# Clearance Watchdog Product Brief

Why the Clearance Watchdog can help you with compliance

## Introduction

Access Control can become quite complex when a lot of people are involved, with lots of clearances for different services, locations or other. And these clearances are not always managed by a central authority such as the Security Department.

Most clearances will have a clearance owner that is responsible for authorizing clearance requests. The clearance owner in such cases, is responsible of authorizing access to a location that is managed by them. In these cases, the security department executes programming (clearance attribution to personnel) in order of the clearance owner.

Most companies will disable personnel profiles when people leave the company, effectively removing physical access for those people.

### Problem Domain

A problem group exists for people who remain active in the company and gather clearances over the years due to all sorts of reasons.

Some examples of rightly receiving extra clearances:

- Working on a specific project where the person receives an all-access clearance to a building that is being revamped, or access to critical areas that are designed for critical services such as IT equipment or research labs.
- Performing a temporary function to replace a colleague that requires a specific clearance.
- Transferring to another department, requiring new or additional clearances.
- Being promoted into another function.

In some cases, people might receive clearances they do not require or are not supposed to have:

- The security department was sent a wrong request by an end user, programming the wrong clearances.
- During programming, due to a human error the user may have received a different clearance.
- It is not always known what clearances belong to a certain profile: clearances can be copied off the profile of a colleague, compounding the issue of all wrong reasons of a person receiving/keeping clearances they should not or no longer have in the first place.

Another issue in a lot of cases becomes removing the rightfully provisioned clearances when they are no longer required by the person:

- Clearance owners may have a lot of other responsibilities to take care of. Requesting the removal of a clearance for a person that no longer requires it is easily overlooked.
- In a lot of cases, it is assumed that another department will handle access rights provisioning, including updating the existing access rights and removing the ones that are no longer needed.
- A temporary change may result in a situation that becomes normal for a longer period, to which people get accustomed. Forgetting to change the access rights when that situation finally comes to an end.
- When a clearance owner needs to

Last but not least, A person might receive an unrequired clearance in the first place due to different reasons. A wrong function level was communicated, giving the person higher clearances than required.

## Existing Clearance Management Tools

Tools have been built into the access control system that assist in managing a lot of these cases. But they are not always a full proof solution:

### Time based settings

Different solutions exist to manage this issue, which allow you to specify an expiration date.

**Problem**: The exact date of expiration is not always known and can depend on other factors, such as filling in for a colleague during a prolonged absence. Managing these expiration dates can become cumbersome to keep adapting to the situation, extending or revoking them as the requirement changes.

### Custom Clearances

You can assign a custom clearance to a person, which allows you to specify an activation and expiration date.

**Problem**: This is done on a per-door-basis (or door group). In large installations this may become cumbersome and incoherent. If for instance you need to change the composition of doors inside a clearance, the custom clearances that were tailored to reflect the main clearance will no longer hold the same access rights.

### Expiring Clearances

Allows the configuration of an expiration date for a clearance.

**Problem**: This is clearance-wide. While the expiration should be limited to a specific individual.

## Expiring Clearances per person

Allows expiration of a specific clearance for a specific person.

**Problem:** the hardware - Expiring Clearances per Person requires an iStar Ultra. Not all locations are equipped with this.

## Reviewing Clearances

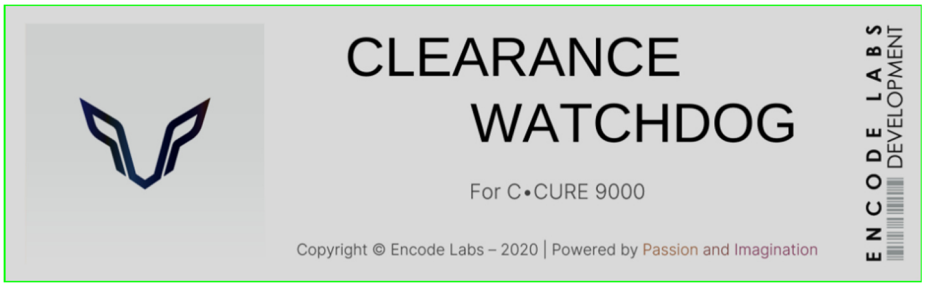
Forces clearance owners to review the list of people having their clearance attributed.

**Problem**: A lot of people will react when they receive a complaint that a person cannot perform their duties because of a missing clearance. The clearance is attributed quite fast. But when not receiving complaints, a clearance owner can easily oversee people that should no longer have the clearance. It is easy to assume a “no complaints, no changes needed” attitude when needing to perform the review.

Clearance owners may have a lot of other responsibilities, and need to delegate clearance reviewing. The replacement may not be aware of all latest changes. Or be worried to remove clearances from people that should still have access.

## What the Clearance Watchdog will NOT solve

Wrongly programmed doors. Critical Areas should **always** be factually audited based on the access logs.




ENCODE LABS DEVELOPMENT
SECURITY & CODING IS OUR PASSION