ELEVATED RIGHTS MANAGER

soterion

EPI·USE LABS
value through innovation

Granting Sensitive Access in a Safe and Structured Environment

From time to time, users need temporary or emergency access for a limited period - often called **firefighter access**. This module allows you to do this effortlessly, while adhering to audit requirements.

Soterion's Elevated Rights Manager grants sensitive access in an automated workflow-driven process, and enables your management team to perform a structured review of any activities that were performed during the Elevated Rights Access check-out period.

Our Process

The Elevated Rights Manager can be tailored to your specific business environment. Elevated Rights Access may be granted to either a role or to an SAP user.

Elevated Rights Roles
Wide access roles can be assigned to pre-approved SAP Users when performing a check out. The particular SAP user will use their SAP User ID to perform the required activities in SAP.

Elevated Rights SAP Users
An SAP user account containing requisite wide access will be unlocked, and the password will be sent to a pre-approved entitled SAP User. The relevant SAP User account will be used to perform the necessary activities in SAP.

Define and map users to Elevated Rights Access

User checks out Elevated Rights Access

User performs emergency activities in SAP

User checks in Elevated Rights Access

Reviewer validates SAP activities
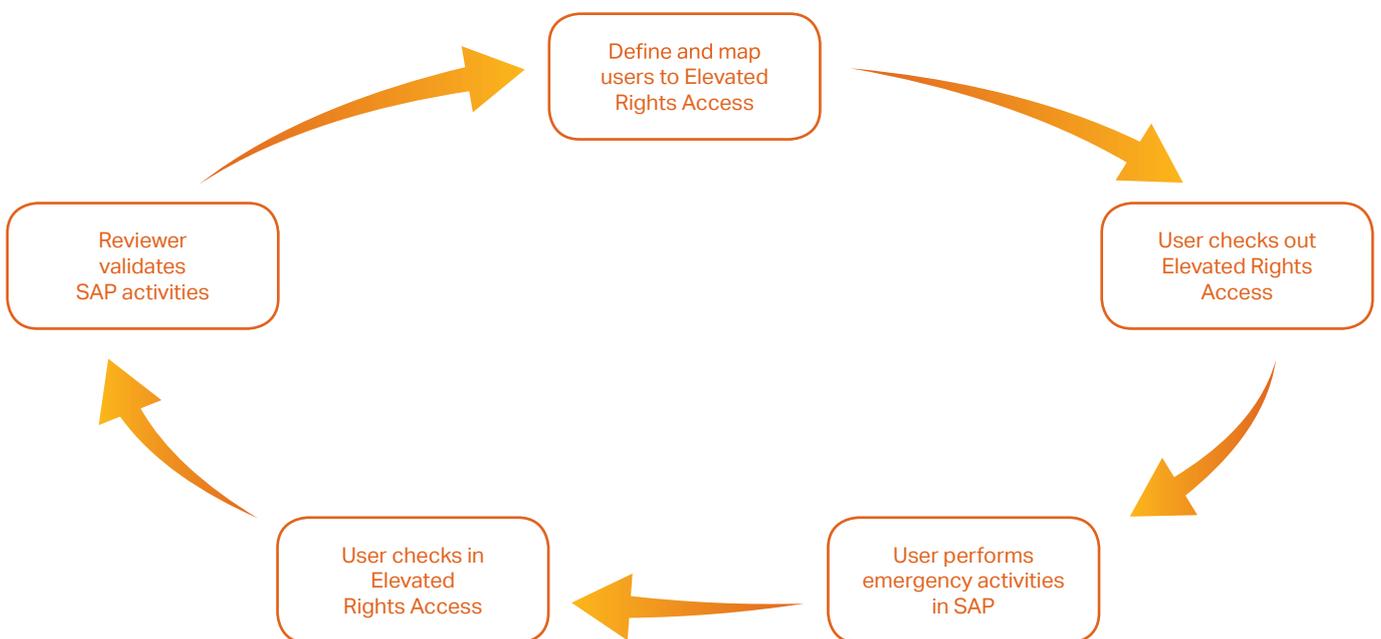
Checking Out Elevated Rights Access

When a user performs a check out, the Elevated Rights Access will be assigned to them for a predefined period to enable them to perform the required emergency activities. Once completed, the user will be able to check the Elevated Rights Access back in. Alternatively, it will automatically be checked in once the allocated period has expired.
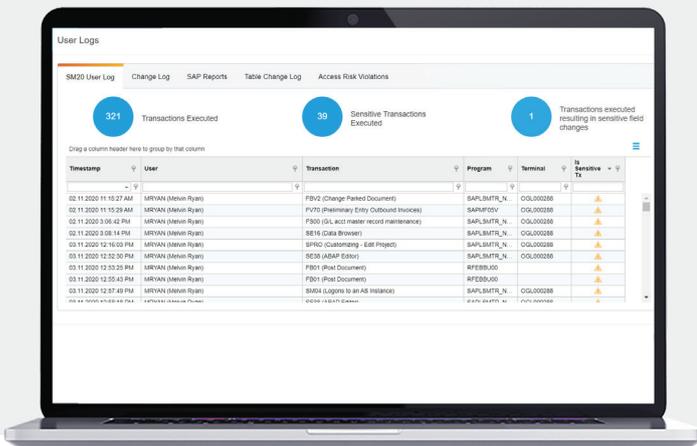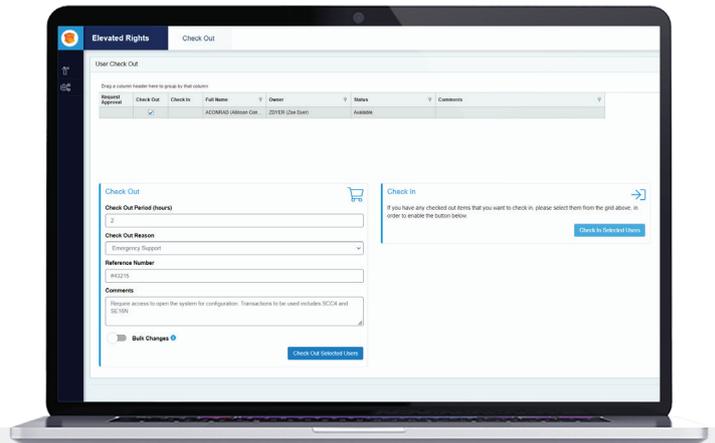
Review of Elevated Rights Access Activities

All changes in SAP will be logged and downloaded to the Soterion Elevated Rights Manager for review. All transactions that were executed and any sensitive fields that were changed can be reviewed by the reviewer. Any sensitive transactions that were executed (SOD or Critical Transactions) will also be highlighted for their attention.
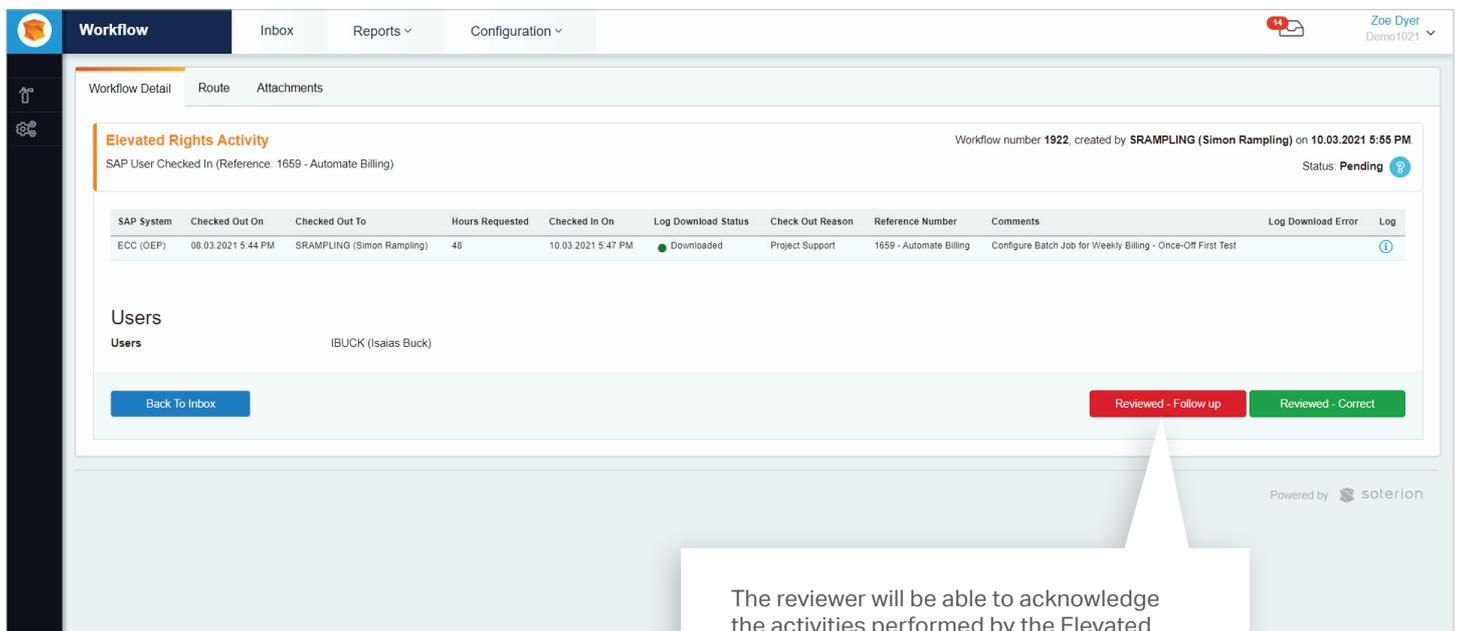
The reviewer will be able to acknowledge the activities performed by the Elevated Rights Access user. The workflow activity can be marked for **"Review - Follow up"** if there are any queries.