

ASSA ABLOY IP Locks C•CURE Integration Guide

C•CURE and Software House are trademarks of Johnson Controls.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Johnson Controls will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Johnson Controls are the property of their respective owners, and are used with permission or allowed under applicable laws.

Products offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your regional sales representative.

This manual is proprietary information of Johnson Controls. Unauthorized reproduction of any portion of this manual is prohibited. The material in this manual is for information purposes only. It is subject to change without notice. Johnson Controls assumes no responsibility for incorrect information this manual may contain.

© 2022 Johnson Controls

All rights reserved.

Table of Contents

Preface	6
Conventions	7
Finding information	8
Customer support center	8
Telephone technical support	8
Chapter 1 - Overview	9
ASSA ABLOY Integration with C•CURE 9000	10
Supported environments	10
Lock scenarios	10
Chapter 2 - Integration Best Practices Hardening Recommendations	12
Encryption	13
Enabling encryption between C•CURE and the DSR	13
Enabling AES encryption between the DSR and Wireless Locks	13
Record Retention Policy	13
Chapter 3 - Data Privacy Notice	14
Data Privacy Notice	15
Chapter 4 - Pre-installation	16
DSR server specifications	17
Windows operating system requirements	17
DSR configuration file verification	17
ASSA ABLOY locks requirements	19
Standalone servers and enterprise servers	20
New DSR 8 projects	20
Upgrades from DSR 5	20
ASSA ABLOY driver and C•CURE installation process	21
Prerequisites	21
Installation troubleshooting	24
Installation logs	24
Existing Index causes SQL script error	24
LocalSystem is not DBowner	25

Chapter 5 - Installation and upgrade	27
Requirements	28
Upgrading	28
Licensing	28
Requirements summary	28
Installation on C•CURE server	30
Encryption	30
Installation impact on target system	37
Licensing	38
Starting CrossFire services	39
Starting the driver service	39
ASSA ABLOY system variables	39
Upgrading	40
Known Limitations	40
Prerequisites	40
Upgrading the DSR	41
Upgrading the ASSA ABLOY integration driver	41
DSR Synchronization	42
Lock Configuration Tool	42
Chapter 6 - Configuring ASSA ABLOY software objects	43
Components of the ASSA ABLOY integration	44
Server component	44
Client components	44
Privileges for access to ASSA ABLOY objects	45
Assigning a privilege	45
Configuring ASSA ABLOY software objects	45
DSRs	46
Configuring a DSR	46
Configuring the DSR object	46
Verifying the Apache services and the DSR are running	48
Viewing download error information	48
Deleting a DSR	49
Downloading the DSR with C•CURE 9000	49
Displaying DSR status in the Monitoring Station	50
Assigning a layout to an operator	51
Checking DSR and reader statuses	52
Configuring an ASSA ABLOY reader	52
Performing a comm session on a reader	57
Replacing a reader	57
Deleting a reader	57
Configuring holidays for ASSA ABLOY readers	58
MagCard fields	58
Configuring an ASSA ABLOY door	61
Modes	62

Manual actions for ASSA ABLOY doors	65
Panic mode	66
Clearances and credentials	66
Clearances	66
Credentials	67
Removing a credential	68
Validating a CHUID	68
Configuring ASSA ABLOY card formats	69
Configuring the scheduler	70
Types of schedule	70
Configuring Access Mode	71
Types of access	71
Configuring Clearance Mode	72
Types of clearance	72
ASSA ABLOY sites with multiple credentials for a single personnel record	74
Specific case instructions	74
ASSA ABLOY Implementation for Supporting PIV-I and FASC-N Card Formats	76
Description	76
FASC-N Configuration at the C•CURE9000 Administration Station	76
PIV-I Configuration at the C•CURE9000 Administration Station	79

Preface

This guide contains information on the configuration for this integration, and outlines the available functions in the C•CURE Administration station and Monitoring station.

This manual assumes that the C•CURE Administration and Monitoring applications, and the DSR software are installed and operating normally.

In this preface:

Conventions	7
Finding information	8
Customer support center	8

Conventions

This guide uses the following text formats and symbols.

Convention	Meaning
Bold	Bold text describes one of the following items: • Interface element • Optional steps in a procedure
<i>Italics</i>	Italicized text refers to another document
Monospace	Monospace text describes one of the following items: • Command, character, or web address to enter • A file name or location

The following items are used to indicate important information.

NOTE

Indicates a note. Notes call attention to information of special importance.

TIP

Indicates an alternative method of performing a task.



Indicates a caution. A caution contains information essential to avoid damage to the system. A caution can pertain to hardware or software.



Indicates a warning. A warning contains information that advises users that failure to avoid a specific action can result in physical harm to the user or to the hardware.



Indicates a danger. A danger contains information that users must know to avoid death or serious injury.

Finding information

You can access C•CURE 9000 manuals and online Help for more information about C•CURE 9000.

Manuals

Navigate to \Manuals\CCURE of the C•CURE 9000 installation media to view C•CURE 9000 software manuals.

Refer to the *C•CURE 9000 Installation and Upgrade Guide* for the list of available manuals.

These manuals are also available from the Software House website:

<http://www.swhouse.com/TechnicalLibrary/TechLibSW.aspx>.

Help files

Press F1, or click **Help** in the **Administration Station**, or **Monitoring Station**, to access **C•CURE 9000 Help**.

Customer support center

Telephone technical support

Software House accepts service calls only from employees of the systems integrator of record for the installation associated with the support inquiry.

Before calling support, ensure that you fulfill the following requirements:

- You are the dealer of record for this account.
- You are certified by Software House for this product.
- You have a valid license and current Software Support Agreement (SSA) for the system.
- You have your system serial number available.
- You have your certification number available.

Support	Days	Times	Additional requirements
Normal	Monday to Friday. Excluding holidays.	8:00am to 8:00pm EST	None
Emergency	7 days. Including holidays.	24 hours	Enhanced SSA support, otherwise billable on time and material basis. Minimum charges apply. See MSRP.

For telephone support contact information, go to http://www.swhouse.com/support/contact_technical_support.aspx.

Overview

This chapter provides an overview of the ASSA ABLOY integration and configuration scenarios.

In this chapter:

ASSA ABLOY Integration with C•CURE 9000	10
Lock scenarios	10

ASSA ABLOY Integration with C•CURE 9000

The driver software integrates the C•CURE 9000 system with the Door Service Router (DSR) software from ASSA ABLOY, and the ASSA ABLOY IP locks. The DSR software manages communication to and from ASSA ABLOY IP locks. The integration supports selected lock models from the Corbin Russwin and Sargent brands. The integration supports hard-wired power locks, Power over Ethernet (PoE) locks, and wireless (WiFi) locks.

Similar to the C•CURE 9000 system, the ASSA ABLOY integration contains both client and server components. You must install the client components on every computer that runs C•CURE 9000 client applications, and you must install the server components on the C•CURE 9000 server computer.

NOTE

Wireless locks do not provide the same performance as readers connected to iSTAR panels.

Supported environments

The functionality of this integration is available in the application server, standalone, SAS, and MAS environments.

MAS environments do not use the following ASSA ABLOY objects:

- Door Service Router
- ASSA ABLOY Reader
- ASSA ABLOY Door
- ASSA ABLOY Scheduler
- ASSA ABLOY Card Format
- ASSA ABLOY Mag Card Fields
- ASSA ABLOY Clearance Mode
- ASSA ABLOY Access Mode

Lock scenarios

Use a lock configuration appropriate for your facility requirements. Wireless connections communicate only with the DSR in response to a door forced alarm, a tamper alarm, a low battery, or a configured event or schedule.

All Wi-Fi

Locks connect to the DSR through the IEEE 802.11 b/g/n wireless infrastructure.

Wi-Fi + Hardwired Power

Wi-Fi battery-powered locksets and Wi-Fi hardwired powered locksets connect to the DSR through the IEEE 802.11 b/g/n wireless infrastructure.

Wi-Fi, Hardwired Power, and PoE

Locks connect to the DSR through the IEEE 802.11 b/g/n wireless infrastructure and PoE. PoE locks connect through a CAT5e cable to an Ethernet router.

PoE Only

Locks connect to the DSR through PoE infrastructure.

Integration Best Practices Hardening Recommendations

This chapter provides best practices recommendation for cyber security considerations and hardening communications between the ASSA ABLOY DSR and the C•CURE 9000 Server.

In this chapter

Encryption 13

Encryption

The ASSA ABLOY Integration is composed of the C•CURE ASSA ABLOY driver and the third party DSR components. Enabling encryption at the DSR and the driver is strongly recommended as it establishes a secure link (TLS1.2) between the C•CURE ASSA ABLOY driver and the third party DSR components.

It's strongly recommended communications between the C•CURE Server and the third party DSR Server utilize a firewalled private network that does not provide access to the internet.

Enabling encryption between C•CURE and the DSR

Encryption between the C•CURE Server and DSR is not enabled by default. It's highly recommended to enable encryption. Follow the steps in [Installation on C•CURE server](#) to enable encryption. The use of signed certificates over self-signed certificates is also recommended.

Enabling AES encryption between the DSR and Wireless Locks

Enabling AES (Advanced Encryption Standard) encryption at the DSR and the ASSA ABLOY readers is recommended. The wireless infrastructure configuration should follow the best network practices for securing a private wireless infrastructure. Refer to the documentation provided by ASSA ABLOY for the DSR for these steps and best practices recommendations.

Record Retention Policy

It is recommended that the customers must consider their Record Retention Policy, and plan to configure C•CURE 9000 and the ASSA ABLOY DSR accordingly to meet their Record Retention Policy requirements.

Data Privacy Notice

This chapter provides a discussion of the ASSA ABLOY IP locks integration data privacy notice.

In this chapter

Data Privacy Notice 15

Data Privacy Notice

This application, as controller, processes the following personnel data for Johnson Controls:

- First Name
- Middle Name
- Last Name
- Card Numbers

This application may also process other personnel data, which may include access control information from the C•CURE 9000 product.

You, or your employer, are the controller of access control information. You, or your employer, are obliged to learn about and comply with all applicable local, state or provincial and federal or national laws and regulations with regard to that personnel data, including personnel data protection, privacy, and security laws and regulations.

Purpose of processing

1. Using credential information and associated card formats, the ASSA ABLOY integration downloads the calculated bit patterns to the DSR, to assign the appropriate access.
2. The ASSA ABLOY integration uses the processed credential information to initialize the C•CURE 9000 Journal Messages.

Pre-installation

This chapter provides pre-installation information for ASSA ABLOY.

In this chapter

DSR server specifications	17
ASSA ABLOY locks requirements	19
Standalone servers and enterprise servers	20
ASSA ABLOY driver and C•CURE installation process	21
Installation troubleshooting	24

DSR server specifications

There are two DSR configurations, large DSR system and small DSR system.

Each system configuration is dependent on the amount of locks deployed and the amount of expected transactions. See the following examples.

Minimum system requirements for full capacity DSR

- Up to 2048 Locks per DSR
- 8 CPU cores or higher
- 16 GB RAM or higher
- 150 GB free HD space or higher

Minimum system requirements for large DSR

- Up to 1024 Locks per DSR
- 4 CPU cores or higher
- 8 GB RAM or higher
- 75 GB free HD space or higher

Minimum system requirements for small DSR

- Up to 128 Locks per DSR
- Desktop, laptop environment, or platform
- Dual CPU cores or higher
- 4 GB RAM or higher
- 50 GB free HD space or higher

Windows operating system requirements

These requirements apply for both small and large configurations.

Windows 64 bit operating systems: Windows 2018, Windows 2012, Windows 2016, Windows 10, or Windows 2019.

The integration installation media includes Postgres 12. This is the only database manager supported for DSR 8.0.13.

DSR configuration file verification

You must ensure that the DSR fully supports 2048 ASSA ABLOY readers by verifying two of the DSR configuration files. The DSR configuration files are typically stored in the following location on the DSR computer:

- C:\Program Files\DSR\apache-tomcat\conf\Catalina\localhost\dsr.xml
- C:\Program Files\DSR\apache-tomcat\conf\Catalina\localhost\dsrsupport.xml

Ensure that the maximum number of AccessPoints is set in both DSR configuration files:

- Maximum number of AccessPoints that can be confirmed in the DSR is set to 2048.

- Maximum number of AccessPoints that be accepted by the DSR in one Authorization is set to 2048.

Example:

```
<!-- This is the maximum number of AccessPoints that can be confirmed in the DSR -->  
<Environment type="java.lang.Long" name="dsr.limit.core.accesspoint.confirm.max" value="2048"  
override="false"/>  
  
<!-- This is the maximum number of AccessPoints that the DSR will accept in one Authorization -  
->  
  
<Environment type="java.lang.Long" name="dsr.limit.core.authorization.accesspointcount.max"  
value="2048" override="false"/>
```

Restart the DSR after making these changes to the configuration files.

NOTE

DSR configuration files in new installations of DSR version already contain 2048 for both values, but the limits might be lower if the DSR has been upgraded from prior versions.

ASSA ABLOY locks requirements

- Use LCT version 4.0.49 or later.
- Upgrade lock firmware using LCT. Select the P5 version for optimal performance.
- The following are the minimum lock requirements (depending on the lock):
 - n18 or later
 - p05_3480 or later
 - p07_3504 or later
 - 3_0m05_sx_public or later

Standalone servers and enterprise servers

The integration driver for DSR 8.0 cannot run on the same server as the driver for DSR 5.0. It also does not communicate to a version 5.0 DSR. Upgrade all DSRs on a standalone server. Upgrade all DSRs on a SAS at the same time. Locks continue to operate during the upgrade process.

If you have multiple SAS with the ASSA ABLOY integration, keep them on the same version of the driver for optimal performance.

Licensing the C•CURE 9000 ASSA ABLOY DSR 8 integration

To enable the C•CURE 9000 ASSA ABLOY integration driver for DSR 8 and C•CURE 9000 2.90 SP1, ensure your C•CURE server is licensed by completing the following steps.

1. Open the C•CURE 9000 **License Manager**.
2. Click the **C•CURE 9000** tab.
3. In the **System Wide Capabilities** section, ensure that the number of **Wireless/IP Locks** matches how many locks are installed.
4. In the **Licensed Features** section, ensure that **AssaAbloy IP Locks** is enabled.

New DSR 8 projects

For new projects, order the main integration license, **CC9000-ASSAABLOY**. This will enable the server component Assa Abloy IP Locks.

There are two license options for the locks:

- **CC9-LKWIP-LIC** - WIRELESS/IP LOCK LIC, CHARGE
- **CC9-LKWIP-LICNC** - WIRELESS/IP LOCK LIC, NO CHARGE

Order the quantity of lock licenses that you need. If the locks are purchased through Software House, order the license with no charge. If the locks are not purchased through Software House, or are already installed on site, order the charged license for each lock. The **Wireless/IP Locks** number should match the number of licensed locks.

Upgrades from DSR 5

For existing DSR 5 projects that are being upgraded to DSR 8, the server component option remains on. For the lock license count, inform your integrator of the number of locks that are currently installed. You then receive a new 2.90 SP1 license with the same number of Wireless/IP Locks enabled.

ASSA ABLOY driver and C•CURE installation process

Prerequisites

Before installation the ASSA ABLOY driver, ensure that the following prerequisites are met:

- You are running C•CURE 9000 v2.90 SP1 or later.
- The C•CURE databases are backed up. For enterprise installations, verify that there are backups for both the MAS and all SAS. For more information, refer to the *C•CURE System Maintenance Guide*.
- The reader firmware is compliant.
- You have the installation media for DSR 8, integration version 3.74.278 or later.
- The previous integration version is installed.
- You have the correct database rights for local or remote database server. See [Enabling SQL permissions](#).
- You have a license that shows the number of wireless IP locks on the system. See [Licensing the C•CURE 9000 ASSA ABLOY DSR 8 integration](#).

NOTE

The CrossFire server component does not start if the license is not properly configured.

Installing DSR 8.0

To install DSR 8.0, complete the following steps:

1. Ensure that the firewall blocks incoming traffic on the port used by the wireless locks. Port 2571 is the default port. This port can be changed in the DSR and lock configuration.
2. Shutdown the DSR.
3. On the C•CURE server, open the **Server Configuration** application. Stop the **SoftwareHouse CrossFire Assa Abloy Driver Service**.
4. Start the new blank DSR 8 server.
5. If you are using the same IP address and name as the old DSR, complete the following.
 - a. Open the Control Panel and click **Network and Sharing Center**.
 - b. Click your network connection, then click **Properties**.
 - c. Select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.
 - d. Select **Use the following IPv4 address**. Enter the same IP address information as the old DSR.
 - e. Click **OK**.
6. Create a firewall rule to block incoming traffic on the port used by the wireless locks. Port 2571 is the default port. This port can be changed in the DSR and lock configuration. The firewall rule prevents the wireless locks from requesting updates during the upgrade process.
7. Double-click the installer exe file to begin the installation.
8. Follow the prompts on screen. Note the account name and password you choose during installation.

NOTE

PostgreSQL database also installs when you install DSR 8.0. Note the account name and password for database access.

Installing the integration driver

To install the integration driver, complete the following steps.

1. On the C•CURE server, open the **Server Configuration** application. Stop the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**.
2. Open the Control Panel and click **Uninstall a program**.
3. Select **CCURE9000 Assa Abloy Integration** and click **Uninstall**.

NOTE

Do not drop the databases during the uninstall. If the databases are dropped, you need to restore a backup of ACVSCore before beginning the install.

4. Optional: If installing the driver on a C•CURE application server where the database is on a separate server, you need to download and install the following on the C•CURE application server prior to running the **CCURE9000AssaAbloyIntegrationInstaller.msi**. Ensure that you download and install the correct version of each for the version of SQL used at your site, and install in the following order:
 - Microsoft ODBC driver for SQL (**msodbcsql.msi**)
 - Microsoft Command Line Utility for SQL (**MsSqlCmdLnUtils.msi**)
5. Double-click **CCURE9000AssaAbloyIntegrationInstaller.msi**.

NOTE

Ensure that you are logged on using the service account to install the driver, otherwise you will not be able to run the installation.

6. Follow the wizard instructions. On the **Service Access Credentials** screen, select **Use the LocalSystem account** if you are running a standalone with local SQL. Otherwise, select **Use Windows authentication credentials** and specify the service account used by the Crossfire services in the fields.

NOTE

If the LocalSystem account was not given SQL rights, the installer rolls back and halt at this point.

7. Once installation is complete, apply the new license in the license application.
8. Restart the **CrossFire Framework Service** and the **CrossFire Server Component Framework Service**.

Post install synchronization

Once the system has completed installation, the DSR attached to the server starts to synchronize. It sends basic configuration to the DSR.

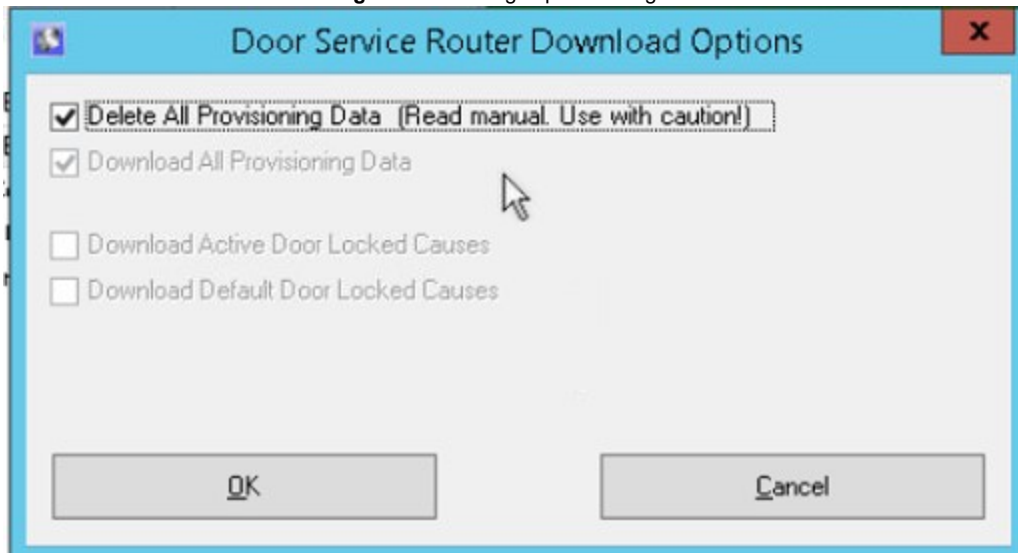
After the synchronization is complete, you need to synchronize the locks to the DSR.

To synchronize the locks to the DSR, complete the following steps.

1. Right-click the DSR object in the **Administration Workstation** and select **Download Door Service Router**.

2. Select the **Delete All Provisioning Data** and **Download all Provisioning Data** check boxes. Click **OK**.

Figure 1: Deleting all provisioning data



Firewall

Ensure that the firewall that protects the DSR allows incoming connections on the following port numbers.

- The port number configured via the ASSA ABLOY LCT that the locks use to communicate with the DSR. The default value is 2571.
- The port number configured in the port number property of the ASSA ABLOY DSR object in C•CURE, that the C•CURE Server uses to communicate with the DSR. The default value is 8080 for unencrypted communication, and 8443 for encrypted communication.

Ensure that the firewall that protects the C•CURE server allows incoming connections on the following port number:

- The port number configured in the C•CURE system variable ASSA ABLOY Callback Port Number, that the DSR uses to communicate with the C•CURE Server. The default value is 41101.

Enabling the locks

To enable the locks, complete the following steps.

1. Right-click the ASSA ABLOY reader object in the **Administration Workstation** and select **Set Property**.
2. From the **Property** list, select **Enabled**.
3. Click the **Value** box and then click **OK** to enable the locks.
4. Once all readers are enabled, turn off the firewall on the DSR. When the locks wake up, they connect to the DSR.
5. Test reader functions to verify operations.

Installation troubleshooting

Installation logs

If you encounter an error during the install, the first step is to check the installation log.

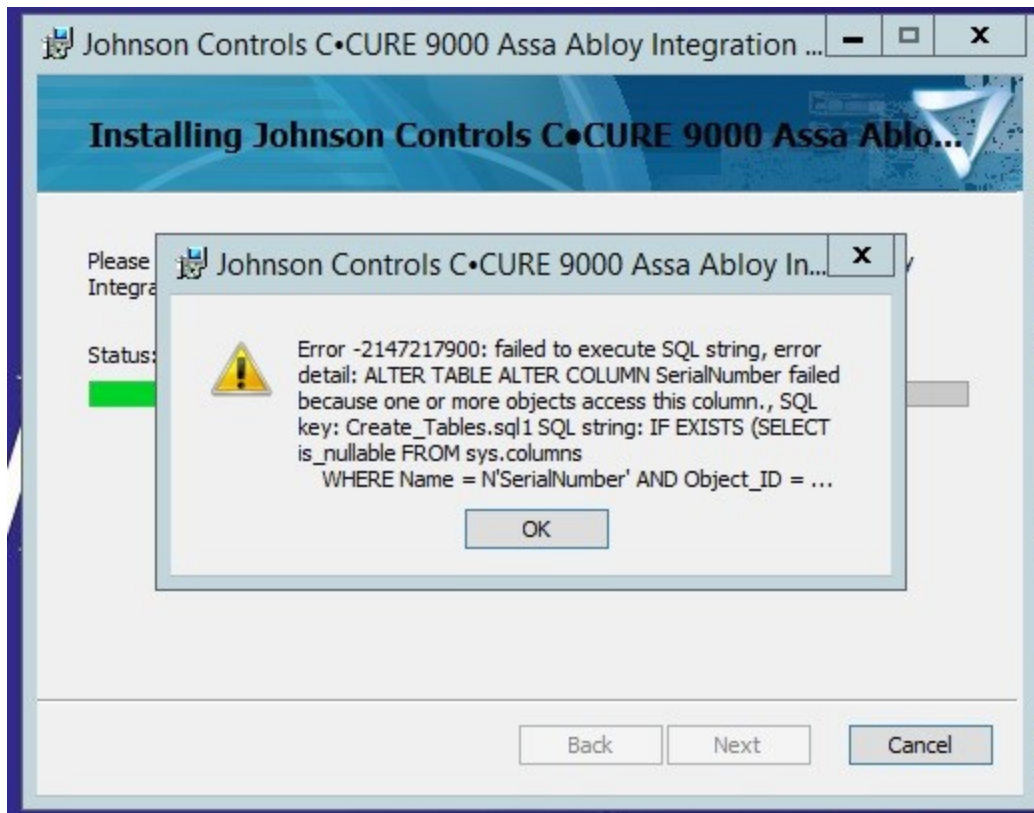
Accessing installation logs

To check the installation log, complete the following steps.

1. From the Windows Start menu, search for and open **Run**.
2. Enter %temp% in the **Open** field and click **OK**.
3. Sort the files by Date Modified. The log files are named MSIxxxxxx.txt and should have a matching time to your install attempt.

Existing Index causes SQL script error

Upgrading a system may encounter an error like this:



This error occurs because there are existing indexes that the install script cannot remove.

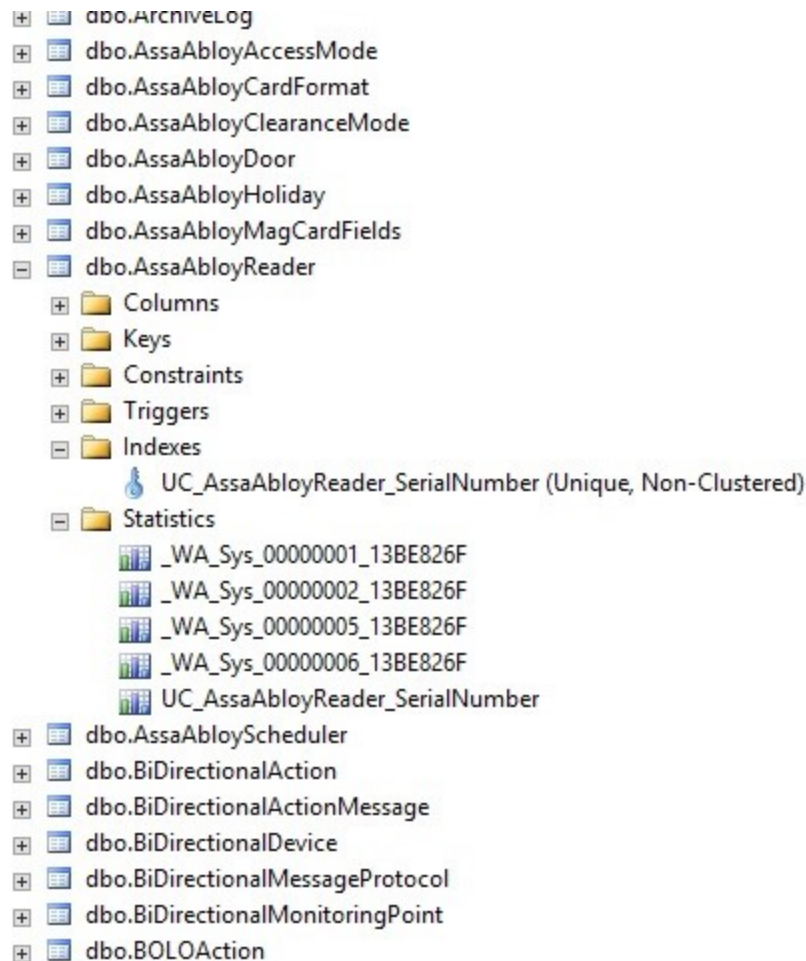
Fixing script error

To fix this error, complete the following steps.

1. Open **SQL Management Studio** and connect to the server.
2. Expand the **Databases** folder, then expand **ACVSCore** and then expand **Tables**.
3. Expand the **DBO.ASSAAbloyreaders** folder, then expand **Indexes** and **Statistics**.
4. Right-click on all of the indexes and statistics and then click **Delete**.
5. Repeat the installation. If you encounter the same error, contact ASSA ABLOY support.

Figure 2 shows the location under ACVSCore\DBO.AssaAbloyreader.

Figure 2: ACVSCore\DBO.AssaAbloyreader



LocalSystem is not DBowner

When installing the new ASSA ABLOY driver, the installation may generate error code 1603 and require that the computer identity is defined under SQL security as well as the service account credentials.

Problem

New installation of ASSA ABLOY integration driver for a domain environment or remote SQL server.

NOTE

The ComputerName\$ referenced in the error is the application ServerName with \$.

Cause

View the installation log to see if it shows the following error. See [Accessing installation logs](#) for steps on how to access the installation log.

```
UpdateEncryptedVars: arg 1: 'DomainNAME\ComputerNAME$'.
```

```
<deleted>
```

```
Database connection not possible. Database treated as not existing. Exception: Login failed for user
```

```
'DomainNAME\ComputerNAME$'.
```

```
CustomAction UpdateEncryptedVars returned actual error code 1603 (note this may not be 100% accurate if translation happened inside sandbox)
```

```
Action ended 13:07:23: InstallFinalize. Return value 3.
```

This is caused by the C•CURE application server not having SQL server permission.

Creating an SQL login for the specified computer C•CURE AppPool identity LocalSystem

To resolve the SQL server permission issue, complete the following steps.

1. Open **SQL Management Studio** and connect to the server.
2. From the **Object Explorer** pane, expand the **Security** folder.
3. Right-click **Logins** and select **New Login...**
4. Enter DOMAIN\ComputerName\$ in the **Login name** field.
5. Select the **Windows Authentication** check box.
6. From the left pane, select **Server Roles**.
7. Ensure the **sysadmin** and **public** check boxes are selected.
8. From the left pane, select **User Mapping**.
9. Select the **ACVSCore** from the **Users mapped to this login** list, and select **db_owner** from the **Database role membership for** list.
10. Click **OK**.

Installation and upgrade

This chapter describes pre-installation requirements, licensing, installation, and upgrade information.

In this chapter:

Requirements	28
Installation on C•CURE server	30
ASSA ABLOY system variables	39
Upgrading	40
Lock Configuration Tool	42

Requirements

To use C•CURE 9000 with ASSA ABLOY IP locks, hardware and software must meet specific requirements, and hold a valid license for all necessary components.

A C•CURE server supports up to 10 enabled DSRs. Each DSR supports up to 2048 readers; attempting to configure an additional reader on a DSR results in an error.

NOTE

Do not run C•CURE 9000 software on the same machine as the DSR software.

Upgrading

Refer to the *C•CURE 9000 Installation and Upgrade Guide* to ensure that your system meets the upgrade requirements. For details on performing the ASSA ABLOY integration and DSR upgrades, see [Upgrading](#).

Licensing

Ensure you have a valid license for the **ASSA ABLOY Integration** option in C•CURE 9000, and a **Wireless/IP lock** license count for each lock in your configuration.

Requirements summary

Table 1: Requirements summary

Component	Requirements
C•CURE server	• C•CURE 9000 v2.90 SP1 • C•CURE 9000 server on same time zone as DSR Refer to the C•CURE 9000 documentation for other C•CURE server requirements.
DSR server	DSR 8 minimum system requirements: • Up to 2048 Locks per DSR - 8 CPU cores or greater - 16 GB RAM or greater - 150 GB free HD space or greater • Up to 128 Locks per DSR - Desktop/ laptop environment/ platform - Dual CPU cores or greater - 4 GB RAM or greater - 50 GB free HD space or greater NOTE: The DSR integration install media includes Postgres version 12, which is the only database manager that DSR 8.0.13 supports.
Windows OS	Win 10, Win 2012, Win 2016 or Win 2019.

Requirements summary (continued)

Component	Requirements
Lockset firmware	Software House only supports ASSA ABLOY hardware with the following firmware versions: • N18, or later • p05_3480, or later • p07_3504, or later • 3_0m05_sx_public, or later Update firmware through the DSR support tool or LCT.
Locks	• If using ASSA ABLOY wireless locks, you must install wireless access points. • You must install locks on all doors that require access control operation. • The number of locks must not exceed the capacity limit of the Wireless/IP Locks license. • The number of locks must not exceed 2048, the maximum allowable on a DSR.
Lock configuration	• Use the Lock Configuration Tool (LCT) to configure locks. Purchase the tool from ASSA ABLOY, as part of the WF-CD1 kit. • You require a DB9 serial (female) to RJ11 cable, or a mini-USB cable, to configure locks with the LCT. Refer to the <i>Lock Configuration Tool User Manual</i>, available from Help in the LCT application, for more information.

Enabling SQL permissions

NT AUTHORITY/SYSTEM is not inserted as a system administrator in SQL by default. You must define it as a system administrator during, or after, SQL installation.

NOTE

For SQL Express installations, you must complete these steps after installation.

1. Open **SQL Management Studio** and connect to the server.
2. From the **Object Explorer** pane, expand the **Security** folder.
3. Expand the **Logins** folder.
4. Double-click **NT AUTHORITY/SYSTEM**.
5. From the left pane, select **Server Roles**.
6. Ensure the **sysadmin** check box is selected.
7. Click **OK**.

Creating an SQL login for the specified computer C•CURE AppPool identity LocalSystem

1. Open **SQL Management Studio** and connect to the server.
2. From the **Object Explorer** pane, expand the **Security** folder.
3. Right-click **Logins** and select **New Login...**
4. Enter `DOMAIN\ComputerName$` in the **Login name** field.
5. Select the **Windows Authentication** check box.

6. From the left pane, select **Server Roles**.
7. Ensure the **sysadmin** and **public** check boxes are selected.
8. From the left pane, select **User Mapping**.
9. Select the **ACVSCore** from the **Users mapped to this login** list, and select **db_owner** from the **Database role membership for** list.
10. Click **OK**.

Installation on C•CURE server

Only qualified integrators or technicians can install this software.

Installing the ASSA ABLOY integration

1. Double-click **CCURE9000AssaAbloyIntegrationInstaller.msi**.

NOTE

Ensure that you are logged on using the service account to install the driver, otherwise you will not be able to run the installation.

2. Follow the wizard instructions.
3. Restart the computer after installation.
4. After restarting the computer, verify that you have a license for the ASSA ABLOY integration. See [Verifying a valid license](#).
5. Start the driver service. See [Starting the driver service](#).

If you did not select the **Start the Tyco CrossFire services** check box during installation, see [Starting CrossFire services](#).

NOTE

See [Installation impact on target system](#) for details on changes in the system after installation.

Encryption

Enable encryption in the DSR to allow communication between C•CURE and the DSR in encrypted mode.



If a `data` folder does not exist in your DSR server's C: drive, you must create one.

Enabling encryption before installing the driver

NOTE

- Enabling encryption slows data transfers between the DSR and C•CURE.
- Use Signed Certificates for optimal performance.

1. On the DSR, run command prompt as an administrator.
2. Type `Java -version`.

3. Create a key pair and key store for the DSR.

a. Type `cd C:\Program Files\Java\jreX.X.X_XXX\bin\`

NOTE

X.X.X_XXX represents the JRE version that you verified in [Step 2](#).

b. Type the following command:

```
keytool -genkeypair -keysize 4096 -keyalg RSA -alias dsrservicekey -keypass dsrdsr -validity 732 -storetype PKCS12 -keystore "C:\data\dsrServiceKeyStore.p12" -dname "CN = XX, OU = XX, O = XX, L = XX, S = XX, C = XX"
```

NOTE

The CN field of the certificate that was just created must match the full computer name of the machine running this DSR. Find the full computer name of the DSR from **Control Panel\System** or **Security\System**.

Table 2: Command variables

Command	Description	Value
CN	Common name	Must match the full computer name of the DSR
OU	Organizational unit	User-defined
O	Organization	User-defined
L	Locality	User-defined
S	State or province	User-defined
C	Two-letter country code for this unit	User-defined

c. Enter a keystore password. The default password is `dsrdsr`. You can enter a new password here.

d. Confirm the keystore password.

NOTE

- If you enter a new password, keep record of it for future use.
- You can use the same keystore for multiple DSRs.

4. If using Self-Signed Certificates, skip to [Step 8](#). If using Signed Certificates, create a certificate signing request.

- From prompt, execute:

```
keytool -certreq -alias dsrservicekey -keystore "C:\data\dsrServiceKeyStore.p12" -file "C:\data\DSR8VM.csr"
```

5. Submit CSR file to certificate authority. The certificate authority will send you a p7b file.

6. Install p7b file.

- Copy PKCS#7 certificate of the DSR (e.g. DSR8VM.p7b) in `C:\data\`.

7. Import certificate to keystore.

- From prompt, execute:

```
keytool -import -trustcacerts -alias dsrservicekey -storepass dsrdsr -storetype PKCS12 -keystore "C:\data\dsrServiceKeyStore.p12" -file "C:\data\DSR8VM.p7b"
```

8. Create a certificate containing the DSR's public key. Type the following command:

```
keytool -exportcert -alias dsrservicekey -storepass dsrdsr -storetype PKCS12 -keystore "C:\data\dsrServiceKeyStore.p12" -file "C:\data\DsrService.cer"
```

9. Load the DSR certificate.

- a. Type the following command:

```
keytool -import -alias dsrservicekey -trustcacerts -file "C:\data\DsrService.cer" -keystore "C:\Program Files\Java\jreX.X.X\lib\security\jssecacerts" -storepass changeit
```

NOTE

The `changeit` part of the command represents the default Java Keystore password. Ensure that you use the actual DSR's Java Keystore password in the command.

The following command may be used to delete the certificate before replacing it:

```
keytool -delete -alias dsrservicekey -keystore "C:\Program Files\Java\jre1.8.0_192\lib\security\jssecacerts" -storepass changeit
```

Deleting a previously installed certificate in the Java store does not cause any harm if the certificate is not present in the Java keystore.

- b. Answer `yes` to the trust question.

10. Open the DSR support tool.

11. Select **Configuration Settings**, then select **Server Settings**.

12. Configure the **WS Security & Port Configuration**. See [Table 3](#) for configuration details.

Table 3: Encryption configuration

Field or radio button	Value
WS-Security	False
SSL-Security	True
Access Data Port	8443
Lock Port	2571
Security Valve	127.0.0.1 0:0:0:0:0:0:1

13. Click **Update Configuration**, then click **OK**.

14. Encrypt the DSR keystore password.

- a. Navigate to `C:\Program Files\DSR`.
- b. Double-click `password-encryption.bat`.

- c. Enter the keystore password. The default password is dsrdsr. You may have changed this in [Step 3](#).
- d. Copy the encrypted keystore password. For example, rcEihJ4AokSV3SzFAXzfyQ==.

15. Edit the DSR xml.

- a. Navigate to C:\Program Files\DSR\apache-tomcat\conf.
- b. Edit server.xml.
- c. Update keystoreFile and keystorePass in the Connector entry at the bottom of the file.

```
<Connector SSLEnabled = "true" acceptCount = "100" clientAuth = "false"
disableUploadTimeout = "true" enableLookups = "false"

keystoreFile = "conf/dsrServiceKeyStore.p12"
keystorePass = "rcEihJ4AokSV3SzFAXzfyQ =="

maxThreads = "25" port = "8443" protocol =
"org.apache.coyote.http11.Http11NioProtocol" scheme = "https" secure = "true"
sslImplementationName = "org.apache.tomcat.util.net.jsse.JSSEImplementation"
sslProtocol = "TLSv1.2" />
```

NOTE

rcEihJ4AokSV3SzFAXzfyQ== is a sample keystore password. Type the encrypted password that you created in [Step 14](#).

- d. Save and close.

16. Install the DSR key store.

- a. Navigate to C:\data.
- b. Copy dsrServiceKeyStore.p12.
- c. Navigate to C:\Program Files\DSR\apache-tomcat\conf.
- d. Paste dsrServiceKeyStore.p12 into the folder.
- e. Restart ASSA ABLOY Door Service Router.

NOTE

[Step 17](#) to [Step 22](#) need to be executed on a single DSR. The resulting file c:\data\clientuser.cer will later be used on all other DSRs connected to the C•CURE 9000 server, in addition to the C•CURE 9000 server itself.

17. Create a key pair and key store for the driver.

- a. Run command prompt as an administrator.
- b. Type cd C:\Program Files\Java\jreX.X.X_XXX\bin\

NOTE

X.X.X_XXX represents the JRE version that you verified in [Step 2](#).

- c. Type the following command:

```
keytool -genkeypair -keysize 4096 -keyalg RSA -alias clientuser -keystore "C:\data\clientUserKeyStore.p12" -
validity 732 -storetype PKCS12 -keypass dsrdsr -
dname "CN = clientuser"
```

- d. Enter the password of the keystore, `dsrdsr` when prompted.
- e. The tool will prompt for additional information, which can all be provided as user-defined values.
18. If using Self-Signed Certificates, skip to [Step 22](#). If using Signed Certificates, create a certificate signing request.
- From prompt, execute:

```
keytool -certreq -alias clientuser -keystore "C:\data\clientUserKeyStore.p12" -file "C:\data\clientuser.csr"
```
19. Submit CSR file to certificate authority. The certificate authority will send you a p7b file.
20. Install p7b file.
- Copy PKCS#7 certificate of the ASSA ABLOY integration (e.g. `clientuser.p7b`) in `C:\data\`.
21. Import certificate to keystore.
- From prompt, execute:

```
keytool -import -trustcacerts -alias clientuser -storepass dsrdsr -storetype PKCS12 -keystore "C:\data\clientUserKeyStore.p12" -file "C:\data\clientuser.p7b"
```
22. Export a certificate containing the driver's public key. Type the following command:
- ```
keytool -exportcert -alias clientuser -storepass dsrdsr -storetype PKCS12 -keystore "C:\data\clientUserKeyStore.p12" -file "C:\data\clientuser.cer"
```

### Enabling encryption, after installing the driver



If an AssaAbloy folder does not exist in location `C:\ProgramData\Tyco`, you must create one.

23. On the DSR, open **Run** with Windows+R hotkeys.
24. In the text field, type `services.msc`.
25. Stop the **ASSA ABLOY Door Service Router** service.
26. Restart the **ASSA ABLOY Door Service Router** service.
27. From `C:\data` on the DSR where [Step 17](#) and [Step 22](#) were performed, copy `clientUserKeyStore.p12`, `clientuser.csr`, `clientuser.cer`, and `clientuser.p7b` to `C:\ProgramData\Tyco\AssaAbloy\` on the C•CURE9000 machine.
28. On each DSR server, complete the following.
- Copy `clientuser.cer` from `c:\data` of the DSR used in [Step 22](#) to `c:\data` of all other DSR which need to communicate with the C•CURE server.
29. On each DSR server, load the driver certificate on the DSR certificate store.
- Run command prompt as an administrator
  - Type `Java -version`.
  - Type `cd C:\Program Files\Java\jreX.X.X_XXX\bin\`

## NOTE

X.X.X\_XXX represents the JRE version that you verified in [Step 29](#).

d. Type the following command:

```
keytool -import -alias clientuser -trustcacerts -file "C:\data\clientuser.cer " -
keystore "C:\Program Files\Java\jreX.X.X_XXX\lib\security\jssecacerts" -storepass
changeit
```

e. Answer yes to the trust question.

## NOTE

The following command may be used to delete the certificate before replacing it:

```
keytool -delete -alias clientuser -keystore "C:\Program
Files\Java\jre1.8.0_192\lib\security\jssecacerts" -storepass changeit
```

30. For security reasons, delete `clientuser.csr`, `clientUserKeyStore.p12`, and `clientuser.p7b` from the DSR used to create the original `clientuser.cer`. You can leave the `clientuser.cer` in the `c:\data` folder of each DSR if you choose.

## Enabling encryption on the C•CURE server

1. Configure the Microsoft Management Console.
  - a. Open **Run** with Windows+R hotkeys.
  - b. Enter `mmc` in the text field. Press Enter or click **OK**.
  - c. From the MMC navigation bar, select **File**.
  - d. Select **Add/Remove Snap-in**. The **Add or Remove Snap-ins** window appears.
  - e. From the list of **Available snap-ins**, select **Certificates**.
  - f. Click **Add >**. The **Certificates snap-in** window appears.
  - g. Select **Computer account**.
  - h. Click **Next**. The **Select Computer** window appears.
  - i. Select **Local computer**.
  - j. Click **Finish**. Click **OK**.
2. Import a certificate for the driver's public key.
  - a. Double click **Certificates (Local Computer)**. All sub-folders appear.
  - b. Navigate to the **Personal** folder.
  - c. From the navigation bar select **Action**.
  - d. Hover over **All Tasks** and select **Import**.
  - e. Click **Next**.
  - f. Click **Browse**. Navigate to `C:\ProgramData\Tyco\AssaAbloy`.
  - g. Select **clientUserKeyStore.p12**.
  - h. Click **Open**. Click **Next**.

- i. Select **Place all certificates in the following store** and enter `Personal` in the **Certificate store** field.

## NOTE

If the system requests a password, enter the keypass password. The default password is `dsrdsr`.

- j. Click **Next**. Click **Finish**.

## NOTE

A dialogue box confirms a successful import. After successful import, check the **Trusted Root** folder. If you do not find the **Root** certificate for the certificate that was imported, then copy and paste the **Root** certificate from the **Personal** folder to the **Trusted Root** folder

3. Record the clientuser certificate's thumbprint.
  - a. Double-click the **clientuser.cer** certificate.
  - b. Select the **Details** tab.
  - c. Scroll down to **Thumbprint**.
  - d. Copy the **Thumbprint** value.

## NOTE

The thumbprint value is the certificate certhash value for use in the [Step e](#) command.

- e. Configure callback channel.
  - Run command prompt as an administrator, and type the following command:

```
netsh http add sslcert ipport=0.0.0.0:41101 certhash=A1B2C3 appid={00000000-0000-0000-0000-000000000000} certstorename=MY
```

## NOTE

- Replace the `certhash` value with the certificate thumbprint value that you recorded in [Step d](#).
- You must use the `appid` value provided.
- The `ipport` number above must match the ASSA ABLOY Callback Port Number system variable in C•CURE 9000.
- Encryption does not turn on until at least one DSR object is added to the system, the system variables are configured correctly, and the C•CURE services are restarted.

- f. Copy the Root Certificates from Client Certificate chain under **Personnel** folder to **Trusted Root** folder.

## Operator permissions

When using encryption, the C•CURE client cannot communicate to the DSR if the certificate on the client machine does not have the full permissions for the current operator. By default, the administrator who installed the integration has these permissions, but all other operators do not.

To give permissions to an operator, complete the following procedure:

### Giving certificate permissions to an operator

1. Open **Run** with Windows+R hotkeys.
2. In the text field, type `mmc`. Press Enter or click **OK**.
3. From the **File** menu, select **Add/Remove Snap-in**.

4. In the **Add or Remove Snap-ins** window, from the list of **Available snap-ins**, select **Certificates**.
5. Click **Add >**.
6. In the **Certificates snap-in** window, select **Computer account**.
7. Click **Next**. The **Select Computer** window appears.
8. Select **Local computer**.
9. Click **Finish**. Click **OK**.
10. In the **Microsoft Management Console**, in the left pane, double-click **Certificates (Local Computer)** to expand all folders.
11. Expand the **Personal** folder, and select **Certificates**
12. In the middle pane, right-click on **clientuser**. Hover over **All Tasks**, and select **Manage Private Keys**.
13. Select or add the user account you want to provide with permissions.
14. In the **Permissions for Administrators** area, select the **Allow Full control** check box.
15. Click **OK**.

## Installation impact on target system

**Table 4: Files Installed**

| Installation                                      | File location starting with C:\Program Files (x86) \                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>All</b>                                        | <ul style="list-style-type: none"> <li>• Tyco\CrossFire\SoftwareHouse.NextGen.AssaAbloy.CustomJournalFormats.dll</li> <li>• Tyco\CrossFire\SoftwareHouse.NextGen.Common.AssaAbloyObjects.dll</li> </ul>                                                                                                                                                                                                                                                                                                                              |
| <b>Client component only</b>                      | <ul style="list-style-type: none"> <li>• Tyco\CCURE Client\SoftwareHouse.NextGen.AssaAbloy.CustomJournalFormats.dll</li> <li>• Tyco\CCURE Client\SoftwareHouse.NextGen.Client.AssaAbloyClient.dll</li> <li>• Tyco\CCURE Client\SoftwareHouse.NextGen.Common.AssaAbloyObjects.dll</li> </ul>                                                                                                                                                                                                                                          |
| <b>Server component only, not included on MAS</b> | <ul style="list-style-type: none"> <li>• Tyco\CrossFire\ServerComponents\SoftwareHouse.NextGen.AssaAbloy.CustomJournalFormats.dll</li> <li>• Tyco\CrossFire\ServerComponents\SoftwareHouse.NextGen.Common.AssaAbloyObjects.dll</li> <li>• Tyco\CrossFire\ServerComponents\SoftwareHouse.NextGen.Server.AssaAbloyDriver.dll</li> <li>• Tyco\CrossFire\ServerComponents\SoftwareHouse.NextGen.Server.AssaDriverService.exe</li> <li>• Tyco\CrossFire\ServerComponents\SoftwareHouse.NextGen.Server.AssaDriverService.config</li> </ul> |

### System database tables added

- DoorServiceRouter
- AssaAbloyReader
- AssaAbloyDoor
- AssaAbloyScheduler
- AssaAbloyCardFormat
- AssaAbloyMagCardFields
- AssaAbloyAccessMode

- AssaAbloyClearanceMode
- AssaAbloyHoliday

## NOTE

These changes do not apply to client-only or MAS installations.

### Certificates added to local computer store

- Personal\clientuser
- Personal\localhost
- Trusted Publishers\localhost

## Licensing

ASSA ABLOY IP Locks require licence validation for driver server components and locksets. Order the main integration license, **CC9000-ASSAABLOY**. This turns on the ASSA ABLOY locks server component. There are two license options:

- **CC9-LKWIP-LIC** - WIRELESS/IP LOCK LIC, CHARGE
- **CC9-LKWIP-LICNC** - WIRELESS/IP LOCK LIC, NO CHARGE

### Licensing for the driver server component

After installing the driver, ensure it has a valid license. See [Verifying a valid license](#) for more information. If you do not have a valid license, contact your integrator.

Enable the driver in the **Server Configuration** application. See [Starting the driver service](#) for more information. By default, the driver is disabled when installed.

### Licensing ASSA ABLOY IP Locksets

ASSA ABLOY locksets count towards the **Wireless/IP Locks** count in the **C•CURE License Manager**. They do not count towards the online reader count. To determine how many lock licenses you have in the C•CURE 9000 system, check the existing C•CURE 9000 license in **License Manager**.

If the number of configured ASSA ABLOY locksets exceeds the limit permitted by the current C•CURE 9000 license, you must purchase additional lock licenses and validate a new license with the higher lock count.

## NOTE

For upgrades from previous versions of the ASSA ABLOY driver using DSR 5, you are entitled to lock licenses at no charge for the number of existing locksets that are in your system.

### Verifying a valid license

1. Navigate to the **Licensing** application at `C:\Program Files (x86)\Tyco\CrossFire`. Double-click `LicenseManager.exe` to open the application.
2. Click the **C•CURE 9000** tab. If you have a valid license, **ASSA ABLOY Integration** appears in **Licensed Features**.

## Starting CrossFire services

The ASSA ABLOY installation stops the CrossFire services. If you select the **Start the C•CURE 9000 services** check box during installation, the services restart after the installation. If you do not select this check box, you must manually start the services.

### Starting the services

1. Navigate to the **Server Configuration** application at `C:\Program Files (x86)\Tyco\CrossFire`. Double click `ACVS.Enterprise.Server.Configuration.exe` to open the application.
2. Click the **Services** tab.
3. Locate **CrossFire Framework Service** under **Framework Services**. If the **Status** displays **Stopped**, click **Start**.
4. Locate **CrossFire Server Component Framework Service** under **Framework Services**. If the **Status** displays **Stopped**, click **Start**.

## Starting the driver service

You must enable and start the driver after installation.

### Starting the driver service

1. Navigate to the **Server Configuration** application at `C:\Program Files (x86)\Tyco\CrossFire`. Double click `ACVS.Enterprise.Server.Configuration.exe` to open the application.
2. Click the **Services** tab. Under **Extension Services**, locate **Johnson Controls ASSA ABLOY Driver Service**.
3. If the service is disabled, select the **Enabled** check box and click **Start**.

#### NOTE

- Stopping a driver does not disable it. After restarting C•CURE, the driver restarts. To disable a driver, clear the **Enabled** check box.
- Non-licensed options display in the **Services** tab, but you are unable to start them.

When the **CrossFire Framework Service**, **CrossFire Server Component Service**, and the **Johnson Controls ASSA ABLOY Driver Service** display a **Running** status, you can configure the ASSA ABLOY objects in C•CURE.

You can configure the **Server Configuration** application in Windows **Computer Management**. You can configure a service to start automatically in **Computer Management**. However, if the driver service is disabled in the **Server Configuration** application, Windows cannot start the service.

## ASSA ABLOY system variables

The ASSA ABLOY integration includes ASSA ABLOY specific system variables. For information on C•CURE system variables, refer to the *C•CURE 9000 System Maintenance Guide*.

**Table 5: ASSA ABLOY system variables**

| System variable                                           | Description                                                                                                                                                                                         |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ASSA ABLOY Enable DSR Connection Encryption</b>        | Set this value to <code>True</code> to encrypt messages.                                                                                                                                            |
| <b>ASSA ABLOY Response Timeout</b>                        | Set timeout value between 15 and 120 seconds. The default value is 60 seconds.                                                                                                                      |
| <b>ASSA ABLOY Callback Port Number</b>                    | The ASSA ABLOY Callback Service port number. 41101 by default.                                                                                                                                      |
| <b>ASSA ABLOY Client Certificate Common Name</b>          | The Client certificate common name is composed of the name of the machine running the integration and the domain name that receives the certificate. The default value is <code>clientuser</code> . |
| <b>ASSA ABLOY Clear DSR On Resync When Missing SQL CE</b> | Set this value to <code>True</code> to clear the DSR if the resynchronization database file for the DSR does not exist.                                                                             |

## Upgrading

This section describes upgrading the DSR and the Johnson Controls ASSA ABLOY Driver.

### NOTE

- Ensure that only a qualified integrator, or technician upgrades this software.
- Only upgrade if you have a tested means of reverting changes.
- The new integration bases reader licenses on **Wireless/IP lock** count in the **C•CURE License Manager**.

## Known Limitations

- To upgrade the ASSA ABLOY integration you must use the same Windows credentials as the initial installation.
- The ASSA ABLOY integration does not support migration from standalone to Satellite Application Server (SAS).

## Prerequisites

- For a full list of requirements, see [Requirements](#).
- To prevent loss of data, back up C•CURE 9000 and all DSRs.
  - Back up virtual machines by creating snapshots of the C•CURE 9000 and DSR environments.
- Before upgrading the driver, shut down and disable the **Johnson Controls ASSA ABLOY Driver Service** to isolate the DSRs from C•CURE 9000.



Upgrade the drive only if you have a tested means of reverting changes.

## Upgrading the DSR

### Upgrading the DSR

1. Disable all readers in the **C•CURE Administration Workstation**.
2. Stop the Apache Tomcat service.
  - Navigate to `C:\Program Files\DSR\apache-tomcat\bin` and run `shutdown.bat`
3. On the C•CURE server, open the **Administration Workstation** application.
  - a. Select **Hardware** in the left pane. In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY DSR**, and click the green arrow.
4. Ensure the DSR object **Status** displays **CommFail**.
5. On the C•CURE server, open the **Server Configuration** application. Stop the **Johnson Controls ASSA ABLOY Driver Service**. This isolates the DSRs from C•CURE.
6. Upgrade all DSRs.

#### NOTE

For all DSR and DSR database upgrades, contact ASSA ABLOY support.

7. After upgrading a DSR, verify communication between the C•CURE 9000 server and the DSR.
  - a. Ping the DSR. Verify the ping is successful with no timeouts.
  - b. Open the **DSR** web page on the C•CURE 9000 server, confirm that the DSRs respond, and that the **Diagnostics** page displays.

#### NOTE

DSR web address: `http://x.x.x.x:8080/dsr`.  
x.x.x.x represents the DSR IP address.

8. Upgrade C•CURE 9000 and apply a valid license.
9. Upgrade the Johnson Controls ASSA ABLOY Driver.
10. Restart the Apache Tomcat service on the DSR server.
  - Navigate to `C:\Program Files\DSR\apache-tomcat\bin` and run `startup.bat`
11. Enable all readers in the **C•CURE Administration Workstation**.

## Upgrading the ASSA ABLOY integration driver

### Upgrading the driver

1. On the DSR server, stop the Apache Tomcat service.
  - Navigate to `C:\Program Files\DSR\apache-tomcat\bin` and run `shutdown.bat`
2. On each DSR, create a firewall rule to block incoming traffic on port 2571. This prevents the wireless locks from requesting updates during the upgrade process.
3. On the C•CURE server, open the **Administration Workstation** application.

- a. Select **Hardware** in the left pane. In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY DSR**, and click the green arrow.
- b. Ensure that both the **Download Status** and **Status** columns display **CommFail** for each DSR object.
4. On the C•CURE server, open the **Server Configuration** application. Stop the **Johnson Controls ASSA ABLOY Driver Service**. This isolates the DSRs from C•CURE.
5. Run the driver installation file as an administrator.
6. After installation, restart the Apache Tomcat service on the DSR.
  - Navigate to `C:\Program Files\DSR\apache-tomcat\bin` and run `startup.bat`
7. After the CrossFire services restart, in the **Server Configuration** application, start the **Johnson Controls ASSA ABLOY Driver Service**.
8. On each DSR, disable the firewall rule that you configured in [Step 2](#).
9. Wait until all iSTAR and apC controllers complete the online and personnel download sequence.
10. Right-click the DSR object in the **Administration Workstation** and select **Download Door Service Router with Delete All Provisioning Data checked**.
11. Verify lock synchronization. PoE locks synchronize immediately. Manually activate wireless locks to test synchronization.

## DSR Synchronization

Follow these guidelines when performing a DSR download:

- Download the DSR during low-traffic time.
- Download one DSR at a time, waiting for one to finish before downloading the next.
- Download DSRs in order of largest to smallest, in terms of number of locks and users.

### NOTE

DSRs with large data sets may take a long time to download. Download speeds depend on the number of personnel, credentials, and authorizations.

## Lock Configuration Tool

Refer to the *ASSA ABLOY Lock Configuration Tool User Manual* for instructions on configuring ASSA ABLOY locks.

You must configure the physical locks, or have an integrator configure them, before you can import the lock objects into the DSR object in C•CURE 9000. If you replace a physical lock, you must configure it using the LCT application.

Before configuring an ASSA ABLOY lock, see [Requirements](#).

## Configuring ASSA ABLOY software objects

This chapter provides configuration information.

In this chapter:

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Components of the ASSA ABLOY integration .....                                 | 44 |
| Privileges for access to ASSA ABLOY objects .....                              | 45 |
| Configuring ASSA ABLOY software objects .....                                  | 45 |
| DSRs .....                                                                     | 46 |
| Downloading the DSR with C•CURE 9000 .....                                     | 49 |
| Displaying DSR status in the Monitoring Station .....                          | 50 |
| Configuring an ASSA ABLOY reader .....                                         | 52 |
| Deleting a reader .....                                                        | 57 |
| Configuring holidays for ASSA ABLOY readers .....                              | 58 |
| MagCard fields .....                                                           | 58 |
| Configuring an ASSA ABLOY door .....                                           | 61 |
| Manual actions for ASSA ABLOY doors .....                                      | 65 |
| Clearances and credentials .....                                               | 66 |
| Configuring ASSA ABLOY card formats .....                                      | 69 |
| Configuring the scheduler .....                                                | 70 |
| Configuring Access Mode .....                                                  | 71 |
| Configuring Clearance Mode .....                                               | 72 |
| ASSA ABLOY sites with multiple credentials for a single personnel record ..... | 74 |
| ASSA ABLOY Implementation for Supporting PIV-I and FASC-N Card Formats .....   | 76 |

# Components of the ASSA ABLOY integration

## Server component

The server component of the ASSA ABLOY integration enables communication between C•CURE 9000 and the DSR, and between the DSR and the locksets. After installing the driver, use the **Server Configuration** application to confirm the driver is running.

### Starting the driver service

1. Navigate to the **Server Configuration** application at `C:\Program Files (x86)\Tyco\CrossFire`. Double-click `ACVS.Enterprise.Server.Configuration.exe` to open the application.
2. Click the **Services** tab. Under **Extension Services**, locate **Johnson ControlsASSA ABLOY Driver Service**.
3. If the service is disabled, select the **Enabled** check box and click **Start**.

For more information on starting the driver, see [Starting the driver service](#).

## Client components

The three main client components include the DSR, ASSA ABLOY Reader, and ASSA ABLOY Door. The client components support features such as dynamic views, reports, queries, journal messages, and audit logs for the C•CURE 9000 integration .

Use the C•CURE 9000 GUI to configure the following components:

- Door Service Router
- ASSA ABLOY Reader
- ASSA ABLOY Mag Card Format
- ASSA ABLOY Mag Card Fields
- ASSA ABLOY Door
- ASSA ABLOY Card Format
- ASSA ABLOY Scheduler
- ASSA ABLOY Access Mode
- ASSA ABLOY Clearance Mode

## DSR

The DSR software object represents the Door Service Router software on the server. Use the GUI to configure the DSR. The DSR controls any reader configured to it. The DSR manages all communication between the ASSA ABLOY readers and C•CURE, such as downloading personnel, schedules and clearances, and uploading activity from the readers to C•CURE.

## Doors, readers, and locks

The ASSA ABLOY reader and the ASSA ABLOY door represent an ASSA ABLOY lock in C•CURE. Configure a lock by editing the associated door and reader properties. Every door requires a reader in C•CURE. When you configure a DSR object, for each discovered ASSA ABLOY reader, a door appears in C•CURE.

## Mag Card Fields

Configure readers to recognize magnetic cards if a facility requires it.

## Card format

The integration automatically creates an ASSA ABLOY card format, if possible, when an appropriate format does not already exist. For the ASSA ABLOY integration, it is no longer necessary to have different CHUID formats.

## Contact scheduler

Configure the ASSA ABLOY Scheduler of battery-powered readers to initiate the uploading and downloading of information to and from the DSR.

## Access mode

Configure reader access control activities to align with user-defined schedules.

## Clearance mode

Configure readers to recognize a cardholder with **CommUser**, **DeadBoltOverride**, **DoubleSwipe** or **Passage Mode** clearance.

## Privileges for access to ASSA ABLOY objects

Configure a privilege software object to allow an operator to access software objects in C•CURE. The permissions within a privilege vary, depending on the object.

### NOTE

You must assign an access level to all users.

## Assigning a privilege

Before assigning a privilege, you must configure one in C•CURE. For information on configuring a privilege, refer to the *C•CURE 9000 Software Configuration Guide*.

After configuring a privilege, you can assign the privilege to an operator.

## Configuring ASSA ABLOY software objects

After installing the ASSA ABLOY integration, configure the following software objects in the **Administration Workstation** application in the following order:

1. DSR
2. Readers
3. Doors

After discovering the readers on the DSR, you can edit the readers and display them in the **Dynamic View** of the **Monitoring Station**, or the **Hardware Tree** of the **Administration Workstation**, and open the DSR objects for editing.

## DSRs

Use the DSR software object to configure a communication connection in C•CURE 9000. Ensure the CrossFire Service, Server Component Framework, and the Johnson Controls ASSA ABLOY driver are running before creating a DSR object. See [Starting the driver service](#) for information on starting services.

### Configuring a DSR

Before configuring a DSR object, ensure that one exists. If one does not exist, you must create one.

#### Creating the DSR object

Create a new DSR object, by completing one of the following steps:

- On the C•CURE server, open the **Administration Workstation** application.
  - a. In the left pane, select **Hardware**.
  - b. In the **Hardware Tree**, select the **Company Name** folder.
  - c. In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY DSR**, and click **New**.
- On the C•CURE server, open the **Administration Workstation** application.
  - a. In the left pane, select **Hardware**.
  - b. In the **Hardware Tree**, right-click the **Company Name** folder.
  - c. Select **ASSA ABLOY DSR**, and select **New**.

### Configuring the DSR object

#### Configuring the General tab

Configure the general characteristics of a new DSR, or edit an existing DSR in the **General** tab. You must have a minimum of Edit privileges to configure the DSR. See [Privileges for access to ASSA ABLOY objects](#)

1. On the **ASSA ABLOY DSR** window, click the **General** tab.
2. Enter a name and description for the DSR in the **Name** and **Description** fields. For encrypted communication between the C•CURE server and the DSR, the **Name** field must match the computer name of the DSR, and the C•CURE server must be able to locate the DSR by its name. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.
3. Select the **Enabled** check box to enable the uploading of content from the DSR to the C•CURE 9000 system and the downloading of content from the DSR to the readers.
4. In the **DSR IP Address** field, enter the IPv4 address of the machine where the DSR software is installed. The IP address is only used for unencrypted communication between the C•CURE server and the DSR.

#### NOTE

For unencrypted communication, ensure the DSR has a static IP address. You may need to repeat this step if the DSR has a dynamic IP address.

5. Enter a communication port number in the **Communication Port** field. The default value for this field is 8080. A port number contains a maximum of four numeric characters. When using encryption, enter 8443 for the port number.

- a. Enter the poll period in the **Poll Period (secs)** field. The poll period is the time interval, in seconds, after which the DSR communicates with C•CURE to check for new or updated records to download. The minimum value is 30, and the maximum is 999.
- b. Status and Download Status are read-only fields. Refer to table for information on possible statuses.

**Table 6: Status and Download Status descriptions**

| Field                  | Status                | Description                                                         |
|------------------------|-----------------------|---------------------------------------------------------------------|
| <b>Status</b>          | <b>Unknown</b>        | Failed initial connection to the DSR for the first time.            |
|                        | <b>Online</b>         | Normal communication between the DSR and C•CURE 9000                |
|                        | <b>CommFail</b>       | Lost connection to the DSR.                                         |
| <b>Download Status</b> | <b>Unknown</b>        | No communication to the DSR, or the DSR driver is not running.      |
|                        | <b>In Progress</b>    | Data is downloading from C•CURE 9000 to the DSR.                    |
|                        | <b>Complete</b>       | Download is complete.                                               |
|                        | <b>Error</b>          | Download rejected by DSR for any invalid configuration information. |
|                        | <b>Critical Error</b> | A timeout occurred.                                                 |

If a DSR response takes longer than the response timeout value, a web service timeout occurs, which results in a **Critical Error**. To define the response timeout, configure the **ASSA ABLOY Response Timeout** system variable in C•CURE. The default value is 60 seconds. You can set response timeout to any value between 15 and 120 seconds. See [ASSA ABLOY system variables](#) for more information on ASSA ABLOY specific system variables.

Refer to the *C•CURE 9000 System Maintenance Guide* for general information on configuring system variables.



The **Monitoring Station** logs and displays errors in the **Journal**. In the event of a **Critical Error**, contact your integrator immediately.

## Configuring the Triggers tab

Configure triggers for each DSR to activate after defined events occur. You can configure events to send an email to a C•CURE Administrator or IT Administrator. You can also configure event triggers to require operator acknowledgment, and outline actions the operator must take after an event occurs. For more information on configuring triggers, refer to the *C•CURE 9000 Software Configuration Guide*.

1. Click the **Triggers** tab.
2. In the **Triggers** area, click **Add**.
3. Select the **Property** field. Click the ellipsis, and select a property option.
4. Select the **Value** field. Select an option from the list.
5. Select the **Action** field. Select **Activate Event**. A new **Event** field appears.
6. Click the ellipsis to the right of the **Event** field to select an existing action, or select **New** from the **Event** list to create a custom action.

## Configuring the State images tab

The **State images** tab displays the icons that C•CURE 9000 uses to indicate the DSR states in the **Monitoring Station**. Edit the icons by completing one of the following:

- Changing an icon to a custom image.
  - a. Click the **State images** tab.
  - b. In the **State images** table, double-click an image in the table.
  - c. Browse your files for a new image.
  - d. Select the replacement image, and click **Open**.
  - e. Click **Save and Close**.
- Restoring a default icon image.
  - a. Click the **State images** tab.
  - b. In the **State images** table, right-click an image in the table, and select **Restore Default**.
  - c. Click **Save and Close**.

## Verifying the Apache services and the DSR are running

- To verify that the Apache services are running on the DSR, navigate to <http://localhost:8080/>
- To verify that the DSR is running on the DSR, navigate to <http://localhost:8080/dsr>
- From the C•CURE server, navigate to <http://<DSRIP>:8080/dsr> where <DSRIP> is the IP address of the DSR.

## Viewing download error information

Use the **Windows Event Viewer** to find error details that may occur during downloads from C•CURE to the DSR or from the DSR to the readers. If a DSR is invalid, and unable to download data from C•CURE, ensure that the DSR is configured correctly and enabled. See [DSRs](#).

You can configure events to send an email to an administrator if a critical error occurs. For details on configuring events, refer to the *C•CURE 9000 Software and Configuration Guide*.

## Viewing information in the Windows Event Viewer

1. On the C•CURE host, open **Run** with the Windows+R hotkeys.
2. In the text field, type `compmgmt.msc`. Press Enter or click **OK**.
3. In the left pane, in **System Tools**, expand **Event Viewer**.
4. Expand **Window Logs**, and select **Application**.
5. In the upper-center pane, select an **Error**, **Information**, or **Warning** event for more details. Details of the event appear in the lower-center pane.

## Deleting a DSR

Deleting a DSR object deletes the locks, schedules, personnel, and other data from that DSR, and remove all associated ASSA ABLOY readers and doors from the C•CURE database. To delete a DSR object, you must have the correct privilege to do so. See [Privileges for access to ASSA ABLOY objects](#) for more information on privileges.



You cannot undo a DSR object delete.

### Deleting a DSR

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, expand the **Company Name** folder.
4. Double-click the DSR you want to delete to open the DSR properties. Clear the **Enabled** check box.
5. Click **Save and Close**.
6. Right-click the **DSR** you want to delete, and select **Delete**.
7. Click **Yes** to confirm deletion of the DSR.
8. Click **OK**.

## Downloading the DSR with C•CURE 9000

The DSR automatically downloads information from C•CURE 9000. However, you can manually download information by completing the following procedure.

### Manually downloading the DSR

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, expand the **Company Name** folder.
4. Right-click the DSR object, and select **Download Door Service Router**.
5. **Optional:** Select the **Delete All Provisioning Data** check box. This restores the DSR to a clean state before downloading provisioning data. This also restores all missing locks back into the DSR, as long as their ASSA ABLOY reader objects are enabled. This is the only way to restore missing locks to the DSR from the C•CURE 9000 system.



Selecting the **Delete All Provisioning Data** check box may render doors inaccessible during download. Perform this action during low traffic hours to limit impact.

6. **Optional:** Select the **Download Active Door Locked Causes** check box. This reissues the door's highest priority cause that was added with a date, time, and a priority. If the only thing in the cause list is the default state, then nothing happens.
7. **Optional:** Select the **Default Door Locked Causes** check box. This reissues the door's default lock causes if the cause list's only entry is the default state.

## NOTE

Selecting the **Download Default Door Locked Causes** check box automatically selects the **Download Active Door Locked Causes** check box. This ensures that all doors get their current top cause command sent to them.

8. Click **OK**.

## NOTE

Download information only displays in the **Journal** after a full download. Individual configuration changes do not display in the **Journal**; to view this information, open the **Server Configuration** application, select the **Diagnostics** tab, and select the appropriate **Switch Filter** check box.

## Displaying DSR status in the Monitoring Station

The **Monitoring Station** does not natively display DSR objects. However, you can view DSR communication status, and the DSR download status, in a dynamic view and in the reader configuration screens.

### Creating a dynamic view for DSRs

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Data Views**. In the upper-left pane, from the **Data Views** list, select **Dynamic View**, and click **New**.
3. Enter a name and description of the dynamic view in the appropriate fields.
4. Click the ellipsis to the right of the **View type** field, and select **ASSA ABLOY DSR**.
5. Configure the check boxes to your requirements.
6. Click **Add**.
7. Select the **Column Property** field. Click the ellipsis, and select **Status** to display the communication status of the DSR.
8. Configure the remaining fields to your requirements.
9. **Optional:** Repeat steps 6 to 8 for any other properties for your dynamic view.
10. Click **Save and Close**.

### Creating a dynamic view for readers

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Data Views**. In the upper-left pane, from the **Data Views** list, select **Dynamic View**, and click **New**.
3. Enter a name and description of the dynamic view in the appropriate fields.
4. Click the ellipsis to the right of the **View type** field, and select **ASSA ABLOY Reader**.
5. Leave the **Query** field blank.
6. Configure the check boxes to your requirements.
7. Click **Add**.

8. Select the **Column Property** field. An ellipsis button appears to the right of the field. Click the ellipsis, and select a property as required.
9. Configure the remaining fields to your requirements.
10. **Optional:** Repeat steps 7 to 9 for any other properties for your dynamic view.
11. Click **Save and Close**.

### Creating a layout

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Data Views**. In the upper-left pane, from the **Data Views** list, select **Application Layout**, and click **New**.
3. Enter a name and description of the dynamic view in the appropriate fields.
4. Click the ellipsis to the right of the **View type** field, and select **ASSA ABLOY Reader**.
5. In the **View Preferences** area, click **X** on the smaller panes, to the left and right, keeping the two large panes in the center.
6. Drag the **Object Viewer** icon into the upper pane.
7. Click the ellipsis to the right of the **Type** field, and select **Dynamic View**.
8. Click the ellipsis to the right of the **Object** field, and select your custom DSR dynamic view. See [Creating a dynamic view for DSRs](#)
9. Click **Save and Close**.
10. Drag the **Object Viewer** icon into the lower pane.
11. Click the ellipsis to the right of the **Type** field, and select **Dynamic View**.
12. Click the ellipsis to the right of the **Object** field, and select your custom reader dynamic view. See [Creating a dynamic view for readers](#)
13. Click **Save and Close**.
14. Click **Save and Close**.

### Assigning a layout to an operator

You can now assign the custom layout to an operator.

### Assigning a layout to an operator

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Configuration**. In the upper-left pane, from the **Configuration** list, select **Operator**, and click the green arrow.
3. Select an operator from the table, and double-click to open the **Operator** window.
4. Select the **Layout** tab, and click **Add**.
5. Select the custom layout that you created in [Creating a layout](#), and click **OK**.
6. Click **Save and Close**.

7. Restart the operator's **Monitoring Station** to display the new layout.

## Checking DSR and reader statuses

After creating a custom layout, you can use it to view DSR and reader status'.

### Checking statuses in the Administration Station

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Data Views**. From the **Data Views** list, select **Application Layout**, and click the green arrow.
3. Right-click your custom layout and select **View**.
4. Check the DSR and reader status'.

### Checking statuses in the Monitoring Station

After assigning the custom layout and restarting the **Monitoring Station**, the new layout displays automatically in that operator's **Monitoring Station**.

## Configuring an ASSA ABLOY reader

Before configuring a reader, you must use the Discover Readers option and it will import the locks from the DSR server into C•CURE. Enabled readers in C•CURE confirm automatically at the next possible opportunity. After adding and confirming a reader, you can configure it in C•CURE.

### Discovering a reader

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, expand the **Company Name** folder.
4. Right-click the DSR that you configured in [Configuring the DSR object](#), and select **Discover Readers**.

An error message appears after 30 seconds if a DSR cannot connect to a specified IP Address. Ensure the IP address is correct for the DSR server, and the **Enabled** check box is selected. When the information is confirmed, discover the readers again. For details on configuring the DSR, see [DSRs](#).

#### NOTE

- Selecting **Discover Readers** automatically creates and assigns a door to each new discovered reader. You must manually assign any preexisting readers in the system to doors.
- If required, add **Discovery Status** and **Last Discovery Status Time** columns to the DSR dynamic view.
- Attempting to enable more readers than your license allows results in readers reverting to a disabled status.

### Configuring the General tab

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, expand the folder containing the DSR.
4. Expand the DSR which contains the reader to configure.

5. Right-click the reader and select **Edit**.
6. Enter a name and description for the reader in the **Name** and **Description** fields. Ensure that the reader name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.

## NOTE

Changing any setting in a battery-powered reader requires the reader to come online before settings can change in the DSR. See [Performing a comm session on a reader](#).

Use the general tab to configure the reader. Not all configuration options are available for each reader. See the following tables for reader configuration information. These tables list what options are available for each reader type.

**Table 7: Access Point Information configuration**

| Access point type | Field or check box                  | Description                                                                                                                                                                                                                                                                                               | Configurable |
|-------------------|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| All               | <b>Reader Type</b>                  | The reader lock type.                                                                                                                                                                                                                                                                                     | Read-only    |
|                   | <b>AccessPoint Type</b>             | The reader power type.                                                                                                                                                                                                                                                                                    |              |
|                   | <b>Serial Number</b>                | A 16-character reader serial number.                                                                                                                                                                                                                                                                      |              |
|                   | <b>Firmware Version</b>             | The firmware version of the reader.                                                                                                                                                                                                                                                                       |              |
|                   | <b>Confirmed</b>                    | Automatically selected after confirming a reader.                                                                                                                                                                                                                                                         |              |
|                   | <b>Online</b>                       | Automatically selected when the reader is online, or cleared when the reader is offline.                                                                                                                                                                                                                  |              |
|                   | <b>Firmware Tampered</b>            | Automatically selected if the reader is tampered with. If selected, the DSR downloads all data to the lock.                                                                                                                                                                                               |              |
| All               | <b>Journal Online/Sync Messages</b> | Select the check box to record and sync reader messages with the DSR. This setting is on by default.                                                                                                                                                                                                      | Yes          |
|                   | <b>Awake Time (seconds)</b>         | Enter a value between 22 and 2550. Awake time is the time a reader remains active for data downloads. For battery-powered readers, avoid long awake times, because it affects the battery life.                                                                                                           |              |
|                   | <b>PIN Required When Defined</b>    | Select the check box to require all personnel who have a PIN defined to enter it at a keypad reader after presenting the credential. If not selected, personnel do not have to enter a PIN. At readers that do not have a keypad there is never a requirement to enter a PIN, regardless of this setting. |              |
|                   | <b>AES Encryption Key</b>           | Enter an encryption key.                                                                                                                                                                                                                                                                                  |              |
| Battery-powered   | <b>Low Battery</b>                  | Select the check box to send a low battery event message to the <b>Monitoring Station</b> when batteries need changing.                                                                                                                                                                                   |              |

**Table 8: Contact Scheduler configuration**

| Access point type | Field                      | Description                                                                                                                                                                                                             | Configurable |
|-------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Battery-powered   | <b>AssaAbloy Scheduler</b> | Click the ellipsis to the right of the field to select a scheduler. <b>CommUser</b> is the default scheduler. You can configure additional scheduler objects in C•CURE. See <a href="#">Configuring the scheduler</a> . | Yes          |

**Table 9: MagField Settings configuration**

| Reader type          | Field                      | Description                                                                                                                             | Configurable |
|----------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Magnetic card reader | <b>AssaAbloy MagFields</b> | Click the ellipsis to the right of the field to select an option. If you do not select an option, the reader uses the default settings. | Yes          |

**Table 10: Visible/Audible Settings configuration**

| Access point type | Field or check box        | Description                                                                                                                            | Configurable |
|-------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------|
| All               | <b>Visible Feedback</b>   | Select the check box to enable visible feedback on the lock. This applies to key presses on the lock. This setting is on by default.   | Yes          |
|                   | <b>Visible Indicators</b> | Select the check box to enable visible indicators on the lock. This applies to card swipes at the lock. This setting is on by default. |              |
|                   | <b>Audible Feedback</b>   | Select the check box to enable audible feedback on the lock. This applies to key presses on the lock. This setting is on by default.   |              |
|                   | <b>Audible Indicators</b> | Select the check box to enable audible indicators on the lock. This applies to card swipes at the lock. This setting is on by default. |              |

Table 11: Status read-only descriptions

| Access point type | Field                     | Field Value          | Description                                                                                           | Configurable |
|-------------------|---------------------------|----------------------|-------------------------------------------------------------------------------------------------------|--------------|
| All               | <b>Sync Status</b>        | <b>Out of Sync</b>   | There was an error sending data from DSR to the lock. Ensure that the reader is configured correctly. | Read-only    |
|                   |                           | <b>Pending</b>       | The DSR is currently downloading data.                                                                |              |
|                   |                           | <b>Synchronized</b>  | The lock is operating normally.                                                                       |              |
|                   |                           | <b>Unknown</b>       | The lock has not communicated its status to the DSR.                                                  |              |
|                   | <b>Last Contact Time</b>  | <b>Time stamp</b>    | The time stamp of the last communication between the DSR and the reader.                              |              |
| Battery powered   | <b>Battery Level</b>      | <b>Voltage</b>       | The battery voltage level of the reader.                                                              |              |
|                   | <b>Battery Status</b>     | <b>Unknown</b>       | The battery level is unknown                                                                          |              |
|                   |                           | <b>Low</b>           | The battery level is low                                                                              |              |
|                   |                           | <b>Normal</b>        | The battery level is normal                                                                           |              |
|                   | <b>Battery Percentage</b> | <b>Battery Image</b> | The graphic displays current battery percentage of the reader batteries. Change batteries below 20%.  |              |

Configure triggers for each reader to activate after defined events occur. You can configure events to send an email to a C•CURE Administrator or IT Administrator. You can also configure event triggers to require operator acknowledgment, and outline actions the operator must take after an event occurs. For more information on configuring triggers, refer to the *C•CURE 9000 Software Configuration Guide*.

### Configuring a trigger

1. Click the **Triggers** tab.
2. In the **Triggers** area, click **Add**.
3. Select the **Property** field. Click the ellipsis, and select a property option.
4. Select the **Value** field. Select an option from the list.
5. Select the **Action** field. Select **Activate Event**. A new **Event** field appears.
6. Click the ellipsis to the right of the **Event** field to select an existing action, or select **New** from the **Event** list to create a custom action.
  - Select the **Details** field to view action configuration information.
7. Select the **Schedule** field, and click the arrow to display a list of pre-configured schedules. Select a schedule to associate with the trigger.

The **Groups** tab displays the groups of which the reader is a member. You can create groups and organize readers and other objects into those groups from the **Configuration** pane of the **Administration Workstation**. You can add an object to a group from the **Monitoring Station**.

### Creating a Group

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Configuration**. In the upper-left pane, from the **Configuration** list, select **Group**, and click **New**.
3. Enter a name and description for the group in the **Name** and **Description** fields.
4. Click the ellipsis to the right of the **Group Type** field, and select a group type.
5. In the **Objects in Group** area, click **Add**.
6. Select the objects to add to the group, and click **OK**.
7. Click **Save and Close**.

### Adding a reader to a group to display in a dynamic view

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**. In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Reader**, and click the green arrow.
3. Right-click a reader, and select **Add to Group**.
4. Select a group, and click **OK**.

The **State images** tab displays the icons that C•CURE 9000 uses to indicate the reader states in the **Monitoring Station**.

### Configuring the state images

Edit the icons by completing one of the following:

- Changing an icon to a custom image.
  - a. Click the **State images** tab.
  - b. In the **State images** table, double-click an image in the table.
  - c. Browse your files for a new image.
  - d. Select the replacement image, and click **Open**.
  - e. Click **Save and Close**.
- Restoring a default icon image.
  - a. Click the **State images** tab.
  - b. In the **State images** table, right-click an image in the table, and select **Restore Default**.
  - c. Click **Save and Close**.

## Performing a comm session on a reader

Ensure comm sessions occur regularly. ASSA ABLOY locks hold a maximum of 10,000 events offline. When a lock comes online, stored events upload to the DSR. If more than the 10,000 events occur offline, the lock only uploads the most recent 10,000 events to the DSR.

Comm sessions can occur in one of the following ways:

- A user enters the comm session PIN at the reader. The PIN is 3232\* on standard readers, or #323232 on Mag readers.
  - Battery-powered readers have a CommUser by default.
  - The PIN does not function after a custom CommUser clearance downloads from the DSR. To re-enable the PIN, you must delete the custom CommUser from the reader.
- A user swipes a card with CommUser clearance.
  - Swiping a card with CommUser clearance wakes the reader, but denies door access to the card holder.
- A scheduler activates the comm session.
- A comm session can be initialized by presenting an invalid card to a lock.

To perform a comm session on a reader through a schedule or card swipe, you must configure the CommUser scheduler and clearance. See [Configuring the scheduler](#) and [Configuring Clearance Mode](#).

## Replacing a reader

If you need to replace a reader in the system, complete the following procedure:

### Replacing a reader

1. Install the replacement reader. Refer to your reader installation guide.
2. Configure the new reader using the LCT. Refer to the *ASSA ABLOY Lock Configuration Tool User Manual*.
3. **Optional:** If it is a battery-powered reader, you must wake the new reader.
4. Discover the new reader and enable it. This automatically confirms the readers and creates a new door. See [Discovering a reader](#).
5. Delete the new door associated with the reader.
6. Open the old reader configuration settings, and clear the **Enabled** check box.
7. Assign the new reader to the old door. This prevents users needing to configure a new door for the replacement reader.
8. Delete the old reader. See [Deleting a reader](#).
9. Rename the new reader, and if it is battery-powered, wake it.

## Deleting a reader

Deleting a reader object from C•CURE does not delete the associated door. Deleting a door does not delete a reader, but does remove all associated clearances in C•CURE for that door.



To prevent data loss, wake battery-powered readers before deleting them. Waking a reader forces it to send stored data to the DSR.

If you need to delete a reader from the system, complete the following procedure:

### Deleting a reader

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**, and complete one of the following steps:
  - In the **Hardware Tree**, expand the **Company Name** folder, the DSR folder and the readers folder.
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Reader**, and click the green arrow.
3. Select the reader to delete. Right-click the reader, and select **Delete**.
4. Click **Yes**.
5. Click **OK**.

## Configuring holidays for ASSA ABLOY readers

Holidays for ASSA ABLOY readers function similarly to holidays for other readers in C•CURE. For information on configuring holidays, refer to the *C•CURE 9000 Software Configuration Guide*.

The ASSA ABLOY integration automatically adjusts the daily schedule, based on whether the day is a regular day or a holiday, up to 6 days in advance.

### NOTE

If the DSR and the C•CURE system do not communicate for more than 5 days, the DSR may have the incorrect information about whether the next day is a regular day or a holiday.

## MagCard fields

While Wiegand Prox formats are described in bits, magnetic formats are described in characters. These characters are represented by five bits each. The first 4 bits represent the character, and the fifth bit represents the lateral parity. All magnetic formats include three extra characters for the Start Sentinel, End Sentinel, and the CRC (Cyclic Redundancy parity Check). The CRC character is parity over the length of the four fields. All card formats must account for these three extra characters.

### NOTE

- Some magnetic cards may have a field separator.
- C•CURE does not support field separators.
- CRC is sometimes referred to as the LRC (Longitudinal Redundancy Check).

If you require encoded magnetic card access for a magnetic card reader, configure the MagCardFields object so that the reader excludes separators during a card read. If you do not configure a MagCardFields object for the ASSA ABLOY reader, the reader uses its default settings. This feature is only supported on magnetic readers.

### NOTE

- By default, an ASSA ABLOY reader supports only one magnetic card format.
- If you require readers to support multiple magnetic card formats, see [Configuring a reader to accept multiple magnetic cards](#).

## Configuring a MagField object for a reader

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, select the **Hardware** folder.
4. Right-click and select **ASSA ABLOY MagCardFields**. Select **New**.
5. Enter a name and description for the MagCardField in the **Name** and **Description** fields. Ensure that the MagCardField name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.

### NOTE

The **Partition** field displays the current partition of the MagCardField object. This field displays only if the C•CURE 9000 system has more than one partition.

6. Configure the fields as required. See [MagCardField configuration options](#).
7. Select the **Enabled** check box.
8. Click **Save and Close**.
9. In the **Hardware Tree**, expand the **Company Name** folder.
10. Expand the DSR which contains the reader to configure.
11. Right-click the reader and select **Edit**.
12. In the **MagField Settings** area, to the right of the **AssaAbloy MagFields** field, click the elipsis.
13. Select the MagField object.
14. Click **Save and Close**.

Table 12: MagCardField configuration options

| Area            | Field                       | Description                                                                                                                                                                                                           |
|-----------------|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Include Fields  | Include Separator (Ex: "=") | Configure the ASSA ABLOY reader to include the separator field while reading encoded magnetic cards.                                                                                                                  |
|                 | Include All Fields          | Configure the ASSA ABLOY reader to include all eight MagFields while reading a magnetic card.                                                                                                                         |
|                 | MagField 1 through 8.       | Configure any combination of individual MagFields.                                                                                                                                                                    |
| Field Positions | Offset Position             | Enter a value, or use the arrows, to configure the <b>Offset Position</b> . This value configures the ASSA ABLOY reader to read a magnetic card from the specified position. The maximum value for this field is 255. |
|                 | Length                      | Enter a value, or use the arrows, to configure the <b>Length</b> . This value configures the ASSA ABLOY reader to read a magnetic card from the specified position. The maximum value for this field is 255.          |

| Area         | Field          | Description                                                                                      |
|--------------|----------------|--------------------------------------------------------------------------------------------------|
| Test Example | MagCard Number | Enter a MagCard number to test a magnetic card. This field can have a maximum of 100 characters. |
|              | Check Result   | Click to test the MagCard Number.                                                                |
|              | Result         | Displays the result of the tested configuration.                                                 |

### Configuring a reader to accept multiple magnetic cards

This section describes the configuration of a reader to accept a 32-character card and a MAG 15 format card.

1. Create a MagFields object and assign it to a reader. See [Configuring a MagField object for a reader](#). Configure the object as required, but with the following specific settings:
  - Select the **MagField 1** check box.
  - In the **Offset Position** field, enter 0.
  - In the **Length** field, enter 16.
2. Create a CHUID format. Refer to the *C•CURE 9000 Personnel Configuration Guide* for details on configuring CHUID formats. Configure the CHUID format as required, but with the following specific settings:
  - In the **CHUID Length** field, type 10.
  - From the **CHUID Format Type** list, select **Card Only**.
3. Create a 32-character card format. Refer to the *C•CURE 9000 Card Formats and Smart Card Keys Guide* for details on configuring card formats. Configure the card format as required, but with the following specific settings:
  - **General** tab
    - From the **CHUID Format** list, select the CHUID format from [Step 2](#).
    - Select the **Magnetic** radio button.
    - In the **Data Length** field, type 19. This represents 16 meaningful characters, and the required control characters.
  - **Format Fields** tab
    - See [Table 13](#) for configuration details.

Table 13: Format Fields configuration

| Field Type         | Start Position | Length | End Position | Values |
|--------------------|----------------|--------|--------------|--------|
| card facility code | 2              | 6      | 7            | 0      |
| card Number        | 8              | 8      | 15           |        |
| Issue code         | 16             | 2      | 17           |        |

4. Repeat [Step 3](#) for users with MAG 15 format cards.

5. Configure the personnel record of a user with a 32-character card format and clearance for the reader. See [Credentials](#). Configure the personnel record as required, but with the following specific settings:
  - From the **CHUID Format** list, select the CHUID format from [Step 2](#).
  - In the **Facility Code** field, type the first 6 digits of the card.
6. Repeat [Step 5](#) for users with MAG 15 format cards.

## Configuring an ASSA ABLOY door

Discovering a reader automatically creates a door in C•CURE. Once the readers or locks are discovered, the application creates the door automatically and assigns the name configured with LCT. See [Configuring an ASSA ABLOY reader](#). Doors display in the **Hardware Tree**, under the associated DSR. Doors use the naming convention `Door - xxxxx`, where `xxxxx` represents the reader name.

### NOTE

You can create the door objects in any folder in the **Hardware Tree**. This document uses the **Company Name** folder as an example.

### Creating an ASSA ABLOY door

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. Complete one of the following steps to create a new door:
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Door**, and click **New**.
  - In the **Hardware Tree**, expand the **Company Name** folder, and right-click the DSR. Select **ASSA ABLOY Door**, and then select **New**.
  - In the **Hardware Tree**, expand the **Company Name** folder, and expand the DSR. Right-click **Doors**, and select **New**.
  - In the **Hardware Tree**, expand the **Company Name** folder, and expand the DSR. Select **Doors**, and click **New** at the top of the **Hardware** pane.

### Configuring the general tab

1. Enter a name and description for the reader in the **Name** and **Description** fields. Ensure that the reader name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.
2. Click the ellipsis to the right of the **Reader** field, and select a reader.
3. In the **Shunt Time (seconds)** field, enter a value between 1 and 255, or use the default value. After granting access, if the door does not close within this time, a **Door Held** status appears in the **Monitoring Station**.
4. In the **Unlock Time (seconds)** field, enter a value between 1 and 255, or use the default value. This value determines how long the lock remains open, after granting access.

### NOTE

After granting access, if the reader is in a **Pending** download state, the door remains open until the download is complete.

5. In the **Alternate Time (seconds)** field, enter a value between 1 and 255, or use the default value. This value determines how long the lock remains open, after granting access to a person with a disability-flagged credential.
6. Select the **Allow Escape Return** check box to enable escape returns.

## NOTE

Escape return allows users to open a door and, by swiping their card, prevent the door from locking again.

7. Select the **Send to Journal** check box to send deadbolt status messages to the journal. This option is on by default.
8. Select the **Send to Monitoring Station** check box to send deadbolt status messages to the **Monitoring Station**. This option is selected by default.
9. Discovering a reader automatically selects the **Alarm Configuration** check boxes. See [Alarm Configuration check boxes](#) for information more information. See the following points of information for configuration options:
  - PoE readers: You cannot clear these check boxes. Generated alarms immediately display in the **Monitoring Station**. To change these settings, you must delete the door, create a new door, assign a reader, and reconfigure the door.
  - Battery-powered readers: You can select or clear these check boxes. Selecting the check boxes for battery-powered readers places a high load on the battery, and lowers the battery life.

## NOTE

Selecting an alarm check box forces readers to wake and report alarms immediately to the DSR. Clearing a check box allows readers to only report an alarm when the reader comes online.

## Modes

You can configure two modes on an ASSA ABLOY door.

### Secured Mode

In **Secured Mode**, closed doors are locked. If an alarm activates, the reader reports the alarm information to the host through the DSR. The reader generates these alarms as they occur, and reports information to the **Journal** and **Monitoring Station**. The housekeeping time interval does not apply to these alarms.

### Passage Mode

In **Passage Mode**, closed doors are unlocked. This mode activates when an access point mode activates or when an operator performs a manual unlock from the **Administration Workstation** or **Monitoring Station**. The reader generates these alarms as they occur, and reports information to the **Journal** and **Monitoring Station**. The housekeeping time interval does not apply to these alarms.

## NOTE

A battery-powered reader does not report an alarm to the **Monitoring Station** if it remains open longer than the shunt time in Passage Mode.

Table 14: Alarm Configuration check boxes

| Mode                          | Status         | Description                       |                                                                                                                       |
|-------------------------------|----------------|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Secured Mode and Passage Mode | Rx Held        | The door handle is held too long. |                                                                                                                       |
| Secured Mode and Passage Mode | Door Ajar/Held | The door is open.                 |                                                                                                                       |
| Secured Mode and Passage Mode | Door Normal    | The door is in a normal state.    |                                                                                                                       |
| Secured Mode only             | Door Forced    | The door was forced.              |                                                                                                                       |
| Secured Mode only             | Access Granted | Access granted at the door.       |                                                                                                                       |
| Secured Mode only             | Access Denied  | Unknown Card                      | Access denied at the door. Unknown card format.                                                                       |
|                               |                | PIN                               | Access denied at the door. Incorrect PIN entry.                                                                       |
|                               |                | Clearance                         | Access denied at the door. The clearance is not authorized for entry.                                                 |
|                               |                | Busy                              | Access denied at the door. The clearancel is authorized for entry, but current lock conditions are preventing access. |

### Editing an existing door

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, expand the **Company Name** folder.
4. Expand the DSR which contains the door to configure.
5. Complete one of the following steps:
  - Select a door, right-click the door, and select **Edit**.
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Door**, and click the green arrow.
    - In the **Dynamic View**, double-click a door to edit.
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Door**, and click the green arrow.
    - In the **Dynamic View**, right-click a door, and select **Edit**.
6. Configure the door, and click **Save and Close**.

### NOTE

The door **Dynamic View** and door **Status List** include a **Clearance Filter Level Status** column. This column does not apply to ASSA ABLOY objects and is not configurable.

Configure triggers for each door to activate after defined events occur. You can configure events to send an email to a C•CURE Administrator or IT Administrator. You can also configure event triggers to require operator acknowledgment,

and outline actions the operator must take after an event occurs. For more information on configuring triggers, refer to the *C•CURE 9000 Software Configuration Guide*.

### Configuring a trigger

1. Click the **Triggers** tab.
2. In the **Triggers** area, click **Add**.
3. Select the **Property** field. Click the ellipsis, and select a property option.
4. Select the **Value** field. Select an option from the list.
5. Select the **Action** field. Select **Activate Event**. A new **Event** field appears.
6. Click the ellipsis to the right of the **Event** field to select an existing action, or select **New** from the **Event** list to create a custom action.
  - Select the **Details** field to view action configuration information.
7. Select the **Schedule** field, and click the arrow to display a list of pre-configured schedules. Select a schedule to associate with the trigger.

The **Groups** tab displays the groups of which the door is a member. You can create groups and organize doors and other objects into those groups from the **Configuration** pane of the **Administration Workstation**. You can add an object to a group from the **Monitoring Station**.

### Creating a group

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Configuration**. In the upper-left pane, from the **Configuration** list, select **Group**, and click **New**.
3. Enter a name and description for the group in the **Name** and **Description** fields.
4. Click the ellipsis to the right of the **Group Type** field, and select a group type.
5. In the **Objects in Group** area, click **Add**.
6. Select the objects to add to the group, and click **OK**.
7. Click **Save and Close**.

### Adding a door to a group to display in a dynamic view

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**. In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Door**, and click the green arrow.
3. Right-click a door, and select **Add to Group**.
4. Select a group, and click **OK**.

The **State images** tab displays the icons that C•CURE 9000 uses to indicate the door states in the **Monitoring Station**.

### Configuring state images

Edit the icons by completing one of the following:

- Changing an icon to a custom image.
  - a. Click the **State images** tab.
  - b. In the **State images** table, double-click an image in the table.
  - c. Browse your files for a new image.
  - d. Select the replacement image, and click **Open**.
  - e. Click **Save and Close**.
- Restoring a default icon image.
  - a. Click the **State images** tab.
  - b. In the **State images** table, right-click an image in the table, and select **Restore Default**.
  - c. Click **Save and Close**.

## Manual actions for ASSA ABLOY doors

Use manual actions to control lock status from within the **Administration Station**. Battery-powered readers do not support manual actions. Battery-powered readers ignore manual action commands. Standard manual actions include: lock, unlock, and momentary unlock.

### NOTE

- Ensure the DSR is online when attempting to perform a manual action. If the DSR is offline, the action fails, and the door remains in its locked or unlocked state.
- Canceling the action reverts the door to its previous state.

You cannot perform manual actions while the driver in the **Server Configuration** application is stopped. After restarting the driver, ensure lock status' are accurate, and that locked and unlocked doors are in the correct state.

### NOTE

Manual actions override an auto-lock schedule on a lock.

After performing a manual action, the following events occur:

- The command sends the manual action to the DSR.
- The action occurs instantly.
- The performed action displays in the **Monitoring Station**.
- In the **Door Status** list, the **Mode Status** column displays the new door status.

### Performing a manual action

1. On the C-CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Door**, and click the green arrow.
4. In the **Dynamic View**, select a door.
5. Right-click the door, and select one of the following manual actions:
  - **Lock**. The **Lock Door** window appears.
  - **Unlock**. The **Unlock Door** window appears.

- **Momentary Unlock.** No screen appears, and the action activates.
6. **Optional:** Configure the **Lock Door** or **Unlock Door** options.
    - a. In the **Start** and **End** fields, enter a start and end time for the action.
    - b. In the **Priority** field, enter a value between 1 and 200. The value you can enter is limited by your operator account.
    - c. **Optional:** In the **Instructions** field, enter instructions that an operator must follow when performing a manual action.

## NOTE

This integration does not support time zones for manual actions.

7. Click **Save and Close**.

## Panic mode

The C•CURE equivalent of a panic mode is **Secure Door**. Use the manual action **Secure Door** to activate the event. You can use other manual actions on secured doors as normal.

Configure the **Secure Door** event by completing the following procedure.

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Configuration**.
3. In the upper-left pane, from the **Configuration** list, select **Event**, and click **New**.
4. Enter a name and description for the reader in the **Name** and **Description** fields. Ensure that the reader name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.
5. Select the **Enabled** check box.
6. Configure the **General** tab settings to align with the facility security requirements.
7. Select the **Action** tab, and click **Add**.
8. Select the **Action** field, and, from the **Action** list, select **Secure Door**.
9. To the right of the **Door** field, click the ellipsis.
10. Select a door.
11. **Optional:** Repeat steps 7 to 10 to add more doors to the event.
12. Click **Save and Close**.

## Clearances and credentials

### Clearances

You can assign a maximum of 9,999 credentials to an ASSA ABLOY lock clearance, including the default **CommUser** credential.

## NOTE

Legacy ASSA ABLOY locks cannot hold 9,999 credentials. Contact your ASSA ABLOY representative for more information on legacy lock capacities.

Excess credentials do not register in the DSR, and attempting to assign more credentials to a clearance causes an error. View logs of excess credential creation attempts in the **Journal**, as well as in the **Windows Event Viewer**. If you require more than 9,999 credentials for a clearance, you must create more clearances and divide credentials among them.

Each clearance includes a schedule and a door. There is no limit to the number of clearances, only to the number of credentials that are using the same clearance.

## NOTE

The ASSA ABLOY integration does not support **Clearance Filter Level** functionality.

For information on configuring clearances, refer to the *C•CURE 9000 Personnel Configuration Guide*.



Before running the integration driver and configuring a clearance, ensure all personnel credentials contain a valid card number. Attempting to use an invalid card number, for example 0, results in an out-of-sync error from the DSR. Configuring a valid card number and reloading provisioning data removes this error.

## Credentials

Add and configure access credentials for a person on their **Personnel** record in the **Administration Workstation**. For each credential, you can specify the credential type, format, expiration date, and current status.

## NOTE

- The ASSA ABLOY integration does not support PIN-only access.
- The ASSA ABLOY integration removes credentials marked as inactive, disabled, lost or stolen from the DSR.

To add a credential, complete the following procedure:

### Adding a credential

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Personnel**.
3. Complete one of the following steps:
  - In the upper-left pane, from the **Personnel** list, select **Personnel**, and click **New**.
    - Configure the **General** tab. Refer to the *C•CURE 9000 Personnel Configuration Guide*.
  - In the upper-left pane, from the **Personnel** list, select **Personnel**, and click the green arrow.
    - Select an existing personnel record, right-click and select **Edit**.
4. Select the **Credentials** tab.
5. Click **Add Card Access**. This button is unavailable if the maximum number of credentials is already configured.

## NOTE

- Define the maximum number of credentials for an individual in the **Personnel System Variable**. Refer to the *C•CURE 9000 System Maintenance Guide*.
- The maximum number of credentials allowable for personnel is five.

6. In the **Card Number** field, enter a card number.

7. **Optional:** To change the default CHUID format, select the **CHUID Format** field, click the ellipsis, and select a format. For information on configuring card formats, refer to the *C•CURE 9000 Card Formats and Smart Card Keys Guide*.
8. Configure the **Standard Fields**, **Card Status**, and **Extended Fields** as required. Refer to the *C•CURE 9000 Personnel Configuration Guide* for more information on configuring credentials.
9. Click **Save and Close**.

**Table 15:** Unsupported configuration options

| Field or check box    | Description   |
|-----------------------|---------------|
| <b>Card Status</b>    |               |
| <b>Temporary</b>      | Not supported |
| <b>PIN Credential</b> |               |
| <b>PIN</b>            | Not supported |
| <b>Auto Generate</b>  | Not Supported |

## Removing a credential

To remove a credential, complete the following procedure:

### Removing a credential from a personnel record

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Personnel**.
3. In the upper-left pane, from the **Personnel** list, select **Personnel**, and click the green arrow.
4. Select a personnel record, right-click and select **Edit**.
5. Select the **Credentials** tab.
6. Click **Remove**.
7. Click **Yes**.
8. Click **Save and Close**.

## Validating a CHUID

When saving a personnel record, C•CURE checks and confirms if the CHUID for each credential is unique in the system. Non-unique credentials display an error, and the save fails. If there is an error, adjust the CHUID fields to ensure the credential is unique.

Before saving, you can confirm if the CHUID is unique by completing a CHUID validation.

### NOTE

- For information on configuring CHUID formats, refer to the *C•CURE 9000 Personnel Configuration Guide*.
- For information on configuring card formats, refer to the *C•CURE 9000 Card Formats and Smart Card Keys User Guide*.

## Validating a CHUID

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Personnel**.
3. In the upper-left pane, from the **Personnel** list, select **Personnel**, and click the green arrow.
4. Select a personnel record, right-click and select **Edit**.
5. Select the **Credentials** tab.
6. Click **Validate CHUID Uniqueness**.
  - If the CHUID is unique, a message appears stating that it is valid.
  - If the CHUID is not unique, an error message appears stating that it is not unique. Adjust the value and try again.
7. Click **OK**.
8. Click **Save and Close**.

## Configuring ASSA ABLOY card formats

The integration automatically creates an ASSA ABLOY card format, if possible, when an appropriate format does not already exist. You must manually create a card format to use with credentials that have the CHUID format **card only**.

### NOTE

- For information on configuring CHUID formats, refer to the *C•CURE 9000 Personnel Configuration Guide*.
- For information on configuring card formats, refer to the *C•CURE 9000 Card Formats and Smart Card Keys User Guide*.

## Creating an ASSA ABLOY card format

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. Complete one of the following steps to create a new card format:
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Card Format**, and click **New**.
  - In the **Hardware Tree**, right-click the **ASSA ABLOY Card Format** folder, if it is present, and select **New**.

### NOTE

- In an enterprise system, ASSA ABLOY card formats need to be defined locally, i.e. for each SAS.
- In an enterprise system, card formats need to be defined locally, i.e. for each SAS.
- In an enterprise system, CHUID formats need to be defined globally.

## Configuring the general tab

1. Enter a name and description for the reader in the **Name** and **Description** fields. Ensure that the reader name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.
2. Click the ellipsis to the right of the **CHUID Format** field, and select a format.
3. Click the ellipsis to the right of the **Card Format** field, and select a format.
4. Click **Save and Close**.

# Configuring the scheduler

Use schedulers to configure access schedules for ASSA ABLOY doors with various properties. There are three types of schedule configurations available. A lock attempt to communicate with the DSR when the lock comes online, as scheduled. If a lock is unable to communicate with the DSR, the lock returns to the sleep period and waits until it comes online again to attempt communication.

## Types of schedule

- Simple
- Day of the week
- CommUser

Battery-powered locks default scheduler is CommUser. CommUser is unavailable to PoE locks.

### NOTE

- The ASSA ABLOY integration does not support day of the month communication.
- You can configure a maximum of 32 time intervals on a lock.

## Creating a scheduler

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, select the top-level **Hardware** folder.
4. Complete one of the following steps:
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY Scheduler**, and click **New**.
  - Right-click the **Hardware** folder, select **ASSA ABLOY Scheduler**, and select **New**.
5. Enter a name and description for the scheduler in the **Name** and **Description** fields. Ensure that the scheduler name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.
6. In the **Contact Scheduler** area, select the **Schedule Type** list, select the required option.
7. Configure the scheduler. See [Scheduler configuration fields](#).
8. Click **Save and Close**.

Table 16: Scheduler configuration fields

| Scheduler | Field or check box     | Description                                                                                                                                                                                                                                       |
|-----------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Simple    | Sleep Period (minutes) | Enter a value in the <b>Sleep Period (minutes)</b> field to define the length of time between lock and DSR communications. The minimum value of this field is 1. The maximum value of this field is 65535. The default value of this field is 60. |

| Scheduler | Field or check box | Description                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DayOfWeek | Day(s) of the Week | Select the <b>Day(s) of the Week</b> check boxes to define what days of the week the lock communicates with the DSR.                                                                                                                                                                                                                                                                                                          |
|           | Times of the Day   | <ul style="list-style-type: none"> <li>Select a <b>Contact Time</b> check box to define what time of day communications with the DSR occur. You can define between one and four communication times. Each contact time applies to each selected day of the week.</li> <li>Either select the hour and minutes, and type over them, or use the up and down arrows to the right of the field to adjust contact times.</li> </ul> |
| CommUser  | None               | <ul style="list-style-type: none"> <li>The <b>CommUser</b> scheduler allows for the association of a clearance with the reader.</li> <li>Using this type of scheduler forces readers to communicate with the DSR when a person whose credential has a CommUser clearance swipes a card, or enters a CommUser PIN.</li> </ul>                                                                                                  |

## Configuring Access Mode

After configuration, an Access Mode downloads to ASSA ABLOY readers. Access Mode enables readers to grant access to cardholders on the configured schedule. Access mode schedules activate linearly, and regardless of door lock status.

### NOTE

You cannot assign a different Access Mode to an unlocked, active reader unless the Access Mode expires, or is deleted. You can assign multiple Access Modes for different time intervals, but readers perform actions based on the priority order.

## Types of access

### ■ First Person Through

- First Person Through** (FPT) requires a time schedule to define when the access type is active.
- Second in priority order.
- If an Access Mode downloads to a door with **Access Point Type** set to **First Person Through**, the door unlocks and remains unlocked after the first valid card swipe during an active schedule.
- Any users with clearance to access a reader configured to FPT, within the schedule, can use the FPT action.
- This option is only available on Prox and iClass readers.

### ■ AutoUnlock

- AutoUnlock** requires a time schedule to define when the access type is active.
- First in priority order.
- If an Access Mode downloads to a reader with **Access Point Type** set to **AutoUnlock**, the door unlocks and remains unlocked after the schedule activates.
- After the schedule expires, the door locks.
- This option is only available on Mag, Prox, and iClass readers.

### NOTE

The **Monitoring Station** only reports a door as locked or unlocked. It cannot distinguish access types.

## Configuring Access Mode

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, select the top-level **Hardware** folder.
4. Complete one of the following steps:
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY AccessMode**, and click **New**.
  - Right-click the **Hardware** folder, select **ASSA ABLOY AccessMode**, and select **New**.
5. Enter a name and description for the access mode in the **Name** and **Description** fields. Ensure that the name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.
6. In the **Configure AccessMode** area, select the **AccessModeType** list.
7. Complete one of the following steps:
  - Select **First Person Through**.
  - Select **AutoUnlock**.
8. To the right of the **ASSA ABLOY Door** field, click the ellipsis.
9. Select a door.
10. To the right of the **Schedule** field, click the ellipsis.
11. Select a schedule.
12. Click **Save and Close**.



Ensure lock and unlock events and schedules do not cause conflicts. Conflicts may result in doors locking or unlocking outside of their intended schedules.

## Configuring Clearance Mode

After configuration, a Clearance Mode enables readers to come online when a user presents a card, with valid access to the reader. When a reader is online, it can communicate with the DSR.

### Types of clearance

#### ■ CommUser

- Swiping a card, with this clearance, wakes the reader and forces it to communicate with the DSR.
- This is the default setting for battery-powered readers.
- You cannot assign CommUser clearance to personnel with non ASSA ABLOY clearances. Attempting to assign a CommUser clearance to these personnel displays an error message in the **Monitoring Station**. Conflicting clearances do not download to the DSR.

#### NOTE

A person can only have one CommUser clearance.

## ■ DeadBoltOverride

- Swiping a card, with this clearance, overrides a deadbolt lock and opens the door.
- You cannot assign a DeadBoltOverride clearance to personnel with CommUser clearance. Attempting to assign a DeadBoltOverride clearance to these personnel displays an error message in the **Monitoring Station**. Conflicting clearances do not download to the DSR.
- Assigning a DeadBoltOverride clearance to personnel supersedes any non ASSA ABLOY clearances.

## ■ DoubleSwipe/ Passage Mode

The DSR and the lock controller determine whether the lock uses **Double Swipe Mode** or **Passage Mode**.

### NOTE

- v.s1 and v.s2 locks with Hx firmware support **Double Swipe** functionality.
- Locks with a configured PERSONA tag in their serial number support **Double Swipe** functionality.
- v.s1, v.s2 locks with Sx firmware support **Passage Mode** functionality.
- Locks without a configured PERSONA tag in their serial number support **Passage Mode** functionality.

- Double Swipe
  - Double swipe is a user-level authentication feature, enabled in C•CURE 9000. Use this feature to configure a doors to enable readers to interpret a double card swipe as a method of locking and unlocking a door.
  - As with other security objects in the system, events, manual actions, or schedules with higher priorities can override a double swipe.
  - When a lock wakes, it sends double swipe lock and unlock data to the journal.
  - Any users associated with this clearance, can use the double swipe action.
  - For more information on configuring the double swipe feature, refer to the *C•CURE 9000 Hardware Configuration Guide*.
- Passage Mode
  - Passage Mode is not schedule specific. If a lock has passage mode active, users that have passage mode access, can access the lock whenever it is available to them.
  - When a reader wakes, if passage mode is active, it sends a message to the journal.

### NOTE

The **Monitoring Station** only reports a door as locked or unlocked. It cannot distinguish access types.

## Configuring clearance mode

1. On the C•CURE server, open the **Administration Workstation** application.
2. In the left pane, select **Hardware**.
3. In the **Hardware Tree**, select the top-level **Hardware** folder.
4. Complete one of the following steps:
  - In the upper-left pane, from the **Hardware** list, select **ASSA ABLOY ClearanceMode**, and click **New**.
  - Right-click the **Hardware** folder, select **ASSA ABLOY ClearanceMode**, and select **New**.
5. Enter a name and description for the clearance mode in the **Name** and **Description** fields. Ensure that the name is unique. The **Name** field has a 100-character limit. The **Description** field has a 500-character limit.

6. In the **Configure ClearanceMode** area, select the **ClearanceMode Type** list.
7. Complete one of the following steps:
  - Select **CommUser**.
  - Select **DeadBoltOverride**.
  - Select **DoubleSwipe/ Passage Mode**.
8. To the right of the **Clearance** field, click the ellipsis.
9. Select a clearance.
10. Click **Save and Close**.

## ASSA ABLOY sites with multiple credentials for a single personnel record

### Specific case instructions

The following instructions are for the very specific case of ASSA ABLOY sites in which one personnel record has more than one credential, but not all of their credentials are supposed to be downloaded to the ASSA ABLOY lock.

#### NOTE

There is a distinction between card format and ASSA ABLOY card format.

### Background

The ASSA ABLOY integration can access all credentials. The integration only attempts to download all credentials that have access rights to an ASSA ABLOY lock, for example through a clearance or a custom clearance. Access rights to the lock are defined for a personnel record. This means that access rights apply equally to each of the credentials on a personnel record. For a credential to download to an ASSA ABLOY lock, an ASSA ABLOY card format must exist to define which card format the driver uses, based on the CHUID format of the credential. If the ASSA ABLOY card format does not exist, the affected credentials do not download. This can be used as an advantage, if a personnel record has more than one credential, but not all of their credentials are supposed to be downloaded to the ASSA ABLOY lock.

### Problem

Under very specific conditions, the ASSA ABLOY driver automatically creates an ASSA ABLOY card format. This may cause undesired credentials to be downloaded to the lock, taking up valuable space and possibly causing the lock to go out of sync if the card format has information that the lock cannot handle.

### Solution

#### NOTE

Deleting the ASSA ABLOY card format will not solve the problem, because it gets recreated.

To solve the issue, create conditions in which the ASSA ABLOY driver does not automatically recreate the ASSA ABLOY card format. An ASSA ABLOY card format is only automatically created if the CHUID format of a credential is exclusively referenced by one single card format. Create another card format that references the CHUID format to solve this. That card format exists solely to make the system ambiguous as to which card format the ASSA ABLOY driver needs to use

for the referenced CHUID format. Once you create the new format, delete the undesired ASSA ABLOY card format and it will not be recreated. Select a name of the new card format that informs the user why the format exists and that they must not delete it.

# ASSA ABLOY Implementation for Supporting PIV-I and FASC-N Card Formats

## NOTE

Make sure that the site uses locks which are capable of reading PIV-I or FASC-N before trying to configure the PIV-I or FASC-N card formats in C•CURE, as all ASSA ABLOY IP locks cannot read PIV-I or FASC-N cards.

## Description

The latest set of code changes to the ASSA ABLOY Integration supports the following two new card formats:

- 128-bit PIV-I
- 200-bit FASC-N

## NOTE

Refer the document **PIVCLASS FIPS-201 READER OPERATION AND OUTPUT SELECTIONS Application Note** for card format details at [https://www.hidglobal.com/doclib/files/resource\\_files/6090-905\\_f.1\\_-\\_pivclass\\_fips-201\\_reader\\_operation\\_and\\_output\\_selections.pdf](https://www.hidglobal.com/doclib/files/resource_files/6090-905_f.1_-_pivclass_fips-201_reader_operation_and_output_selections.pdf)

(Section 3 describes card format FASC-N details and section 8.6 contains an example of the 128-bit BCD Output.)

## FASC-N Configuration at the C•CURE9000 Administration Station

### CHUID Configuration

Follow the below procedure for CHUID configuration:

1. Select the template **Full FASC-N CHUID Format (200 bit)**, the default values for the configuration are shown in [Figure 3](#) on [page 77](#).

**Figure 3: CHUID Format Template (creating from Full FASC-N CHUID Format (200 bit))**

CHUID Format (Creating from Full FASC-N CHUID Format (200 bit) Template)

Save and Close Create Copy

Name:

Description: 200 bit CHUID Format used by TWIC/PIV II Cards

☐ Enabled

General

CHUID Length: 32 ☐ Used by 128 bit SmartID

CHUID Format Type: Extended Format

☐ Use this format to decipher unknown CHUIDs in Journal

CHUID Fields

| Id | Field Name           | Length | Start Position | End Position |
|----|----------------------|--------|----------------|--------------|
| 0  | Card Number          | 6      | 1              | 6            |
| 3  | Agency Code          | 4      | 7              | 10           |
| 4  | System Code          | 4      | 11             | 14           |
| 5  | Credential Series    | 1      | 15             | 15           |
| 6  | Credential Issue     | 1      | 16             | 16           |
| 12 | Personnel Identifier | 10     | 17             | 26           |
| 13 | Association Category | 1      | 27             | 27           |

Apply current CHUID Format to credentials using the selected CHUID Format

Check whether this change will be valid

Apply this CHUID Format

2. Enter name in the Name field.
3. Select the check box **Enabled**.
4. Click **Save and Close** to save the configuration.

## Card Format Configuration

Follow the below procedure for Card Format configuration:

1. Enter name and description in the **Name** and **Description** field respectively.
2. Enter the data length as 200 in the **Data Length** field of **Card Format Description** section under the **General** Tab.
3. Select the **General** Tab and configure the following details. Refer to [Figure 4](#) on [page 78](#) for Card Format - Assa FASCN Card Format, **General** Tab.
  - a. Select the CHUID format ( as defined in [CHUID Configuration](#) on [page 76](#) section) from the **CHUID Format** field of **Card Format Description** section under the **General** Tab.

**Figure 4:** Card Format FASCN - General Tab

The screenshot shows a software window titled "Card Format - Asa FASCN Card Format". At the top, there are buttons for "Save and Close" and "Save and New". Below these are input fields for "Name" (containing "Asa FASCN Card Format") and "Description". The main area has two tabs: "General" (selected) and "Format Fields". Under the "General" tab, there is a "Card Format Description" section containing a "CHUID Format" dropdown (set to "Asa FASCN CHUID") and a "Data Length" input field (set to "200"). Below this, there are radio buttons for "Magnetic" and "Wiegand / Proximity" (selected). At the bottom, there is a "Reverse Swipe Setting" section with five radio button options: "Read as Normal Swipe" (selected), "Read as Duress", "Ignore Reverse Swipe (ISC only)", "Reverse Swipe is Not Allowed", and "Must Always Use Reverse Swipe (iSTAR only)".

4. Select the **Format Fields** Tabs - and configure the details as shown in [Table 17](#) on [page 78](#).

**Table 17: Format Fields Tab Configuration Details**

| Field Type                | Start Position | Length | End Position | Encoding    |
|---------------------------|----------------|--------|--------------|-------------|
| Card Number               | 1              | 6      | 6            | BCD (4-bit) |
| Agency Code               | 7              | 4      | 10           | BCD (4-bit) |
| System Code               | 11             | 4      | 14           | BCD (4-bit) |
| Credential Series         | 15             | 1      | 15           | BCD (4-bit) |
| Credential Issue          | 16             | 1      | 16           | BCD (4-bit) |
| Personnel Identifier      | 17             | 10     | 26           | BCD (4-bit) |
| Association Category      | 27             | 1      | 27           | BCD (4-bit) |
| Organizational Category   | 28             | 1      | 28           | BCD (4-bit) |
| Organizational Identifier | 29             | 4      | 32           | BCD (4-bit) |

5. Click **Save and Close** to save the configuration.

1. Select the template **Full PIV-I CHUID Format (128 bit)**, the default values for the configuration are shown in [Figure 6](#) on [page 80](#).

**Figure 6:** CHUID Format Template (creating from PIV-I CHUID Format (128 bit))

CHUID Format (Creating from PIV I CHUID Format (128-bit) Template)

Save and Close Create Copy

Name:

Description: 128 bit CHUID Format used by PIV I Cards

☐ Enabled

General

CHUID Length: 80 ☐ Used by 128 bit SmartID

CHUID Format Type: Extended Format

☐ Use this format to decipher unknown CHUIDs in Journal

CHUID Fields

Add Remove Validate Fields Move up Move Down

| Id | Field Name  | Length | Start Position | End Position |
|----|-------------|--------|----------------|--------------|
| 0  | Card Number | 40     | 1              | 40           |
| 8  | CardInt1    | 20     | 41             | 60           |
| 9  | CardInt2    | 20     | 61             | 80           |

Apply current CHUID Format to credentials using the selected CHUID Format

Check whether this change will be valid

Apply this CHUID Format

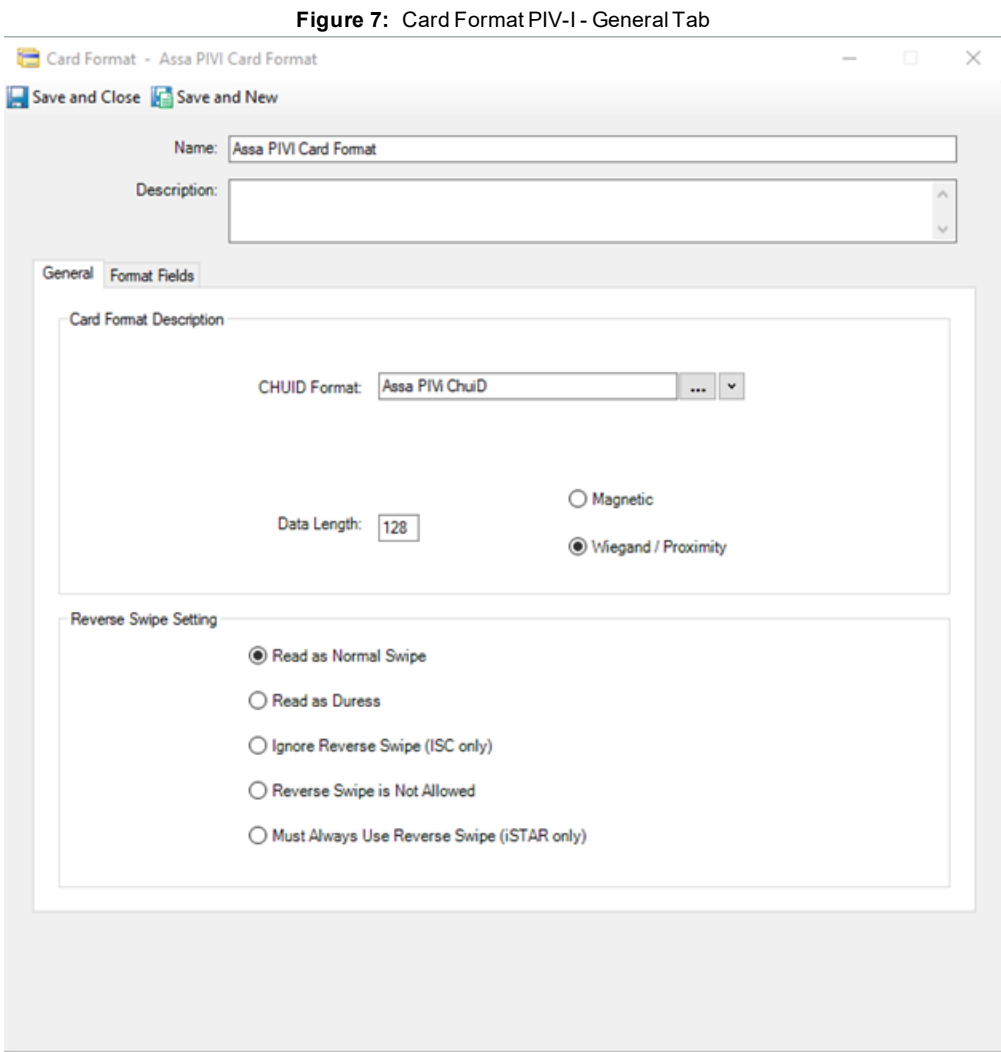
2. Enter name in the **Name** field.
3. Select the check box **Enabled**.
4. Click **Save and Close** to save the configuration.

## Card Format Configuration

Follow the below procedure for Card Format configuration:

1. Enter name and description in the **Name** and **Description** field respectively.
2. Enter the data length as 128 in the **Data Length** field of **Card Format Description** section under the **General** Tab.
3. Select the **General** Tab and configure the following details. Refer to [Figure 7](#) on [page 81](#) for Card Format - Assa PIV-I Card Format, **General** Tab.

- a. Select the CHUID format ( as defined in [CHUID Configuration](#) on [page 76](#) section) from the **CHUID Format** field of **Card Format Description** section under the **General** Tab.



4. Select the **Format Fields** Tabs and configure the details as shown in [Table 17](#) on [page 78](#).

**Table 18: Format Fields Tab Configuration Details**

| Field Type  | Start Position | Length | End Position | Encoding    |
|-------------|----------------|--------|--------------|-------------|
| Card Number | 1              | 40     | 40           | BCD (4-bit) |
| CardInt1    | 41             | 20     | 60           | BCD (4-bit) |
| CardInt2    | 60             | 20     | 80           | BCD (4-bit) |

5. Click **Save and Close** to save the configuration.

The PIV-I Card Format is consumed by a Credential object. Matching fields Credential-Card Format must be set in the Credential object.

**Figure 8: Credential Configuration PIV-I**

[illegible]