DMP ACCESS CONTROL EXPLANATION

WHAT IS ACCESS CONTROL

Access control *is the locking and unlocking of doors electronically by either a schedule or an event via a logical controller. DMP XR panels can offer true access control in both ways.*

1. Scheduled locking and unlocking. This is having the panel lock and unlock individual doors via schedule. It does not require any credentials be presented. It requires the programmer to create the schedule for a door or doors.

2. Event-based access control. This is where the panel locks or unlocks a door based on something that happens. An alarm could be the event, a zone state-change could be the event. The presentation of a credential at a reader is the event. That could be thought of as a credential-based access event. Credential based access requires consideration in planning and programming.

DMP panels process zone detection and access from one central control unit. They use area logic to process burglary detection and credential-based access control. Scheduled door control and event-based access control merely ties a schedule or event to a door output number, not an area. Let's dig a little deeper into credential-based access control and how it relates to areas.

CREDENTIAL BASED-ACCESS CONTROL

Most people understand how a simple burglary alarm operates. Zones are assigned to areas, and areas are groups of zones. The panel arms and disarms areas, not zones.

Here are the similarities between credential-based access control and burglary zones.

1. Like zones, door controllers are assigned to areas.
2. Like zones, we group them to areas for the same reason – operational commonalities.

AT A GLANCE

What Is Access Control

Credential-Based Access Control

What Is An Access Area

Profiles

Schedules

Scenarios

3. Like zones are assigned to an area in zone programming or **ZONE INFORMATION**, the assignment of door controllers to areas is defined in door controller programming, or **DEVICE SETUP**.

What a person can or cannot do in terms of accessing the keypad menu, arming/disarming burglary elements, and accessing doors, is dictated by user profiles. "**USER CODE PROFILES**" is a section of panel programming that exists to create groups of permission/restriction templates for users. User codes are tied to profiles and when a code is entered at a reader/keypad, the profile dictates what action that code can perform.

For a profile to be able to arm/disarm burglary elements, the appropriate burglary areas must be entered into the profile's "**ARM/DISARM AREAS**" section. If the profile will need to be able to unlock/access doors, the appropriate access areas must be entered into the profile's "**ACCESS AREAS**" section. Knowing this will help you to understand that profiles do not access doors by door number, they instead access "**ACCESS AREAS**", which are merely areas that have a door or doors assigned to them.

WHAT IS AN ACCESS AREA

Let's define access areas and how we assign them to doors. Why do we put all the perimeter door contacts on a small building in the same area in a burg system? Why do we put the interior motions in a different area? These zones share a commonality with one another. The doors could all be armed and disarmed at the same time by any user, but they need to be able to be separately armed from the interior motions as well.

The doors have commonality with each other so we can assign them to one area. The motions did not have the same arming commonality with the doors, but they had the same commonality with each other, so we assign them to another area. If we apply that concept to credential-based access control, we use the same logic, but we ask different questions to determine commonality.

1. Who should be able to unlock this door with a credential?
   a. When can they unlock this door?
   b. When can they not unlock this door?
2. Who should never be able to unlock this door with a credential?

The people who can't unlock every door typically are the biggest factor of how to associate door controllers to areas. For example, you have two access doors on a building with three different types of employees, and you want to enforce access by department. Manufacturing employees can get into the manufacturing door but not the office door. Office employees can get into the office door, but not the manufacturing door. The manager can access both doors. In this scenario, we have commonalities and differences.

The commonalities are:

1. The manufacturing door is accessible by all manufacturing employees.
2. The office door is accessible by all office employees.
3. Both doors are accessible by management employees.

The differences are:

1. The office door cannot be accessed by manufacturing employees
2. The manufacturing door cannot be accessed by office employees

PROFILES

If profiles are granted access to areas, and not particular doors, how many areas and profiles do we need, and who gets what in their profile?

The flexibility of the panel allows for things to be accomplished in several ways. One way we can solve this challenge is to create two access areas; one for manufacturing and one for the office. If we give manufacturing profiles access only to the manufacturing area, and we give office profiles access only to the office area, we have successfully limited profiles to respective areas. What about the manager? What do we give his profile so that he can access both areas?

We'll give him both areas in his profile. So, while just associating all the doors to one access area would have worked for a manager, it would not have been able to limit access for the other employees. And while creating three areas – one area for each profile with the right door(s) assigned to them – would have also been a solution, it was not necessary.

There are many things to consider when designing a credential-based access system. The panel does not differentiate a "burg" area from an "access" area. An area is merely that which can be armed and disarmed. Access areas assigned to a door can be armed. This can affect a person's ability to gain access. An armed area cannot be accessed. That's not to say that a person with a credential or access card can't unlock the door with their card.

For a person to unlock a door that belongs to an area that is armed, they must first be able to **DISARM** that area with their credential or access card before they will be granted access. This is accomplished by also giving them disarm permission to that access area in their profile. This is a type of "conditional" credential-based access control. Instead of confining a cardholder to a shift schedule, we instead designate a person that must card in first before anyone else can.

That first person would have the ability to disarm the armed access area, and no one else would. When the access area is armed, nobody can card in until the person with the ability to disarm the access area cards in. Afterwards, when the access area is disarmed, anybody with that access area in their profile will be able to card in until the area is armed again.

SCHEDULES

Finally, we have profile schedules. Profile schedules are a way to put a time-based limit on a person's ability to access a door with a credential. It exists to say when a profile can access a door that typically stays locked outside of and sometimes during the scheduled times. Some confuse this with scheduled locking/unlocking. If the door is unlocked via schedule or other means for long periods of time, there is no need for tightly managed access control at that door. People just open the door and walk through it.

Here are how profile schedules are used to restrict access:

XR150/550 Panels

1. A time schedule is created in the panel.
2. The time schedule is assigned to the profile.
3. If the access event occurs within the scheduled times, and the user has access to that area, the user will be granted access.

XR100/500 Panels

1. An access profile is given an access area or areas, and a shift number or numbers 1-4
2. Schedules are created for any access areas that require shift-restriction. When the schedule is created, it is assigned to an area, and given a shift number.
3. When access is requested, the panel checks the credential's profile to see if they have that door controller's access area in their profile. It then checks their shift number. The panel compares their shift number to shift schedules running in that access area. If their shift number exists in that area, and if they're accessing the door during that shift's time, the user will be granted access.

Output Schedules say when the door is automatically locked and or unlocked

Profile schedules say when a person can access a locked door with their credential.

Override makes a door on a lock/unlock schedule stay locked if its access area is armed. Override is found in Device Setup.

Regardless of whether the door is locked or unlocked by schedule, a person can access that door if they have:

1. that door's access area in their profile's access areas
2. a schedule assigned to their profile and the access is during that time
3. that door's access area in their profile's arm/disarm areas if the access area is armed

A door will unlock via schedule if:

1. the output schedule exists for that door
2. its access area is disarmed if override is turned on for that device

SCENARIOS

Let's say that a business's lobby door unlocks at 8:00 AM and locks at 5:00 PM M-F. That's scheduled access control. There is also an exterior reader by the door for credential-based access control. From 8-5, M-F, anybody can walk through the front door since the schedule unlocked the door. After it locks at the end of the day, the only people who can get in are people who have that door's access area in their profile, and during the scheduled time (if any) that is applied to the profile. At 9:00 PM, the access area automatically arms via schedule. Since override is turned on for that door controller, it stays locked until someone with disarm privileges for that area gets there and disarms that area. Since the access area is now disarmed, anyone who has that access area in their profile can unlock it with a swipe (if inside of their scheduled time) until it unlocks via its door schedule at 8:00 AM.

Planning a multi-area access control system:

The front section of the business is an office and a customer counter. Its only exterior door is accessed by a card outside of the hours of 8:00 AM to 5:00 PM M-F (it is automatically unlocked by a schedule during that time). The back section of the business is used for assembly and shipping. Those two exterior doors are always electronically locked and are only unlocked with credentials. The detached warehouse has a man door and an overhead door. The only door controlled by the panel is the man door. It is always locked and is only using credential-based access. There is a door connecting the front and rear of the main building, but there is no electric lock on it.

The site has multiple physical areas with multiple access points, some of which need different rules. The only way to achieve this is through multiple access areas that can be configured independently for single doors, or groups of doors that have the same rules.

How should we assign access doors to areas? By finding their commonalities and differences and comparing them to the customer's needs.

- The front door is on a lock/unlock schedule, and outside of that schedule accessed by front sales and management cards only.
- The two doors in back are always locked and can only be accessed by all personnel with cards and can be grouped together.
- The warehouse man door is on a detached building but follows the same rules as the two doors in the back of the main building. It can be grouped with those doors, or it can be in its own area for a degree of separation. If the customer foresees the rules ever changing for the warehouse door, it will need to be in its own area. It will be just as easy to put it in its own area, so we will do so.

Here's how we'll plan the system...

Mag locks, HID Prox readers, and DMP door controllers will be at all exterior man doors. Qualified personnel will be issued credential.

Area 5 will be called "Front Access"

Area 6 will be called "Rear Access"

Area 7 will be called "Warehouse Access"

The front door needs to be on a 5-day automatic lock/unlock schedule controlled by the panel. Outside of that schedule, credentials belonging to management and sales personnel can unlock that door with a swipe. No other credentials will work. No other doors on this system should follow that rule. The front door's controller module will therefore be assigned to Area 5, "Front Access"

The rear worker-access perimeter doors will both operate on the same rule. They will always both be locked and be accessible by the same people. All cardholders will be able to access these doors at all times. The door controllers for these two doors will be assigned to Area 6, "Rear Access".

The warehouse man door currently operates on the same rule as the rear worker-access doors, but it is conceivable that it could operate on a different rule in the future. The door controller will be assigned to Area 7, "Warehouse Access".

In this configuration, electronically controlled doors with access and scheduling commonalities have been grouped into areas. It is important not to confuse a ***panel*** area with a ***physical*** area, because one panel area can span ***multiple*** physical areas, such as controlling the door locks on doors in two adjacent rooms, or ***part*** of a physical area such as controlling one perimeter door in the building with perimeter doors controlled by another panel area.

PRACTICE

DOOR NAME

FRONT DOOR

ASSEMBLY DOOR

SHIPPING DOOR

WAREHOUSE

AREA NAME

FRONT ACCESS

REAR ACCESS

WAREHOUSE ACCESS