18380-00
3.26.2020

METER

SKALA® SYSTEM USER SECURITY GUIDE

Updated: March 2020

SKALA SECURITY BASICS

SKALA has been built with security as a priority and to protect data and applications. Enhanced security options can be enabled to reflect the structure and needs of a specific organization. Protecting data is a joint responsibility between the customer and METER. SKALA security features enable customers to empower users to do their jobs safely and effectively.

Implement the security controls that are appropriate for the sensitivity of the data.

PHISHING

Phishing is a social engineering process aimed at collecting sensitive data from end users, including, but not limited to, information such as user names, passwords, credit card details, and other sensitive information. These attacks can occur through email, text messaging, voice calls, and other avenues. METER employees will never email or call asking for login credentials, so please do not reveal them to anyone. Please report suspicious emails or activities in SKALA directly to support.skala@metergroup.com.

WHAT SKALA IS DOING ABOUT PHISHING

METER views security as a critical aspect of customer success, and accordingly, the SKALA team continues to implement and enhance the software's security posture. Recent and ongoing efforts include, but are not limited to, the following.

- METER reviews and monitors logs to enable proactive alerts regarding potential system and security issues.
- METER works with leading security vendors and experts on identifying and utilizing the most effective security controls and tools.
- METER performs ongoing internal security education and engagement activities for internal employees.
- METER creates development processes that treat security as a first order design element.

WHAT SKALA IS DOING ABOUT PHISHING

In addition to internal security efforts, METER recommends customers implement the following changes to enhance security.

- Implement two-factor techniques to restrict access to the network.
- Educate users about suspect emails and how to identify and report Phishing attempts.
- Use security solutions from leading vendors.
- Designate a security contact within the organization so that METER can more effectively communicate with you. Please contact your SKALA representative with this information.

METER has a security incident response team to respond to any security issues. To report a security incident or vulnerability to METER, contact support.skala@metergroup.com. Please describe the issue in detail, and the team will respond promptly.

AUDITING

SKALA provides an audit or event log interface, which includes information regarding use of the SKALA platform. These audit trails can be instrumental in understanding and diagnosing potential or real security issues. The audit features do not secure the organization, so someone in the organization should perform regular audits to detect potential abuse.

To verify the security of the SKALA system, METER recommends performing periodic audits to monitor for unexpected changes or usage trends.

The SKALA system logs the following events for auditing and security purposes:

Failed Login Attempt
Successful Login
Changes to User
Changes to Reading
Changes to Product
Changes to Product Group
Changes to Batch
Changes to Instrument
COA Generation
Changes to Manual Reading Type
Changes to Corrective Action
Changes to HACCP
Changes to Location
Changes to reports
Changes to Customer
Changes to Repair Record
Successful Calibration Certificate Sync
Failed Calibration Certificate Sync
Changes to Reports, Finalized Device Certificate
Calibration Certificate Uploaded
Changes to Cycle

AUTHENTICATE USERS

Authentication is the method that ensures that users only access the SKALA system when authorized to do so.

METER has designed SKALA to support a variety of authentication methods including passwords, pins, and RFID hardware allowing SKALA use in the way that works best in each user's environment.

METER recommends reviewing these options described below and selecting the configuration that best meets user security needs.

PASSWORD AND PIN

SKALA provides all SKALA users with a unique login and a corresponding unique password and/or Pin. This information must be entered by the user to access the system. Administrators can configure a number of aspects related to users authentication systems, which helps ensure that users utilize secure passwords.

OPTIONAL SITEWIDE SECURITY SETTINGS

(Optional) Expiration Policies for Passwords and Pins

The password and pin expiration setting forces a password expiration and reset after the assigned period of time.

- 90 days
- 180 days
- 265 days

(Optional) Auto-Logout Timing When Inactive

The optional inactivity time-out settings are applied when a given user is inactive in the SKALA system. These settings help improve accountability by ensuring that the active user is the user that signed in.

- 1 minute
- 2 minute
- 5 minute
- 10 minute

(Optional) Minimum Password and Pin Requirements

This setting increases the minimum requirements to 5-digit pins and 8-digit passwords, with additional restrictions related to repeating digits in the PIN.

(Optional) RFID Support for Authentication

SKALA supports HID/RFID authentication, allowing users to enter the SKALA system using a fob, ID badge, or other RFID/HID compatible identifier.