ANTI-PASSBACK DEFINITION AND SET UP

Antipassback is an access control feature that prevents cardholder misuse, by putting certain restrictions on the use of their cards. When the Antipassback feature is enabled, cardholders are restrictions from re-entering an Area until they have exited that Area.

Each AxiomV™ cardholder record in the database has two fields for area tracking – one for the last APB Area entered, and one for the Current Area, which may or may not be an APB area. If the last reader that a cardholder used was an APB reader, then both fields will contain the entering area of that Access Point record. If the last reader was not an APB reader, but had an entering area assigned, then the Current Area field will contain the entering area for that Access Point and the APB Area will contain the entering area from the last APB reader used.

Hard and Soft Antipassback

Hard Antipassback does not allow access to be granted if the antipassback criterion is violated. *Soft Antipassback* does allow access if the antipassback criteria is violated but posts the message "*Access Granted APB Reader*" to signify that a violation has occurred. Generally *Soft Antipassback* is only used during a training period before *Hard Antipassback* is enabled.

Timed Antipassback

Timed Antipassback resets the area of the cardholder after a specified time delay. This is used in applications where the cardholder reads their card to get in but uses a Request-to-Exit device to get out. The time delay is settable for each access point from 1 to 127 seconds or minutes.

Reader Antipassback

For *Reader APB*, the reader's *Entering Area* in the *Access Point* configuration record is compared with the *Current Area* of the cardholder as recorded in the AxiomV™ database. If they match, a *Reader APB* violation exists. In short, *Reader APB* is only concerned with the area the cardholder is moving into, and restricts the cardholder from re-entering the area without first reading into another area.

Area Antipassback

Area APB is more restrictive then Reader APB. In addition to the Reader APB check outlined above, the system also performs a check on the exiting area in the Access Point configuration record. First the system checks that the *Entering Area* and the *Current Area* **are not** the same. Then the system checks to see that the *Exiting Area* and the *Current Area* **are** the same. Antipassback is violated if either check fails. Area Antipassback not only checks to see if the cardholder is trying to enter the Area that they are already in, but also checks to see if the cardholder is trying to leave an Area that they are not in. This higher level of antipassback is mostly used in applications with Areas inside of other Areas.

Global Antipassback

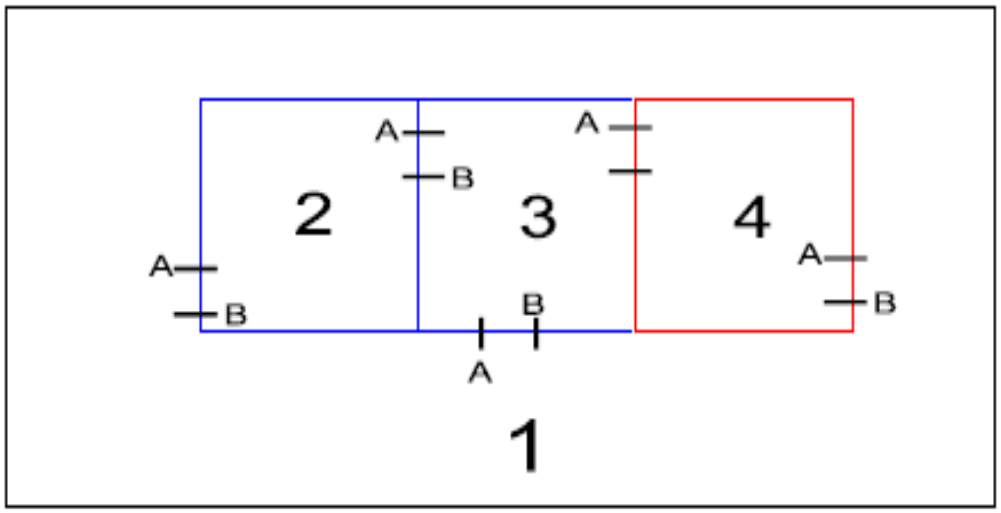
When antipassback is enabled it functions within a network since networks don't communicate to each other while panels within a network do. Checking 'Required PC Decision' with antipassback enabled means that the AxiomV™ software will control antipassback for the site and that antipassback can function across networks. This will be true as long as the AxiomV™ server is running.

Example

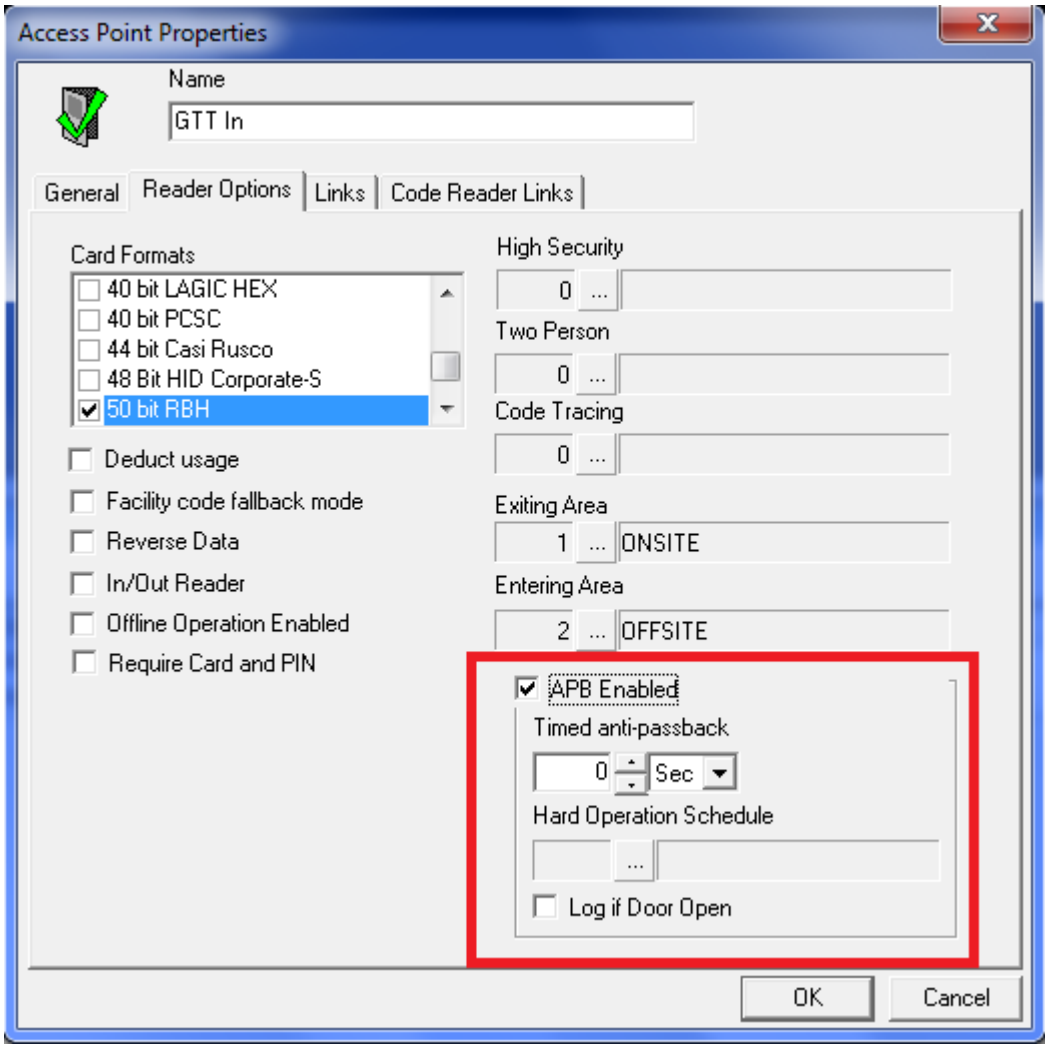
In the diagram below, there are four areas numbered 1 to 4, programmed as antipassback areas. Each door to each area has two card readers: A and B. All readers are set for hard antipassback, and each access point has both its entering area and its exiting area defined. This establishes the cardholder flow for area to area.
Let's say John enters Area 2 from Area 1. Once John is in Area 2, his card allows him to:
Exit Area 2 to Area 1.Exit Area 2 to Area 3.
While in Area 2, if John were to pass his card back to someone in Area 1, the card does not allow access to Area 2 because the cardholder location has been recorded as Area 2, and therefore Area 2 cannot be re-entered. In addition, if John were to follow someone into Area 3 without presenting his card, he could not gain access to Area 4 because his cardholder location has been recorded as Area 2, which is not connected to Area 4. He would not be exiting Area 2 when trying to enter Area 4.

Area

A predefined physical location such as warehouse or office, with entry and exit through *access points* controlled and monitored by AxiomV™.



APB Enabled Check this box to enable Antipassback. (Found by right clicking on an Access Point and selecting configuration.)



Timed Antipassback

Use this setting to set the minimum amount of time that must expire, before a card that was presented to this reader previously, may be used again at this same reader.

M **To use Reader/Area antipassback but not *Timed Antipassback* ensure that the time in *Timed Antipassback* is set to zero. Once a time is set in *Timed Antipassback* then *Timed Antipassback* will be in effect instead of any other form of antipassback.**

Hard Operation Schedule

Use the Browse/Ellipsis button to select the Schedule, during which, access will be denied when either a Reader Antipassback or an Area Antipassback violation occurs. When the violation occurs outside of this Schedule, access is permitted and reported as an "Access Granted Antipassback Reader".