieval system, or transmitted or distributed in any form by any means, electronic, mechanical photocopying, recording or otherwise, without the prior written permission of General Electric Company. Information contained herein is subject to change without notice.

Trademark Notices

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company.

Microsoft® is a registered trademark of Microsoft Corporation, in the United

States and/or other countries. All other trademarks are the property of their

respective owners.

We want to hear from you. If you have any comments, questions, or suggestions about our documentation, send them to the following email address:

doc@ge.com

Table of Contents

1 About This Guide

The Proficy CSense Secure Deployment Guide is intended for process control engineers, integrators, IT professionals, and developers responsible for deploying and configuring CSense.

1.1 What is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- Confidentiality: Ensures only the people you want to see information can see it.
- Integrity: Ensures the data is what it is supposed to be.
- Availability: Ensures the system or data is available for use.

General Electric Company recognizes the importance of building and deploying software with these concepts in mind and encourages customers to take appropriate care in securing their General Electric Company products and solutions.

1.2 Defense in Depth

Defense in Depth is the concept of using multiple layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability but would also need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent the firewall and the username/password authentication.

General Electric Company recommends a Defense in Depth security strategy for your products and solutions.

1.3 Security Information on the Web

For more on General Electric Company and security, see: http://www.ge.com/security.

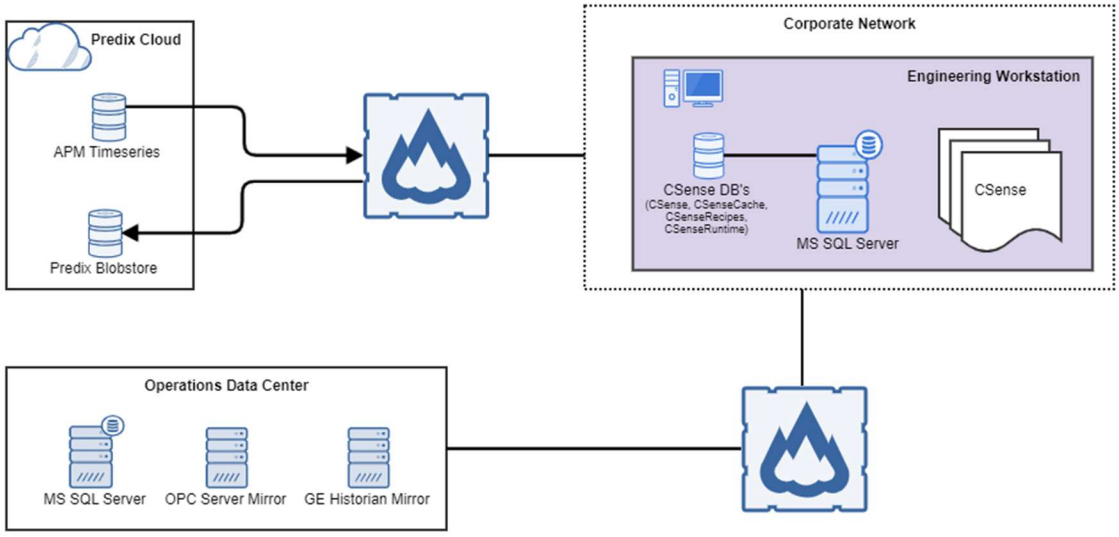
Be sure to consult the General Electric Company support site regularly to stay up to date on security patches and updates.

2 Network Architecture and Secure Deployment

CSense supports a wide variety of industrial sectors and organizational models. The appropriate architecture for an installation varies based on these and other factors. This section provides two example reference architectures along with an explanation of the security benefits and applicability of the architectural choices. Use the examples as guidance. The appropriate architecture may be a variant of the examples based on the organization's operational needs and risk management decisions.

2.1 Single Computer

This is the deployment scenario that will be used by the process engineer or analytic developer using a Troubleshooter or Developer license. In this scenario CSense will be installed on an engineering workstation/laptop located on the Corporate Network. Analytic development/testing and data analyses are entirely performed on this workstation with access to data located in the Data Center and Predix Cloud only. The Data Center is on a segregated network that uses mirrors of the data servers located in the Plant Network. There should not be a direct route from the Corporate Network to the Plant Network.

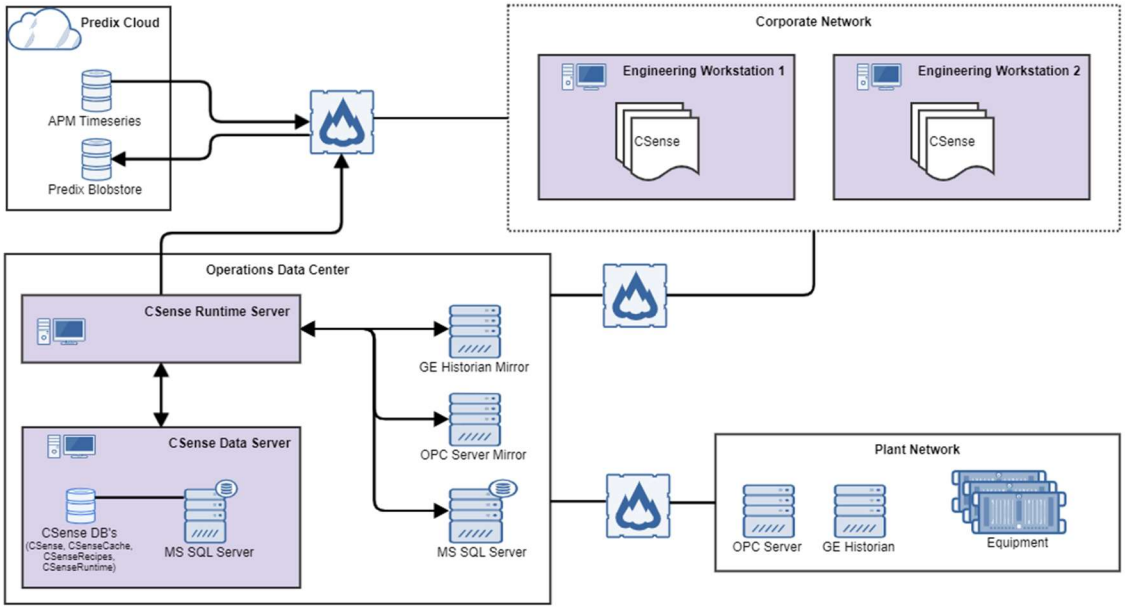


2.2 Separate Development and Runtime Server

In an Enterprise Environment this is the typical deployment scenario that will be used in a plant where analytics are being developed as well as running those analytics on live data for the plant. In this scenario analytic development/testing will be performed on separate machines using Troubleshooter and/or Developer licenses located on the Corporate Network. Execution of analytics on live data using a Runtime license will happen on a different machine located in the Data Center. This Data Center will also contain the single CSense Data Server installation running on SQL Server that will be shared by all CSense installations.

The Data Center is on a segregated network that uses mirrors of the data servers located in the Plant Network, which in turn is also on a segregated network. There should be not be a direct route from the

Corporate Network to the Plant Network.



3 CSense System Configuration

3.1 CSense Ports

By default, CSense does not configure or require specific ports during installation. See the section on Firewall Configuration in this document for more information on setting up your firewall for specific capabilities and scenarios.

3.2 Windows Services

The following Windows Services are installed to run in the listed Windows Accounts:

Services	Process	Default Windows Account
Proficy CSense Run-time	ActionObjectServices.exe	Local System Account (NT AUTHORITY\SYSTEM) or Specified account
Proficy CSense Run-time List Server	ActionObjectListServer.exe	Local System Account (NT AUTHORITY\SYSTEM) or Specified account

3.3 Applications

The table below shows the CSense applications available after installation, indicating which applications require administrative rights on the local system, and which applications require logins on the instance of

SQL Server where the CSense databases were installed.

CSense Application	Process Name	Default Windows User Account	Windows User Account Requires Local Admin rights	Windows User Account Requires SQL Server Login	CSense Database access
Start Center	Start Center.exe	Launching user	No	No	-
Action Object Manager	Action Object Manager.exe	Launching user	Yes	Yes	CSenseRuntime CSense CSenseCache
Architect	Architect.exe	Launching user	No	No	-
Continuous Troubleshooter		Launching user	No	Yes	CSenseRecipes CSense
Discrete & Batch Troubleshooter	Discrete and Batch Troubleshooter.exe	Launching user	No	Yes	CSenseRecipes
Decision Tree	DecisionTree.exe	Launching user	No	No	-
MPC Editor	MPC Editor.exe	Launching user	No	No	-
Realtime Action Objects	MGDynamo.exe	Local System Account (NT AUTHORITY\SYSTEM) or Specified account	Yes	No	CSenseCache
Scheduled Action Objects	Scheduled ActionObject.exe	Local System Account (NT AUTHORITY\SYSTEM) or Specified account	Yes	Yes	CSenseRuntime CSense CSenseCache

3.4 Database Setup

Each CSense installation will require access to a MS SQL Server Instance. This instance can be on the local machine or located on a shared centralized machine that will be used by all CSense installations. CSense will create the required CSense databases on the target SQL Server instance, and set up the correct database users and roles. The following sections describes the setup and configuration of MS SQL Server:

- Server Configuration
- Logins and Server Roles
- Databases
- Database Users and Roles

3.4.1 Server Configuration

CSense allows the user to install a Managed SQL Server instance. A managed instance is a dedicated local SQL Express server that is installed and configured as part of the CSense installation and requires no user input. It is a named instance called CSENSE. Users will typically connect to the instance by providing

<*machinename*>\CSENSE.

For the managed instance, SQL Server Authentication is disabled, the SA administrator account is disabled as well as the ***csense_db_user*** account. Both SQL Server Authentication and the ***csense_db_user*** can be enabled. Enabling of both allows reading of data from ***csense*** and ***cache*** database from third party applications. See *Adding additional CSense users after installing CSense* for more information. This managed instance has the following protocols enabled by default:

- Shared Memory
- Named Pipes
- TCP/IP

Users upgrading from either CSense 7.0 or CSense 7.0 SP1 do not have the option to install a managed instance.

Alternatively, a dedicated centralized installation of SQL Server can be shared by multiple CSense installations. The Data Server installation option will configure the databases needed for CSense use. The ***csense_db_user*** account using SQL Server Authentication will be created but disabled. Both SQL Server Authentication and the ***csense_db_user*** can be enabled. Enabling of both allows reading of data from ***csense*** and ***cache*** database from third party applications. See *Adding additional CSense users after installing CSense* for more information.

NOTE: See the guide on *Security Best Practices and Guidelines* on how to configure and secure your managed or unmanaged instance.

3.4.2 SQL Server Logins and Server Roles

After installing and setting up CSense, the following logins will be created if they do not already exist on the target instance of MS SQL Server.

Login	Server Roles	Login Type	Status
<Installing User>	dbcreator securityadmin serveradmin (NOTE: These roles are required prior to installation)	Windows Authentication	Enabled
NT AUTHORITY\SYSTEM	public	Windows Authentication	Enabled
csense_db_user	public	SQL Authentication	Disabled
*<Additional Users>	public		

* NOTE: See the guide on adding additional CSense users to your target system later in this document.

3.4.3 Databases

During installation, the CSense installer will create and configure the following databases on the target MS SQL Server instance. The installing user will be configured as the database owner of all created CSense databases.

Database Name	Database Owner (dbo)
CSenseRuntime	dbo (Installing User)

CSenseRecipes	dbo (Installing User)
CSense	dbo (Installing User)
CSenseCache	dbo (Installing User)

3.4.4 Database Users and Roles

During installation, the CSense installer will create the required Databases and set up Database Users and Database Roles for the relevant CSense databases on the target instance of MS SQL Server. Roles will be assigned to the created Database Users, and the Database Users mapped to the relevant SQL Server Logins.

CSenseRuntime Database

SQL Server Login	Database User	Database Roles
<Installing User>	dbo	db_owner
NT AUTHORITY\SYSTEM	csense_runtime	csense_admin csense_execute
* <Additional Users>	<Additional Users>	csense_admin csense_cache

* Follow the guides on adding additional CSense users later in this document.

CSenseRecipes Database

SQL Server Login	Database User	Database Roles
<Installing User>	dbo	db_owner
* <Additional Users>	<Additional Users>	csense_cache

CSense

SQL Server Login	Database User	Database Roles
<Installing User>	dbo	db_owner
NT AUTHORITY\SYSTEM	csense_runtime	csense_execute
csense_db_user	csense_db_user	csense_data_reader
* <Additional Users>	<Additional Users>	csense_admin
* <Additional Users>	<Additional Users>	csense_troubleshooter

* Follow the guides on adding additional CSense users later in this document.

CSenseCache

SQL Server Login	Database User	Database Roles
<Installing User>	dbo	db_owner
NT AUTHORITY\SYSTEM	csense_runtime	csense_execute

csense_db_user	csense_db_user	csense_data_reader
* <Additional Users>	<Additional Users>	csense_admin

* Follow the guides on adding additional CSense users later in this document.

3.5 DCOM Configuration

During installation, CSense will register several COM servers on the target system with specific permissions, authentication, and identity. Of these, the following COM Servers are used for deploying and browsing deployed analytics:

- Action Object Server
- Scheduled Action Object
- OPC Classic Server Enumerator
- List Server service

3.5.1 CSense Real-time Action Objects

The Action Object Server is installed as a Local Server and is used to host real-time deployed analytics. The table below lists the DCOM configuration applied during installation:

Application Name	Action Object Server
Application Level	Local Server
Authentication Level	Default
Launch and Activation Permissions	Use Default
Access Permissions	Use Default
Configuration Permissions	Users group (READ) Administrators group (FULL CONTROL) SYSTEM (FULL CONTROL)
Identity	Launching User

3.5.2 CSense Scheduled Action Objects

The Scheduled Action Object is installed as a Local Server and is used to host deployed scheduled analytics. The table below lists the DCOM configuration applied during installation:

Application Name	ScheduledActionObject
Application Level	Local Server
Authentication Level	Default
Launch and Activation Permissions	Use Default
Access Permissions	Use Default
Configuration Permissions	Users group (READ) Administrators group (FULL CONTROL) SYSTEM (FULL CONTROL)
Identity	Launching User

3.5.3 CSense List Server service

The CSense List Server service is installed as a Local Service and is by the various Action Object Management components for deployed analytics. The table below lists the DCOM configuration applied during installation:

Application Name	Proficy CSense Run-time List Server
Application Level	Local Service
Authentication Level	Default
Launch and Activation Permissions	Use Default
Access Permissions	Use Default
Configuration Permissions	Users group (READ) Administrators group (FULL CONTROL) SYSTEM (FULL CONTROL)
Identity	The system account (services only)

3.5.4 OPC Classic Server Enumerator Service

This 3rd party Local Service is provided by the OPC redistributable available from the OPC Foundation. The table below lists the DCOM configuration applied during installation:

Application Name	OPCEnum
Application Level	Local Service
Authentication Level	None
Launch and Activation Permissions	EVERYONE (Local Launch, Remote Launch, Local Activation, Remote Activation) INTERACTIVE (Local Launch, Remote Launch, Local Activation, Remote Activation) Administrators group (Local Launch, Remote Launch, Local Activation, Remote Activation) SYSTEM (Local Launch, Remote Launch, Local Activation, Remote Activation)
Access Permissions	EVERYONE (Local Access, Remote Access) SELF (Local Access, Remote Access) SYSTEM (Local Access)
Configuration Permissions	EVERYONE (FULL CONTROL) INTERACTIVE (FULL CONTROL) Administrators group (FULL CONTROL) SYSTEM (FULL CONTROL)
Identity	The system account (services only)

4 Firewall Configuration

CSense uses the following default ports for communication:

Default Port on Windows (Note, this port may be different on your target system)	Protocol	Description	Notes
135	TCP or UDP	Default port for RPC communication used by DCOM	This is required for all remote connections that require DCOM, e.g. connections to an OPC Classic Server.
443	HTTPS	Default port for SSL connections	Downloading data from Predix APM Timeseries. Uploading data to Predix Blobstore Installing/Updating custom Python packages using PIP
1433	TCP/IP	Default port for SQL Server	Required if a shared remote instance of SQL Server is used for the Data Server installation.

In addition to the above, CSense can connect to 3rd Party Data Connectors. Consult the documentation of these for their Firewall configuration.

5 Encryption of Credentials

By default, all user account information which is stored by CSense is protected by encryption. This includes the following scenarios:

- User account information relating to sources and sinks in the Architect is stored encrypted within the blueprint or troubleshooter project file.
- User account information stored in superblocks is encrypted.

6 Logging and Auditing

CSense logs are found in the standard Windows event logs. For the Action Object Manager, information logged to the event log is also sent to the Runtime database.

7 Security Best Practices and Guidelines

7.1 Downloading Data from the Cloud

You may choose to download data from the secure Predix Cloud environment, such as when using the Timeseries Source in CSense.

When downloading data from the Predix Timeseries storage in the Predix Cloud environment using the Timeseries source in the Continuous Troubleshooter or Batch & Discrete Troubleshooter, downloaded data is temporarily cached in the CSense SQL Server database while the relevant Troubleshooter project file remains open int the CSense Troubleshooter application. The cached data is deleted when the Troubleshooter project is closed.

When downloading data from the Predix Timeseries Cloud storage using the Import from Predix Timeseries option in the Troubleshooter:

- You will be asked to acknowledge that data is being downloaded from secure Cloud storage to local storage and provide authorization for data retrieval.
- Ensure that your SQL Server installation is secured using industry best practices.

If you choose to export the data to a local file and store this elsewhere:

- Determine exactly where the data is going to be stored.
- Ensure that the environment where that data is stored is properly secured.
- Ensure that access to that exported data is restricted to only those users who have a need to use the data.

7.2 Securing your CSense OPC Classic Server

NOTE: This section requires a good level of understanding and familiarity with COM/DCOM configuration and Windows Security. See the DCOM Configuration Guide in the CSense help documentation for further information.

Modern Windows Operating Systems like Windows 10 and Windows Server 2019 block remote COM/DCOM access by default except for members of the Administrators group. This should be verified on your installation and if needed, follow the steps described below to create a more secure environment.

All Real-time Action Objects executing in CSense are OPC Classic Servers as well. This implies that OPC Classic Clients can establish connections, including connecting remotely, to CSense OPC Classic Servers. Real-time Action Objects that makes use of OPC Classic Server Source/Sink blocks will make items available that can be browsed for from these OPC Classic Clients. The values of these items can be read from and written to from OPC Classic Clients. Real-time Action Objects that *do not* make use of OPC Classic Server Source/Sink blocks can be connected to but there will be no items to read from/write to from OPC Classic Clients.

This behavior is by design and is required to comply with the OPC Classic specification. The CSense Runtime installation may operate on sensitive data/environments. The following can be done to restrict

access to CSense OPC Classic Servers in these environments. These restrictions are global and affects all CSense OPC Classic Servers on a given machine.

A quick change is to disable the OPCEnum Windows Service. This will prevent OPC Classic Clients from browsing for available OPC Classic Servers on a given machine. However, this will still allow OPC Classic Clients to connect if they know or can guess the CLSID or PROGID of the CSense OPC Classic Server.

To disable remote connections to CSense OPC Classic Servers, perform the following steps:

1. Use the DCOM configuration tool (DCOMCNFG) and Deny the **Remote Launch** and **Remote Activation** permission for all groups under the **Launch and Activation Permissions** for the **OPCEnum** entry. Note, changing the settings of **OPCEnum** may influence other software installations using OPC Classic on the same machine since **OPCEnum** is a shared component.

2. Use the DCOM configuration tool (DCOMCNFG) and Deny the **Remote Launch** and **Remote Activation** permission for all groups under the **Launch and Activation Permissions** for the **Action Object Server** entry.

To disable remote connections from Architect to Real-time Action Objects and obtaining indirect access to the CSense OPC Classic Servers, perform the following step:

1. Use the DCOM configuration tool (DCOMCNFG) and Deny the **Remote Launch** and **Remote Activation** permission for all groups under the **Launch and Activation Permissions** for the **Proficy CSense Run-time List Server** entry.

Alternatively, if a level of control over connections is required, use firewall rules with a whitelist approach to allow only a certain minimal set of machines to connect to the CSense Runtime Server machine. To establish user level control, create a group for whitelisted users and provide remote access to this group only

To create a whitelisted group for remote access, perform the following steps:

1. Create a dedicated domain user group, e.g. CSense Remote Access

2. Add the users that require remote access to this domain group

To configure COM/DCOM remote access for the CSense Remote Access domain group start the DCOM configuration tool (DCOMCNFG) and perform the following steps:

1. On the **My Computer** entry, open **Properties** and go to the **COM Security** tab:

    a. Under **Launch and Activation Permissions** click **Edit Limits** and *allow* the **Remote Launch** and **Remote Activation** permissions for the CSense Remote Access domain group.

    b. Under **Access Permissions** click **Edit Limits** and *allow* the **Remote Access** permission for the CSense Remote Access domain group.

2. For each of the following entries under **DCOM config**:

    a. Action Object Server

    b. Proficy CSense Run-time List Server

3. Set the following permissions using the **Security** tab:

    a. Under **Launch and Activation Permissions** select **Custom** and *allow* the **Remote Launch** and **Remote Activation** permissions for the CSense Remote Access domain group.

    b. Under **Access Permissions** select **Custom** and *allow* the **Remote Access** permission for the CSense Remote Access domain group.

7.3 Changing and restricting accounts for CSense Action Objects & Services

By default, all CSense services are installed to the Local System Account. However, in order to connect to remote SQL Servers using Windows authentication, or connecting to remote OPC Classic Servers, you may be required to change the account in which CSense runtime services and application are running. Changing the accounts in which CSense services are running, is a two-step process involving:

1. Configuring the CSenseRuntime database with the correct SQL logins, roles and permissions, and
2. Changing the Windows user account in which the service is currently running.

7.3.1 CSense SQL Server configuration

1. Identify the Windows user account you require your CSense services to run in. This user account requires administrative rights on the local machine.
2. Create a SQL Server login for the Windows user account on the local instance of SQL Server where the **CSenseRuntime** database exists.
3. Ensure that the created *SQL Server Login* has at least the ***public*** server role assigned.
4. Create a *database user* on the ***CSenseRuntime*** database.
5. Map the created *database user* to the *SQL Server login* you created.
6. Assign the ***csense_cache*** database role to the database user
7. Assign the ***csense_admin*** database role to the database user
8. Assign the ***csense_execute*** database role to the database user

7.3.2 CSense Service configuration

1. Stop all running Action Objects and close all CSense applications
2. Open the Windows Services application on your CSense host system
3. Find the "Proficy CSense Run-time" service in the listing of services

4. Stop the "Proficy CSense Run-time" service if it is running. (You may be required to stop all CSense services at this point)

5. Right-click on the "Proficy CSense Run-time" service and select **Properties**

6. Navigate to the "Log On" tab and change the selection on this tab to "This account"

7. Specify the Windows account and password that you have configured with a SQL Login in the previous section

8. Apply your changes by clicking OK

9. Start the "Proficy CSense Run-time" service

7.4 Adding additional CSense users after installing CSense

Setting up additional users depends on the installation option and the IT environment.

7.4.1 Express Installation

After installing CSense, the installing Windows user account is properly configured by the installer for using CSense and no additional steps are required for the user account.

7.4.2 Advanced Installation with existing local SQL Server

If the installing Windows user account is different from the Windows user account that will be using the CSense software, then additional steps must be completed to set up the new user account. Note, these steps must be completed for each Windows user account using CSense on the target system.

The table below describes the privileges needed for the SQL Server and Windows logins needed for each user account that want to make use of CSense. “User Account” is a generic term that satisfy the following conditions:

- Can login to Windows
- The Windows login is mapped to a SQL Server login that has the public Server Role assigned

“User Account” can be implemented using individual user accounts or groups, either on the local machine or on an Active Directory Domain level.

License Type	Windows Privileges	Database	SQL Server Database Roles
CSense Troubleshooter	User	CSenseRecipes	csense_cache
		CSense	csense_troubleshooter
CSense Runtime	Local Machine Administrator	CSenseRuntime	csense_cache csense_admin
		CSense	csense_admin
		CSenseCache	csense_admin

License Type	Windows Privileges	Database	SQL Server Database Roles
CSense Developer	Local Machine Administrator	CSenseRecipes	csense_cache
		CSenseRuntime	csense_cache csense_admin
		CSense	csense_admin csense_troubleshooter
		CSenseCache	csense_admin

The steps required depends on your CSense license. Note your CSense license and choose from the following procedures.

7.4.2.1 Adding users for CSense Troubleshooter licenses

To add a Windows user account as a Troubleshooter user:

1. Identify the Windows user account. Note that all local and domain user accounts may run the Troubleshooter, no special rights and permissions are required.

2. Create a *SQL Server login* for the Windows user account on the target instance of SQL Server where the ***CSenseRecipes*** database exists.

3. Ensure that the created *SQL Server Login* has at least the *public* server role assigned.

4. Create a *database user* on the ***CSenseRecipes*** database.

5. Map the created *database user* to the *SQL Server login* you created.

6. Assign the ***csense_cache*** database role to the database user

7. Create a *database user* on the ***CSense*** database.

8. Map the created *database user* to the *SQL Server login* you created.

9. Assign the ***csense_troubleshooter*** database role to the database user.

7.4.2.2 Adding users for CSense Runtime licenses

To add a Windows user account as a CSense runtime user:

1. Identify the Windows user account. Note that all users of the CSense runtime edition require administrative rights on the local machine.

2. Create a *SQL Server login* for the Windows user account on the target instance of SQL Server where the ***CSenseRuntime*** database exists.

3. Ensure that the created *SQL Server Login* has at least the ***public*** server role assigned.

4. Create a *database user* on the ***CSenseRuntime*** database.

5. Map the created *database user* to the *SQL Server login* you created.

6. Assign the ***csense_cache*** database role to the database user

7. Assign the ***csense_admin*** database role to the database user

7.4.2.3 Adding users for CSense Developer licenses

To enable the use of the CSense Developer edition for a user:

1. Identify the Windows user account. Note that all users of the CSense Developer edition require administrative rights on the local machine in order to deploy analytics.

2. Create a *SQL Server login* for the Windows user account on the target instance of SQL Server where the ***CSenseRecipes***, ***CSenseRuntime, CSense and CSenseCache*** databases exist.

3. Ensure that the created *SQL Server Login* has at least the *public* server role assigned.

4. Create a *database user* on the ***CSenseRecipes*** database.

    a. Map the created *database user* to the *SQL Server login* you created.

    b. Assign the ***csense_cache*** database role to the database user

5. Create a *database user* on the ***CSenseRuntime*** database.

    a. Map the created *database user* to the *SQL Server login* you created.

    b. Assign the ***csense_cache*** database role to the database user

    c. Assign the ***csense_admin*** database role to the database user

6. Create a *database user* on the ***CSense*** database.

    a. Map the created *database user* to the *SQL Server login* you created.

    b. Assign the ***csense_admin*** database role to the database user.

    c. Assign the ***csense_troubleshooter*** database role to the database user.

7. Create a *database user* on the ***CSenseCache*** database.

    a. Map the created *database user* to the *SQL Server login* you created.

    b. Assign the ***csense_admin*** database role to the database user

7.4.3 Enabling CSense data to be read by third party applications

To enable reading of data by external applications you must enable the csense_db_user login by following these steps:

1. Start Action Object Manager

2. Select Action

3. Select Proficy CSense Run-time Properties

4. Choose Enable SQL Login and select Set Password

5. Provide a strong password.

For a managed instance this will also enable SQL Server Authentication. For a non-managed instance this must be enabled on the server by a Database Administrator. See *Security Best Practices and Guidelines* for more information.

7.5 Securing your CSense Databases

If the installation of CSense has a managed SQL Server instance, then no additional steps are required to secure the server. We recommend that you do not enable the SA administrator account, and that you set a strong password for the ***csense_db_user*** account.

For non-managed SQL Server instances, we recommend that you disable SQL Server Authentication if you do not require to read CSense data from third party applications. If reading of CSense data is required we recommend that you set a strong password for both the SA administrator, and the ***csense_db_user*** accounts when enabling SQL Server Authentication.

The permissions required to enable SQL Server Authentication are sysadmin or Control Server.

7.6 Restricting DCOM for COM Servers

CSense makes extensive use of COM/DCOM technology. In environments where analytics run on the CSense Runtime Server that operates on sensitive data, all remote access to CSense COM/DCOM Servers may need to be blocked.

Modern Windows Operating Systems like Windows 10 and Windows Server 2019 block remote COM/DCOM access by default except for members of the Administrators group. This should be verified on your installation.

Use the DCOM configuration tool (DCOMCNFG) and Deny the **Remote Launch** and **Remote Activation** permission for all groups under the **Launch and Activation Permissions** for the following entries:

- Action Object Server
- ScheduledActionObject
- Proficy CSense Run-time List Server
- Learning Server

7.7 Securely connecting to 3rd party data providers

CSense makes use of external data providers via source or sink blocks in blueprints, or data preparation import/export operations in data recipes. In such cases, it is recommended that you work only with those external data providers that use some form of authentication. It is important to note that all provided credentials for connecting to 3rd party data providers are encrypted by CSense.

When connecting with such external data providers, selecting to use Windows authentication (preferred) may require you to change the Windows user account used to run certain CSense applications and/or services. See the section on Changing and restricting accounts for CSense Action Objects in this document for more information on how to change the Windows user accounts in which these applications and services are run.

7.7.1 Connecting to a Remote SQL Server Database

This addresses a situation where a CSense application (for example, the Architect, the Troubleshooter, or Run-time services) needs to log into a SQL Server database using Windows authentication. To achieve this, the Windows user account in which the application is run must have a login configured on the remote SQL Server database. See the section on Changing and restricting accounts for CSense Action Objects in this document for more information on how to change the Windows user accounts in which these applications and services are run.

7.8 Password protecting Blueprints and Superblocks

7.8.1 Password Protection for Superblocks and Blueprints

You can set a password for a superblock or blueprint to restrict blueprints and superblocks from unauthorized viewing or editing.

- For blueprints, this is done in the Architect under **Blueprint > Set password**.
- For superblocks, this is done in the Architect under **Superblock > Set password**.

Once you have done this, the details of a blueprint or superblock with password protection are visible only to those users with the password.

NOTE: Password protected blueprints can still be deployed as Action Objects without requiring a password to be entered. Such blueprints cannot be opened for viewing or editing without providing the password.

7.8.2 Choosing a Password

Avoid common or obvious passwords when creating accounts, such as 'admin' or 'password'. Choosing such passwords could provide an avenue for unauthorized system access.

Additionally, be sure to choose strong passwords, containing a mixture of upper and lower-case characters, special characters and numbers.

We also encourage passwords with at least 8 characters or more.

7.9 User provided Scripts/Code

CSense provides secure native blocks and operations for building analytics and solutions. The native capabilities provided by CSense can be extended by making use of the following features to execute user provided external code/script:

- Python Scripting Block (Python)
- .NET Scripting Block and Operations (VB.NET, C#)
- Custom assemblies in the .NET Wrapper Block and Operations (Any .NET language)
- SQL Operations

Ensure that you adhere to industry best practices when creating scripts/code to be used in your analytics.

Do not use scripts/code or assemblies from untrusted sources.

Additional actions that can be taken to mitigate risks of user provided scripts/code:

- A vetting strategy to inspect any user provided scripts/code and assemblies before allowing these analytics to execute, ensuring that those scripts/code meet the standards you require for security and that the organization is not exposed to scripts/code that has unintended consequences.

- Configure the firewall for the accounts where these scripts/code will run to restrict access to other machines and the internet.

- Action Object deployment is limited to local administrators. Ensure that only trusted users are added to this group to ensure untrusted user accounts can't deploy action objects and bypass your vetting process.

- Change the service account where these action objects will be deployed to have more restrictive permissions. See the section on C*hanging and restricting accounts for CSense Action Objects* in this document for more information on how to change the accounts for the services running the deployed action objects.

7.10 Plaintext Passwords in the Silent Install INI file

The CSense Silent Install option requires that a username and password be specified in plaintext if the services are installed to a custom account.

Make sure that sensitive passwords in the INI file are treated with the correct level of access so that the passwords are not accessed by unauthorized users.

This only applies if:

- Silent install is used to install CSense
- An INI file is used to configure the installation options
- The services are installed to an account that is not the default Local System account

7.11 Making your OPC UA Server connections more secure

By default CSense generates a self-signed Application Instance Certificate during installation. This certificate is exchanged with an OPC UA Server when a connection is made to the server.

CSense allows one to replace the self-signed Application Instance Certificate with a Certificate Authority (CA) issued Application Instance Certificate. The self-signed certificate can also be signed by a CA if desired.

The CSense Certificate Manager Command Line Interface (cmcli) can be used to update or replace the generated Application Instance Certificate with any other valid Application Instance Certificate.

Refer to the CSense help documentation for more information on using the Certificate Manager Command Line Interface to update your Application Instance Certificate.

8 General Recommendations and Information

This section describes additional recommendations and information.

8.1 Firewall Protection

It is important to deploy Proficy CSense in a firewall-protected environment to prevent unauthorized access. Use of firewalls should be part of your Defense in Depth strategy.

8.2 Securing SQL Server with Industry Best Practices

You should adhere to industry best practices for securing your SQL Server installation. A description of such best practices is available at https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation.

8.3 Anti-Virus Software

General Electric Company encourages customers to use third-party anti-virus (AV) software of their choice and to keep it up to date with the latest updates.

8.4 Patching

8.4.1 Patching Software

General Electric recommends that customers keep software up to date by applying the latest Software Improvement Module (SIM) and service packs to their deployed GE Digital products. SIMs and service packs fix bugs and address security vulnerabilities. Service packs serve the same function as SIMs, while also adding new functionality.

8.4.2 Patching Third-Party Software

General Electric also recommends that customers keep operating systems, databases, and other third-party software in their environment up to date with the latest patches from the software vendor.

8.5 Platform Configuration and Hardening

General Electric Company recommends configuring operating systems, databases, and other platforms as per vendor recommendations or industry standards.

The following organizations publish best practices, checklists, benchmarks, and other resources for securing systems:

- Center for Internet Security – http://www.cisecurity.org
- NIST – http://checklists.nist.gov
- Microsoft - http://technet.microsoft.com/security/default.aspx