

Anti-Passback Applications

Creating anti-passback applications requires coordinated and integrated use of multiple product features in your IEI eMerge™ system.

This tech note provides overviews of the following use cases for anti-passback applications.

1. Simple timed anti-passback for preventing the use of a single badge to allow multiple cars into the parking garage.
2. Regional anti-passback for use in mustering and roll call applications that require knowing who may be in a particular region, and/or knowing who has reported to a mustering station.
3. Regional anti-passback for use in controlling passback and tailgating behavior.
 - Tailgate violations
 - Passback violations
 - Customizing Passback and Tailgate rules for individuals
 - Gracing users

We cover these cases separately below.

Case 1.

Your customer wants to stop employees from admitting cars other than their own to the parking garage. This is a simple implementation of “timed” anti-passback.

Create the region

For this application we need create only one region in addition to the default region called “**Uncontrolled Space**.”

1. Select **Setup : Access Control : Regions**.
2. Under the **Name** drop-down click the **add** link to add a new region.
3. Enter the name “Parking” for this new region.
4. In the section called **Passback Violations** select the **Default passback violation action** from the drop-down. In this case select **Hard**.

NOTE: Select **Hard** to deny access in case of violations. Select **Soft** to allow access but log the event in the system log. You can also assign an event to execute in case of violations and this event can require a system Monitor to acknowledge the event.

5. In the section called **Misc. Information** enter the number of seconds to **Deny multiple accesses**. In this case we may wish to deny access for as much as ten minutes to ensure that the employee has parked and is probably in the building before their badge will work again at the parking garage reader. Enter “600” seconds (ten minutes).

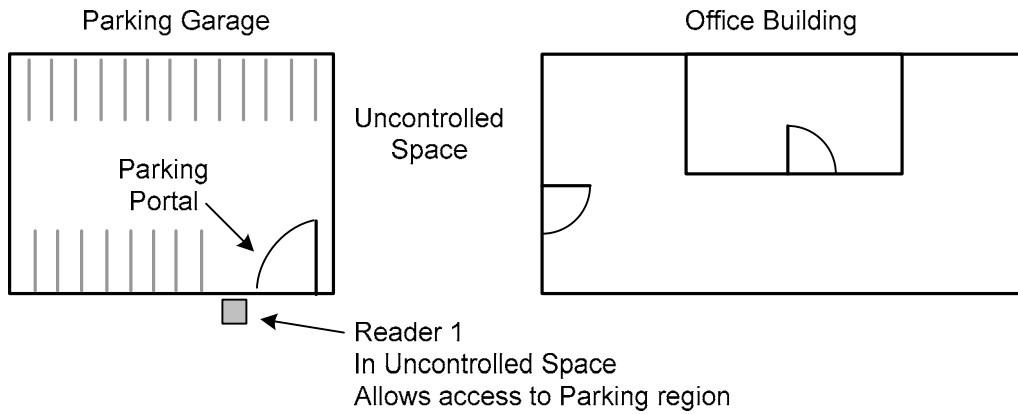
Assign the reader to the Uncontrolled Space region

The reader that allows entrance to the parking garage region must be assigned to a region other than the Parking Garage, in this case, Uncontrolled Space.

1. Select **Setup : Access Control : Readers/Keypads**.
2. If a reader is not yet configured do so now. Click **Help** if you need assistance with this.
3. From the **Reader is in region** drop-down select **Uncontrolled Space** and click **Save**.

Specify that this portal’s reader allows access to the Parking Garage Region

1. Select **Setup : Access Control : Portals**.
2. If a portal is not yet configured do so now, and call this the Parking Portal. Click **Help** if you need assistance with this.
3. In the **Card Readers/Keypads** section select the reader that allows access to the parking garage region as **Reader 1**.
4. To the far right in the **Card Readers/Keypads** section, select **Parking Garage** from the **Allows access to region** drop-down.
5. Click **Save**.



Summary discussion

In this case a valid card read will allow access to the Parking Garage and a 600 second timer will start. Once the timer has elapsed, (or the access card is used in another region) the card will again allow access to the Parking Garage. Before 600 seconds has elapsed, access will not be allowed and an "Access denied [PASSBACK]..." message will be entered in the Activity Log.

NOTE: You can exempt individuals from this denial of access. On the **Personal Information** page in the **Access Control** tab, set the person's **Regional anti-passback privileges** to **Exempt**.

Case 2.

Your customer wants regional anti-passback for use in mustering and roll call applications that require knowing who may be in a particular region, and/or knowing who has reported to a mustering station. Typically, mustering is for use during evacuations such as fire alarms.

Create the regions

Although almost any number of regions can be created for this application, for demonstration purposes, we need create only two regions in addition to the default region called **Uncontrolled Space**. The Mustering reader can be in Uncontrolled Space.

1. Select **Setup : Access Control : Regions**.
2. Under the **Name** drop-down click the **add** link to add a new region.
3. Enter the name "Secret Lab" for this new region.
4. In the sections called **Passback Violations** and **Tailgate violations**, select the **Default passback violation action** from the drop-down. In this case select **Hard**.

NOTE: Select **Hard** to deny access in case of violations. Select **Soft** to allow access but log the event in the system log. Select **Ignore** for no actions to be taken.

5. Click **Save**.
6. Under the **Name** drop-down click the **add** link to add another region.
7. Enter the name "Office Space," and click **Save**.

NOTE: If you wish event actions to take place in cases of passback or tailgate violations you can select them from the Hard and Soft event drop-downs. If you have not yet created these events select **Setup : Alarms : Events** and create the events you need.

Assign the readers to the regions

This application requires portals with readers on both sides, one to allow ingress, the other to allow egress. The reader that allows entrance to the Secret Lab region must be assigned to a region other than the Secret Lab, in this case, the Office Region. The reader on the other side of the door must be assigned to the Secret Lab region. The reader assigned as the mustering reader is typically located in Uncontrolled Space.

1. Select **Setup : Access Control : Readers/Keypads**.
2. From the **Name** drop-down select the reader on the outside of the Secret Lab door and from the **Reader is in region** drop-down select **Office Region**.
3. Click **Save**.
4. From the **Name** drop-down select the reader on the inside of the Secret Lab door and from the **Reader is in region** drop-down select **Secret Lab**.
5. Click **Save**.
6. From the **Name** drop-down select the reader to be used as the mustering reader and from the **Reader is in region** drop-down select **Uncontrolled Space**.
7. Click **Save**.

NOTE: The door between Uncontrolled Space and Office Space must also have readers on both sides. In this scenario this is the door by which employees enter the building. Assign the reader on the outside to **Uncontrolled Space** and the reader on the inside to **Office Space**.

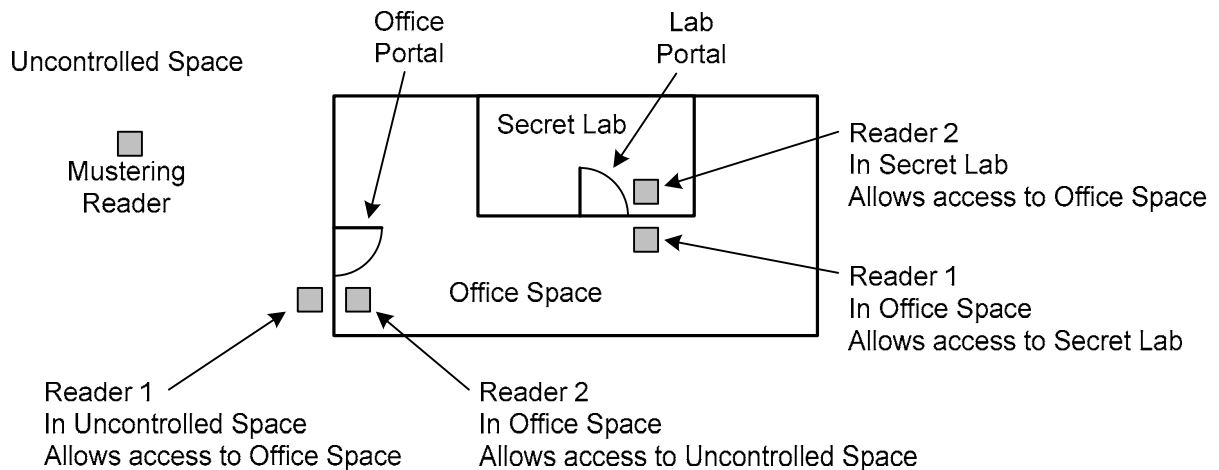
Configure the Secret Lab portal with two readers

This application requires portals with readers on both sides, one to allow ingress, the other to allow egress. Only when people are required to “badge out” can the system keep track of who is in a region.

1. Select **Setup : Access Control : Portals**.
2. In the **Card Readers/Keypads** section, select the reader **outside** the Secret Lab door from the **Reader 1** drop-down. Select the reader **inside** the Secret Lab from the **Reader 2** drop-down.
3. Click **Save**.

NOTE: To the far right of the **Reader 1** and **Reader 2** drop-downs check the **Allows access to region** column. **Reader 1** should allow access to the **Secret Lab** region. **Reader 2** should allow access to the **Office Region**. That is, a reader is in one region and allows access to another.

NOTE 2: The portal between **Uncontrolled Space** and the **Office Space** must also have two readers and be configured similarly to the portal between the **Office Space** region and the **Secret Lab**.



Summary discussion

This scenario allows the system to keep track of who is in each region.

For example, an employee arrives and enters the building through the Office Portal by presenting their access card to Reader 1. The system now logs them as being in the region called “Office Space.” You can see this in the **Occupancy**, **Roll Call**, and **Roster** reports. Select **Administration : Reports : People**.

NOTE: To see regional information in the Roster report you will need to select **Setup : Site Settings : Network Controller** and in the bottom right corner of the **Misc. Information** section of that page place a check in the box labeled **Show Region and Passback Grace info in the Roster and People reports**.

This scenario also allows you to use mustering.

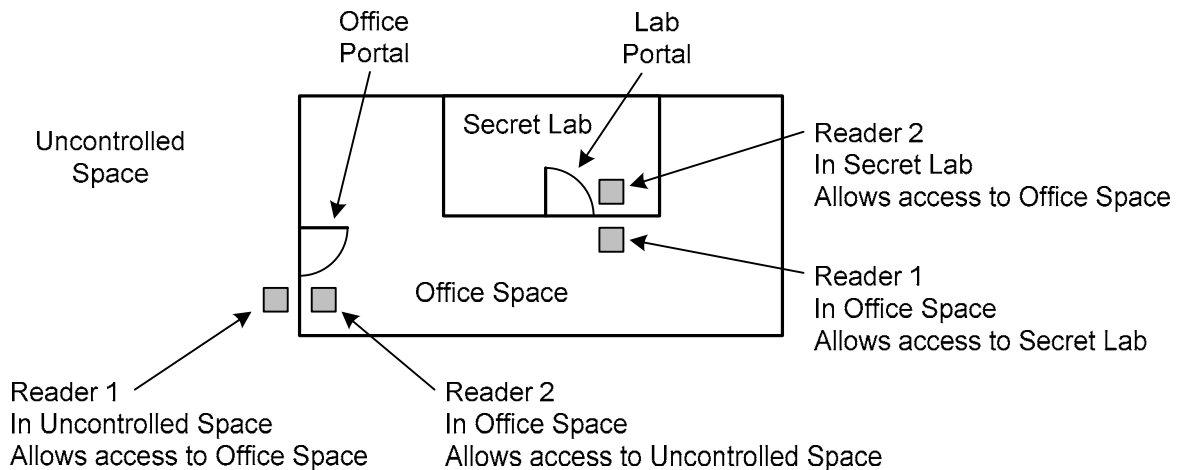
For example, a fire alarm is triggered while numerous employees are known to be in the building. The employees should leave the building, go to the mustering reader, and present their access cards. Security personnel can then easily determine who has arrived at the mustering station and who may still be in the building.

Case 3.

Your customer wants a regional anti-passback application for use in controlling Passback and Tailgate behaviors that violate security protocols. This requires knowing who is in each defined region in a building.

- **Passback violation:** a card read to enter a region where the card holder is already known to be. (This is a subset of tailgate violations.)
- **Tailgate violation:** a card read in any region when the card holder is known NOT to be in that region.

For this application we can use the same configuration of readers and portals as in case 2 above, except that we do not need a mustering reader.



Summary discussion

Example 1, Tailgating:

- Jane Doe arrives at work, presents her access card to Reader 1 outside the Office Portal, and enters the Office Space.
- She proceeds to the Lab Portal, presents her access card, and enters the Secret Lab.
- She leaves for lunch with a co-worker and fails to present her access card to Reader 2 inside the Secret Lab.
- She proceeds to the Office Portal and presents her access card to Reader 2.

In this case, the system has Jane Doe in the Secret Lab but her access card was presented to a reader in the Office Space region. This is a Tailgate violation. If you have set the **Default Tailgate violation action** in this region to **Hard**, access will be denied. The system will enter this into the Activity Log and execute whatever event you have configured for a tailgate violation in this region. (See the procedure below.)

Configuring behavior for Tailgate violations in the Office Space region

1. Select **Setup : Access Control : Regions**.
2. From the **Name** drop-down select **Office Space**.
3. In the **Tailgate Violations** section, select the **Default tailgating violation action**.

NOTE: Select **Hard** to deny access in case of violations. Select **Soft** to allow access but log the event in the system log. Select **Ignore** for no actions to be taken.

4. In the **Tailgate Violations** section, select from the event drop-downs the events to execute when violations occur in this region.
5. Click **Save**.

NOTE: If you have not yet created alarm events, select **Setup : Alarms : Events** and create them now.

NOTE 2: The behaviors selected here will only execute for the Office Space region. This allows you to assign differing behaviors to regions with differing security needs. To configure violation behavior for the Secret Lab region, select it from the **Name** drop-down, select the behaviors to execute in case of violations in that region, and click **Save**.

Example 2, Passback:

- Jane Doe arrives at work, presents her access card to Reader 1 outside the Office Portal, and enters the Office Space.
- She proceeds to the Lab Portal, presents her access card, and enters the Secret Lab.
- She leaves with a co-worker for a meeting in the Office Space and fails to present her access card to Reader 2 inside the Secret Lab.
- When the meeting ends she returns to the Lab Portal and presents her access card to Reader 1 outside the Secret Lab.

In this case, the system has Jane Doe in the Secret Lab but her access card was presented to enter the Secret Lab. This is a Passback violation. If you have set the **Default Passback violation action** in this region to **Hard**, access will be denied. The system will enter this into the Activity Log and execute whatever event you have configured for a Passback violation in this region.

Example 3, Customizing Passback and Tailgate rules for individuals:

It is likely that some employees, such as security and emergency response personnel, should be exempted from denial of access due to tailgate or passback violations.

Exempting people from Passback and Tailgate rules

6. Select **Administration : People : Change/delete** and find the individual's Personal Information page.
7. In the **Access Control** tab select **Exempt** from the **Regional anti-passback privileges** drop-down.
8. Click **Save**. This person will now not be denied access due to any Passback or Tailgate violations they may commit.

NOTE: Alternatively it is possible to require, that for some individuals, all Passback and Tailgate violations should be treated as Hard violations and access should be denied. To do this, select **Hard Always** from the **Regional anti-passback privileges** drop-down.

Example 4, Gracing users:

In many Passback and Tailgate applications it is desirable to “wipe the slate clean” at least once per day. It is also often required that a system monitor, such as a security guard, be able to “Grace” specific individuals on an as needed basis.

- **Grace:** An access card holder is exempted from the Passback and Tailgating rules for their next access only.

Setting a daily time for gracing all users

1. Select **Setup : Access Control : Regions**.
2. In the **Misc Information** section select the time of day from the drop-downs labeled **All users are graced daily at**.
3. Click **Save**.

Gracing all users at any time

1. Select **Administration : Reports : People : Roster**.
2. At the top of the Roster Report click the button **Grace all shown**.

Gracing an individual user

Individuals can be Graced from their **Personal Information** page or from a Roster Report.

NOTE: The Roster Report can only be used to grace individuals if you have configured People Reports to show region and passback grace information. This can be done by selecting **Setup : Site Settings : Network Controller** and in the **Misc. Information** section of that page check the box labeled **Show Region and Passback Grace info in the Roster and People reports**.

1. Select **Setup : Monitor : Passback Grace**.
2. Enter search criteria for a specific user or group of users.

NOTE: If the search specifies only one person, that person's **Personal Information** page is displayed. The **Grace** button is in the **Access Control** tab.

If the search results are a group of people a roster report of that group of people is displayed.

3. Click the **Grace** button.