Configureren van Anti-passback

Anti-passback beginselen

Anti-passback is een belangrijk kenmerk dat de veiligheid van de site sterk verhoogd. Verbonden met de toegewezen hardware van de deur, wordt het misbruiken van kaarten voorkomen. Zonder Anti-passback, is er niets dat een gebruiker tegenhoudt om het gebouw te betreden door gebruik van zijn kaart, en daarna deze kaart door te geven aan een andere gebruiker, zodat deze ook toegang krijgt.

Het gebruik van Anti-passback zones moet eerst ingesteld worden. Voor meer details aangaande het instellen van zones en zone groepen, zie: applicatie nota AN1023 - Configureren van zones en zone groepen.

Verschillende situaties vereisen verschillende Anti-passback types. Net2 ondersteunt 3 types van Anti-passback.

Logische Antipass-back

Volledige Anti-passback wordt gebruikt bij systemen waar IN en UIT lezer de toegangen controleren. Omdat het systeem weet of de gebruiker zich binnen of buiten een bepaalde zone bevindt, kan hij intelligent zijn aangaande het wel of niet autoriseren van een gebruiker. Een gebruiker moet eerst een zone verlaten hebben wil hij terug geautoriseerd worden. Heel vaak worden er tourniquets gebruikt in combinatie met een volledige Anti-passback. Dit wordt vaak gebruikt aan de hoofdingang van een gebruik of om de toegang tot clubs te controleren.

Tijdgestuurde logische Anti-passback

Tijdgestuurde logische Anti-passback combineert het beste van de twee hierboven vermelde methoden. Zolang een gebruiker de Anti-Passback regels volgt, en zich buiten een zone badged, krijgt hij direct terug toegang. Maar, indien een gebruiker een andere persoon met zijn badge buiten badged, zal hij pas na een specifieke geprogrammeerde tijdperiode zelf terug toegang krijgen. Dit laat een Anti-passback controle toe op een site, maar de beheerders moeten de gebruiker niet reseten moesten deze de regels overtreden hebben. Na een voorgeprogrammeerde van ontoegankelijkheid, wordt hun Anti-passback status gereset.

Tijdgestuurde Anti-passback

Met een tijdgestuurde Anti-passback, wordt wanneer een gebruiker toegang krijgt via een bepaalde lezer, deze lezer gedurende een voorgeprogrammeerde tijd uitgeschakeld voor deze kaart. Dit kan nuttig zijn wanneer geen Uit lezer is. Bijvoorbeeld, op een parking is enkel de toegang naar de parking gecontroleerd. De uitgang van de parking wordt gewoonlijk niet gecontroleerd. Het instellen van tijdgestuurde Anti-passback, gedurende 15 minuten, zou het onmogelijk zijn dat een gebruiker die juist de parking betreden heeft, zijn kaart doorgeeft aan een vriend of een collega.

Anti-passback configureren

Selecteer Anti-passback uit het boomstructuur menu, dit toont het configuratie paneel. Alvorens Anti-passback te kunnen instellen, moeten er zones en zonegroepen geconfigureerd worden.

Kies een zonegroep uit de lijst waaraan u Anti-passback wenst te koppelen. Het volgende diagram toont het Anti-passback configuratie paneel. U kunt zien dat bij het selecteren van de Zonegroep gebouwencomplex, zoals gedefinieerd onder Zones, het systeem automatisch weet dat hij deuren moet controleren die toegang geven tot deze zone en buiten deze zone gaan.

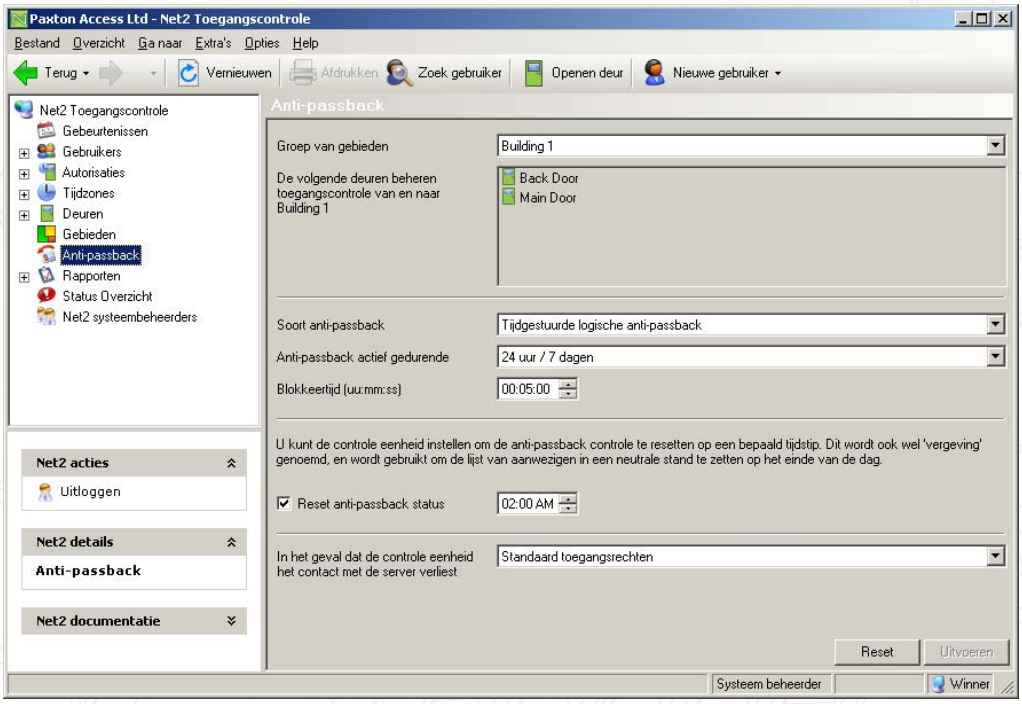
Een deur kan slechts tot één Anti-passback groep behoren. Bijvoorbeeld, indien u een Anti-passback instelt voor het gebouwencomplex, is het niet mogelijk om eveneens Anti-passback te hebben voor gebouw 1. De Hoofdingang zou anders tweemaal gebruikt zou zijn. U kunt natuurlijk Anti-passback controle hebben op de parking en eveneens in het gebouwencomplex, want daar is geen conflict met de lezers.

Selecteer het type Anti-passback dat u wenst te gebruiken.

Anti-passback kan actief gemaakt worden onder de tijdzone controle, deze laat een strenge Anti-passback toe gedurende bepaalde uren, en minder strenge controle gedurende andere uren. Indien tijdgestuurde of tijdgestuurde logische gebruikt werd, dan moet de uitsluitperiode ingebracht worden. Dit is de tijd gedurende de welke de gebruiker die lezer niet kan gebruiken.

Het systeem kan geconfigureerd worden dat de Anti-passback status op een gespecificeerde tijd gereset wordt. Dit betekend dat iedere gebruiker in een neutrale stand komt te staan en de volgende dag zonder probleem zijn kaart terug kan gebruiken.

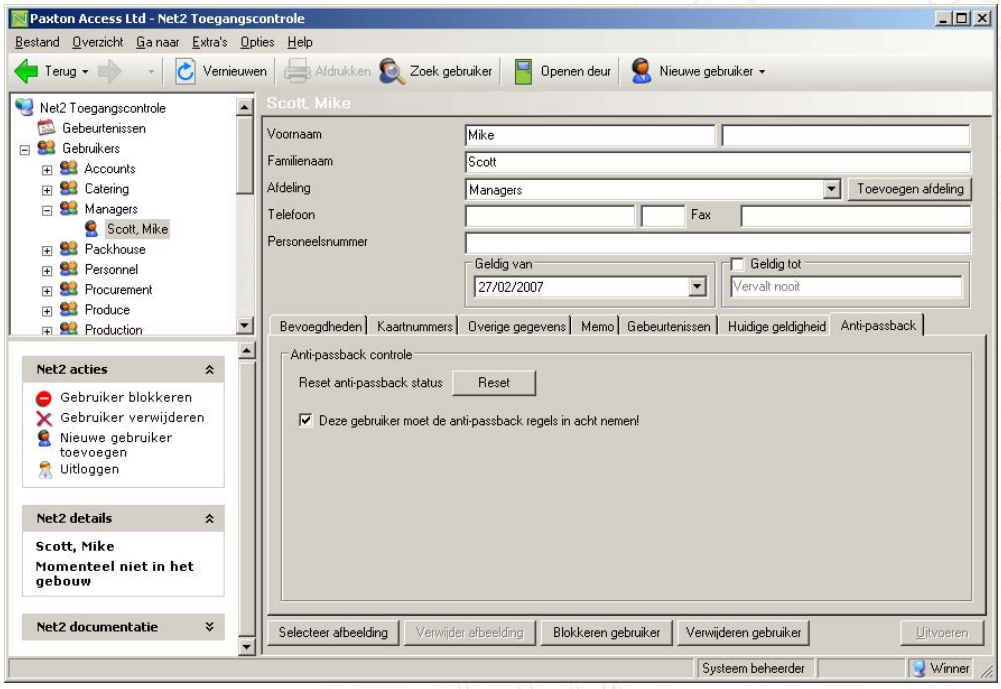
Om de Anti-passback te laten werken, moet de Net2 server constant communiceren met de ACU's. In het geval dat de server het contact verliest met de controle eenheden kan u via de software kiezen of u de toegang aan de gebruikers weigert of dat u hen de standaard toegangrechten geeft.



De 'Reset' knop laat toe om de Anti-passback status van alle gebruikers te reseten. Hun volgende geldige toegang zal hun locatie bepalen in het systeem.

Standaard, moeten de gebruikers de Anti-passback regels opvolgen. Er bevindt zich in het Anti-passback venster in het gebruikersveld de mogelijkheid om de Anti-passback regel te deactiveren. Dit betekend dat bijvoorbeeld, veiligheidspersoneel altijd toegang krijgen tot de deuren, die anders misschien geblokkeerd zouden zijn? Bijvoorbeeld, bij het achtervolgen van een indringer is het niet aangewezen om dan geblokkeerd te zijn aan een of meerdere deuren.

In hetzelfde venster met de gebruikersgegevens bevindt zich eveneens een knop, die wanneer deze ingedrukt wordt, de Anti-passback status van de gebruiker zal reseten. Hun volgende geldige toegang zal hun locatie in het systeem bepalen.



Belangrijke nota's

Anti-passback vereist dat de Net2 server applicatie draait. Indien u Anti-passback wenst te gebruiken, is het aan te raden om Net2 Server te installeren op een voor hem toegewezen computer.

De huidige specificaties voor compatibele PC hardware, netwerk en besturingssysteem zijn beschikbaar op onze website via de volgende link:

http://paxton.info/720