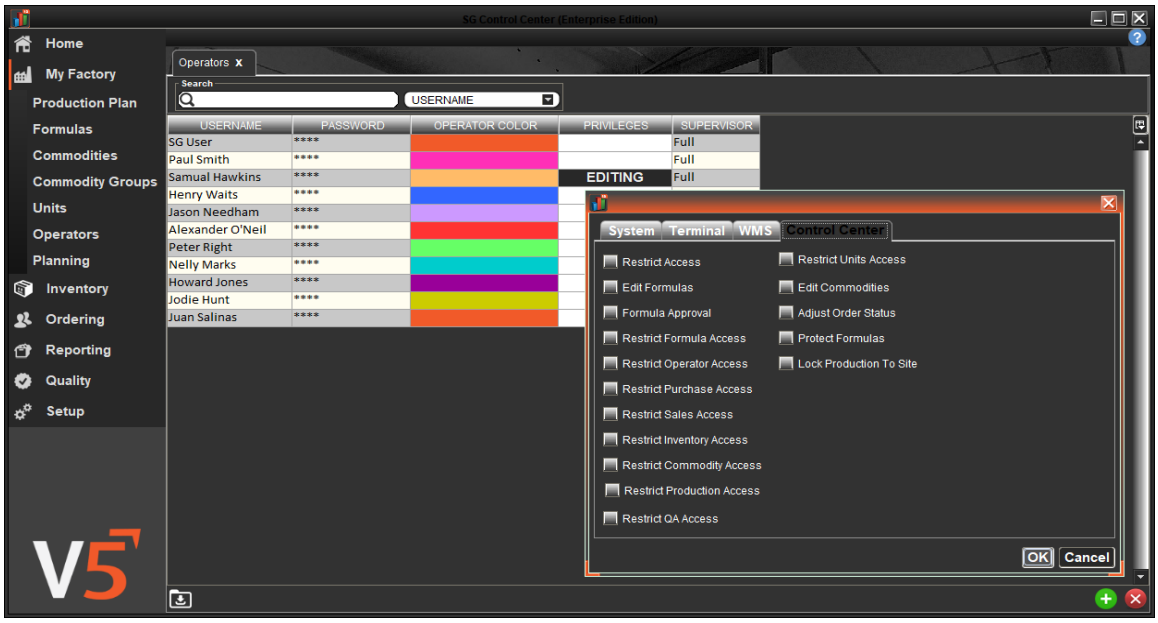
Authentication & Authorization Design

Introduction

User access and credentials are specified within the V5 Traceability application. The database holds data relating to the username, password, user color, an avatar, permissions & privilege levels. A 4-digit pin is used in a typical deployment, providing 10,000 possible combinations for users to access the system. Utilizing permissions, operators can be set to only access features and only perform certain actions if they are set to a supervisor level.



Database authentication credentials can be held in a local file, embedded in the software or can utilize OS user-domain profiles. Access is determined by the user permission list set against the database instance.

Operating System User Domain Profiles (optional)

When utilizing operating system user-domain profiles, active directories can be used to manage operator access. In this approach, no password needs to be set against the operator within the V5 database, however the username must exist in order to provide traceability throughout the logging systems. In this instance, the operator would simply sign into the terminal and the v5 system would use that user account to; A) Validate the operator in the system B) Connect to the database. This allows for a single-sign-on approach to be adopted whereby removing the user from the active directory list or changing their password will automatically and intrinsically affect the access to the V5 system.

We also implement authorization methodology when connecting to the web-servlet API if this approach is adopted. Oauth is used in conjunction with tokens in order to validate that correct access is granted. Once access is granted, external applications can send URI requests and receive JSON data in response.

In conclusion, we offer a dynamic approach to suit the security needs and topology of the client's infrastructure.