Better by design™

WHITE PAPER

Accountable operational technology

Reliable® controls

Accountable operational technology

Implementing RC-WebView in a Title 21 CFR Part 11 environment

Facility automation and operational technology (OT) systems play a crucial role in establishing accountability in the built environment. In some industries, stringent regulations impose further accountability on built-environment professionals. One such regulation is the Code of Federal Regulations (CFR) Title 21, which prescribes rules for the U.S. Food and Drug Administration. Part 11 establishes the requirements for electronic records and signatures in processes and facilities regulated by Title 21.

At its essence, Part 11 prescribes that electronic data in regulated industry processes meet the same legal requirements as paper records. Some of these include:

- The ability to discern invalid records
- The ability to generate electronic copies of records
- Automatic generation of an audit trail
- Control over user access
- Use of unique secure signatures
- Secure linking of those signatures to records

Title 21 CFR Part 11 has significant implications for pharmaceutical, medical device, biologic, biotech, contract research, and other regulated industries. Although many countries have their own regulations for businesses in these fields, the size of the US market for food and pharmaceutical consumables makes Title 21 a common validation standard worldwide, particularly for manufacturing and logistics companies.

Compliance for organizations in these industries is a commercial imperative. Significant costs and negative impacts are associated with nonconformance, including lost revenue, penalties, lawsuits, destruction of product, refusal to test, and breach of contract.

Title 21 CFR Part 11 provides guidance for maintaining computer systems, including hardware and software, controls, and documentation in all regulated processes. All computer systems that store data reported to the FDA or used to make quality decisions must be compliant. In labs, this includes records that prove quality, safety, strength, efficacy, or purity. In clinical environments, this includes data reported in clinical trials. In manufacturing, this includes decisions about product quality.

Reliable Controls Authorized Dealers are equipped to provide simple, flexible, sustainable accountability in Title 21 CFR Part 11 environments with RC-WebView. RC WebView is easy-to-use, browser-based building management software that allows operators and administrators to efficiently manage any BACnet internet-connected building. RC WebView is purpose built to be a component of a Title 21 CFR Part 11–validated system for FDA-regulated processes and indoor environmental control.

Title 21 CFR Part 11 compliance features in RC-WebView

The following RC-WebView features align with the requirements of Title 21 CFR Part 11:

- Digitally signed audit logs to ensure authenticity
- Dual approval for system security and user account changes
- Printout watermark security option
- Automatic password expiry trigger after a specified number of days
- Option to lock out a user after a specified number of failed logon attempts
- Improved security support to include TLS 1.2

Tables 1 and 2 detail how RC-WebView provides compliance with Title 21 CFR Part 11, specifically regarding electronic records and signatures.

Table 1: Electronic records

Section	Title 21 CFR Part 11 requirements	Does RC-WebView provide compliance?	Notes
§11.10	**Controls for closed systems**		
	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:		
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	□ Yes □ No ☑ N/A	We factory-test RC-WebView to verify intended operation. However, system validation is unique in every case and must be carried out by the customer.
(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	☑ Yes □ No □ N/A	RC-WebView generates an audit trail for all operator actions that you can view, print, and export. View the audit trail locally using the browser user interface (BUI); send the audit trail to any printer connected to the network; and export it directly using RC-WebView. You can also view, print, and export all alarm history and configure printed records to include a watermark for security.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	☑ Yes □ No □ N/A	The audit trail and alarm history records are stored in a SQL Server database; you can view, print, and report them at any time throughout the records-retention period.

(d)	Limiting system access to authorized individuals.	☑ Yes □ No □ N/A	Assign each user with a unique ID and password a defined level of system access or control.
(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	☑ Yes □ No □ N/A	RC-WebView requires the operator's user ID and password to access the site, and an additional, unique approval password to validate the source of any data input or instruction.
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	☑ Yes □ No □ N/A	RC-WebView implements operational steps and sequencing as a function of controller logic. Use RC-WebView to control operator security levels that allow or deny system access.
(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	☑ Yes □ No □ N/A	Administrators fully manage user access in RC-WebView. User ID and password changes must be completed by a minimum of two administrators.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	☑ Yes □ No □ N/A	RC-WebView requires the operator's user ID and password to validate the source of any data input or instruction.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	□ Yes □ No ☑ N/A	Building administrators are responsible for hiring and training appropriate staff to perform assigned tasks. RC-WebView supports this requirement by validating that only users with appropriate security rights can access the system. As user roles change, RC-WebView allows you to manage security settings.
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	☑ Yes □ No □ N/A	RC-WebView complements any IT security policies that deter record and signature falsification by providing mandatory user re-authentication.
(k)	Use of appropriate controls over systems documentation including:		
(1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	☑ Yes □ No □ N/A	RC-WebView provides permission-based access to online help. Any other control system documentation can be provided by the installing party.
(2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	□ Yes □ No ☑ N/A	It is not possible to modify the control system operation and maintenance documentation using the RC-WebView BUI.
§11.30	**Controls for open systems**		

	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	□ Yes □ No ☑ N/A	A closed control system means system access is controlled by persons who are responsible for the content of the electronic records on that system. Administrators who require an open control system are responsible for establishing internal policies and procedures to meet Title 21 CFR Part 11 requirements.
§11.50	**Signature manifestations**		
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		
(1)	The printed name of the signer;	☑ Yes □ No □ N/A	The RC-WebView audit trail logs operator actions using their assigned user ID or, if required, their full name.
(2)	The date and time when the signature was executed; and	☑ Yes □ No □ N/A	The RC-WebView audit trail logs date and time.
(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	☑ Yes □ No □ N/A	The RC-WebView audit trail records operator actions to change system data (e.g., logging on, acknowledging alarms, changing setpoints). Operators must provide a reason for each change.
(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	☑ Yes □ No □ N/A	The RC-WebView audit trail shows the user ID, time, and action of all changes made to the system. You can view, print, and export the audit trail to any third-party tool.
§11.70	**Signature/record linking**		
	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	☑ Yes □ No □ N/A	RC-WebView records all changes to the system with the operator's user ID. Audit records include a digital thumbprint to prevent the falsification of records.

Table 2: Electronic signatures

Section	Title 21 CFR Part 11 requirements	Does RC-WebView provide compliance?	Notes
§11.100	**General requirements**		

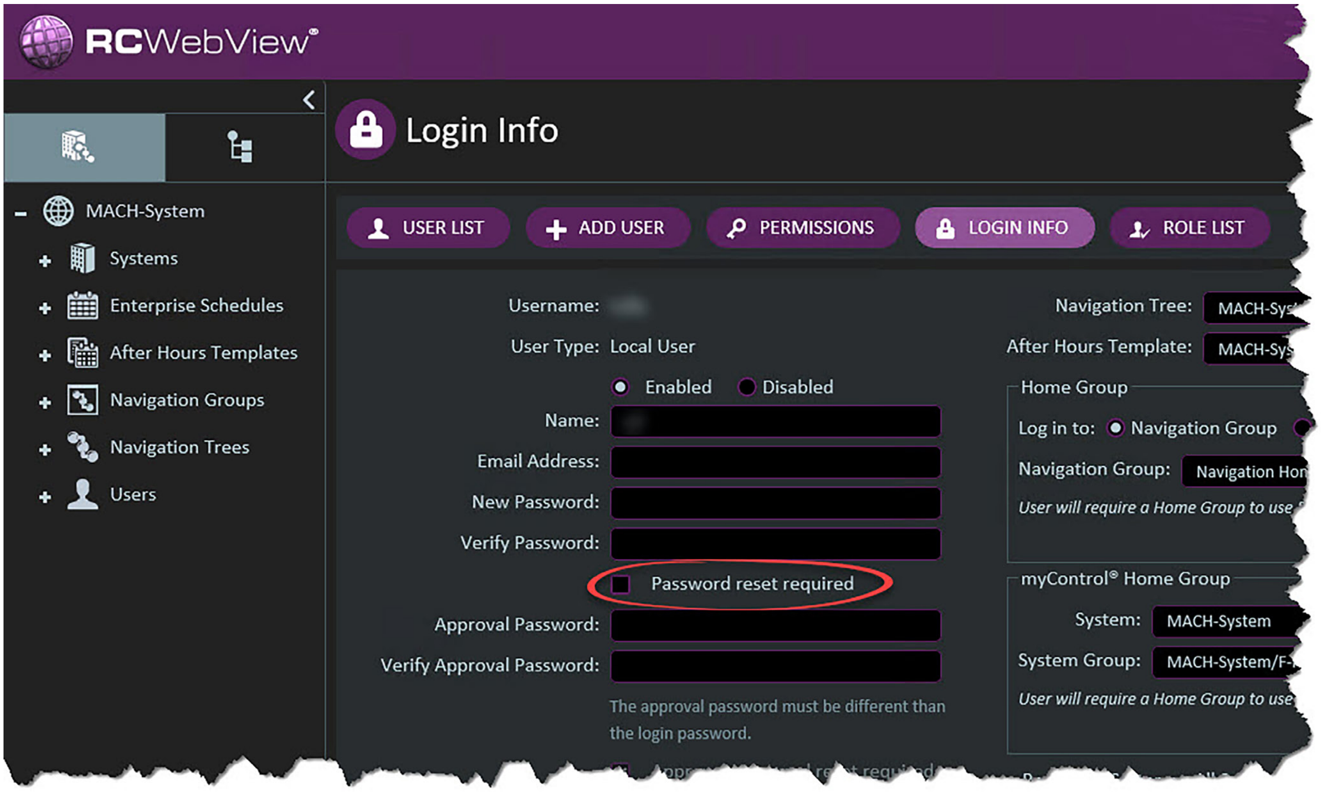
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	☑ Yes □ No □ N/A	Administrators have full control over user IDs and passwords and can develop policies and procedures to ensure user credentials are not reassigned. RC-WebView does not persist deleted user accounts or prevent account reuse.
(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	□ Yes □ No ☑ N/A	Always verify the identity of any user before assigning credentials.
(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	□ Yes □ No ☑ N/A	Administrators are responsible for notifying the FDA of their intention to recognize electronic signatures to be the legally binding equivalent of handwritten signatures.
(1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	□ Yes □ No ☑ N/A	Administrators are responsible for notifying the FDA of their intention to recognize electronic signatures to be the legally binding equivalent of handwritten signatures.
(2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	□ Yes □ No ☑ N/A	Administrators are responsible for notifying the FDA of their intention to recognize electronic signatures to be the legally binding equivalent of handwritten signatures.
§11.200	**Electronic signature components and controls**		
(a)	Electronic signatures that are not based upon biometrics shall:		
(1)	Employ at least two distinct identification components such as an identification code and password.	☑ Yes □ No □ N/A	RC-WebView requires two components for user identification: a user ID and password.
(i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	☑ Yes □ No □ N/A	RC-WebView requires complete user credentials on initial logon. The software prompts the user to re-authenticate their signature when they make the first change. They do not need to repeat this for subsequent changes during the same session within a system-specified time limit. RC-WebView prevents users from transferring a session to a second workstation.
(ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	☑ Yes □ No □ N/A	RC-WebView requires complete user credentials on initial logon. The software prompts the user to re-authenticate their signature when they make the first change. They do not need to repeat this for subsequent changes during the same session within a system-specified time limit. RC-WebView prevents users from transferring a session to a second workstation.

(2)	Be used only by their genuine owners; and	□ Yes □ No ☑ N/A	Administrators are responsible for ensuring the genuine user signs their electronic signature and that they do not disclose their password to others.
(3)	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	☑ Yes □ No □ N/A	RC-WebView requires two or more administrators to change a user's electronic signature. If a foreign party attempts to use a verified electronic signature, RC-WebView locks out the account.
(4)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	□ Yes □ No ☑ N/A	RC-WebView does not support biometric devices.
§11.300	**Controls for identification codes/passwords**		
	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:		
(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	☑ Yes □ No □ N/A	RC-WebView does not allow duplicate user IDs.
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	☑ Yes □ No □ N/A	Administrators can configure RC-WebView to automatically expire passwords at a certain date, by administrator lockout, or after invalid logon attempts.
(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	□ Yes □ No ☑ N/A	Administrators are responsible for implementing loss-management procedures.
(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	☑ Yes □ No □ N/A	RC-WebView automatically locks out users for attempted unauthorized access and automatically reports unauthorized attempts to administrators by email.
(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	□ Yes □ No ☑ N/A	Administrators' management procedures should include periodic testing or validation of any devices that may risk the integrity of a user's identification.

Passwords

Basic authentication establishes a user identity with reasonable assurance through a memorized secret authenticator such as a personal identification number or password. For the authenticator to be effective, it should be known only by the user. This means passwords should be kept secret even from administrators who create and maintain user accounts.

In the RC-WebView Login Info dialog box, administrators can select the Password Reset Required check box (Figure 1) to require a user to change their password the next time they log on. Requiring a password reset provides user accountability by allowing an administrator to create new account credentials while obfuscating the password. It can be used at any time to manually initiate a password reset as part of a standard security policy.



Username: [redacted]

User Type: Local User

● Enabled ○ Disabled

Name: [redacted]

Email Address:

New Password:

Verify Password:

□ Password reset required

Approval Password:

Verify Approval Password:

The approval password must be different than the login password.

Navigation Tree: MACH-Sys

After Hours Template: MACH-Sys

Home Group

Log in to: ● Navigation Group

Navigation Group: Navigation Hon

User will require a Home Group to use

myControl® Home Group

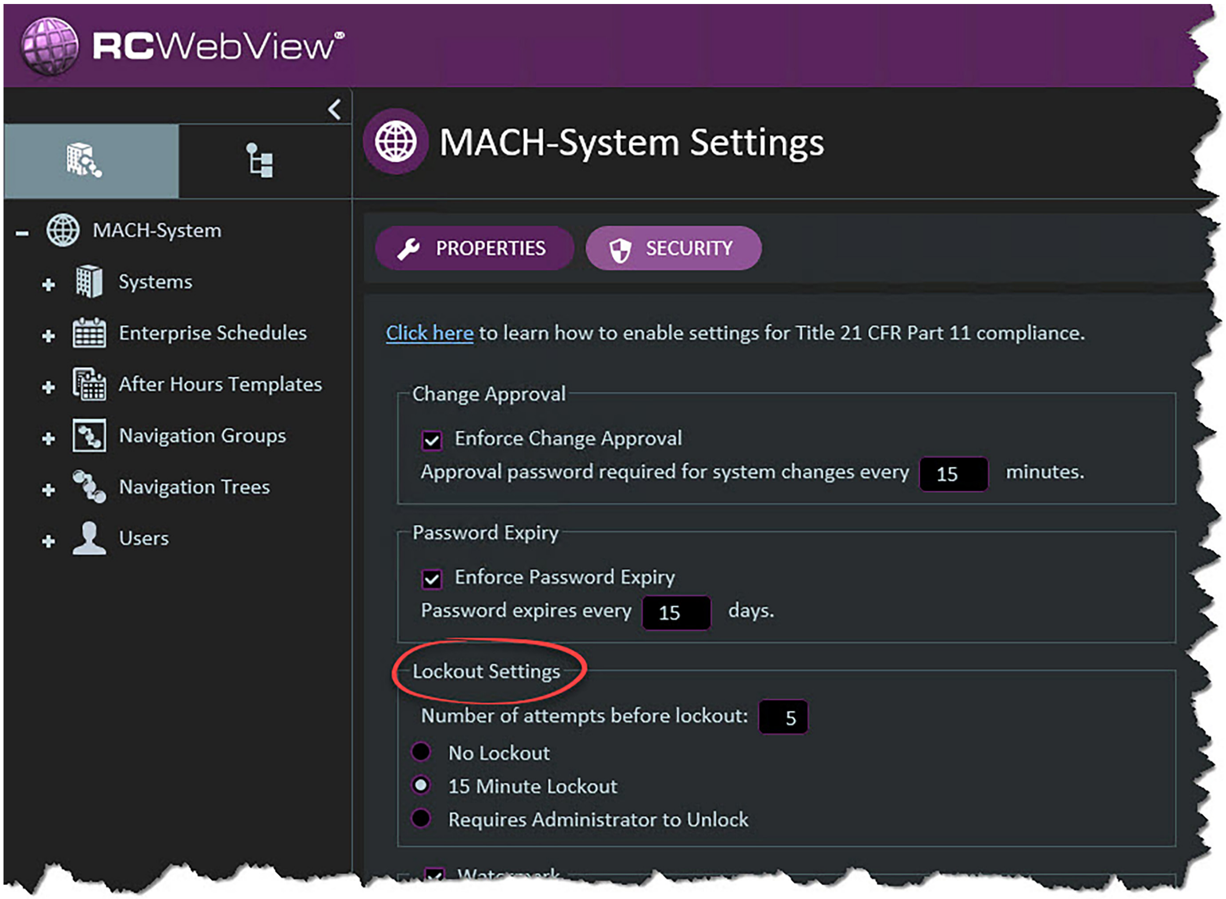
System: MACH-System

System Group: MACH-System/F-

User will require a Home Group to use

Figure 1: Password Reset Required check box in the RC-WebView Login Info page.

A brute-force attack is a trial-and-error method of guessing authentication mechanisms such as passwords. This approach can be high or low tech and is surprisingly effective. To prevent a brute-force attack and unauthorized system access, RC-WebView includes an optional password lockout function that automatically locks out a user account if an incorrect password is entered multiple times. Administrators can configure this function in the Enterprise Website Settings page (Figure 2).



MACH-System Settings

Click here to learn how to enable settings for Title 21 CFR Part 11 compliance.

Change Approval

☑ Enforce Change Approval

Approval password required for system changes every 15 minutes.

Password Expiry

☑ Enforce Password Expiry

Password expires every 15 days.

Lockout Settings

Number of attempts before lockout: 5

○ No Lockout

● 15 Minute Lockout

○ Requires Administrator to Unlock

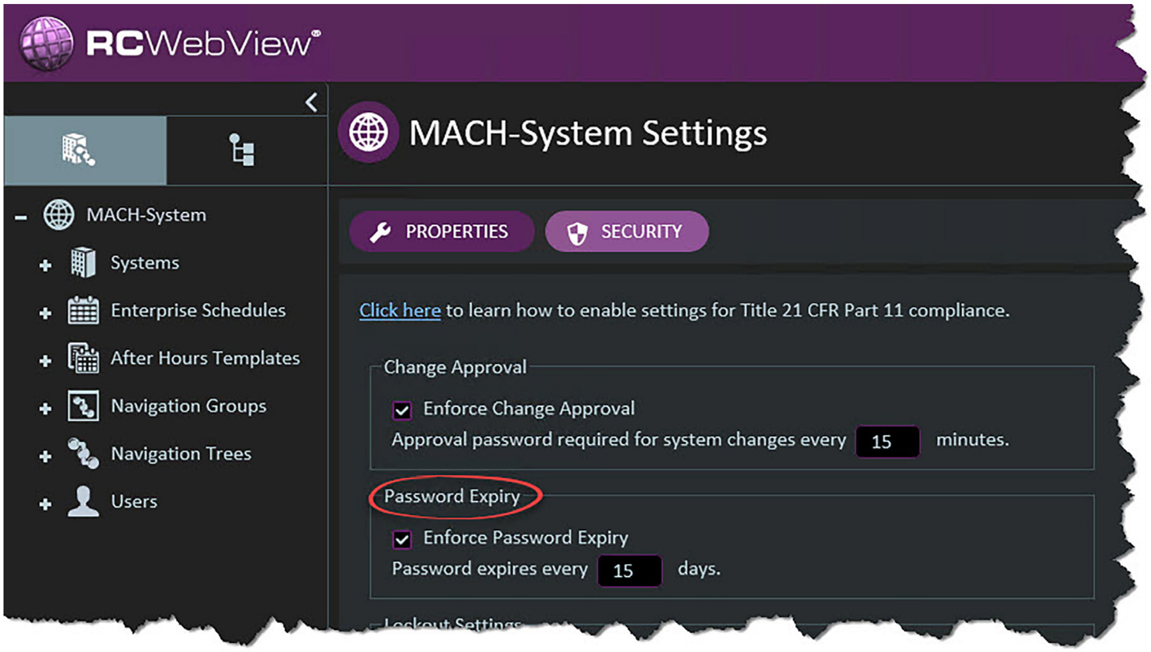
☑ Watermark

Figure 2: Lockout Settings area in the Enterprise Website Settings page in RC-WebView.

An administrator can set the number of permitted unsuccessful logon attempts before the user account is locked out. They can also select the 15 Minute Lockout check box to keep the user account locked out for 15 minutes once the number of permitted logon attempts is exceeded. Alternatively, the user account can be locked out indefinitely if the administrator selects the Requires Administrator to Unlock check box.

Password expiry requires that users periodically change their passwords. If a password has been exposed to an unauthorized party, the threat is automatically mitigated when the user updates their authenticator. In RC-WebView, administrators can configure password expiry in the Enterprise Website Settings page.

Selecting the Enforce Password Expiry check box requires users to change their password at the interval specified in the Password Expires Every < > Days box (Figure 3). For example, users could be forced to change their password every 90 or 180 days.



RCWebView®

MACH-System Settings

- MACH-System
  - + Systems
  - + Enterprise Schedules
  - + After Hours Templates
  - + Navigation Groups
  - + Navigation Trees
  - + Users

PROPERTIES | SECURITY

Click here to learn how to enable settings for Title 21 CFR Part 11 compliance.

Change Approval

☑ Enforce Change Approval

Approval password required for system changes every 15 minutes.

Password Expiry

☑ Enforce Password Expiry

Password expires every 15 days.

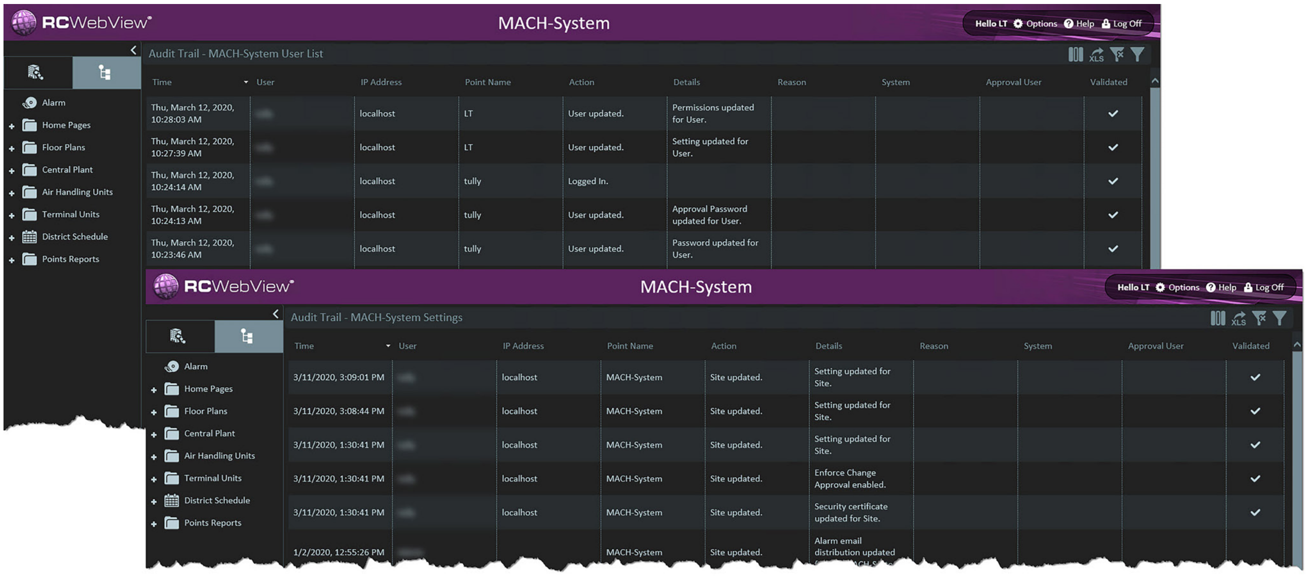
Lockout Settings

Figure 3: Password Expiry area in the Enterprise Website Settings page in RC-WebView.

Audit trail

RC-WebView tracks and records all user activity in an audit trail. For ease of access, the audit trail automatically filters entries relative to the context of the active view. If an auditor wants to review or audit any changes made to user accounts and permissions, they can navigate to the User List page and open the Audit Log worksheet. All changes to user accounts, including those made by adminstrators, are displayed.

If an auditor wants to review changes made to the Enterprise Website, such as security settings, they can navigate to the Enterprise Website Settings page and open the Audit Trail worksheet. All changes made to the website configuration, again including those made by administrators, are displayed (Figure 4). An auditor can click the Clear All Filters icon to view comprehensive audit trail.



RCWebView® MACH-System — Hello LT · Options · Help · Log Off

- Alarm
- + Home Pages
- + Floor Plans
- + Central Plant
- + Air Handling Units
- + Terminal Units
- + District Schedule
- + Points Reports

Audit Trail - MACH-System User List

Time	User	IP Address	Point Name	Action	Details	Reason	System	Approval User	Validated
Thu, March 12, 2020, 10:28:03 AM	[redacted]	localhost	LT	User updated.	Permissions updated for User.				✓
Thu, March 12, 2020, 10:27:39 AM	[redacted]	localhost	LT	User updated.	Setting updated for User.				✓
Thu, March 12, 2020, 10:24:14 AM	[redacted]	localhost	tully	Logged In.					✓
Thu, March 12, 2020, 10:24:13 AM	[redacted]	localhost	tully	User updated.	Approval Password updated for User.				✓
Thu, March 12, 2020, 10:23:46 AM	[redacted]	localhost	tully	User updated.	Password updated for User.				✓

RCWebView® MACH-System — Hello LT · Options · Help · Log Off

- Alarm
- + Home Pages
- + Floor Plans
- + Central Plant
- + Air Handling Units
- + Terminal Units
- + District Schedule
- + Points Reports

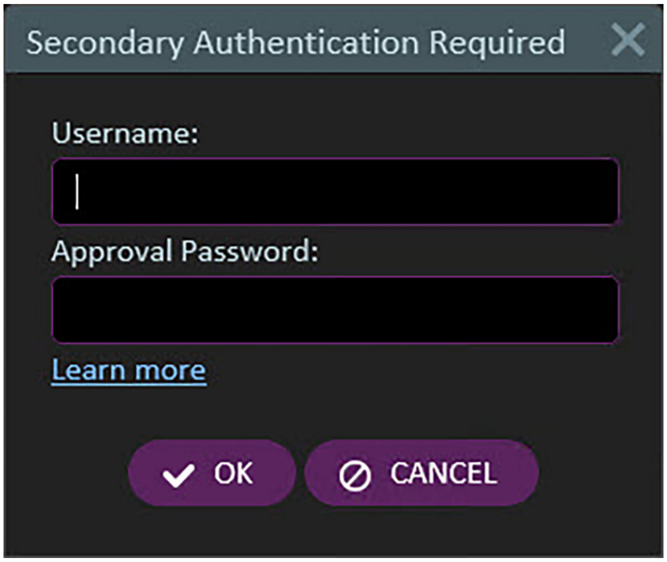
Audit Trail - MACH-System Settings

Time	User	IP Address	Point Name	Action	Details	Reason	System	Approval User	Validated
3/11/2020, 3:09:01 PM	[redacted]	localhost	MACH-System	Site updated.	Setting updated for Site.				✓
3/11/2020, 3:08:44 PM	[redacted]	localhost	MACH-System	Site updated.	Setting updated for Site.				✓
3/11/2020, 1:30:41 PM	[redacted]	localhost	MACH-System	Site updated.	Setting updated for Site.				✓
3/11/2020, 1:30:41 PM	[redacted]	localhost	MACH-System	Site updated.	Enforce Change Approval enabled.				✓
3/11/2020, 1:30:41 PM	[redacted]	localhost	MACH-System	Site updated.	Security certificate updated for Site.				✓
1/2/2020, 12:55:26 PM	[redacted]		MACH-System	Site updated.	Alarm email distribution updated				

Figure 4: RC-WebView Audit Trail worksheet, automatically filtered to display user list and site settings activity.

To improve administrative accountability, RC-WebView requires dual approval for changes to website security settings as well as logon and approval passwords. When an administrator saves a security change, a second administrator is prompted to provide an approval password (Figure 5).

For organizations that must comply with Title 21 CFR Part 11, a two-step process is required to authenticate changes to the OT system, its data, and records. Users who are authorized to manipulate the system are required to provide two passwords: one to log on to the system and another to commit any changes. This fail-safe means a malicious user would need to compromise two unique passwords to effect any change in the OT system.


Secondary Authentication Required

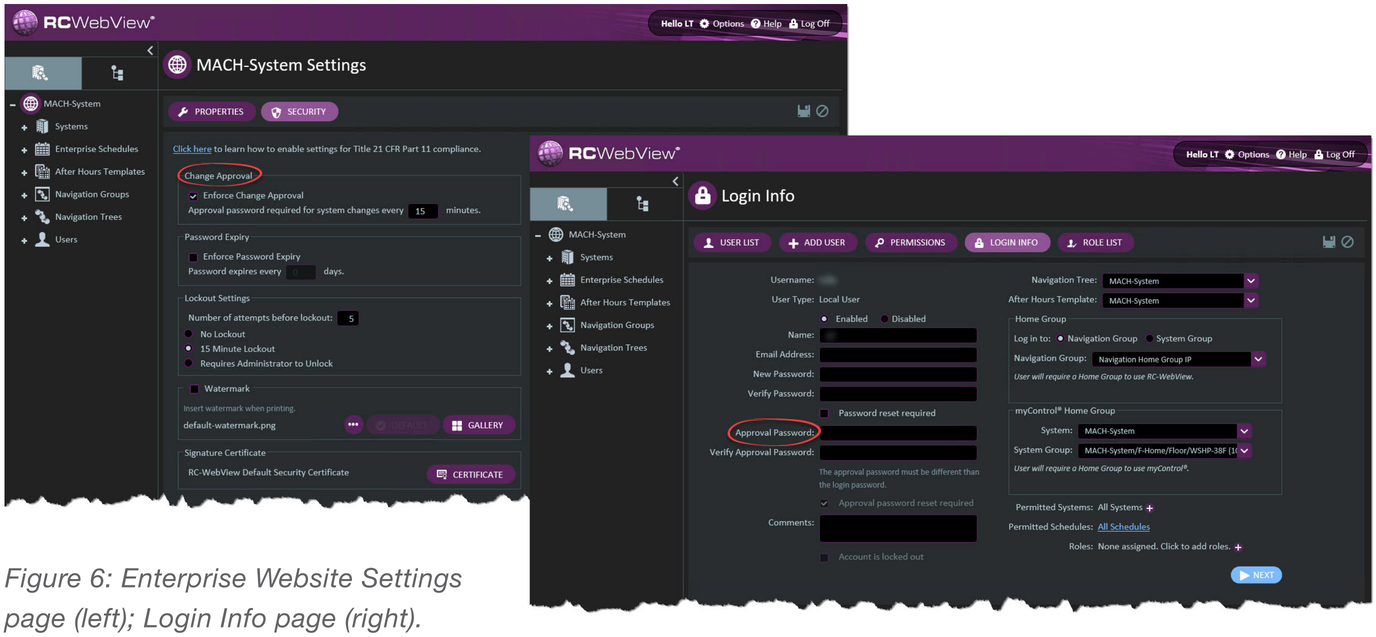
Username:

Approval Password:

Learn more

Figure 5: RC-WebView Secondary Authentication Required dialog box.

In RC-WebView, this two-step change approval process is set up in the Enterprise Website Settings page (Figure 6). If the Enforce Change Approval check box is selected in the Login Info page (Figure 6), a valid approval password and reason must be entered any time a change is made to the OT system using the BUI (Figure 7). By default, when this check box is selected, the Approval Password box displays in the Login Info page (Figure 6), and by default the Password Reset Required check box is automatically selected.



MACH-System Settings

Click here to learn how to enable settings for Title 21 CFR Part 11 compliance.

Change Approval

☑ Enforce Change Approval

Approval password required for system changes every 15 minutes.

Password Expiry

□ Enforce Password Expiry

Password expires every 0 days.

Lockout Settings

Number of attempts before lockout: 5

○ No Lockout

● 15 Minute Lockout

○ Requires Administrator to Unlock

□ Watermark

Insert watermark when printing.

default-watermark.png

Signature Certificate

RC-WebView Default Security Certificate

Login Info

Username: [redacted]

User Type: Local User

● Enabled ○ Disabled

Name: [redacted]

Email Address:

New Password:

Verify Password:

□ Password reset required

Approval Password:

Verify Approval Password:

The approval password must be different than the login password.

☑ Approval password reset required

Comments:

□ Account is locked out

Navigation Tree: MACH-System

After Hours Template: MACH-System

Home Group

Log in to: ● Navigation Group ○ System Group

Navigation Group: Navigation Home Group IP

User will require a Home Group to use RC-WebView.

myControl® Home Group

System: MACH-System

System Group: MACH-System/F-Home/Floor/WSHP-38F (1(

User will require a Home Group to use myControl®.

Permitted Systems: All Systems +

Permitted Schedules: All Schedules

Roles: None assigned. Click to add roles. +

Figure 6: Enterprise Website Settings page (left); Login Info page (right).

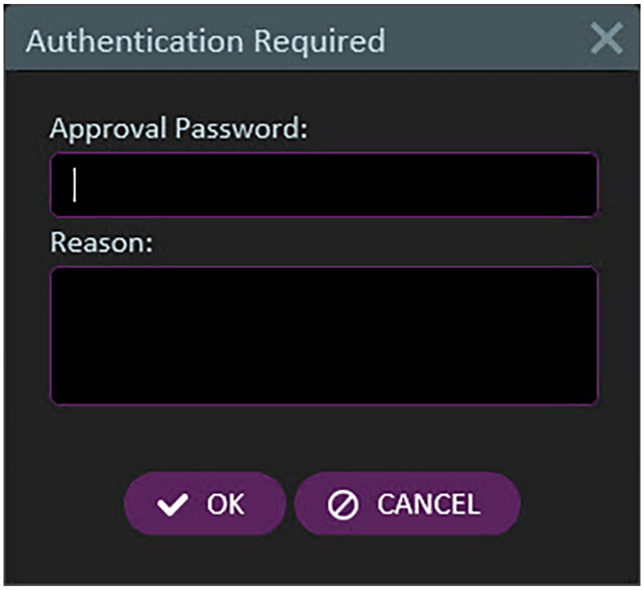
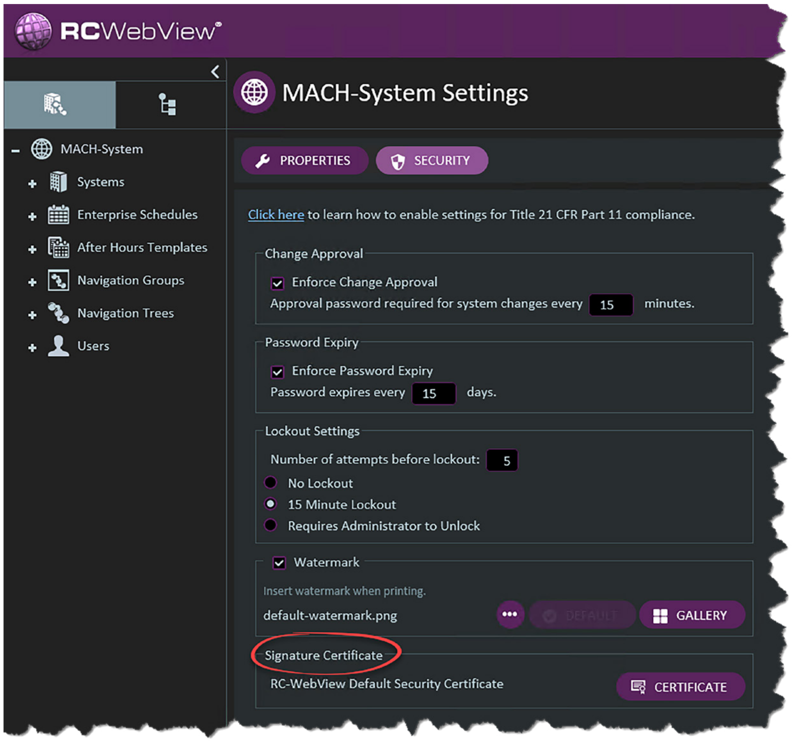


Figure 7: Authentication Required dialog box for change approval in RC-WebView.

The next time a user with the authority to manipulate the system logs on, they are prompted to enter an approval password. As with user account passwords, administrators can set the approval password directly and initiate a manual reset as required. An administrator can also define a grace period for making changes. The Approval Password Required for System Changes Every < > Minutes box (Figure 8) defines the amount of time in which a user can make changes following successful change authentication using the approval password. Where authentication is not required for every change, this feature means a user can execute several changes with a single authorization within a set period of time.

Data integrity

By using a digital signature certificate, RC-WebView validates that log data have not been manipulated outside the software. RC-WebView automatically creates a default signature certificate that OT administrators can use to implement their own certificate. Digital signature certificates are managed in the Enterprise Website Settings page (Figure 8).



MACH-System Settings

Click here to learn how to enable settings for Title 21 CFR Part 11 compliance.

Change Approval

☑ Enforce Change Approval

Approval password required for system changes every 15 minutes.

Password Expiry

☑ Enforce Password Expiry

Password expires every 15 days.

Lockout Settings

Number of attempts before lockout: 5

○ No Lockout

● 15 Minute Lockout

○ Requires Administrator to Unlock

☑ Watermark

Insert watermark when printing.

default-watermark.png

Signature Certificate

RC-WebView Default Security Certificate

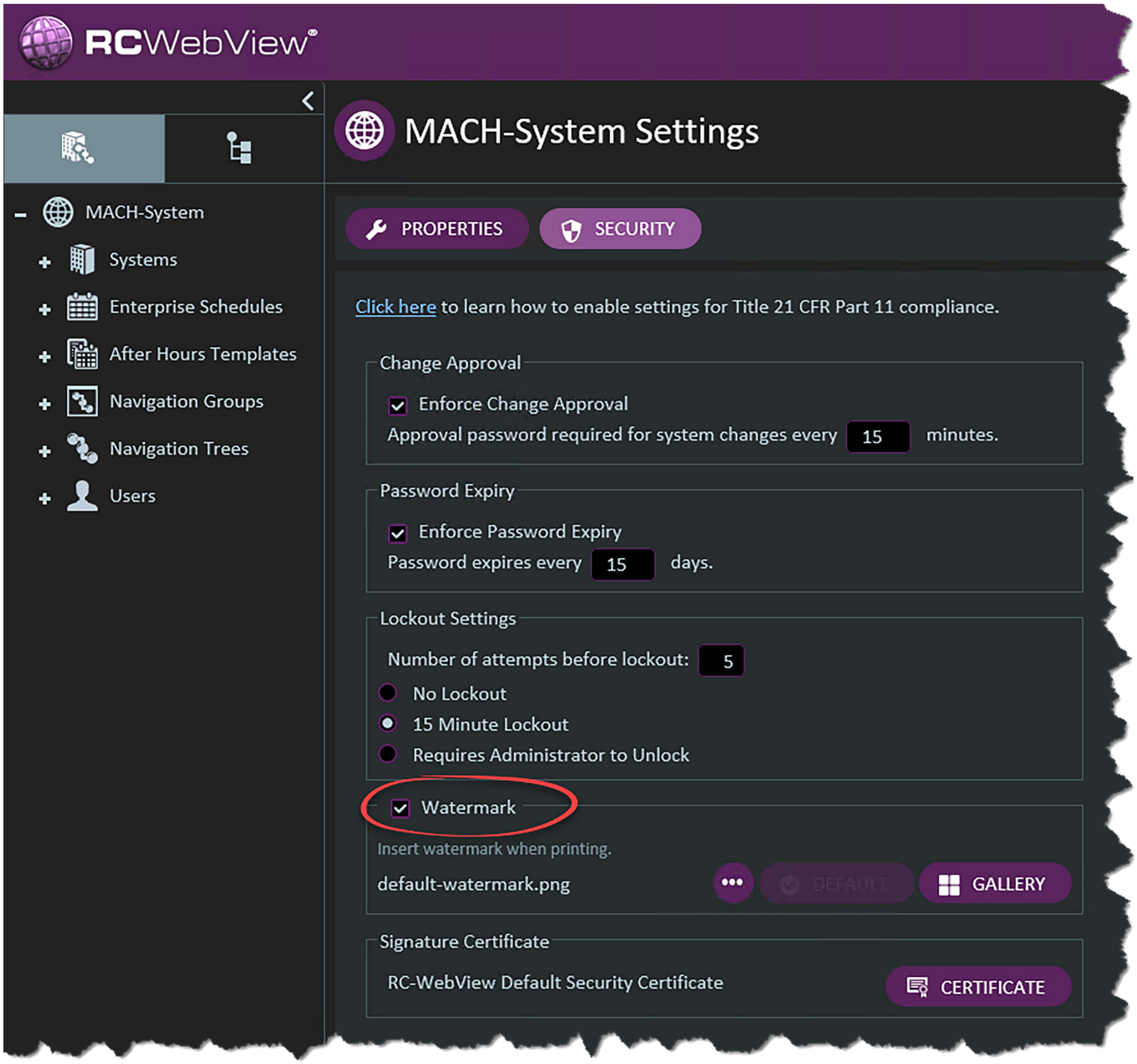
Figure 8: Signature Certificate area in the Enterprise Website Settings page in RC-WebView.

Data validation is visible in two ways:

- The Validated column in the Audit Trail worksheet displays a check mark for all validated records of operator activity.
- The signature certificate is used to digital sign Excel exports of audit trail and historical logs. A signed Excel workbook contains a data sheet, including the information from the log, and a signature sheet that details the digital validation.

Using the information in the signature certificate, an auditor can validate the authenticity of the entries.

Adding a watermark to an image is a security mechanism that makes it difficult to graphically manipulate digital files without detection. An administrator can select the Watermark check box in the Enterprise Settings page (Figure 9) to superimpose a watermark over all files printed directly from the BUI (Figure 10).



MACH-System Settings

Click here to learn how to enable settings for Title 21 CFR Part 11 compliance.

Change Approval

☑ Enforce Change Approval

Approval password required for system changes every 15 minutes.

Password Expiry

☑ Enforce Password Expiry

Password expires every 15 days.

Lockout Settings

Number of attempts before lockout: 5

○ No Lockout

● 15 Minute Lockout

○ Requires Administrator to Unlock

☑ Watermark

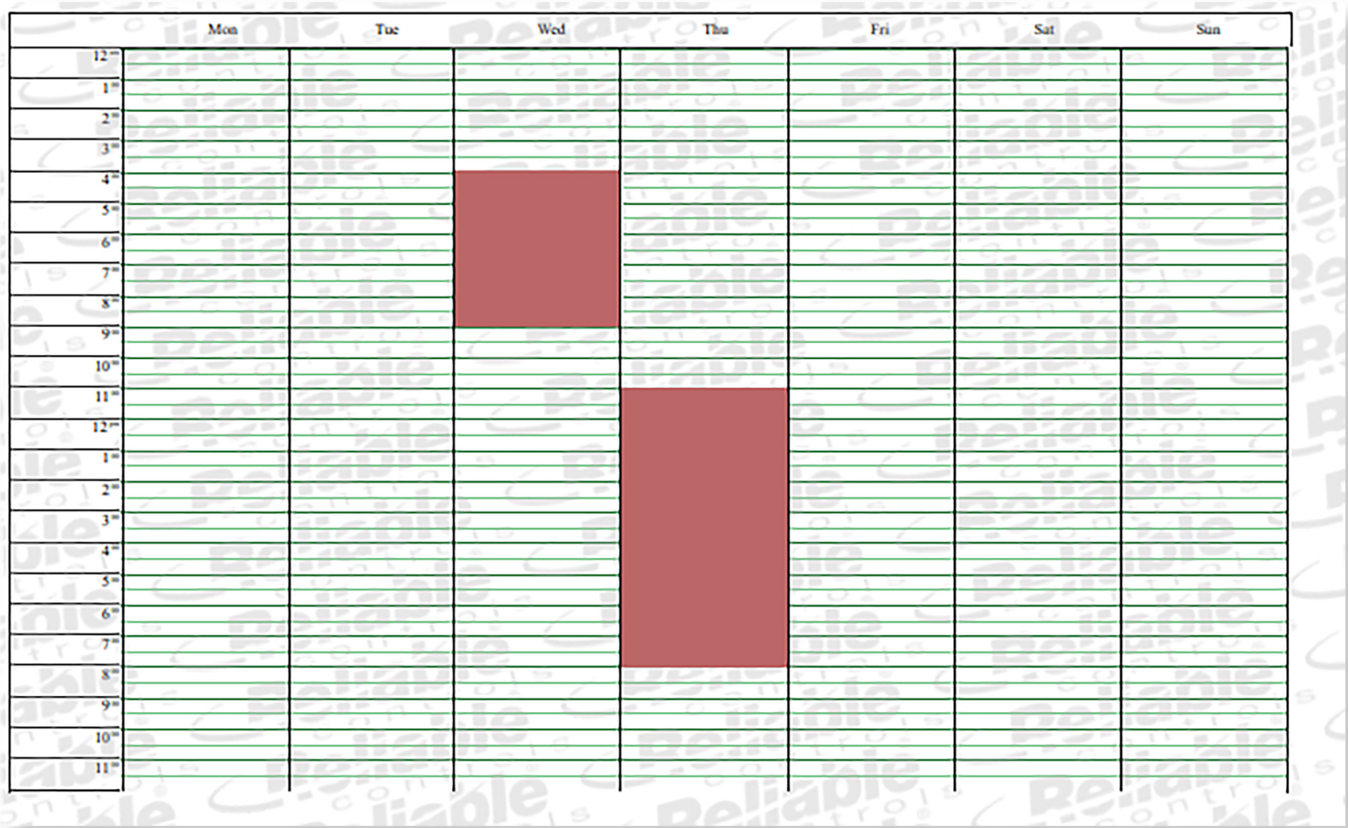
Insert watermark when printing.

default-watermark.png

Signature Certificate

RC-WebView Default Security Certificate

Figure 9: Watermark check box in the Enterprise Website Settings page.



	Mon	Tue	Wed	Thu	Fri	Sat	Sun
12am							
1am							
2am							
3am							
4am			🟥				
5am			🟥				
6am			🟥				
7am			🟥				
8am			🟥				
9am							
10am							
11am				🟥			
12pm				🟥			
1pm				🟥			
2pm				🟥			
3pm				🟥			
4pm				🟥			
5pm				🟥			
6pm				🟥			
7pm				🟥			
8pm							
9pm							
10pm							
11pm							

Figure 10: File with a watermark printed from RC-WebView.

RC-WebView provides a default watermark image, but administrators can choose a custom image if desired. RC WebView resizes the image and repeats it with transparency across the page at an angle.

Summary

This paper summarizes combined experiences of authors over 20 years in the building controls industry. It does not cover all aspects of Title 21 CFR Part 11 but describes how RC-WebView software from Reliable Controls provides an accountable BUI for OT systems that is simple, flexible, and sustainable. Reliable Controls Authorized Dealers are ideally equipped to ease the burden on built-environment professionals in regulated industries with assurance that their electronic data is accurate and available.

Reliable Controls develops innovative and dependable building controls that help facility professionals operate their buildings in an environmentally responsible way. Our outstanding customer loyalty stems from our ability to be good listeners and to deliver practical, easy-to-use building solutions that provide an excellent return on investment, year over year. We are proud to have achieved ISO 9001 and 14001 certifications for our quality and environmental management processes. For more information about Reliable Controls, please visit reliablecontrols.com.

Contact us

reliablecontrols.com/help/contact

SYSTEM VALIDATION * * * FULL DATA SECURITY * * * RISK ASSESSMENT * * * WORLD CLASS IT * * *
FDA 21 CFR Part 11 Compliance

We reserve the right to make technical changes to the products or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. Reliable Controls Corporation does not assume any responsibility for any errors or incomplete information in this document.

Better by design™

Reliable® controls