Supervisory Controller Password Management

Secure Your Operations: Essential Password Management for Supervisory Controllers

Effective password management is crucial for maintaining the security, integrity, and reliable operation of your Supervisory Controllers at each site. This document outlines your responsibilities in creating and managing passwords, ensuring that authorized personnel can access these critical systems when needed, while preventing unauthorized access.

This guide is based on industry best-practices, see *NIST SP 800-82* for more information

https://csrc.nist.gov/pubs/sp/800/82/r3/final

As our valued customer, you play a vital role in the first line of defense for your operational technology. Proper password hygiene on your Supervisory Controllers is fundamental to protecting your systems from potential disruptions, unauthorized adjustments, and data breaches.

Quick Summary for Reference

Change default passwords —> create temp admin —> delete temp admin —> store credentials in vault —> rotate annually or on compromise

Your Core Responsibility: Site-Level Password Management

For each Supervisory Controller installed at your sites, your organization is responsible for:

- **Creating Strong, Unique Passwords:** Upon commissioning and on an ongoing basis, ensure that all default passwords are changed. Passwords should be robust, incorporating a mix of uppercase and lowercase letters, numbers, and special characters. Avoid easily guessable passwords or common phrases. Each controller should ideally have a unique password.
- **Securely Managing and Distributing Site Passwords:** Establish a secure internal process for storing and distributing these site-specific controller passwords. Access should be granted on a need-to-know basis to trusted members of your local team who require it for their duties.
- **Regularly Reviewing and Updating Passwords:** Implement a schedule for annual password changes as recommended in the NIST guidelines. Passwords should also be changed immediately if there is any suspicion of compromise or when an individual with access leaves your employment or changes roles.
- **Controlling Access:** Maintain a log or system to track who has access to controller passwords. Ensure that when personnel change roles or leave the company, their access is promptly revoked by changing the relevant passwords.
- **Crucial Responsibility for Password Retention:** The responsibility for maintaining and being able to supply the necessary password(s) to authorized technicians or contractors for access rests with your organization. Failure to maintain access to these passwords will result in significant delays and costs to regain system access, potentially requiring a full controller clean out and reprogramming.

026-4293 R0

COPELAND

Initial System Setup and Startup Procedure

The proper setup and commissioning of your Supervisory Controllers is vital for their performance and security. Please note the following procedure regarding administrative access during this phase:

1. **First time login:** Upon its very first power-up, the controller will start in a "Setup in Progress" mode. The first required action is for the system to prompt you to set a new password that meets complexity requirements. This initial step establishes the first System Administrator account, which must then be used to create a permanent admin account for the end-user customer.

2. **Requirement for Administrative Access:** During the initial startup and commissioning, the installing contractor or technician will need administrative-level privileges on the Supervisory Controller. This access is essential for configuring core system settings, including network parameters (IP address, subnet mask, gateway) and communication port settings necessary for the controller to function correctly within your infrastructure.

3. **Creating a Temporary Administrative Account:**
   - The startup personnel are instructed to create a user account with System Administrator-level privileges. This account should be secured with a strong, unique password. Once system startup is complete, this account is to be deleted.

4. **Mandatory Disablement of Startup Admin Account:**

   a. **This is a critical security measure:** Once the initial startup procedures are finalized, all necessary configurations are complete, and the system's operational status has been verified, **the Primary System Administrator MUST delete the Startup System Administrator account created for startup purposes.**

   b. Leaving this account active poses an unnecessary security risk.

5. **Transition to Ongoing Management:** Following startup, all administrative access should transition to the corporate-managed System Administrator credentials or other formally established and securely managed site-specific administrative accounts, adhering to the Principle of Least Privilege.

Understanding Role-Based Access and Corporate-Managed Passwords

To enhance security and ensure appropriate access levels, certain user accounts associated with specific roles will have passwords managed by [Your Company Name/Corporate IT] and distributed to designated individuals within your organization or to authorized third parties. This approach adheres to the **Principle of Least Privilege**, meaning users are only granted access to perform their specific job functions.

Below are the defined personas and the general scope of their access facilitated by these corporate-managed credentials:

1. **Store Manager (or designated site lead):**
   - Typical Responsibilities: Monitoring overall system status, viewing key performance indicators (for example, temperatures, energy usage), receiving alerts, and understanding the general operational health of the systems.
   - General Scope of Access: Typically monitoring access (view-only). This role is generally restricted from making system configuration changes or overriding critical operational setpoints. The password for this persona will be managed by the corporation and distributed to the designated Store Manager.
2. **Maintenance Staff (your internal technical team):**
   - Typical Responsibilities: Performing routine maintenance, troubleshooting operational issues, responding to alarms, adjusting operational setpoints within approved limits, and conducting diagnostics.
   - General Scope of Access: Access to operational parameters and diagnostic tools. This role may have the ability to make limited adjustments necessary for daily operations and upkeep. The password for this persona will be managed by corporate and distributed to authorized maintenance personnel.
3. **Contractor (authorized third-party service provider):**
   - **Typical Responsibilities:** Providing specialized maintenance, troubleshooting complex problems beyond the scope of internal staff, performing system repairs, or conducting planned upgrades.
   - **General Scope of Access:** Access is typically granted for specific tasks and limited durations. Permissions will be sufficient to perform the required work, which may include more in-depth system interaction than regular maintenance staff. The password for this persona will be managed by the corporation and distributed securely to the approved contractor for the duration of their engagement.

4. **System Administrator (designated internal):**
   - Typical Responsibilities: Full system oversight, software updates, user account management, advanced configuration changes, network settings, and high-level troubleshooting. This role is also invoked temporarily by startup personnel as outlined in the "Initial System Setup and Startup Procedure" section.

General Scope of Access: Comprehensive administrative access. This role has the highest level of permissions and is responsible for the overall health and security configuration of the supervisory controllers. The password for the ongoing System Administrator persona is managed by and is the responsibility of the control network or corporate network owner.

Important Note on Corporate-Managed Passwords:

- These passwords will be communicated through secure channels to the appropriate individuals based on their role.
- It is critical that these corporate-distributed passwords are not shared by the designated recipients with unauthorized individuals.
- If a designated individual changes role or leaves the company, the System Administrator must be notified immediately so that access can be revoked and passwords updated.

Best Practices for Your Internal Password Management

For any passwords you create and manage directly at the site level (complementary to the corporate-managed persona accounts), please adhere to the following:

- **Complexity and Length:** Aim for passwords that are at least 12-16 characters long.
- **Uniqueness:** Avoid using the same password across multiple controllers or other systems.
- **Confidentiality:** Do not write passwords down in easily accessible locations. Consider using a secure password manager if appropriate for your environment.
- **No Sharing of Individual Credentials:** If individual logins are used on controllers beyond the corporate personas, each user should have their own unique credential.
- **Awareness and Training:** Ensure your staff understands the importance of password security and these procedures.

CRITICAL WARNING: Password Recovery and Access

- It is imperative to understand that **Copeland is not responsible for maintaining secure password access. Please ensure that your organization is prepared to manage and provide secure passwords for Supervisory controller access to authorized uses in order to avoid service, installation, and maintenance interruptions.**
- **Sole Responsibility:** Your organization is solely responsible for the secure management, storage, and retention of all passwords configured on your controllers.
- **Access for Service:** You must be able to provide the current, correct password to any authorized internal maintenance staff, technicians, or third-party contractors requiring access to the controller for service, maintenance, or troubleshooting.
- **Consequences of Lost Passwords:** If a password is lost, regaining access may be difficult, time-consuming, and could lead to significant system downtime. Failure to maintain access to these passwords will result in significant delays and costs to regain system access, potentially requiring a full controller clean-out and reprogramming. Such delays could result in days of lost service, travel time, and expenses of thousands of dollars.

Please ensure robust internal procedures are in place for password documentation and secure storage to prevent loss of access.

Your Commitment to Security

By diligently managing passwords for your Supervisory Controllers, you significantly contribute to the overall security and resilience of your operations. This includes both the passwords you create and manage locally and the careful handling of corporate-distributed passwords for specific personas, as well as the secure management of temporary accounts during startup.

We are committed to supporting you in these efforts. Should you have any questions regarding password management or the access levels for different personas, please do not hesitate to contact your account representative or our technical support team.

Together, we can ensure your systems remain secure and operate efficiently.

Visit our website at copeland.com/en-us/products/controls-monitoring-systems for the latest technical documentation and updates.
For Technical Support call **833-409-7505** or email **ColdChain.TechnicalServices@Copeland.com**

026-4293 R0

COPELAND