Software House

C•CURE 9000 Least Privileges Configuration Guide

GPS0069-CE-EN
Version 1.0
Rev A
Revised 2025-06-20

Johnson Controls

Introduction

Effective management of access rights is crucial to maintaining the integrity and security of any system. This document emphasizes the importance of adhering to best practices when assigning permissions within the C•CURE 9000 security-management system. Granting permissions beyond the necessary scope can lead to unauthorized access and potential misuse of information. Therefore, it is imperative to assign each account only the roles and permissions required to perform their specific job functions, and nothing more. This approach ensures that the system remains secure, and that information is protected from unwanted changes.

As cybersecurity threats affect all connected devices, it is important to ensure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a solution's functional operation.

Legal disclaimer

The cybersecurity practices described in this guide are recommended practices to facilitate the secure installation and configuration of the products described herein. However, Johnson Controls cannot guarantee that the implementation of the cybersecurity practices or recommendations described in this guide will ensure the security of the relevant product or system, or prevent, or alter the potential impact of any unauthorized access or damage caused by a cybersecurity incident. This guide is provided “as is”, and Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the cybersecurity practices or recommendations described in this guide. Johnson Controls disclaims all liability for any damages that may occur as a result of, or despite, reliance on this guide or compliance with any cybersecurity practices or recommendations set forth herein.

Contents

1 C•CURE 9000 Configuration Overview

This section helps C•CURE 9000 administrators implement best practices for a secure C•CURE 9000 v3.10 system installation. You will learn what is needed to get the CrossFire service to run on your system, while avoiding the security risks created by granting excessive privileges.

1.1 Knowledge Level

The person responsible for hardening must be experienced in C•CURE 9000 administration and networking technologies. Completion of the C•CURE 9000 basic and advanced installation courses is recommended.

Please use the following link to access training materials, which requires registration and logon credentials: https://www.swhouse.com/support/training_home

1.1.1 Important Terms

C•CURE 9000 Privileges: A Privilege Object is a collection of rights configured to allow Operators access to security Objects such as Readers, Doors, Inputs, Outputs and Privileges. These individual rights are called Permissions.
--> Each access control Object has multiple Permissions associated with it such as No Access, Read, Edit, View, Delete and New.
--> Read and Edit are mutually exclusive. If you choose Read in the C•CURE 9000 Privilege Editor, you cannot select Edit. If you choose Edit, you cannot select Read.
--> You may grant a Permission or deny a Permission.
--> When you create a new Privilege, all Permissions are set to No Access. You can modify the settings to grant Permissions to only the objects your Operators require.

Database Access: Users with SQL Administrator Windows privileges may perform this action. Johnson Controls recommends using SQL Server Management Studio to grant access.
--> The only non-human account which requires SQL Server access is the CROSSFIRE_SERVICE_ACCOUNT. All other service accounts access the SQL Server database via CrossFire.

Least Privileges: The lowest level of access for an account that will still allow proper use of C•CURE 9000. Note that “privileges” are separated into two groups: Windows Privileges and C•CURE 9000 Privileges.

Local Security Policy: To open the Local Security Policy application, type "secpol.msc" in the search bar or navigate to it through Administrative Tools in the Start menu.
--> All non-human accounts require the Local Policy privilege, Logon as a Service. The CROSSFIRE_SERVICE_ACCOUNT requires more, as described in section 2.2.

services.msc**:** The Microsoft Management Console (MMC) file that opens the Services console, a built-in Windows tool used to manage and configure system services.

Windows Privileges: Refers to the access token produced by the system when the user logs on, containing a list of the user's access rights.
--> File/Folder Access, Network Access & Registry Access can be granted by Windows Domain manager/IT Administrator. For additional details refer to the Microsoft documentation.

1.1.2 About the Installation Directories

Depending on your installation, directories will have slightly different names and / or locations. Use this section to determine which directory is used for your installation. Following this section, *"*[*%ProgramFiles%*]" represents your specific option.

The default installation directories for a new installation of C•CURE 9000 are as follows:

- **C:\Program Files (x86)\JCI**
  - Custom-installation directories and drives are allowed.
  - For the purposes of this document, *"*[*%ProgramFiles(x86)%*]" represents these options.
- **C:\Program Files\JCI**
  - Your system might have this 64-bit directory located on a custom drive, but the C•CURE 9000 installation will install certain applications (i.e. ADSDK-64 & victor Client) to this location only and does not allow custom installation locations.

If you have an existing installation of a prior version, the default directory is "Tyco" instead of "JCI." Please make note of the correct directory paths for your configuration.

1.1.3 About the "ProgramData" Directory

Installing C•CURE 9000 creates subdirectories under the following directory:

- **C:\ProgramData**
  - Your system may have "ProgramData" on a custom drive.
  - Older installations will have "Tyco" instead of "JCI", but this document will reference "JCI" only.
  - There are several subfolders of ProgramData to which this document will refer.
  - For the purposes of this document, "[*%ProgramData%*]" represents the folder "ProgramData" on any drive.

Please make note of the correct directory path for your configuration.

1.2 Security Feature Set

C•CURE 9000 offers the following user authentication and authorization features:

Table 1.2.1: User authentication and authorization features

Feature	Description
No backdoor passwords	C•CURE 9000 does not have a "master" or "backdoor" password.
Hidden password entry	Because C•CURE 9000 utilizes input fields of type: Password for password entry, any typed password is only represented by a series of dots; for example: •••••••
No hardcoded password	No passwords/credentials are visible in C•CURE 9000 code, configuration, or log files.
Encrypted password	The C•CURE 9000 database contains encrypted passwords/credentials.

User changeable passwords	The C•CURE 9000 user can change their account password without the assistance of an administrator.

User account password policy	User accounts are a combination of Windows AD and C•CURE 9000 rules.
	• C•CURE 9000 contains rules which govern password formation, expiration, reuse, and other restrictions including password length, history, and complexity.
	• All Windows accounts prompt a password change the next logon.
	• Johnson Controls recommends using a password of 15 characters or more from three or more of the following groups:
	  ○ Upper Case
	  ○ Lower Case
	  ○ Numerals
	  ○ Special characters

Password rules	The local Microsoft Windows operating system or the domain controller manages policies such as predefined number of logon attempts, character length, use of alphanumeric characters, and user-defined lockouts except in the case of SiteServer.
Windows login credentials	C•CURE 9000 uses the Windows login credentials to manage permissions but does not store or have any visibility of the credentials. The local Microsoft Windows operating system or the domain controller manages password rules and policies such as predefined number of login attempts, character length, use of alphanumeric characters, and user-defined lockouts.
Maximum log on attempts	Restrict the user to the configured number of consecutive authentication attempts allowed before that account is locked from further authentication retries.
SiteServer Password Policy	After 20 password attempts, the user cannot perform another attempt for 10 minutes. After 10 minutes, the user can retry as if no previous password attempts were made. Note: These values – number of attempts and time intervals – are fixed values.
Microsoft Active Directory support	To enable centralized authentication, use a Microsoft Active Directory server for the management of user accounts and logon authentication. C•CURE 9000's user authentication is designed for seamless deployment in an Active Directory domain environment utilizing Windows Single Sign-On (SSO). C•CURE 9000 uses Windows log on credentials by default. At the Windows logon, users are automatically logged on to the Administration and Monitoring Stations.
Single-use password	When the iSTAR controller boots for the first time it prompts to change the password before proceeding to any other screens.
Role Based Access Control (RBAC) authorizations	C•CURE 9000 offers Role Based Access Control (RBAC) authorizations. Roles are defined in C•CURE 9000 as operator privileges with different object level permissions. C•CURE 9000 administrators can assign authorizations to individual operators and objects within C•CURE 9000.
Operator Auto Log Off	Starting in v2.90 SP3, operators assigned an inactivity-time limit will be automatically logged out. This time limit can be configured using two new System Variables: *Monitoring Shift Duration* and *Session Timeout*.

1.3 About Human Accounts

When C•CURE 9000 is installed, one “SuperUser” account is created with System All C•CURE 9000 privilege. It is recommended that one human user account is created for each person who operates C•CURE 9000.

1.4 About the Non-Human Service Accounts

This document describes the following service accounts:

- CROSSFIRE_SERVICE_ACCOUNT
- CROSSFIRE_SERVER_COMPONENT_ACCOUNT
- ISTAR_DRIVER_SERVICE_ACCOUNT
- REPORT_SERVICE_ACCOUNT
- IMPORT_WATCHER_SERVICE_ACCOUNT
- GLOBAL_SEARCH_SERVICE_ACCOUNT
- APC_DRIVER_SERVICE_ACCOUNT
- CROSSFIRE_GPI_SERVICE_ACCOUNT
- TYCO_WEB_BRIDGE_SERVICE_ACCOUNT
- ADHDVR_DRIVER_SERVICE_ACCOUNT
- AD_INTELLEX_DRIVER_SERVICE_ACCOUNT
- AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT
- HA_ENROLLMENT_SERVICE_ACCOUNT
- HA_ID_SERVICE_ACCOUNT

These do not affect the Human accounts that are used to operate C•CURE 9000.

NOTES:

- Microsoft Windows imposes a 15-character limit on all user account names. This document uses placeholder names greater than 15 characters, such as “CROSSFIRE_SERVICE_ACCOUNT”.
- The registry keys for each service account are created when C•CURE 9000 is installed.
- It is recommended to uncheck the change password at next logon option on the Windows User dialog box, but this does not affect privilege levels and is only an ease-of-use modification.
- This document might not completely align with the Windows UI due to updates from Microsoft. The steps will not change; however, if you experience a disconnect between this document and your UI please refer to Microsoft documentation for guidance.

2 Least-Privileges Configuration Steps

2.1 Solution Prerequisites

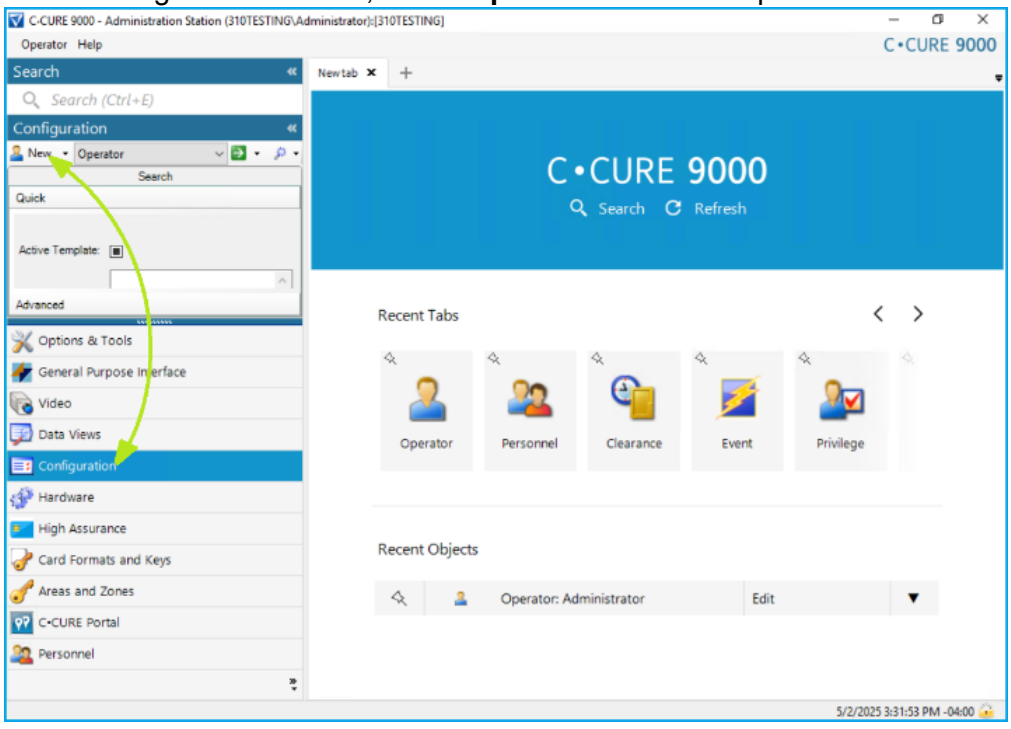
The first step is to add a valid C•CURE 9000 license and ensure services are running.
Next, create a Windows user for each service for which you are configuring these least privileges.

Some helpful guidance during this process:

- It is possible to create all Windows accounts at one time, but we recommend that you follow the steps below, one service at a time.
- If you don't assign logon as a service, it will automatically get assigned when you run the service as the account in services.msc
- On a system that has no previous C•CURE 9000 installations, the installer will create a folder named “JCI.” On a system that has a prior C•CURE 9000 installation, the folder named “Tyco” will be preserved but the subfolders will be migrated to the new “JCI” installation folder.
- Ensure each configured device can receive outbound connections from associated service. Outbound connections will be created to the configured devices.

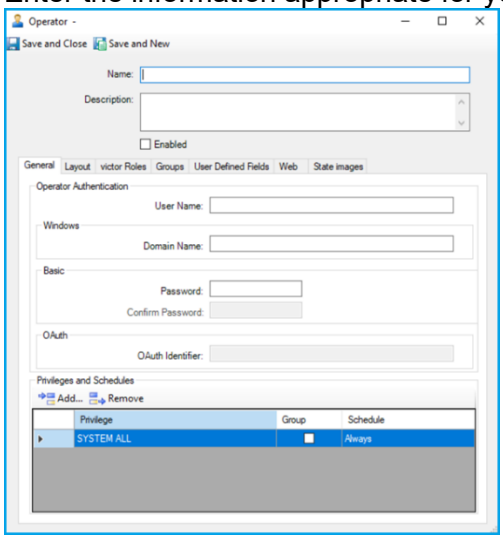
2.2 Creating a Human Operator Account

1. Open the **C•CURE 9000 Administration Workstation** application.
   In the left-hand pane, select **Configuration**.
   In the Configuration window, select **Operator** from the drop-down and click the **New** button.



The Operator dialog displays.

2. Enter the information appropriate for your deployment scenario.



Under Operator Authentication:

- **Name**: that person's Windows login name.
- **Domain Name**: the domain name for that user id.
- **Password**: that person's Windows password.
- NOTE: Ensure that your operators have been granted the minimum level of access in order to do their job.

2.3 CrossFire Framework Service

This section describes how to assign both Windows Privileges and C•CURE 9000 privileges to the CROSSFIRE_SERVICE_ACCOUNT.

REMEMBER: "CROSSFIRE_SERVICE_ACCOUNT" is a placeholder name. Windows imposes a 15-character limit on all user account names.
It is recommended that you follow the steps in this section first, before attempting the subsequent sections, as they reference this section for certain details.

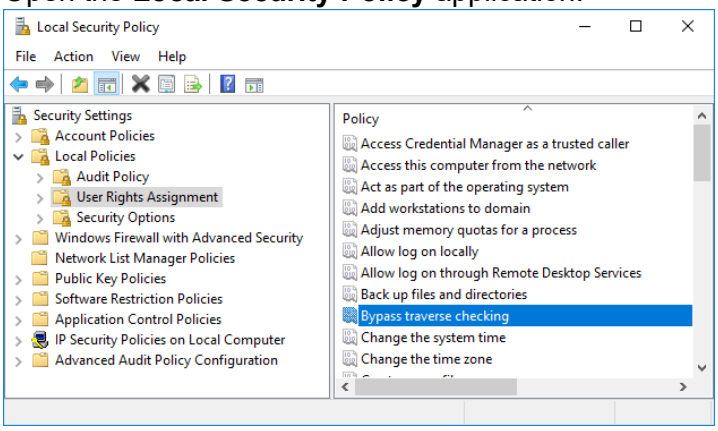
2.3.1 Create the Windows User Account

Use the process appropriate for your edition of the Windows operating system to create a Windows user account for the CROSSFIRE_SERVICE_ACCOUNT.

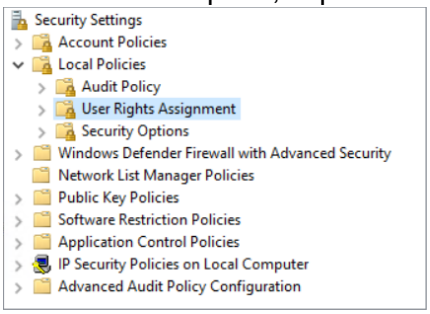
2.3.2 Set “Bypass Traverse Checking” Privilege

This section described in-depth the process for updating **User Rights Assignments** for the current system.

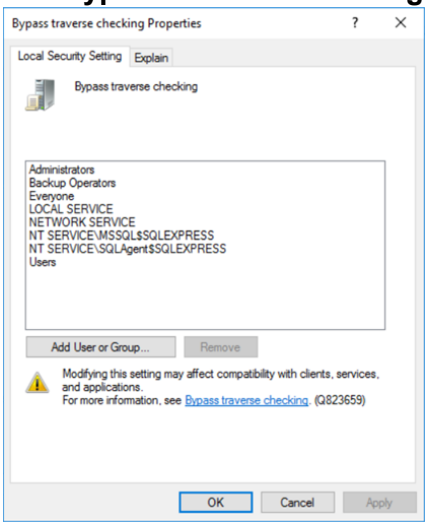
1. Open the **Local Security Policy** application.



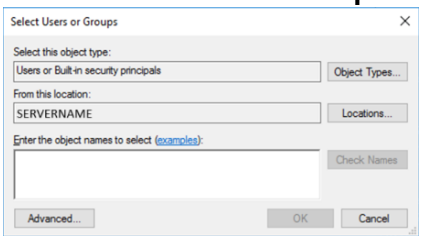
2. In the left-hand pane, expand the **Local Policies** folder and select **User Rights Assignment**.



3. In the right-hand pane, double-click on the **Bypass traverse checking** list item.
   The **Bypass traverse checking Properties** dialog displays:

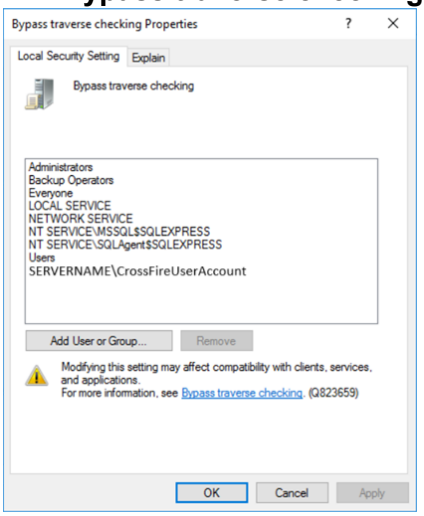


4. Click the **Add User or Group...** button.
   The **Select Users or Groups** dialog displays:



5. Under **Enter the object names to select**, type in name of the CROSSFIRE_SERVICE_ACCOUNT.

6. Click the **OK** button.
   The **Bypass traverse checking Properties** dialog displays:



7. Click **Apply**, then click **OK**.

2.3.3 Set “Debug Programs” Privilege

1. Using steps 1 & 2 from section 2.3.2 navigate to User Rights Assignments
2. Double-click on **Debug programs**
3. Using steps 4 through 6, assign the CROSSFIRE_SERVICE_ACCOUNT to this user right

2.3.4 Set “Log on as a Service” Privilege

1. Using steps 1 & 2 from section 2.3.2 navigate to User Rights Assignments
2. Double-click on **Log on as a service**
3. Using steps 4 through 6, assign the CROSSFIRE_SERVICE_ACCOUNT to this user right

2.3.5 Set “Profile Single Process” Privilege

1. Using steps 1 & 2 from section 2.3.2 navigate to User Rights Assignments
2. Double-click on **Profile single process**
3. Using steps 4 through 6, assign the CROSSFIRE_SERVICE_ACCOUNT to this user right

2.3.6 Set “Profile System Performance” Privilege

1. Using steps 1 & 2 from section 2.3.2 navigate to User Rights Assignments
2. Double-click on **Profile system performance**
3. Using steps 4 through 6, assign the CROSSFIRE_SERVICE_ACCOUNT to this user right

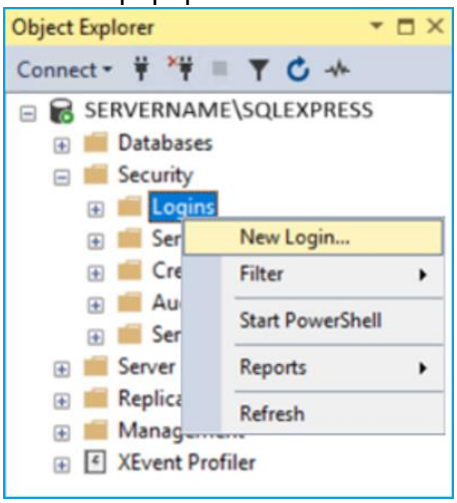
2.3.7 Set “Network Logon” Privilege

NOTE: This privilege is only required for enterprise systems.

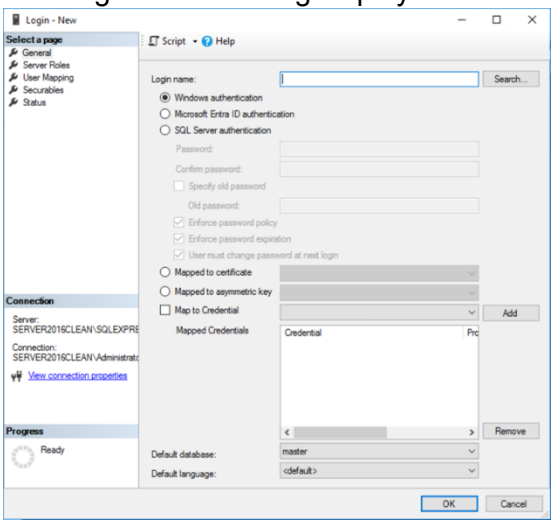
1. Using steps 1 & 2 from section 2.3.2 navigate to User Rights Assignments
2. Double-click on **Network Logon**
3. Using steps 4 through 6 from section 2.3.2, assign the CROSSFIRE_SERVICE_ACCOUNT to this user right

2.3.8 Create SQL Server Login

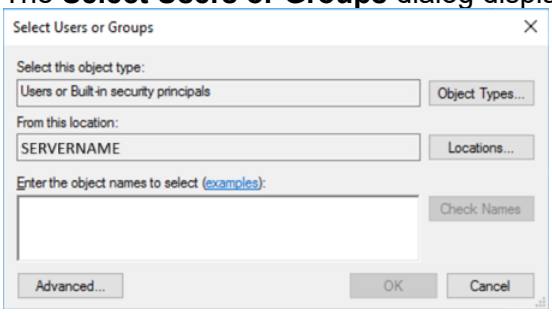
1. Open SQL Server Management Studio (SSMS)
2. Connect to the C•CURE 9000 database
3. In **Object Explorer**, expand the **Security** object, right-click on the **Logins** object and select **New Login** from the popup menu



The Login – New dialog displays.

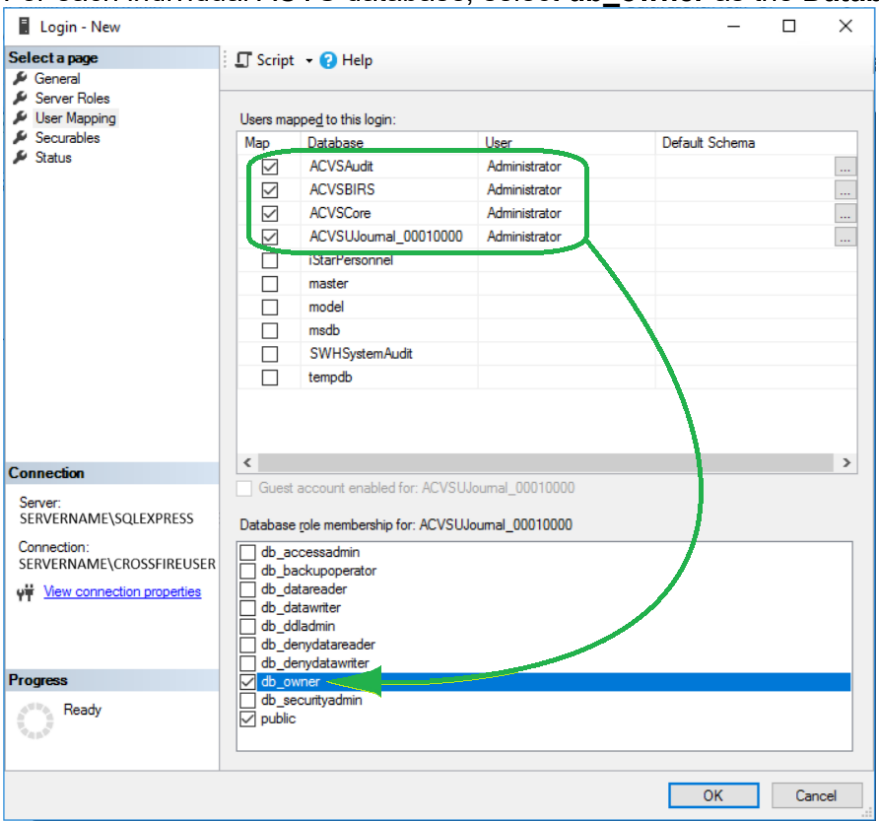


4. Confirm that the **Windows authentication** radio button is selected.
5. Next to the **Login name** field, click the **Search** button.
   The **Select Users or Groups** dialog displays:

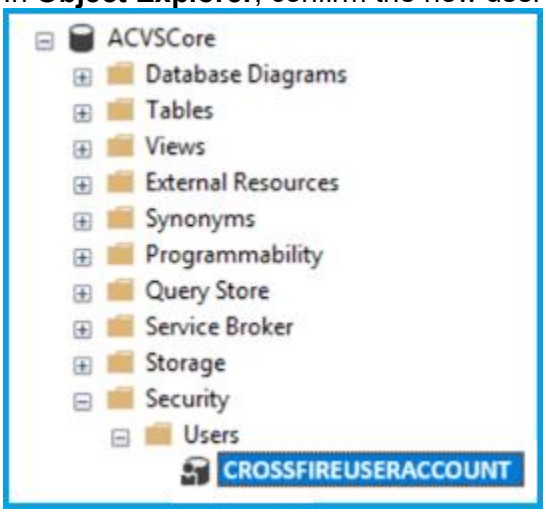


6. Under **Enter the object names to select**, type in name of the CROSSFIRE_SERVICE_ACCOUNT and click the **OK** button.
7. Under **Select a page**, click the User mapping object.

8. For each individual ACVS database, select **db_owner** as the **Database role membership**.



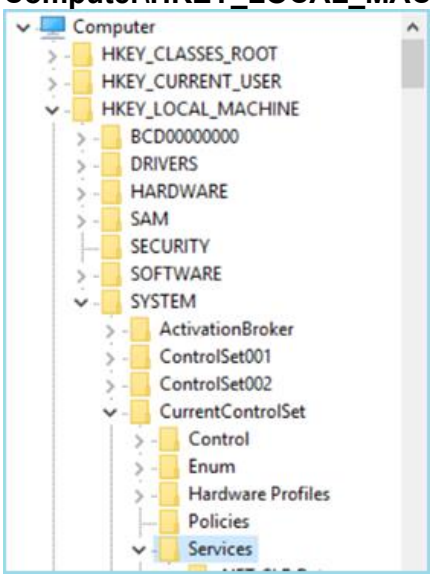
9. Click OK to finish adding this login.
10. In **Object Explorer**, confirm the new user was added.



2.3.9 Set Registry Access Permissions

1. Run regedit.msc
2. Navigate to

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services



3. Add full control of the following registry keys for the CROSSFIRE_SERVICE_ACCOUNT:

   CrossFire

   CrossFire: Action Processor

   CrossFire: DatabaseAccess

   CrossFire: EventServer

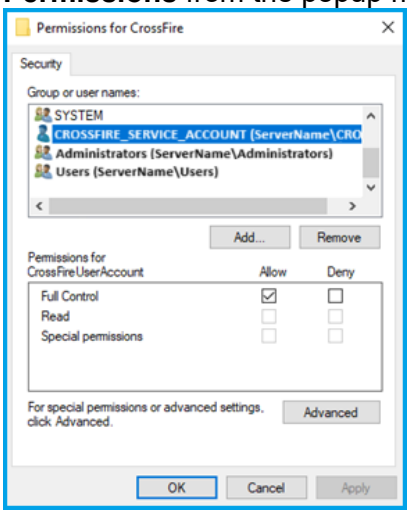
   CrossFire: Synchronization

   CrossFire: Synchronization Conflicts

   CrossFire: Synchronization Queue

   CrossFire: Synchronization Stored Procedures

a. Right-click on each of the above-named CrossFire objects in the Registry Editor and click **Permissions** from the popup menu to display the **Permissions for [SERVICE]** dialog.



b. Select the CROSSFIRE_SERVICE_ACCOUNT Windows user account in the “Group or user names” window
c. select Full Control, then click Apply, then click OK
d. Repeat for the 8 other CrossFire objects noted above

4. Use the Windows Command prompt to configure URL reservations for HTTP.

a. Press Win + X and select Command Prompt (Admin) or Windows PowerShell (Admin) to open Command Prompt as Administrator
b. Use the following commands to add URL reservations:

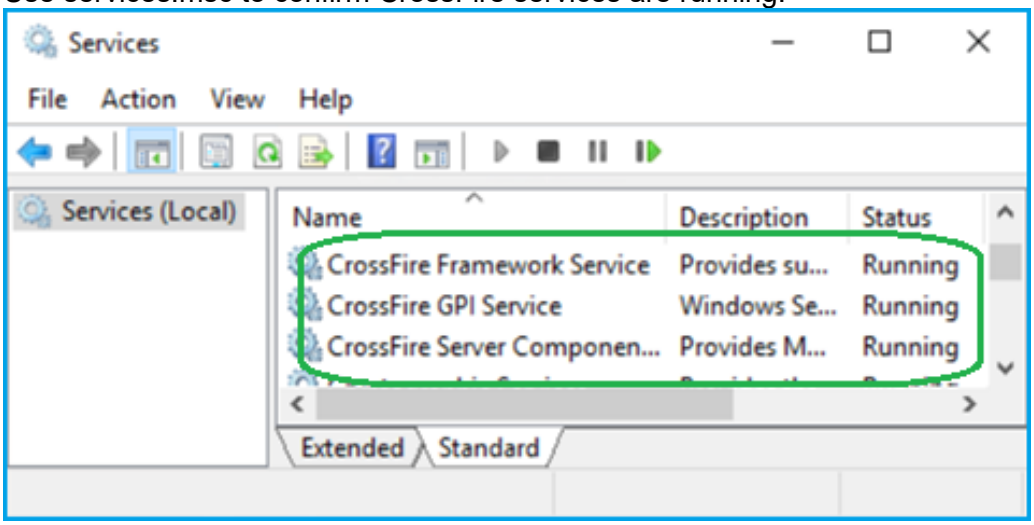
netsh http add urlacl url=http://+:8998/CrossFire/IClientSession/ user=CROSSFIRE_SERVICE_ACCOUNT

netsh http add urlacl url=http://+:8998/CrossFire/IClientSessionOneWay/ user= CROSSFIRE_SERVICE_ACCOUNT

netsh http add urlacl url=http://+:8996/ user= CROSSFIRE_SERVICE_ACCOUNT

c. Returns “URL reservation successfully added” for all 3.

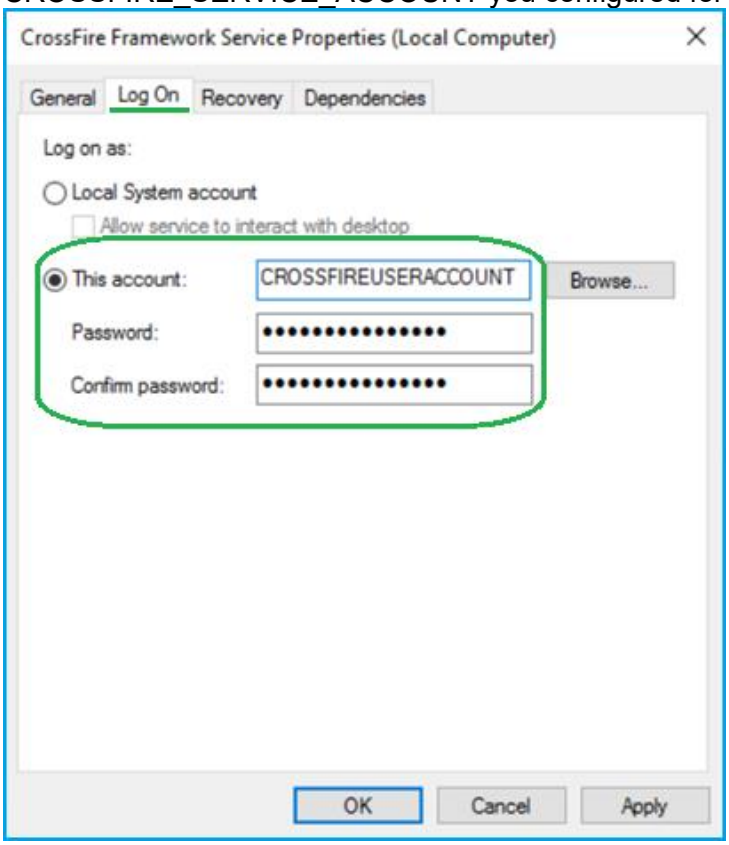
5. Use services.msc to confirm CrossFire services are running.



6. Right-click on **CrossFire Framework Service** and click **Stop** on the popup menu. This will stop all three CrossFire services.

7. Right click on **CrossFire Framework Service** again and click Properties on the popup menu. The **CrossFire Framework Service Properties (Local Computer)** dialog displays.

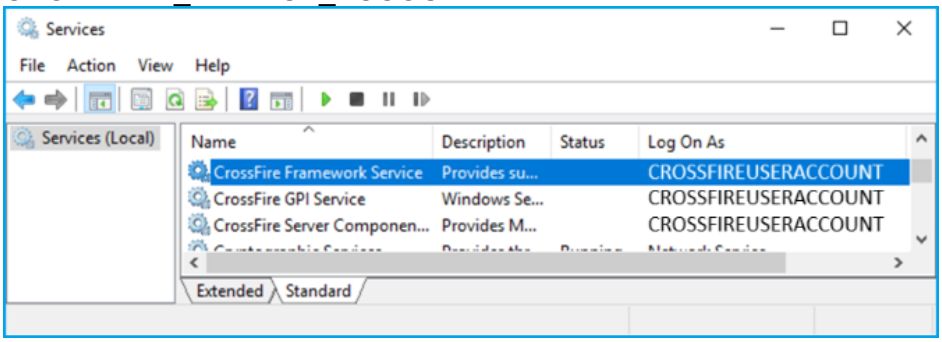
8. In the **Log On** tab, change the Logon User Account from Local System account to the CROSSFIRE_SERVICE_ACCOUNT you configured for this service.



Click **Apply**, then click **OK**.

9. Repeat the previous step for the other CrossFire services.

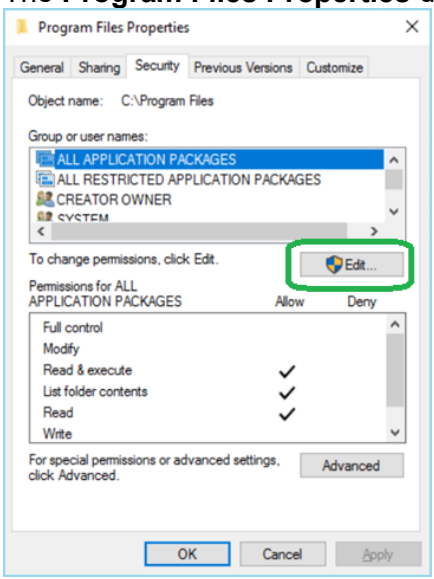
10. In services.msc, confirm the **Log On As** column has the correct value for your CROSSFIRE_SERVICE_ACCOUNT.



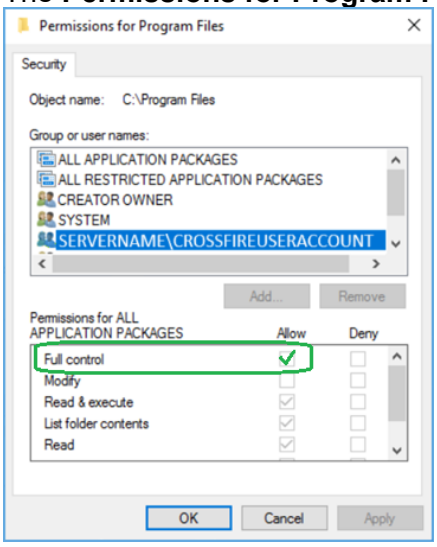
11. Right-click on **CrossFire Framework Service** and click **Start** on the popup menu. This will start all three CrossFire services.

2.3.10 Set Folder Access Privilege

1. Using Windows File Explorer, navigate to the **Local Disk (C:)**.
2. Right-click on the **Program Files** folder and select **Properties** from the popup menu.
   The **Program Files Properties** dialog displays.



3. On the **Security** tab, click the **Edit** button.
   The **Permissions for Program Files** dialog displays.



   Assign **Full control** to the CROSSFIRE_SERVICE_ACCOUNT.

4. Repeat for the following paths:

   - [*%ProgramFiles(x86)%*] (see section 1.1.2)
   - [*%ProgramData%*]\JCI (see section 1.1.3)

5. NOTE: [*%ProgramFiles(x86)%*]\CrossFire\ImportLog (see section 1.1.2) is the default folder where Import Result log files are created, but this can be redirected via the system variable "Import Result Error Log File Directory." If your system configuration uses a folder other than the default, check to ensure the CROSSFIRE_SERVICE_ACCOUNT has **Read** access and **Write** access to your folder.

2.3.11 OPTIONAL: Email Server Privilege

If you are intending to use C•CURE 9000 to send email, you must do one of the following 2 steps:

- In the Administration Workstation > Email Configuration window, specify a user account with network access to your email server.

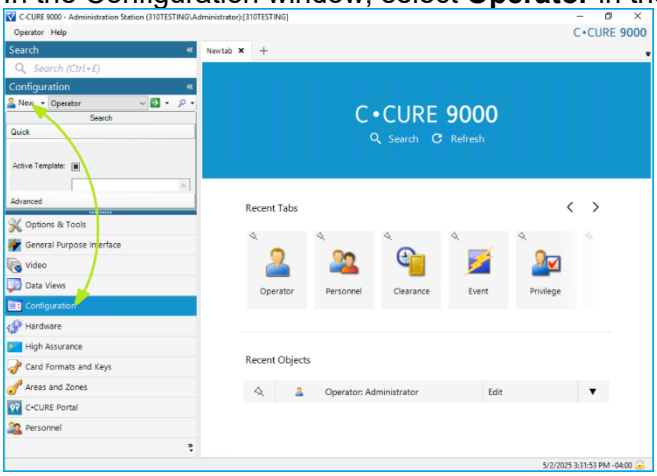
  OR

- The CROSSFIRE_SERVICE_ACCOUNT requires access to the email port (default is 25) and the network on which the email server resides.

2.3.12 Creating the Non-Human C•CURE 9000 Operator Account

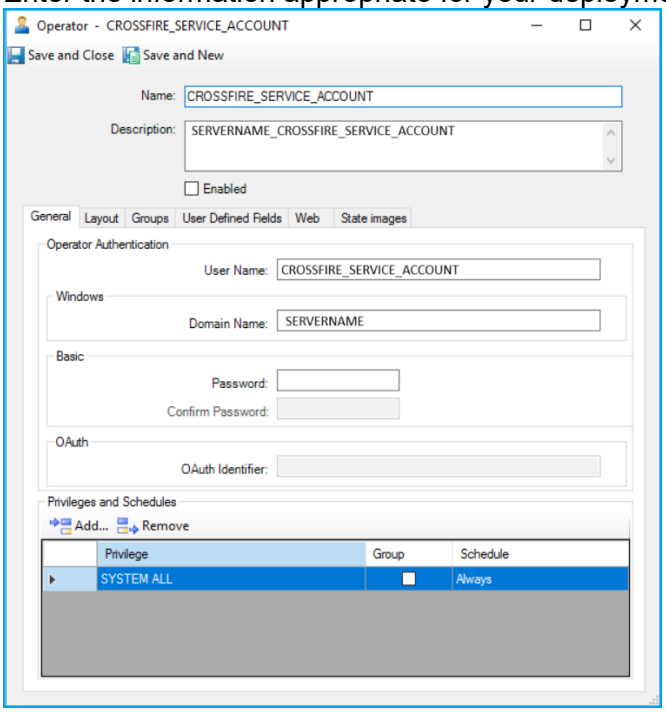
1. Open the C•CURE 9000 Administration Workstation.

   In the left-hand pane, select **Configuration**.
   In the Configuration window, select **Operator** in the dropdown list and click **New**.



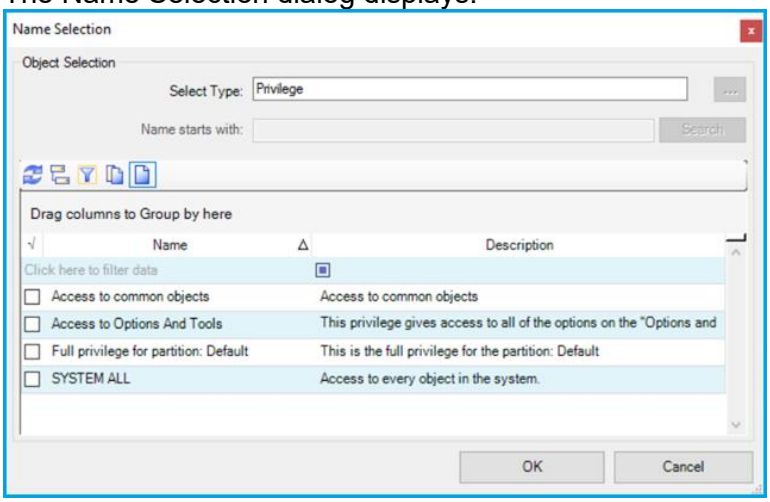
   The Operator dialog displays.

2. Enter the information appropriate for your deployment scenario.



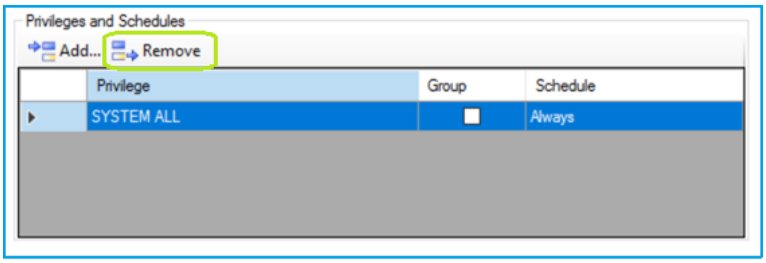
a. SYSTEM ALL privilege is added by default under Privileges and Schedules.
b. Under Operator Authentication:
User Name: The CROSSFIRE_SERVICE_ACCOUNT Windows username.
Domain Name: the crossfire service account's domain name.
Password: the CROSSFIRE_SERVICE_ACCOUNT's windows password.

c. OPTIONAL: To add a different privilege, click the Add button.
The Name Selection dialog displays.

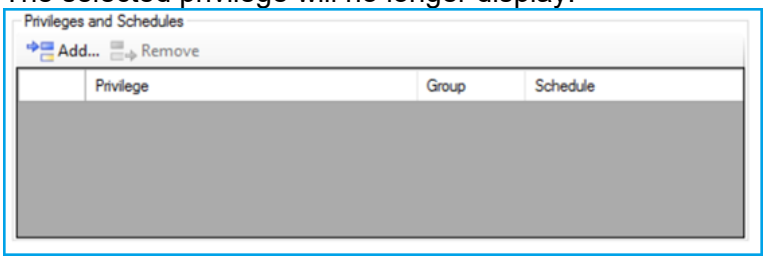


Select the desired privilege name and click the OK button to continue.

d. To remove a privilege, select the privilege name under Privileges and Schedules in the Operator dialog, then click the Remove button.



The selected privilege will no longer display.



2.4 CrossFire Server Component Framework Service

1. Using the actions described in section 2.3.9 give full control of the following registry key to the CROSSFIRE_SERVER_COMPONENT_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CrossFireServerComponentFramework

2. Using the actions described in section 2.3.12 add the CROSSFIRE_SERVER_COMPONENT_ACCOUNT Windows user as a System All operator in C•CURE 9000.

3. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the CROSSFIRE_SERVER_COMPONENT_ACCOUNT you configured for this service.

   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

4. Open Server Configuration Application

   a. Start the service.
   b. Ensure the service is running.

2.5 iSTAR Driver Service

1. Using the actions described in section 2.3.9 give full control of the following registry key to the ISTAR_DRIVER_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CrossFireiSTARDriverService

2. Using the actions described in section 2.3.10 assign **Read** & **Write** permissions to the ISTAR_DRIVER_SERVICE_ACCOUNT Windows user for the following path:

   [*%ProgramFiles(x86)%*]\JCI\CrossFire\ServerComponents (see section 1.1.2)

3. Using the actions described in section 2.3.12 add the ISTAR_DRIVER_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

4. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the ISTAR_DRIVER_SERVICE_ACCOUNT you configured for this service.

   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

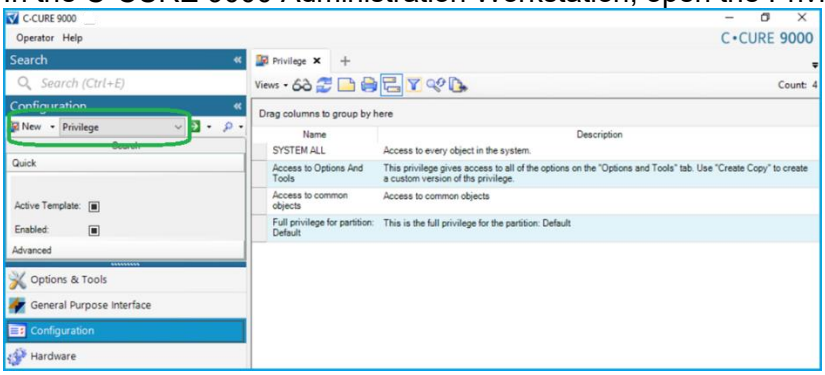
5. Open Server Configuration Application

   a. Start the service.
   b. Ensure the service is running.

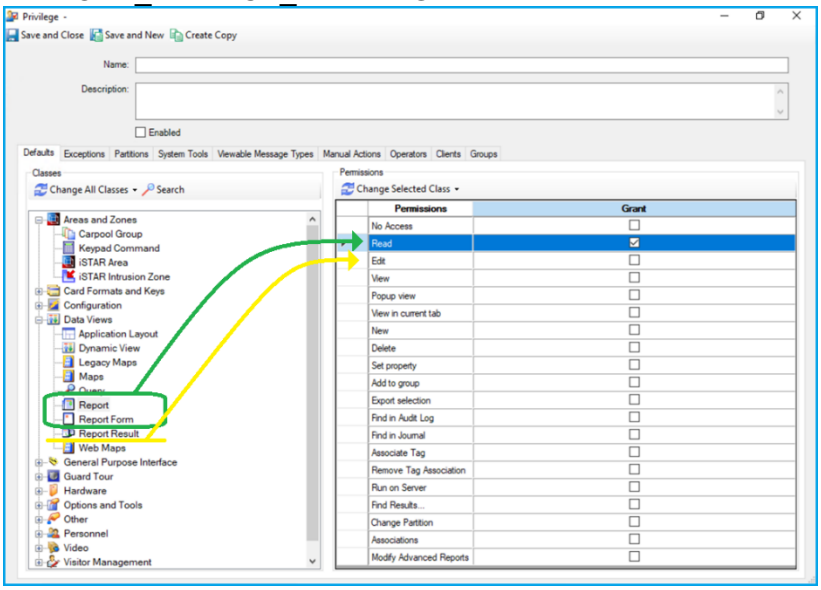
2.6 Report Service

1. Use the following steps to assign privileges to the **Report** object, the **Report Form** object, and to all the objects needed to report on.

   a. In the C•CURE 9000 Administration Workstation, open the Privilege Editor.



b. Create a new privilege. Provide a descriptive name for the new privilege; we suggest "REPORT_SERVICE_PRIVILEGE."



c. Assign **Read** access to the **Report** object, the **Report Form** object, and to all the objects needed to report on.
d. Assign **Edit** access to the report result object.
e. Save and Close.

2. Using the actions described in section 2.3.9 give full control of the following registry key to the REPORT_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CrossFireReportServer

3. Using the actions described in section 2.3.12 add the REPORT_SERVICE_ACCOUNT Windows user as an operator in C•CURE 9000.

   a. Assign the REPORT_SERVICE_PRIVILEGE (see above) to the operator.

4. Assign Windows user account access to the temp folder under the name of the user account and the level of write-access of the folder where they want to export the reports.

5. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the REPORT_SERVICE_ACCOUNT you configured for this service.

   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

6. Open Server Configuration Application.

   a. Start the service.
   b. Ensure the service is running.
   c. Ensure the operator can run reports (SWH12 - Operator report)

2.7 Import Watcher Service

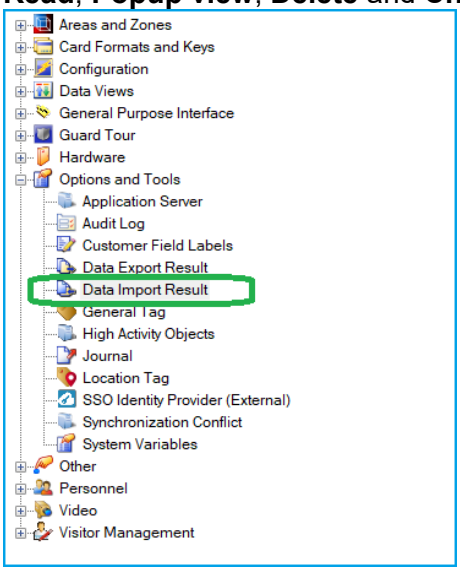
1. Using the actions described in section 2.3.9 give full control of the following registry key to the IMPORT_WATCHER_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CrossFireImportWatcher

2. Using the actions described in section 2.3.10 assign **Read** & **Write** permissions to the IMPORT_WATCHER_SERVICE_ACCOUNT Windows user for the folder from which it imports.

3. Using the actions described in section 2.3.12 add the IMPORT_WATCHER_SERVICE_ACCOUNT Windows user as an operator in C•CURE 9000.

   - Using the actions described in section 2.5, create a privilege for the IMPORT_WATCHER_SERVICE_ACCOUNT C•CURE 9000 operator and assign that privilege **Read**, **Popup view**, **Delete** and **Change Partition** Permissions.



4. OPTIONAL: If you are using LDAP Import, the LDAP database for LDAP import needs **Read** access to LDAP database and temporary file. Using the actions described in section 2.3.10 assign Read access to the IMPORT_WATCHER_SERVICE_ACCOUNT for the following path:
   - CrossFire\ServerComponents

5. OPTIONAL: If you are using ODBC Import, ensure that the IMPORT_WATCHER_SERVICE_ACCOUNT Windows user has ODBC **Read** & **Write** access to the data source.

6. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the IMPORT_WATCHER_SERVICE_ACCOUNT you configured for this service.

   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

7. Open Server Configuration Application.

    a. Start the service.
    b. Ensure the service is running.
    c. Ensure you are able to import a sample event.

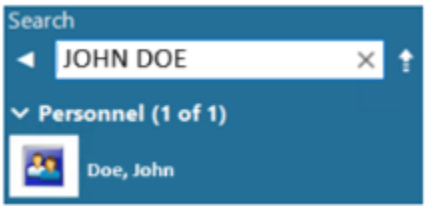
2.8 Global Search Service

1. Using the actions described in section 2.3.12 add the GLOBAL_SEARCH_SERVICE_ACCOUNT Windows user as an Operator with the **Access to common objects** C•CURE 9000 privilege.

2. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the GLOBAL_SEARCH_SERVICE_ACCOUNT you configured for this service.
    - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

3. Open the Server Configuration Application.

    a. Start the service.
    b. Ensure the service is running.
    c. To test, search for a personnel record that is known to exist:



2.9 APC Driver Service

1. Using the actions described in section 2.3.9 give full control of the following registry key to the APC_DRIVER_SERVICE_ACCOUNT Windows user:

    Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CrossFireApcDriverService

2. Using the actions described in section 2.3.10 assign **Read** & **Write** permissions to the APC_DRIVER_SERVICE_ACCOUNT Windows user for the following path:

    [*your installation directory*]\CrossFire\ServerComponents (see section 1.1.2)

3. Using the actions described in section 2.3.12 add the APC_DRIVER_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

4. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the APC_DRIVER_SERVICE_ACCOUNT you configured for this service.

    - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

5. Open the Server Configuration Application.

    a. Start the service.
    b. Ensure the service is running.

2.10 CrossFire GPI Service

In order for a GPI device to connect to C•CURE 9000, the Windows user CROSSFIRE_GPI_SERVICE_ACCOUNT requires Windows access privileges to any serial port or network port used by the GPI device. For further information, refer to the GPI device's documentation.

1. Using the actions described in section 2.3.9 give full control of the following registry key to the CROSSFIRE_GPI_SERVICE_ACCOUNT Windows user:

    Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CrossFireGPIService

2. Using the actions described in section 2.3.12 add the CROSSFIRE_GPI_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

3. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the CROSSFIRE_GPI_SERVICE_ACCOUNT you configured for this service.
    - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

4. Open the Server Configuration Application.

    a. Start the service
    b. Ensure the service is running

2.11 Tyco Web Bridge Service

The TYCO_WEB_BRIDGE_SERVICE_ACCOUNT needs all Windows privileges required by the plugins used with the C•CURE 9000 system.

1. Using the actions described in section 2.3.9 assign full control of the following registry key to the TYCO_WEB_BRIDGE_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TycoWebBridge

2. Using the actions described in section 2.3.12 add the TYCO_WEB_BRIDGE_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

3. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the TYCO_WEB_BRIDGE_SERVICE_ACCOUNT you configured for this service.
   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

4. Open the Server Configuration Application.

   a. Start the service
   b. Ensure the service is running

2.12 AD HDVR Driver Service

1. Using the actions described in section 2.3.9:

   a. assign **Read** & **Write** access of the following Local Machine registry key to the AD_HDVR_DRIVER_SERVICE_ACCOUNT Windows user:

      Computer\HKEY_LOCAL_MACHINE\SOFTWARE\American Dynamics

   b. Assign **Read** access of the Time Zone registry area and Current User registry to the AD_HDVR_DRIVER_SERVICE_ACCOUNT Windows user:

      Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
      Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

2. Using the actions described in section 2.3.10:

   a. Assign **Full control** permissions to the AD_HDVR_DRIVER_SERVICE_ACCOUNT Windows user for the following paths:
   [*%ProgramData%*]\American Dynamics (see section 1.1.3)

   b. Assign **Read & Execute** permissions and **Write** permissions to the AD_HDVR_DRIVER_SERVICE_ACCOUNT Windows user for the following path:
      [*%ProgramFiles%*]\American Dynamics (see section 1.1.2)
      [*%ProgramFiles(x86)%*]\CrossFire\ServerComponents (see section 1.1.2)

3. Using the actions described in section 2.3.12 add the AD_HDVR_DRIVER_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

4. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the AD_HDVR_DRIVER_SERVICE_ACCOUNT you configured for this service.
    - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

5. Open the Server Configuration Application.

    a. Start the service.
    b. Ensure the service is running.

Note: Network connections will make outbound connections to the individual recorders.

- Network connections (Handled through the Exacq SDK)
- For C•CURE 9000 configurations the service launches “HDVRAnalyticsPlugins.exe”
- Device discovery requires **Full access** to the following registry keys:

    Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SSDPSRV

    Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\UPnPControl Point

2.13 AD Intellex Driver Service

1. Using the actions described in section 2.3.9:

    a. Assign **Read** & **Write** access to the following Local Machine registry keys to the AD_INTELLEX_DRIVER_SERVICE_ACCOUNT Windows user:

        Computer\HKEY_LOCAL_MACHINE\SOFTWARE\American Dynamics

        Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Sensormatic-VPD
        Computer\HKEY_CLASSES_ROOT\Intellex

        Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Sensormatic-VPD

        Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

    b. Assign **Read** access to the following Time Zone registry area and Current User registry keys to the AD_INTELLEX_DRIVER_SERVICE_ACCOUNT Windows user:

        Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones

        Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft

Computer\HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\

Computer\HKEY_CLASSES_ROOT\CLSID

c. Assign **Full Control** of the following registry key for device discovery to the AD_INTELLEX_DRIVER_SERVICE_ACCOUNT Windows user:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\UPnPControl Point

2. Using the actions described in section 2.3.10 assign **Full control** permission to the AD_INTELLEX_DRIVER_SERVICE_ACCOUNT Windows user for the following path:

[*%ProgramData%*]\American Dynamics (see section 1.1.3)

4. Using the actions described in section 2.3.12 add the AD_INTELLEX_DRIVER_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

5. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the AD_INTELLEX_DRIVER_SERVICE_ACCOUNT you configured for this service.
   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

6. Open the Server Configuration Application.

   a. Start the service.
   b. Ensure the service is running.

2.14 AD VideoEdge Driver Service

1. Using the actions described in section 2.3.9:

   a. Assign **Read** & **Write** access of the following Local Machine registry keys to the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\American Dynamics

   b. Assign **Read** access of the following Time Zone registry area and Current User registry keys to the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

   Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft

   Computer\HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\

c. Assign **Full** access of the following registry key for device discovery for VideoEdge Recorders to the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT Windows user:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\UPnPControl Point

2. Using the actions described in section 2.3.10:
   a. Assign **Full control** permissions to the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT Windows user for the following paths:
      [*%ProgramData%*]\American Dynamics (see section 1.1.3)
      [*%ProgramFiles(x86)%*]\CrossFire\ServerComponents (see section 1.1.2)
   b. Assign **Read & Execute** permissions and **Write** permissions to the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT Windows user for the following path:

      [*%ProgramFiles%*]\American Dynamics (see section 1.1.2)

3. Using the actions described in section 2.3.12 add the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT Windows user as a System All operator in C•CURE 9000.

4. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the AD_VIDEOEDGE_DRIVER_SERVICE_ACCOUNT you configured for this service.

   - You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

5. Open the Server Configuration Application.

   a. Start the service.
   b. Ensure the service is running.

Note: Network connections will make outbound connections to the individual recorders.

2.15 HA Enrollment Service

1. Using the actions described in section 2.3.9 give **Read access** of the following registry key to the HA_ENROLLMENT_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CCureHA.EnrollmentService

2. Using the actions described in section 2.3.10 assign **Read** permissions to the HA_ENROLLMENT_SERVICE_ACCOUNT Windows user for the following path:

   [*%ProgramFiles(x86)%*]\CrossFire\ServerComponents\HACertificates
   (see section 1.1.2)

3. Using the actions described in section 2.3.12 add the HA_ENROLLMENT_SERVICE_ACCOUNT Windows user as a **System All** operator in C•CURE 9000.

4. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the HA_ENROLLMENT_SERVICE_ACCOUNT you configured for this service.

5. You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

6. Open Server Configuration Application
   a. Start the service.
   b. Ensure the service is running.

2.16 HA ID Service

1. Using the actions described in section 2.3.9 give **Read access** of the following registry key to the HA_ID_SERVICE_ACCOUNT Windows user:

   Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CCureHA.IDService

2. Using the actions described in section 2.3.10 perform the following:
   a. Assign **Read** & **Write** permissions to the HA_ID_SERVICE_ACCOUNT Windows user for the following paths:

      [*%ProgramFiles(x86)%*]\CrossFire\ServerComponents\HACertificates (see section 1.1.2)

      [*%ProgramFiles(x86)%*]\CrossFire\ServerComponents\NetCoreExe\idservice(see section 1.1.2)
      [*%ProgramData%*]\CCUREHighAssurance\Enrollment\ (see section 1.1.3)

3. Using the actions described in section 2.3.12 add the HA_ID_SERVICE_ACCOUNT Windows user as a **System All** operator in C•CURE 9000.

4. Start services.msc and, in the Log On tab, change the Logon User Account from Local System account to the HA_ID_SERVICE_ACCOUNT you configured for this service.

5. You can confirm this was done if the **Log On As** column has the correct value for your newly configured service account.

6. Open Server Configuration Application
   a. Start the service
   b. Ensure the service is running