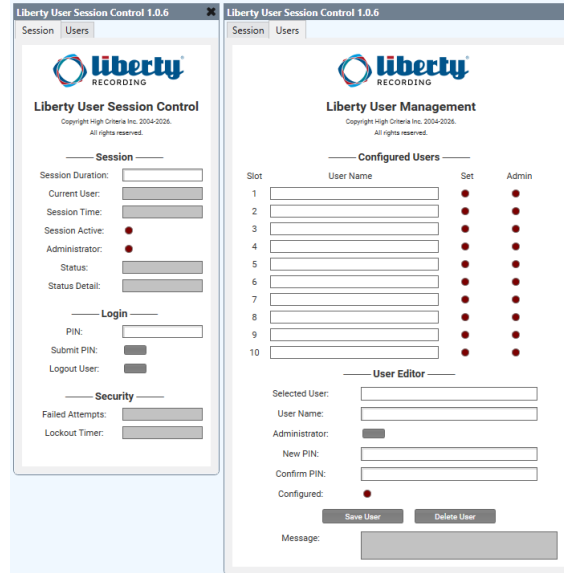




Setup & Configuration Guide:

Liberty User Session Control Plugin for Q-SYS

Version 1.0.6 – August 2026

Introduction

The Liberty User Session Control Plugin provides PIN-based user authentication and session management for Q-SYS control systems. The plugin allows a Q-SYS design to identify the currently logged-in user, determine whether that user has administrator privileges, maintain a configurable session timeout, and automatically log the user out when the session expires.

The plugin supports up to ten configured users. Each user is assigned a unique six-digit PIN and may optionally be granted Administrator privileges.

Administrator users are responsible for user management, including creating users, changing user information or PINs, assigning Administrator privileges, and deleting users. User-management functions are available only from the **Users** page of the plugin within Q-SYS Designer.

This guide provides instructions for:

- Creating the initial Administrator account
- Adding and managing additional users
- Logging in and out of a user session
- Configuring session and security settings
- Using the plugin controls within a Q-SYS design
- Understanding status, failed-login, and lockout behavior

Table of Contents

INITIAL SETUP	3
ADDING THE LIBERTY USER SESSION CONTROL PLUGIN.....	3
CREATING THE FIRST ADMINISTRATOR.....	4
PIN Requirements	5
LOGGING IN FOR THE FIRST TIME.....	5
ADDING ADDITIONAL USERS	6
EDITING AN EXISTING USER	7
Administrator Protection	7
DELETING A USER.....	7
CONFIGURING USER SESSION CONTROL IN Q-SYS DESIGNER	8
THE SESSION PAGE CONTROLS	9
SECURITY AND LOCKOUT BEHAVIOR	11
PIN STORAGE AND PROTECTION	11
THE USERS PAGE CONTROLS.....	12
CONTROL PINS.....	13
COMMON STATUS AND ERROR MESSAGES.....	14
LIBERTY RECORDER CONTROL 2.4.7 AND LATER.....	16

INITIAL SETUP

ADDING THE LIBERTY USER SESSION CONTROL PLUGIN

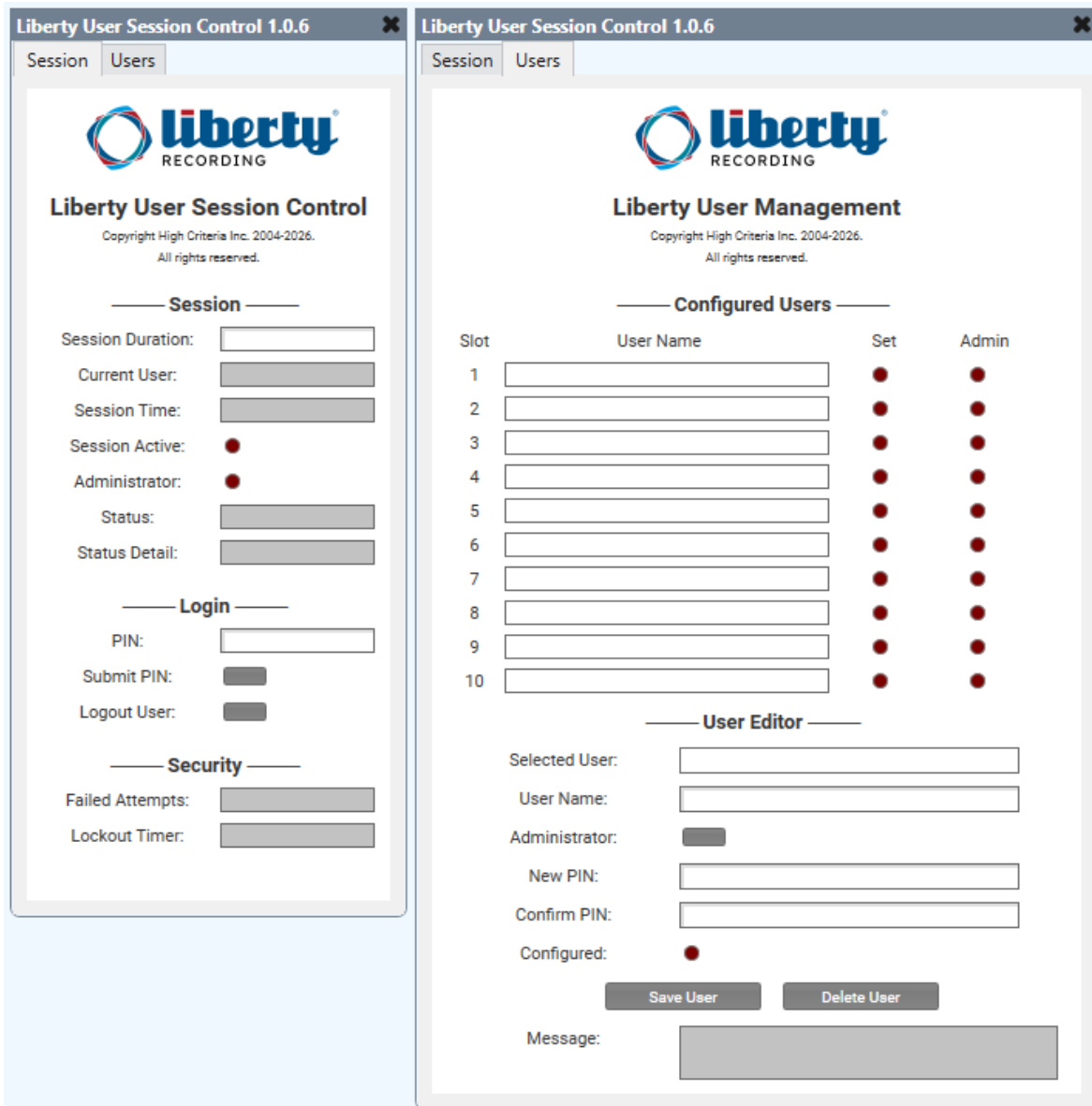
Add the **Liberty User Session Control** plugin to the Q-SYS Designer schematic and open the plugin. The plugin contains two pages:

Session

- Used to log users in and out and to display the current session state.

Users

- Used to create, edit, and delete user accounts. User management is performed directly within Q-SYS Designer and is not exposed through the plugin's external control pins.



Liberty User Session Control 1.0.6

Session Users

Liberty User Session Control
Copyright High Criteria Inc. 2004-2026.
All rights reserved.

— Session —

Session Duration:

Current User:

Session Time:

Session Active: ☒

Administrator: ☒

Status:

Status Detail:

— Login —

PIN:

Submit PIN:

Logout User:

— Security —

Failed Attempts:

Lockout Timer:

Liberty User Session Control 1.0.6

Session Users

Liberty User Management
Copyright High Criteria Inc. 2004-2026.
All rights reserved.

— Configured Users —

Slot	User Name	Set	Admin
1		☒	☒
2		☒	☒
3		☒	☒
4		☒	☒
5		☒	☒
6		☒	☒
7		☒	☒
8		☒	☒
9		☒	☒
10		☒	☒

— User Editor —

Selected User:

User Name:

Administrator: ☐

New PIN:

Confirm PIN:

Configured: ☒

Message:

CREATING THE FIRST ADMINISTRATOR

When the plugin is first added to a design and no users have been configured, the plugin begins in **Bootstrap Mode**. Bootstrap Mode allows the first user account to be created without requiring an existing login.

IMPORTANT: The first configured user is automatically assigned Administrator privileges. At least one Administrator must always remain configured because only an Administrator can add, modify, or delete other users.

Open the **Users** page of the plugin. The Message field will indicate:

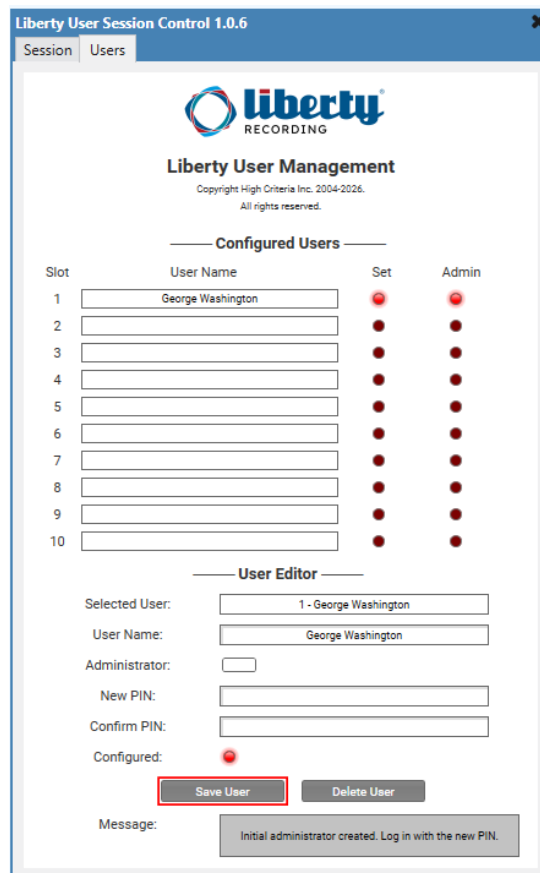
“Bootstrap mode: create the first administrator account.”

To create the first user:

1. Select an empty user slot.
2. Enter the user's name in **User Name**.
3. Enter a six-digit PIN in **New PIN**.
4. Enter the same PIN again in **Confirm PIN**.
5. Click **Save User**.

The first user is automatically configured as an Administrator. After the user is successfully created, the Message field will indicate:

“Initial administrator created. Log in with the new PIN.”



Liberty User Session Control 1.0.6

Session Users

Liberty
RECORDING

Liberty User Management
Copyright High Criteria Inc. 2004-2026.
All rights reserved.

— Configured Users —

Slot	User Name	Set	Admin
1	George Washington	☒	☒
2		☐	☐
3		☐	☐
4		☐	☐
5		☐	☐
6		☐	☐
7		☐	☐
8		☐	☐
9		☐	☐
10		☐	☐

— User Editor —

Selected User: 1 - George Washington

User Name: George Washington

Administrator: ☐

New PIN:

Confirm PIN:

Configured: ☒

Save User Delete User

Message: Initial administrator created. Log in with the new PIN.



PIN Requirements

Each user PIN must:

- Contain exactly six numeric digits
- Match the value entered in Confirm PIN
- Be unique to that user
- Not use a prohibited predictable PIN

Common repeating or sequential PINs, such as **000000** or **123456**, are rejected by the plugin.

LOGGING IN FOR THE FIRST TIME

After creating the initial Administrator, select the **Session** page.

Enter the Administrator's six-digit PIN in the **PIN** field and click **Submit PIN**.

After a successful login:

- **Current User** displays the user's configured name.
- **Session Active** illuminates.
- **Administrator** illuminates for an Administrator account.
- **Session Time** begins counting down.
- **Status** changes to an active/OK state.
- **Status Detail** displays **Session Active**.

The screenshot shows the 'Liberty User Session Control 1.0.6' application window. It has two tabs: 'Session' (selected) and 'Users'. The main content area displays the Liberty Recording logo and the title 'Liberty User Session Control'. Below this, it shows 'Copyright High Criteria Inc. 2004-2026. All rights reserved.' The interface is divided into three sections: 'Session', 'Login', and 'Security'. The 'Session' section includes fields for 'Session Duration' (300), 'Current User' (George Washington), 'Session Time' (299), 'Session Active' (indicated by a red dot), 'Administrator' (indicated by a red dot), 'Status' (OK, in a green box), and 'Status Detail' (Session Active). The 'Login' section includes a 'PIN' field, a 'Submit PIN' button, and a 'Logout User' button. The 'Security' section includes 'Failed Attempts' (0) and 'Lockout Timer' (0).

The Administrator may now return to the **Users** page to create or manage additional accounts.

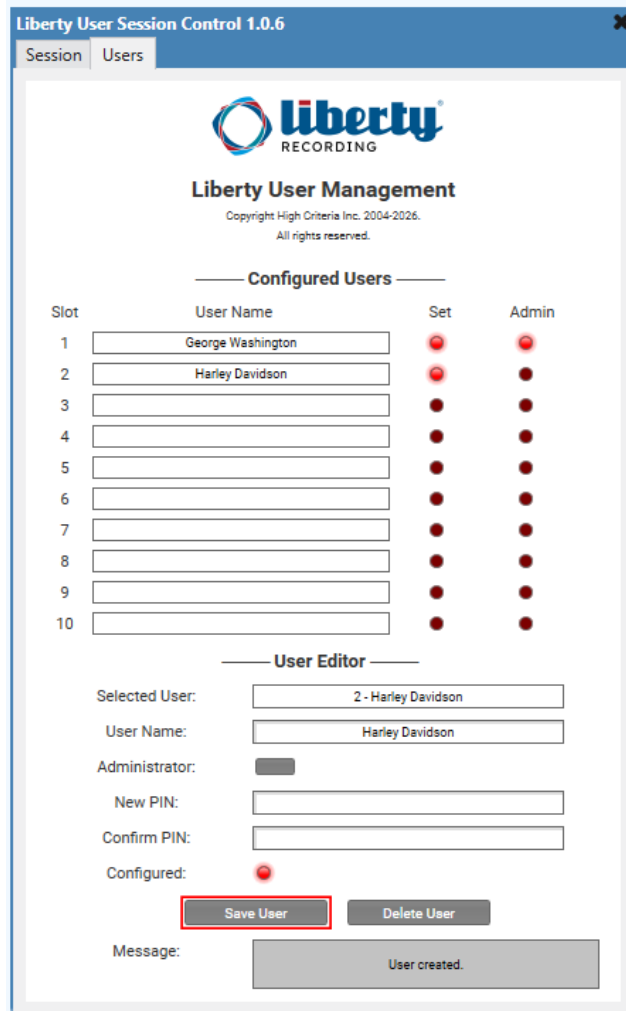
ADDING ADDITIONAL USERS

Once the first account has been created, an Administrator must be logged in before any user-management changes can be made.

To add another user:

1. Log in using an Administrator PIN.
2. Open the **Users** page.
3. Select an empty user slot.
4. Enter the new user's name.
5. Enable **Administrator** if the new user should also have user-management privileges.
6. Enter a six-digit PIN in **New PIN**.
7. Enter the same PIN in **Confirm PIN**.
8. Click **Save User**.

The Message field will display **User created** when the account has been successfully saved.



Slot	User Name	Set	Admin
1	George Washington	☒	☒
2	Harley Davidson	☒	☒
3		☐	☐
4		☐	☐
5		☐	☐
6		☐	☐
7		☐	☐
8		☐	☐
9		☐	☐
10		☐	☐

User Editor	
Selected User:	2 - Harley Davidson
User Name:	Harley Davidson
Administrator:	☐
New PIN:	
Confirm PIN:	
Configured:	☒
Save User Delete User	
Message:	User created.

The Configured Users section provides a quick overview of all ten user slots and indicates which slots are configured and which configured users have Administrator privileges.

EDITING AN EXISTING USER

An Administrator may modify an existing user's name, Administrator privileges, or PIN.

1. First, log in as an Administrator and open the **Users** page. Select the desired user from **Selected User**.
2. Modify the **User Name** or **Administrator** setting as required.
3. To leave the user's existing PIN unchanged, leave **New PIN** and **Confirm PIN** blank.
4. To change the user's PIN, enter the new six-digit PIN in both **New PIN** and **Confirm PIN**.
5. Click **Save User** to apply all changes.

When a PIN is changed at the same time as other user information, the Message field displays **User and PIN updated**.

Administrator Protection

The plugin always requires at least one configured Administrator. The final Administrator account cannot have its Administrator privileges removed.

If a currently logged-in Administrator removes their own Administrator privilege while another Administrator remains configured, the change is allowed, but Administrator access ends immediately after the user is saved.

DELETING A USER

Only an Administrator may delete users.

Select the configured user and click **Delete User**.

To protect against accidental deletion, the plugin requires the **Delete User** button to be clicked a second time within three seconds.

The plugin does not allow:

- The currently logged-in user to delete their own account
- The final remaining Administrator account to be deleted

After a successful deletion, the user slot becomes available for a new account.

The image shows a web form titled "User Editor". It contains several input fields: "Selected User:" with a dropdown menu showing "2 - Harley Davidson"; "User Name:" with a text box containing "Harley Davidson"; "Administrator:" with a checkbox that is currently unchecked; "New PIN:" and "Confirm PIN:" with empty text boxes; and "Configured:" with a red dot indicator. Below these fields are two buttons: "Save User" and "Delete User", with the "Delete User" button highlighted by a red rectangle. At the bottom, there is a "Message:" field containing the text "Press Delete User again within 3 seconds to confirm.".

CONFIGURING USER SESSION CONTROL IN Q-SYS DESIGNER

When the plugin is selected in the schematic, several security-related properties are available.

Properties	
Liberty User Session Control 1.0.6 Properties	
Session Security	
Fault Display Seconds	3
Failed Attempt Limit	5
Lockout Seconds	30
Show Debug	No
Graphic Properties	
Label	Liberty User Session Control 1.0.6
Position	487,146
Fill	
Script Access	
Code Name	LibertyUserSessionControl1.0.6
Script Access	None

Fault Display Seconds

- Controls the minimum amount of time that a fault condition remains visible in the plugin's Status and Status Detail fields.

Default: 3 seconds

Range: 3–30 seconds

Failed Attempt Limit

- Defines the number of invalid PIN attempts permitted before PIN entry is temporarily locked.

Default: 5 attempts

Range: 1–20 attempts

Lockout Seconds

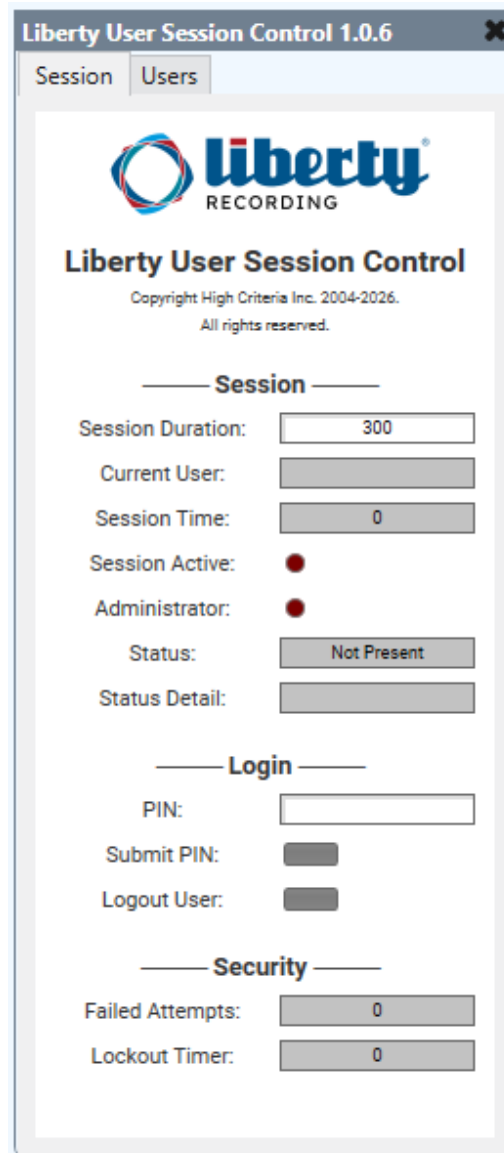
- Defines how long PIN authentication remains locked after the Failed Attempt Limit has been reached.

Default: 30 seconds

Range: 5–600 seconds

THE SESSION PAGE CONTROLS

The Session page contains the controls and status fields associated with normal user authentication.

The screenshot shows a web application window titled "Liberty User Session Control 1.0.6". It has two tabs: "Session" (selected) and "Users". The main content area features the Liberty Recording logo and the title "Liberty User Session Control" with a copyright notice "Copyright High Criteria Inc. 2004-2026. All rights reserved." Below this, there are three sections: "Session", "Login", and "Security". The "Session" section includes fields for "Session Duration" (300), "Current User" (blank), "Session Time" (0), "Session Active" (red dot), "Administrator" (red dot), "Status" (Not Present), and "Status Detail" (blank). The "Login" section includes a "PIN" field, "Submit PIN" button, and "Logout User" button. The "Security" section includes "Failed Attempts" (0) and "Lockout Timer" (0) fields.

Session	
Session Duration:	300
Current User:	
Session Time:	0
Session Active:	●
Administrator:	●
Status:	Not Present
Status Detail:	

Login	
PIN:	
Submit PIN:	
Logout User:	

Security	
Failed Attempts:	0
Lockout Timer:	0

Session Duration

- Defines the duration of a successful user session in seconds. The default value is **300 seconds**, or five minutes.
- When a user successfully logs in, Session Time begins counting down from the configured Session Duration. When the timer reaches zero, the user is automatically logged out.

Current User

- Displays the name of the currently authenticated user. The field is blank when no session is active.



Session Time

- Displays the number of seconds remaining in the current user session.

Session Active

- Illuminates while a valid user session is active.

Administrator

- Illuminates when the currently logged-in user has Administrator privileges.
- This output can be used within a Q-SYS design to enable controls or functions intended only for administrative users.

Status

- Provides the standard Q-SYS status indication for the plugin.
- During normal operation:
 - **Gray / Not Present** indicates that no user session is active.
 - **Green / OK** indicates an active user session.
 - **Red / Fault** temporarily indicates an authentication or configuration error.

Status Detail

- Provides additional information associated with the current Status.
- During an active session, the field displays: **"Session Active"**
- When an error occurs, the field temporarily displays the reason for the fault.

PIN

- Used to enter a user's six-digit PIN.
- The PIN field is cleared automatically after a login attempt.

Submit PIN

- Submits the PIN currently entered in the PIN field for authentication.

Logout User

- Immediately ends the current user session.

Failed Attempts

- Displays the current number of unsuccessful PIN attempts.

Lockout Timer

- Displays the number of seconds remaining when PIN authentication has been temporarily locked.

SECURITY AND LOCKOUT BEHAVIOR

If an incorrect PIN is submitted, the Failed Attempts value increases.

By default, after five unsuccessful attempts, PIN authentication is temporarily locked for 30 seconds.

During lockout:

- Additional login attempts are rejected.
- Lockout Timer displays the remaining lockout duration.
- Status temporarily indicates a fault.
- Status Detail identifies that PIN entry is locked.

When the lockout period expires, PIN authentication is automatically restored. A successful user login clears previous failed-login and lockout conditions.

PIN STORAGE AND PROTECTION

User PINs are **not stored in plaintext** by the Liberty User Session Control Plugin. When a PIN is created or changed, the plugin generates a unique 16-byte random salt and derives a 32-byte credential hash using PBKDF2 with SHA-256 and 50,000 iterations. Only the resulting hash and its associated salt are retained. The original PIN is discarded after processing.

The credential hashes and salts are stored within a private Custom Controls embedded component inside the plugin. They are not exposed as normal plugin controls or control pins. Q-SYS specifically documents embedded components as the preferred mechanism for persistently storing secrets within plugins; controls within an embedded component are accessible only to the plugin in which they are embedded and are retained as part of the Q-SYS design state.

When a user enters a PIN, the plugin does not retrieve or decrypt the original PIN. Instead, it applies the same PBKDF2 operation using that user's stored salt and compares the newly derived value to the stored credential hash. PINs, credential hashes, and salts are also intentionally excluded from the plugin's diagnostic logging.

For additional information, refer to:

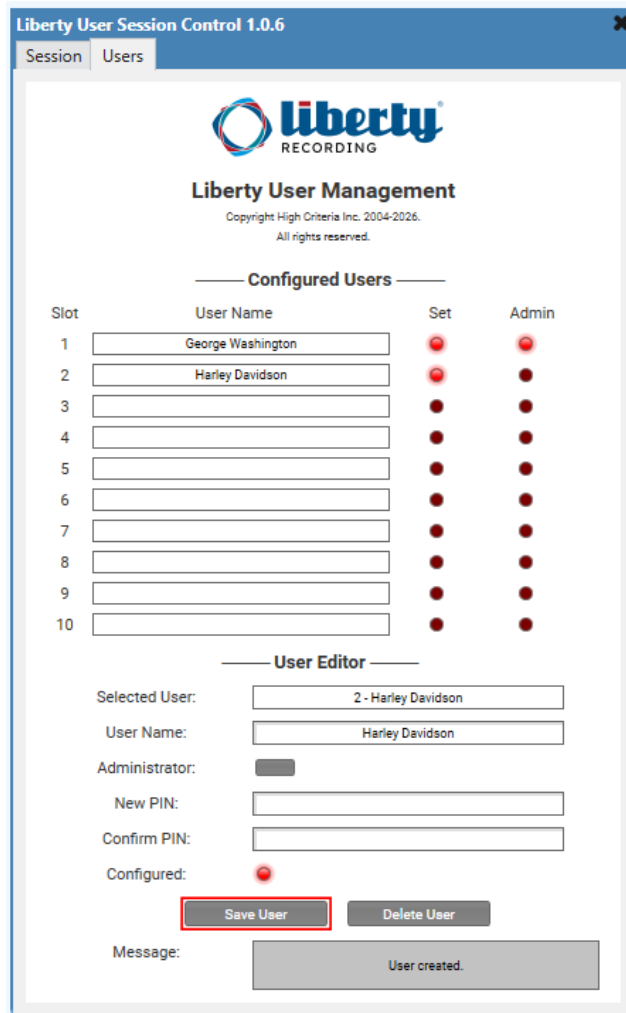
- **Q-SYS — Storing Secrets in Plugins:**
https://help.qsys.com/DeveloperHelp/Content/Code_Examples/Storing_Secrets_in_Plugins.htm
Q-SYS describes the use of private embedded Custom Controls for persistent secret storage.
- **Q-SYS — Crypto Library:**
https://help.qsys.com/Content/Control_Scripting/Using_Lua_in_Q-Sys/Crypto.htm
Q-SYS's documented PBKDF2 example uses **50,000 iterations, a 32-byte derived value, SHA-256, and a 16-byte salt**—the same parameters used by this plugin.
- **NIST SP 800-63B — Digital Identity Guidelines, Authentication and Authenticator Management:**
<https://pages.nist.gov/800-63-4/sp800-63b.html>

NIST recommends that stored passwords be salted and hashed using a suitable password-hashing scheme and a cost factor intended to increase the expense of offline guessing attacks.

- **NIST SP 800-132 — Password-Based Key Derivation:**
<https://doi.org/10.6028/NIST.SP.800-132>

THE USERS PAGE CONTROLS

The Users page is intended for system configuration and administration within Q-SYS Designer. User-management controls are not exposed as external control pins.



Liberty User Session Control 1.0.6

Session Users

Liberty
RECORDING

Liberty User Management
Copyright High Criteria Inc. 2004-2026.
All rights reserved.

— Configured Users —

Slot	User Name	Set	Admin
1	George Washington	☒	☒
2	Harley Davidson	☒	☒
3		☐	☐
4		☐	☐
5		☐	☐
6		☐	☐
7		☐	☐
8		☐	☐
9		☐	☐
10		☐	☐

— User Editor —

Selected User:

User Name:

Administrator: ☐

New PIN:

Confirm PIN:

Configured: ☒

Message:

Configured Users

- Displays the ten available user slots and provides visual indicators showing whether each slot is configured and whether the user is an Administrator.

Selected User

- Selects the user slot to create or modify.



User Name

- Defines the name associated with the selected user.
- User names must be unique.

Administrator

- Determines whether the selected user has user-management privileges.
- The first configured user is automatically an Administrator.

New PIN / Confirm PIN

- Used to create or change the selected user's six-digit PIN.
- For an existing user, these fields may be left blank when making other changes if the PIN should remain unchanged.

Configured

- Indicates whether the selected user slot contains a completely configured user account.

Save User

- Saves changes to the selected user.
- For a new user, User Name, New PIN, and Confirm PIN are required.
- For an existing user, Save User updates the user's name or Administrator status and also changes the PIN when a new PIN and confirmation are supplied.

Delete User

- Deletes the selected user after a second confirmation press within three seconds.

Message

- Displays user-management instructions, confirmations, and error messages.

CONTROL PINS

Only controls useful for Q-SYS system logic and UCI integration are exposed as plugin control pins. User-configuration controls from the Users page are deliberately excluded from the control-pin list.

Bidirectional / Input Controls

- **Session Duration** – Session duration in seconds
- **PIN** – PIN entry
- **Submit PIN** – Submits PIN authentication
- **Logout User** – Ends the active user session

Control Pins	
Admin	☐
Current User	☐
Disable	☐
Failed Attempts	☐
Lockout Timer	☐
Logout User	☐
PIN	☐
Session Active	☐
Session Duration	☐
Session Time	☐
Status	☐
Status Detail	☐
Submit PIN	☐

Output Controls

- **Current User** – Name of the authenticated user
- **Session Time** – Remaining session duration
- **Session Active** – Indicates an active session
- **Admin** – Indicates that the active user is an Administrator
- **Status** – Standard Q-SYS plugin status
- **Status Detail** – Additional session or fault information
- **Failed Attempts** – Number of unsuccessful PIN attempts
- **Lockout Timer** – Remaining lockout duration

COMMON STATUS AND ERROR MESSAGES

“Enter PIN”

- No PIN was entered before Submit PIN was pressed.

“PIN must be 6 numeric digits”

- The submitted PIN does not contain exactly six numeric digits.

“Invalid PIN”

- The submitted PIN does not match a configured user.

“Too many invalid PINs – temporarily locked”

- The Failed Attempt Limit has been reached and PIN authentication has been temporarily disabled.

“PIN entry locked – XX seconds remaining”

- A login was attempted while the temporary lockout was still active.

“No users configured”

- No user accounts have been created. Create the initial Administrator account from the Users page.

“Session Duration must be greater than 0”

- The configured session duration is invalid.

“Administrator access required”

- A user-management function was attempted without an active Administrator session.

“At least one administrator must remain configured”

- An attempt was made to remove Administrator privileges from the final Administrator.

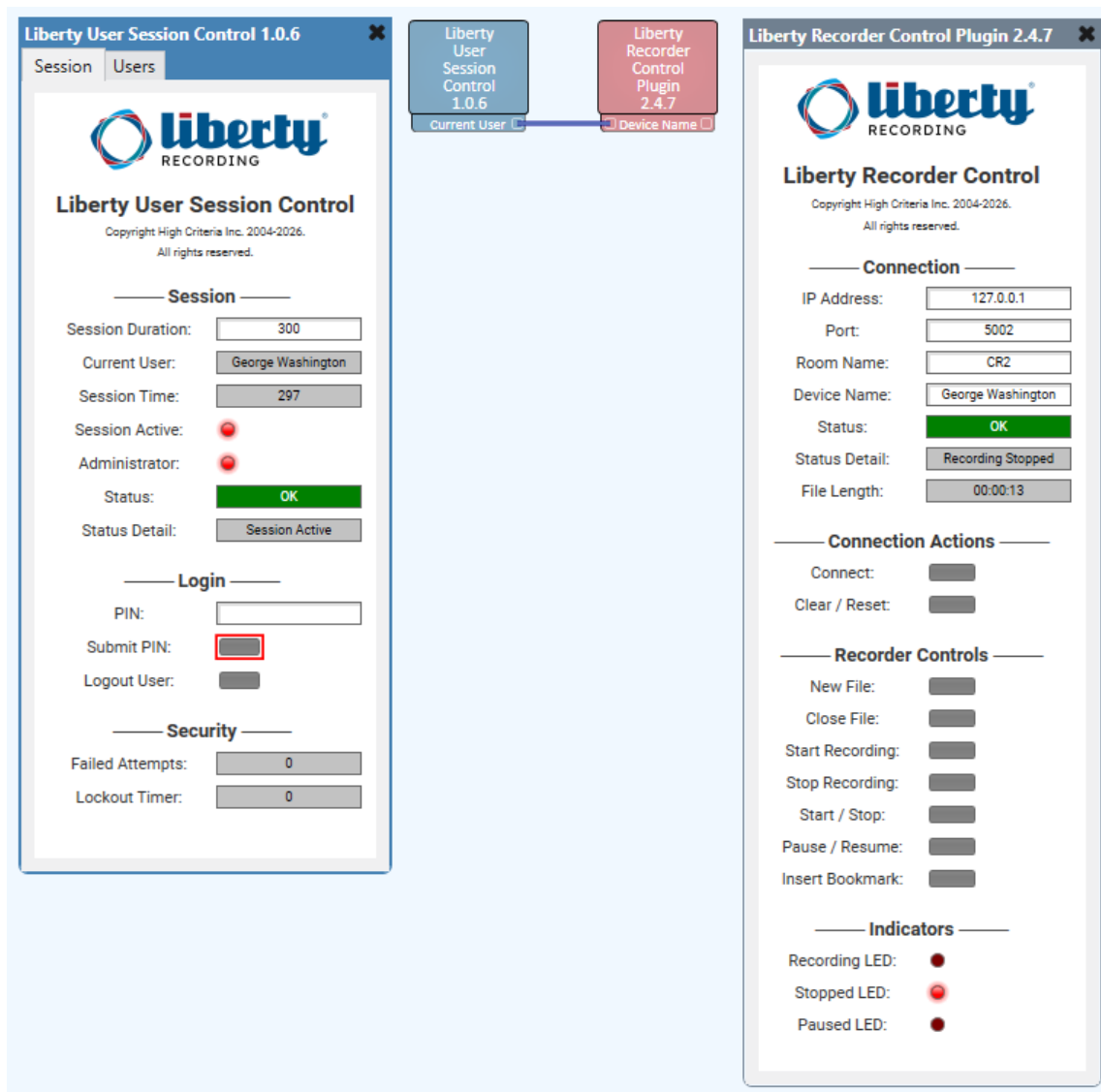
“The currently logged-in user cannot be deleted”

- An Administrator attempted to delete the account associated with the active session.

“The last administrator cannot be deleted”

- An attempt was made to delete the final configured Administrator.
- For temporary authentication faults, the Status field automatically returns to the appropriate normal state after the configured **Fault Display Seconds** interval.

LIBERTY RECORDER CONTROL 2.4.7 AND LATER



The screenshot displays two side-by-side application windows. The left window, titled 'Liberty User Session Control 1.0.6', has tabs for 'Session' and 'Users'. The 'Session' tab is active, showing session details for user 'George Washington' with a duration of 300, session time of 297, and status 'OK'. It also includes a 'Login' section with a PIN field and a 'Security' section with failed attempts and lockout timer. The right window, titled 'Liberty Recorder Control Plugin 2.4.7', shows connection settings (IP: 127.0.0.1, Port: 5002, Room: CR2, Device: George Washington) and recorder controls (New File, Close File, Start/Stop Recording, etc.). A diagram at the top shows the 'Current User' output from the session control window connected to the 'Device Name' input of the recorder control window.

When used with Liberty Recorder Control Plugin 2.4.7 or later, Liberty Helper Service 3.6 or later, and Liberty Court Recorder 9.1 or later, the Liberty User Session Control Plugin can provide operator identification for recorder actions initiated from Q-SYS.

The Current User output from the User Session Control Plugin can be connected to the Device Name input of the Liberty Recorder Control Plugin. When a user successfully logs in, the Current User value contains the name assigned to that user. The Recorder Control Plugin then supplies this value to Liberty Helper Service, which passes it to Liberty Court Recorder when recorder commands are executed.

This allows Liberty Court Recorder to associate actions initiated from the Q-SYS interface with the individual user who was logged in at the time.



EXAMPLE

In the example below, George Washington has logged into the Liberty User Session Control Plugin. The Current User value is passed to the Device Name field of the Liberty Recorder Control Plugin.

With the proper UCI setup in Q-SYS, recorder controls should only be made available to users after a valid User Session Control login.

If George Washington then activates the Start Recording control from the Q-SYS UCI, Liberty Helper Service passes the associated Device Name to Liberty Court Recorder. Liberty Court Recorder records the action in the Windows Event Log as:

App "George Washington" started recording in Liberty Court Recorder under profile <lcr_room>

This provides an audit trail showing which authenticated Q-SYS user initiated a recorder action, rather than identifying the action only as originating from the Q-SYS system.

Integration Flow

User Session Control (Q-SYS)

Current User: George Washington

↓

Liberty Recorder Control 2.4.7+ (Q-SYS)

Device Name: George Washington

↓

Liberty Helper Service 3.6+ (Windows PC)

Device Name: George Washington

↓

Liberty Court Recorder 9.1+ (Windows PC)

Windows Event Log records the user associated with the recorder action.

Note: The Liberty Recorder Control Plugin automatically detects the capabilities of the connected Liberty Helper Service. If an older version of Liberty Helper Service is detected that does not support the Device Name value, the Recorder Control Plugin will continue to operate without user-identification forwarding. This compatibility condition is identified in the Recorder Control Plugin's debug log.