17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.

SpaceOps-2023, ID # 103

Practical Access Control and Traceability in Control Centre Workstations

Julio Vivero[1], **Laura Jamilis**[2], **Antonio Perez**[2]

[1] Business partner- International markets, GMV, Av. de la Granvia, 16-20, Edificio Nova Gran Via, 2nd floor – 08902, Hospitalet de Llobregat, Spain.
[2] Project Manager, GMV, Av. de la Granvia, 16-20, Edificio Nova Gran Via, 2nd floor – 08902, Hospitalet de Llobregat, Spain.

Abstract

Control centres are the most sensitive element of a mission when in operations. They are the eyes, the ears, the brain and the muscles of every mission. Everything that happens in the operation of a mission happens in the control centre. It is therefore paramount that the control centre behaves reliably and is well-protected against any scenario that can, depending on the mission, compromise its confidentiality, integrity and / or availability. Such threat scenarios can be motivated by intentional attacks –external or internal- or by accidents caused by well-intended actions from users (e.g., employees, contractors, etc.).

After a thorough risk analysis, several measures need to be applied to mitigate the above threat impacts following a concept of defence in depth. Often, these measures are also dictated by internal or external regulations the operator, or the control centres need to comply with.

The problem is that control centres have very specific characteristics which prevent the application of solutions which are commonplace in almost any other IT infrastructure. User authentication and authorization is a clear example. In control centres computers need to be always on, showing telemetry data, so that operators can immediately spot and react to any anomaly. 24/7 operations also require non interruptible monitoring and shift change as smooth as possible. Consequently, generic accounts for controllers or operators can be preferred to individual accounts and authentication mechanism limited to the minimum.

However, restricting access to the control centre workstations and having traceability is an important deterrent and detection control for insider threats (unlikely but highly impacting) as well as effective mechanism for improving traceability of actions to users thus reducing bad-practices and improving training of operators.

We face therefore this duality, on one hand user authentication, authorization and traceability at workstations is an important, often mandatory to comply with regulations, security control but on the other hand there are no technological solutions to fit the specificities of control centres. This duality is often solved by having a strong physical access control to the control room, well-trained trustworthy operators, and accepting the remaining residual risk.

Keywords: Control centres, security, authentication, authorization, traceability, contactless badge.

1. Introduction

Control centres play a crucial role in the successful execution of a mission by monitoring and controlling various aspects of the operation. They are responsible for coordinating the various activities and ensuring that all systems are functioning properly. As such, they are considered to be the most sensitive element of a mission during operations, and require strict security measures to protect against unauthorized access and potential threats.

The problem of user authentication and authorization in control centers is a complex one, as the specific characteristics of these environments make it difficult to apply standard solutions. Due to the nature of control centres, they require constant monitoring and real-time reaction to any anomalies, which means that the computers need to be always on and displaying telemetry data. Additionally, the 24/7 operations and shift changes require non-interruptible monitoring and smooth transitions. These requirements often lead to the use of generic accounts for controllers or operators, rather than individual accounts, and the use of minimal authentication mechanisms.

However, restricting access to the control center workstations and having traceability is important for deterring and detecting insider threats, as well as for improving the traceability of actions to users, which can help reduce bad practices and improve operator training. This creates a duality, as user authentication, authorization, and traceability at workstations are important security controls, but there are currently no technological solutions that can meet the specific needs of control centers.

This duality is often resolved by implementing strong physical access controls to the control room, hiring well-trained and trustworthy operators, and accepting the residual risk that remains. This approach can help to mitigate the risks associated with user authentication and authorization in control centers, while still allowing for the smooth and uninterrupted operation of these critical systems.

Not many solutions exist today that can successfully address this duality between the need for user authentication, authorization, and traceability at workstations and the specific characteristics of control centers. Some conceptual studies have explored the possibility of using face recognition and constant authentication as a solution, but to the best of our knowledge, there are no control center ready operational solutions that have been implemented using this approach.

These solutions are still in the experimental phase and are not yet mature enough to be used in control centers. However, this approach may become more viable in the future with the advancements in facial recognition technology and the increasing need for security in control centres.

Another approach that is being researched is the use of multi-factor authentication methods that can provide a balance between security and usability. This can include the use of smart cards, biometrics, and other forms of authentication that can provide a high level of security without interrupting the operator's workflow.

Overall, the best solution for a control center would depend on the specific requirements of the organization and the level of risk they are willing to accept. Customized solutions that take into account the unique characteristics of control centers may be more effective in addressing the duality of user authentication, authorization, and traceability.

In the following sub-sections we describe the characteristics of Biolock. A GMV solution that addresses these challenges and is currently used in some space organizations.

2. Solution functionalities

This section contains a description of the main system functions and capabilities and step-by-step procedures for system access and use. Biolock main goal is to reinforce access control and user traceability at the workstations.
When Biolock is active and the computer is locked, the application allows a continuous visualization of the screen.

The main characteristics of Biolock are:

- Centralized administration tool used to register workstations, enrol users and monitor accesses and events.
- User and workstation groups can be created to simplify access granting to groups of users.
- High availability: Inter & Intra site.
- Workstations are autonomous: they can be locked & unlocked without connection to the CA.
- Biometric data, if used, is stored in a separate database server (for legal and security reasons).

The main Biolock’s components are:

- The server or Central Admin.
- A client or Workstation.
- Action panel.

2.1 The server or Central Admin.

This section describes the main functionalities of the Central Admin, such as the user management, workstation management, association actions and audit operations. These key functionalities are:

- Register, edit or remove users.
- Configuration of blocking timeouts when no activity detected.
- Configuration of lock position on the screen.
- Send Emergency locks and unlocks.
- Register, edit or remove workstations.
- Creation, edition and removal of user and workstation groups.
- Retrieval of lock audit and pending actions from workstations.

It is particularly important to describe the emergency unlock functionality in Biolock. There might be crisis situations at the Control Centre with a high level of tension and stress. In this situation the simple need of having to authenticate to each workstation one wants to interact with can add an additional level of distress. Hence, a person with the required level of authorisation can request the temporal unlocking of all workstations (or a group of them) in the Control Centre. This unlocking, as well as the person authorising it, are logged at the central admin console.

All these functionalities are accessible through a number of views in the solution.

2.1.1 User view

The User View shows the users and user groups stored on the database. This allows to:

- Create, modify and delete a user
- Enrol a RFID card to a specific user
- Create and modify user groups

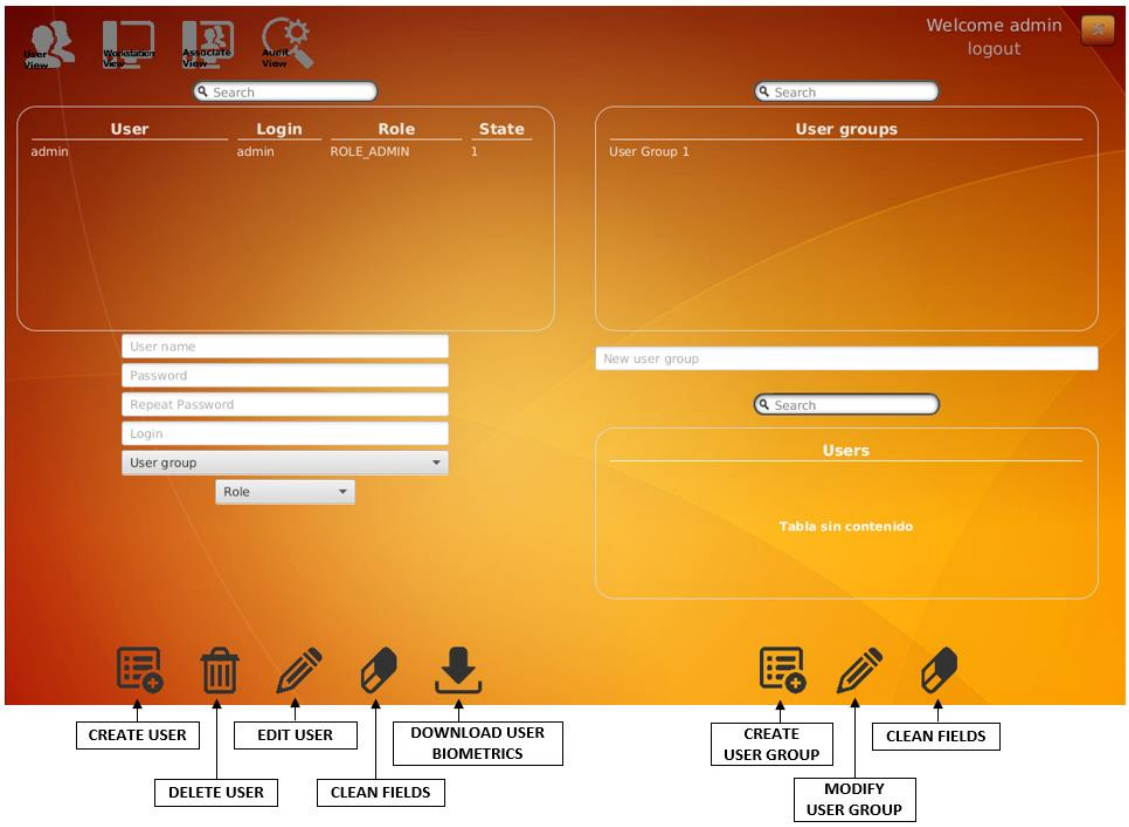

Figure 1. User view

The user view is divided into two parts: the users and the user groups. On the user part, it shows the users table, which gives the information about the users (username, role, etc.). The Role indicates which actions a user is allowed to perform (See section 4. Roles for more information about the permissions). When double-clicking in a user, the

detailed information regarding that specific user, including its group and its biometrics data information is displayed on the screen.

On the user group part, there is a table that shows all the groups in the database. If a user group is double clicked, it shows all its users in the bottom-right table.

2.1.2 Workstation view

The second icon on the toolbar redirects to the Workstation view. This view is organized in the same way as the User View. In this screen the user will be able to:

- Modify and delete a workstation
- Create, modify and configure workstation groups
- Send lock and unlock emergency commands to the registered workstations

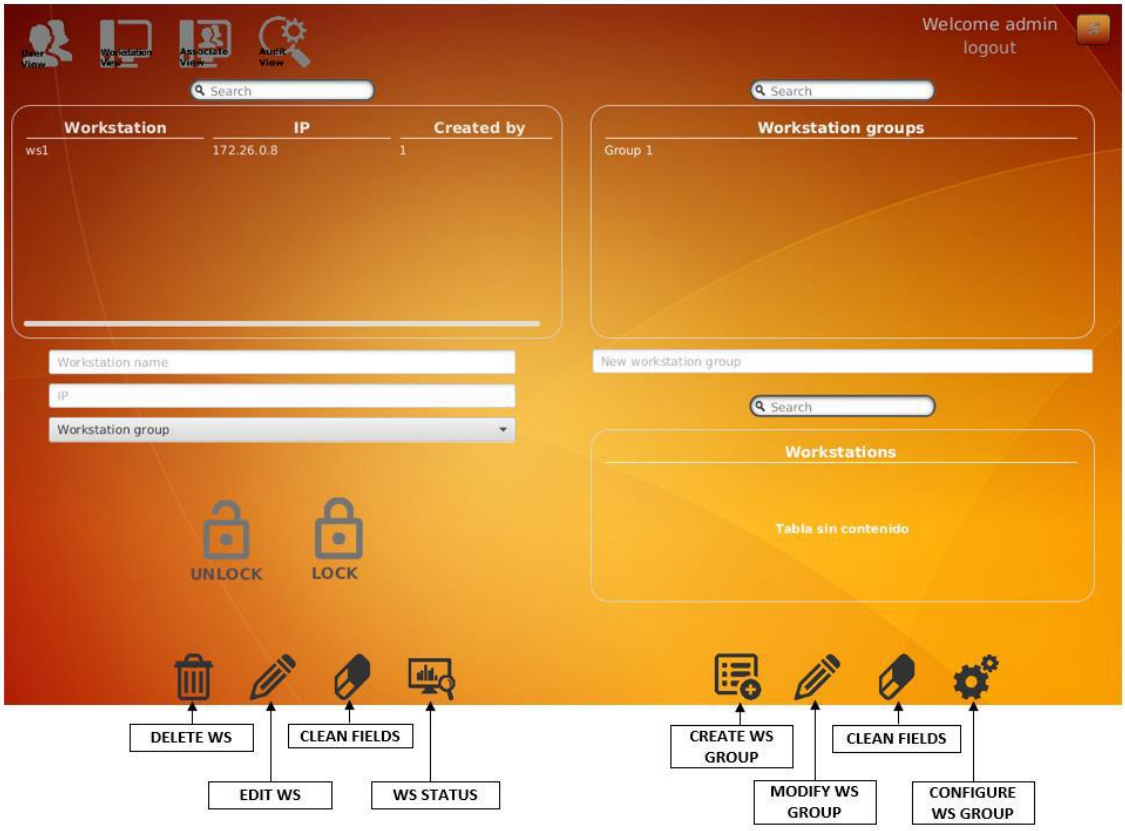

Figure 2. Workstation view

When Biolock's software is installed in a workstation, the workstation will appear in the top-left table automatically. Then, the user will be able to configure to which workstation group the workstation belongs. When the workstation is assigned to a workstation group, there are several parameters that can be configured for all the workstations pertaining to the same workstation group:

- Lock timeout: Inactivity timeout before the workstations on the group automatically lock
- Lock icon position: Position of the lock label on the screen, configurable by moving the lock label over the black square which represents the workstation screen
- 2FA: If enabled, to unlock the workstation, RFID card and the password of the user will be required.

In addition, as shown in Figure 2, in the workstation view there are two icons that allow the administrator to send an emergency lock or unlock to a workstation group.

When the unlock button is clicked, the workstation selected and all the workstations belonging to the same workstation group will be unlocked. Analogously, if the locked button is clicked, all the workstations belonging to the workstation group will be locked.

2.1.3 Associate view

The associate view allows to establish relationships between workstations groups and user groups or between single workstations and user groups.

Figure 3. Associate view

On this view, the relations between the available users and workstations can be established. In order to have permissions to lock or unlock a workstation, the relation between the user group and the workstation or workstation group must be configured on this page.

2.1.4. Audit view

The Audit view includes several features that allow traceability of the whole system functioning. It is accessible by the users with role “Administrator” and “Operator”. This view is divided in 3 sub-sections:

2.1.4.1 Lock audit

The lock audit view displays all locking and unlocking events that took place on the system. The table contents are retrieved from the database, where are stored in real-time. In order to inspect the elements, there are some filtering options which allow to retrieve a subset of events after applying certain restrictions. The filtering options available are:

- Username: Display only events generated by a certain user
- Workstation name: The name of the workstation whose events are going to be filtered
- Date: Events occurred on a certain day

2.1.4.2 Pending actions

Pending actions displays all actions that are being executed on the system but are not finished yet.

The table prompts the user with some basic information about the action which may be enough on some basic scenarios to diagnose any system issue.

When more detailed information of an action is needed, a double click on the action opens a new window which displays all raw information of the action on its current state of execution for a more detailed diagnose of the system functioning.

2.1.4.3 User's access

User's access is intended to provide a clean, visually, readable, dynamic and easy way to display association information between the workstation groups and the users.

To get the report, the user must perform double click on any workstation entry and the rest of the tables will be filled in with all association data related with it, as displayed on Figure 4.

Figure 4. User's access view

4.2 A client or Workstation.

Biolock's software can be installed in a workstation through a script that eases the installation process. When executing the installation script, the workstation is automatically registered in the Central Admin and after the "Lock timeout" it will be automatically locked. To unlock it, it will be required a registered RFID card (and a password if configured) to unlock it again.

The main functionalities of the workstation are mainly controlled and configured by the Central Admin as has been described in the previous sections.

In addition, the workstation offers the possibility of configuring the application logs verbosity in case there is the need to debug any behavior of the workstation.

4.3 Action panel

To expose functionalities such as emergency unlocks or manual locks to a workstation's user, an Action Panel has been implemented.

Figure 5. Main Action Panel View

That panel consists of a small GUI that displays all available operations. The available operations are:

- **Global Group Emergency Lock (top-left icon):** Allows sending an emergency lock to the workstation group the current workstation belongs to. This operation requires user biometric identification.
- **Global Group Emergency Unlock (top-right icon):** Allows sending an emergency unlock to the workstation group the current workstation belongs to. This operation requires user biometric identification.
- **Manual locking (bottom-left icon):** Allows manually locking the current workstation.
- **Check the status of the workstation (bottom-right icon):** Requests a workstation state to the Central Admin. This operation requires the user to introduce a valid user password combination**.**

4.4 Roles

In Biolock there are 3 different roles that can be assigned to a user. In the table below the permissions of each one of them are listed.

	OPERATOR	**AUDIT**	**ADMIN**
Unlock a workstation	✓	✓	✓
Login to Central Admin	✗	✓	✓
Views allowed to see in Central Admin	None	Audit View	All
Retrieve WS status from Action Panel	✗	✗	✓
Send emergency Lock/Unlock from Action Panel	✓	✓	✓

Table 1. Roles

5. Results

GMV's **Biolock** is a solution designed specifically to address this duality in control and operational rooms. Biolock allows control centres to maintain workstations always visible with telemetry data, while still implementing user authentication and authorization.

Biolock allows operators to quickly authenticate by using a contactless badge on a reader, and then interact with the workstation while it remains unlocked. The workstation will then automatically lock again when it is idle.

The solution is controlled and monitored from a central server, which allows the management of user privileges, workstations, and logs. This centralization allows for a more efficient administration of the system and also provides a centralized point for security monitoring and incident response.

The solution integrates seamlessly into both routine and LEOP (Launch and Early Orbit Phase) operations of the control centre and contributes to cybersecurity operations by providing protection and detection capabilities. This solution addresses the duality between the need for user authentication, authorization, and traceability at workstations and the specific characteristics of control centres by allowing for a balance between security and usability.