

Paxton Specificatie

Sectie 5

Paxton10

Bewerk dit document indien nodig - dit document kan worden gebruikt voor een standalone Entry deurintercom systeem, of waar nodig worden samengevoegd met een Paxton online op maat gemaakte toegangscontroleoplossing.

**[Vierkante haakjes]:** Standaard -– Opties.
**{Krulhaken}:** Opmerkingen

SECTION 3

TOEGANGSCONTROLE – PaxLock

**1.1 SAMENVATTING**

1. Sectie bevat
	1. Elektronische toegangscontrole
	2. Producten
2. Producten
	1. De [Paxton10 Software controller] bevat de software, de centrale database van het systeem en zorgt voor opslag van gebeurtenissen, instellingen en gebruikers.
	2. 2. De [Paxton10 Deurcontroller] zorgt voor de aansturing van een deur, poort of slagboom. Op de deurcontroller wordt randapparatuur aangesloten zoals lezers en sloten.
	3. 3. De [Paxton10 Videocontroller] biedt naast de aansturing van een deur, poort of slagboom de mogelijkheid om netwerkcamera’s te koppelen zodat live videobeelden bekeken kunnen worden of opgenomen worden.
	4. 4. De [Paxton10 Alarmconnector] is de interface tussen het toegangscontrole en het inbraakalarm of brandmeldsysteem en biedt de mogelijkheid om de status van deze systemen te monitoren.
	5. 5. De [Paxton10 Wireless Connector] dient voor de communicatie via de software en de draadloze deurbeslagen, deze communicatie gebeurt via bluetooth.
	6. 6. De [Paxton10 Camera] kan live videobeelden weergeven en opnemen in 4K resolutie en is voorzien van ingebouwd geheugen voor Edge storage.
	7. 7. Een voedingseenheid (PSU), voorziet de stroom die nodig is om de controllers van stroom te voorzien.
	8. 8. Een [Paxton10 Secure Slimline lezer] die verschillende kaarten en tags(credentials) leest om gebruikers te verifiëren en toegang te verlenen of weigeren.
	9. 9. Een [Paxton10 Secure Vandaalbestendige lezer] die verschillende kaarten en tags (credentials) leest om gebruikers te verifiëren en toegang te verlenen of weigeren. De lezer is voorzien van een vandaalbestendige lezer.
	10. 10. Een [Paxton10 Secure Lezer keypad] biedt de mogelijkheid om een PIN of code in te voeren of verschillende kaarten en tags (credentials) leest om toegang te verlenen of weigeren.
	11. Een [desktoplezer] [Paxton10 Desktoplezer] die de methode biedt voor het registreren van credentials in het systeem en om aan gebruikers te koppelen.
	12. De [beheersoftware] [Paxton10 Software] zorgt voor de communicatie naar de hardware en configuratie van het systeem. Daarnaast biedt het de mogelijkheid voor het gebruikersbeheer.
3. Systeem
	1. De producten hierboven vormen samen een compleet toegangscontrole systeem, en worden gebruikt om deuren te beheren en toegangspunten van de locatie te monitoren.
	2. De producten hierboven vormen samen een Video Management Systeem (VMS) en biedt videobewaking en de mogelijkheid om videobeelden op te nemen.
	3. Het systeem dient schaalbaar te zijn zodat extra hardware van dezelfde fabrikant toegevoegd kan worden.
	4. Alle hardware dient plug-and-play te zijn.
	5. Het systeem dient voorzien te kunnen worden van meerdere toegangspunten.
	6. Het systeem dient voorzien te kunnen worden van meerdere bestuurbare apparaten.
	7. Het systeem dient voorzien te kunnen worden van meerdere monitorbare apparaten.
	8. Het systeem dient geïntegreerd te kunnen worden met een brandmeldsysteem (BMS) of inbraakalarmsysteem.
	9. Het systeem dient voorzien te kunnen worden van meerdere beveiligingscamera's.

**1.2                PROJECT VEREISTEN**

1. Het systeem bewaakt en controleert de toegang tot de locatie via elektronische toegangscontrollers die gebruikmaken van kaartlezers, keypads. Toegang is mogelijk door gebruik van smartphones. Het systeem is opgebouwd volgens een 1 deurs deurcontroller architectuur. De deurcontroller wordt aangesloten doormiddel van TCP/IP op het netwerk en kan gevoed worden doormiddel van PoE.
2. Het systeem moet in staat zijn om een lift besturing te integreren en schakelbare apparaten te bieden. Alle systeem- en toegangscontrole gebeurtenissen van het systeem worden gelogd in de software.
3. Het systeem dient schaalbaar te zijn van 1 deur tot 1000 deuren. Het dient per deur uitgebreid te kunnen worden.
4. Iedere deurcontroller heeft de mogelijkheid om de hardware van één deur te beheren. Als een lezer voor binnen- en buiten benodigd is dan is hier één deurcontroller voor benodigd.
5. Op iedere deurcontroller staan alle gegevens die benodigd zijn om de toegang te beheren in een offline situatie.
6. De controllers maken gebruik van IPv6 technologie, zodat de hardware plug-and-play is. De controllers dienen automatisch gedetecteerd te kunnen worden.
7. Het systeem is te beheren van een onbeperkt aantal devices voor het beheer van het systeem, genereren rapporten en real-time monitoren van activiteiten.
8. Er zijn geen licentiekosten of terugkerende kosten voor het gebruik van de software. Het is niet gewenst om software op een werkstation of server te installeren.
9. Het systeem ondersteunt minimaal 50.000 credentials.
10. Het systeem biedt minimaal de volgende functionaliteiten:
	1. Toegangscontrole
	2. Deurmonitoring (Deur geforceerd en deur te lang open)
	3. Camerabewaking
	4. Videomanagement
	5. Gebeurtenissen rapportage
	6. Plattegronden
	7. Triggers en acties
	8. Anti-passback
	9. Inbraakalarm integratie
	10. Brandmeldsysteem integratie
	11. Aanwezigheidsrapporten
	12. Remote toegang
	13. Smartphone app voor systeembeheer
	14. Smartphone app voor gebruikersbeheer
	15. Desktoplezer
	16. Ondersteuning voor meerder kaartleestechnieken inclusief bluetooth
	17. Licentievrije software en levenslange gratis updates zonder extra kosten
	18. Integratie met video intercomsysteem.
	19. Draadloze deurbeslagen

**1.3                DEFENITIES**

1. Anti-passback: Wordt gebruikt om het gebruik van doorgegeven credentials tegen te gaan zodat onbevoegde personen geen toegang kunnen krijgen tot de locatie.
2. AWG (American Wire Gauge): Een meeteenheid voor de diameter van draden.
3. Browser: Een computerprogramma dat gebruikt wordt om websites mee te bekijken.
4. Client: Een device waarmee het toegangscontrole systeem beheerd kan worden
5. COM (Common): Een contact van een relais
6. Controller: Een intelligente besturingseenheid die gebruikt wordt om de toegang te controleren en monitoren.
7. DDR3 (Double Data Rate typ 3): Het type RAM met een hoge bandbreedte.
8. Apparaat: Een camera, lamp, alarm, toegangspunt of ander stuk hardware die via de software gemonitord of aangestuurd kan worden.
9. Edge storage: Een methode waarbij de videobeelden op de camera worden opgeslagen
10. EMC: Electromagnetic Compatibility
11. Intercomsysteem: Een deurintercomsysteem dat of standalone kan functioneren of in combinatie met een toegangscontrole systeem. En wordt gebruikt om met bezoekers te communiceren door middel van audio en video.
12. FCC: Federal Communications Commission
13. I/O: Input/Output. Een input wordt gebruikt voor het monitoren van een contact of sensor. Een output is een relais waarmee een apparaat in- of uitgeschakeld worden.
14. IC: Industry Canada.
15. IP: Internet Protocol
16. LAN: Local area network.
17. Mbps: Megabits per second
18. Binnenpost: Hardware waarmee de oproep van een intercomsysteem ontvangen kan worden zodat het mogelijk is om met een bezoeker te communiceren.
19. N.C. (Normally Closed): Het verbreekcontact op een relais
20. N.O. (Normally Open): Het maakcontact op een relais
21. Bewoner/gebruiker: De gebruiker van de binnenpost
22. Open zicht: Zonder obstakels of interferentie.
23. Buitenpost: Hardware die bij een tegenpunt wordt geplaatst waarmee het voor een bezoeker mogelijk is om contact op te nemen met de bewoner van een locatie
24. PC: Personal computer: Wordt gebruikt als een werkstation om de software mee te gebruiken
25. PoE: Power over Ethernet
26. RAM (Random Access Memory): Een geheugen module die wordt gebruikt om tijdelijk informatie op te slaan. Deze informatie dient snel beschikbaar te zijn en zorgt voor een vloeiende werking van de software of besturingssysteem
27. Reader: Hardware die aangesloten wordt op een deurcontroller waarmee een gebruiker geïdentificeerd kan worden om toegang te krijgen tot een deur.
28. RoHS: Restriction of Hazardous Substances.
29. Aanwezigheidsrapporten: Een overzicht van gebruikers die op de locatie aanwezig zijn.
30. RS-485: Een TIA/EIA communicatie standaard voor seriële communicatie
31. RSS-210: ICIC-standaard voor vergunningsvrije radioapparatuur.
32. RSS-GEN: IC standaard voor algemene vereisten en informatie voor de certificering van radioapparatuur.
33. Software controller: Hardware dat de software en database van het systeem bevat.
34. SIP: Session Initiation Protocol.
35. Solid State Drive (SSD): Een opslag apparaat dat gebruikt van flash geheugen.
36. Systeem: De te installeren hardware en software, gecombineerd met eventuele bestaande hardware en software, om aan de eisen van het project te voldoen.
37. TCP: Transport Control Protocol
38. Credential: Een identificatie methode voor een gebruiker. Dit kan een PIN, kaart of tag zijn. Hiermee wordt bepaald of een gebruiker toegang krijgt tot de deur.
39. Triggers en acties: Een softwarefunctie waarmee regels gemaakt kunnen worden om extra sturingen aan het systeem toe te voegen.
40. UDP: User Datagram Protocol
41. UL: Underwriters Laboratories
42. Unicast: Een communicatieprotocol waarbij informatie naar één ontvanger gestuurd wordt
43. UPS: Uninterruptibe power supply
44. USB: Universal Serial Bus. Een communicatiepoort die gebruikt wordt op meeste computers
45. Vandaalbestendig (VB): Geeft aan of een product bestemd is tegen vandalisme.
46. Bezoeker: Een onbekende gebruiker die op de locatie op bezoek komt
47. WAN: Wide area network.
48. Wiegand: Gepatenteerd magnetisch principe dat gebruik maakt van speciaal behandelde draden die in de identificatiekaart zijn ingebed. Ook bekend als lezergegevensuitvoerformaat en Wiegand-signaal.

**1.4                SYSTEEM BESCHRIJVING**

1. Algemeen
	1. Het systeem beheert de toegang van de gebruikers door de deuren op de locatie.
	2. Het systeem beheert het opnemen van videobeelden via IP-camera’s op locatie.
	3. Gebruikers worden geïdentificeerd in het systeem op basis van de volgende punten:

a. Het aanbieden van een credential aan een lezer

b. Het aanbieden van een smartphone, smartwatch of tablet aan de lezer

c. Het intoetsen van een unieke pincode op een keypad

d. Een audio of visuele bevestiging van de aanwezigheid van een gebruiker

 e. Een combinatie van het bovenstaande

* 1. Het systeem dwingt het gebruik van facility of site codes met credentials niet af. Elke credential heeft een unieke encryptie voor hoge veiligheid.
	2. Het systeem voorziet in unieke kaartserienummers zodat de beheerder niet hoeft bij te houden welke kaartnummers er aangeschaft dienen te worden.
	3. Een PC, laptop of tablet wordt gebruikt om het toegangscontrole systeem te beheren.
1. Een wachtwoord is vereist voor het inloggen van de software
	1. Er is een app beschikbaar om het systeem mee te beheren en om gebruikers toe te voegen

a. De app is beschikbaar voor Android en iOS apparaten

1. Hardware
	1. De volgende hardware is beschikbaar:
2. Een server
3. Deurcontrollers
4. Video controllers
5. Camera's
6. Alarm Connector
7. Zender/ontvanger voor de draadloze deurbeslagen
8. Kaartlezers
9. Lezer keypads
10. Desktop lezer
11. Voedingen
	1. Alle hardware is plug-and-play.
	2. Alle hardware is voorzien van een duidelijk aansluitlabel voor het snel en eenvoudig installeren van de hardware
	3. Het systeem is voorzien van gratis updates
12. Software
13. De database met alle hardware en gebruikersinformatie wordt op de server bewaard.
14. De server is voorzien van de systeemsoftware en doormiddel van een weblink kan er toegang gekregen worden tot de software
15. De software is zonder installatie toegankelijk voor een onbeperkt aantal werkstations."
16. De software moet toegankelijk zijn met de nieuwste versie van de volgende browsers:
17. Google Chrome
18. Apple Safari
19. De toegang tot de software wordt beveiligd door middel van een wachtwoord
20. De softwaretoegang kan voor iedere gebruiker aangepast worden afhankelijk van hun rechten
21. De software is voorzien van de volgende mogelijkheden:
22. Een grafische gebruikersinterface
23. Tooltips voor ieder softwareonderdeel met een uitleg van de functie
24. Ondersteuning voor smartphones, tablets en PC's
25. Het is mogelijk om tegelijkertijd vanuit meerdere werkstations het systeem te beheren en verschillende functies tegelijk te gebruiken
26. Er zijn geen jaarlijkse licentiekosten voor het systeem of de software. Het systeem kan doormiddel van gratis updates uitgebreid worden.
27. Functionaliteiten
	1. Het systeem en de software biedt de volgende mogelijkheden:
		1. Toegangscontrole
		2. Videomanagement
		3. Integratie met 3rd party camera's
		4. Mogelijkheid tot integreren van een PTZ-camera
		5. Video Wall
		6. Exporteer video
		7. Exporteer screenshots
		8. Video bookmarks
		9. Smart search
		10. Video scrubbing
		11. Video playback
		12. Inbraakalarm integratie
		13. Brandmeldsysteem integratie
		14. Gebruikers importeren
		15. Dynamische plattegronden
		16. Personaliseerbare dashboards
		17. Favorieten
		18. Gebruikersverificatie
		19. Aanwezigheidsrapporten
		20. Mogelijkheid om aanwezigheidsrapporten te mailen
		21. Mogelijkheid om de aanwezigheidsrapporten te bekijken via een smartphone
		22. Triggers en acties om extra functionaliteit toe te voegen aan het systeem
		23. Anti-passback
		24. Software bevoegdheden voor een bedrijfsverzamelgebouw
		25. Multiformat kaartleestechniek voor ondersteuning van meerdere kaartleestechnieken inclusief Bluetooth
		26. Remote toegang voor het beheer op afstand
		27. Beheerders app voor Android en iOS apparaten
		28. Een app voor Android en iOS voor mobile access
		29. Beveiligde https-verbinding tussen het systeem en de client
		30. Opties voor gegevensbeheer
		31. De software is te gebruiken in meerder talen en iedere gebruiker kan onder de eigen taal inloggen
	2. De functies zijn standaard beschikbaar zonder extra kosten

**1.5                PRESTATIE EISEN**

1. Alle wijzigingen die in de software gemaakt worden zullen in real-time gesynchroniseerd worden met de hardware.
2. Gedistribueerde verwerking:
	1. Het systeem is volledig gedistribueerd verwerkingssysteem, zodat informatie (inclusief tijd, datum, geldige codes, toegangsniveaus en soortgelijke gegevens) op zodanige wijze naar de verwerkingsverantwoordelijke wordt gedownload dat elke verantwoordelijkheidsverantwoordelijke beslissingen neemt over de toegangscontrole van die specifieke locatie.
	2. 2. Als de communicatie naar de server onderbroken is zullen de controllers alle gebeurtenissen opslaan totdat de communicatie hersteld is. Wanneer de communicatie hersteld is worden al deze gebeurtenissen gesynchroniseerd met de software.
3. Systeem limieten:
	1. Het systeem ondersteunt ten minste:
		1. 1.000 deuren
		2. 1.000 camera's
		3. 50.000 gebruikers met ieder een unieke credential
		4. Onbeperkt aantal bevoegdheden
		5. Onbeperkt aantal rapporten
4. Netwerkvereisten
	1. De client communiceert met de server via HTTPS, en maakt gebruik van een SSL-encryptie.
		1. Systeemgebeurtenissen worden bewaard en kunnen via de client bekeken worden
		2. Wijzigingen die op de client gemaakt zijn worden direct in de database opgeslagen
	2. De server communiceert met de hardware doormiddel van HTTPS
		1. Toegangsgebeurtenissen worden naar de server gecommuniceerd
		2. Wijzigingen in de database zullen gecommuniceerd worden naar de hardware
	3. Het systeem maakt gebruik van standaard netwerkprotocollen zodat het systeem op bedrijfsnetwerken geïnstalleerd kan worden.
	4. Het is niet nodig om handmatig IP-adressen toe te kennen aan de hardware

**1.6                KWALITEITSVERZEKERING**

1. De software ontvangt gratis updates gedurende de levensduur van het systeem
2. Alle geleverde hardware is voorzien van minimaal 5 jaar garantie met uitzondering van de server welke voorzien is van 2 jaar garantie. De volgende defecten zijn gedekt:
	1. Elektrisch
	2. Elektronisch
	3. Componenten
	4. Mechanisch
3. Alle hardware wordt voorzien van gratis firmware updates
	1. **GERELATEERDE DOCUMENTEN**
4. Het systeem moet communiceren met andere fysieke delen van de faciliteit en met elke constructie, zowel nieuw als gerenoveerd.
5. Tijdens het installeren en plaatsen van de hardware dient de installateur rekening te houden met alle in de regio geldende richtlijnen.
	1. **NALEVING**
6. Het systeem moet voldoen aan:
	1. The General Data Protection Regulation (GDPR) 2019
	2. EN60839-11-1 Grade 2
	3. EN60839-11-1 Grade 3
7. Alle lezers moeten voldoen aan:
	1. EN 301 489-1 for EMC {EU}
	2. EN 300 330 for Radio {EU}
	3. EN 60950-1 for Safety {EU}
	4. IEC/EN 60950-1 for Safety {ROW}
	5. FCC Part 15C for Radio {US}
	6. UL294 for Safety {US}
	7. RSS-GEN, 210 for Radio {Canada}
	8. CS C22.2 NO. 205-M1983 for Safety {Canada}
	9. IP67 for Moisture resistance
8. De vandaalbestendige lezers moeten voldoen aan:
	1. EN 301 489-1 for EMC {EU}
	2. EN 300 330 for Radio {EU}
	3. EN 60950-1 for Safety {EU}
	4. IEC/EN 60950-1 for Safety {ROW}
	5. FCC Part 15C for Radio {US}
	6. UL294 for Safety {US}
	7. RSS-GEN, 210 for Radio {Canada}
	8. CS C22.2 NO. 205-M1983 for Safety {Canada}
	9. IP67 voor vochtbestendigheid
	10. IK10 voor slagvastheid
9. De Alarm connectors moeten voldoen aan:
	1. EN 55032 for EMC {EU}
	2. EN 50130-4 for EMC {EU}
	3. EN 60950-1 for safety {EU}
	4. FCC Part 15B for EMC {US}
	5. UL 294 for safety {US}
	6. ICES-003 for EMC {Canada}
	7. CSA C22.2 NO. 205-M1983 for safety {Canada}
10. De Wireless connectors moeten voldoen aan:
	1. EN 301 489-1 for EMC {EU}
	2. EN 300 328 for Radio {EU}
	3. EN 60950-1 for Safety {EU}
	4. UL/CSA 60950-1 for Safety {US/Canada}
	5. IEC 60950-1 for CB scheme
	6. FCC Part 15C for Radio {US}
	7. RSS-GEN, 210 for Radio {Canada}
11. De server moet voldoen aan:
	1. EN 60950-1 for safety {EU}
	2. EN 55022 for EMC {EU}
	3. EN 55024 for EMC {EU}
	4. EN 61000-3-2 for EMC {EU}
	5. EN 61000-3-3 for EMC {EU}
	6. Europe RoHS for Environmental compliance {EU}
	7. FCC 47 CFR Part 15, Subpart B for EMC {US}
	8. UL/CSA 60950-1 for safety {US/Canada}
	9. ICES-003 for EMC {Canada}
	10. IEC 60950-1 for safety
	11. CISPR 22 for EMC
	12. CIPSR 24 for EMC
	13. IEC/EN 61000-4 Series for EMC
12. Controllers moeten voldoen aan:
	1. EN 55032 for EMC {EU}
	2. EN 55024 for EMC {EU}
	3. IEC/EN 62368-1 for Safety {EU}
	4. FCC part 15B for EMC {US}
	5. UL 294 for Safety {US}
	6. CSA C22.2 NO. 205-M1983 for safety {Canada}
	7. ICES-003 for EMC {Canada}
	8. IEC 62368-1 for CB scheme
13. De desktoplezer moet voldoen aan:

1.       EN 301 489-1 for EMC {EU}

2.       EN 300 330 for Radio {EU}

3.       IEC/EN 60950-1 for Safety {EU}

4.       FCC Part 15C for Radio {US}

5.       RSS-GEN, 210 for Radio {Canada}

6.       UL/CSA 62368-1 for Safety {US/Canada}

1. De camera's moeten voldoen aan:
2. RoH53 2015/863 {EU}
3. EN 55032 for Emissions {EU}
4. EN 50130-4 for Safety {EU}
5. EN 60950-1 for safety {EU}
6. FCC part 15B for EMC {US}
7. ICES-003 {Canada}
8. UL/CSA 60950-1 for safety {US/Canada}
	1. **ALGEMENE EISEN VOOR FUNCTIONALITEIT**
9. Door gebruik te maken van een deurcontroller is het mogelijk om:
10. Een elektronisch slot van een deur aan te sturen
11. De deurstand(open/dicht) te monitoren door middel van een magneet contact
12. Deur geforceerd alarmen te genereren
13. Gebeurtenissen naar de server communiceren
14. Extra connectoren aan te sluiten voor extra functionaliteiten
15. Door gebruik te maken van een Video controller is het mogelijk om:

1. Een elektronisch slot van een deur aan te sturen

2. De deurstand(open/dicht) te monitoren door middel van een magneet contact

3. Deur geforceerd alarmen te genereren

4. Om de videobeelden van vier 3rd party camera’s op te slaan

5. Gebeurtenissen naar de server communiceren

6. Extra connectoren aan te sluiten voor extra functionaliteiten

1. Het is mogelijk om extra apparatuur aan te sturen en te monitoren door middel van overgebleven in- en uitgangen van een controller die niet gebruikt worden voor het beveiligen van de deur.
2. Door gebruik te maken van een Alarm connector is het mogelijk om:
3. Te integreren met een inbraakalarmsysteem of brandmeldsysteem
	* 1. Het in-en uitschakelen van het inbraakalarmsysteem
		2. Monitor de inschakelstatus van het inbraakalarmsysteem
		3. Monitor of het inbraakalarmsysteem in alarm is
		4. Monitor de status van het brandmeldsysteem
4. Het is mogelijk om extra apparatuur aan te sturen en te monitoren door middel van overgebleven in- en uitgangen van een controller die niet gebruikt worden voor het beveiligen van de deur.
5. Door gebruik te maken van een kaartlezer is het mogelijk om een credential te lezen
	1. Een gebruiker kan een credential of smartcredential aanbieden bij een lezer om toegang te krijgen tot een deur
		1. Wanneer een ongeldige credential aangeboden is wordt de toegang geweigerd
	2. Een gebruiker kan een credential aanbieden bij een lezer om een apparaat te bedienen
		1. Wanneer een ongeldige credential aangeboden is wordt het apparaat niet bedient
	3. Er wordt een visuele feedback getoond tijdens het aanbieden van een credential
		1. De visuele feedback geeft aan of de credential geldig of ongeldig is
	4. Er wordt een pieptoon aan de gebruiker gegeven wanneer een credential aangeboden wordt
		1. De pieptoon geeft aan of de credential geldig of ongeldig is
6. Door gebruik te maken van een keypads is het mogelijk voor een gebruiker om gebruik te maken van een PIN of code
	1. Het is mogelijk om dubbele verificatie toe te passen door gebruik te maken van een kaart en een PIN om de veiligheid van de locatie te verhogen
	2. Het systeem vereist een gebruikersauthenticatiemodus die geschikt is voor het apparaat of toegangspunt dat bediend moet worden. De lezer werking modus verandert automatisch op verschillende tijdstippen van de dag of dagen van de week, afhankelijk van de configuratie.
7. Door gebruik te maken van een software controller is het volgende mogelijk;
	1. Toegang tot de software voor configuratie, onderhoud, beheer en monitoring van het systeem.
	2. Bewaar de systeemdatabase op een centrale locatie.
	3. Registreren van systeem en toegangscontrole gebeurtenissen, om deze live of op een later tijdstip deze te kunnen bekijken.
8. Het moet mogelijk zijn om verschillende hardware te gebruiken in het systeem om aan de vereisten van het project te voldoen:
9. Het systeem maakt gebruik van de bestaande netwerkinfrastructuur van de locatie. {Verwijderen als niet dit niet van toepassing is voor het project}
10. Het systeem moet operationeel blijven wanneer:
	1. Het systeem blijft functioneren wanneer de software controller offline gaat of uitstaat.
	2. Iedere deurcontroller of connector zal blijven functioneren wanneer netwerk of andere deurcontrollers niet bereikbaar zijn.
	3. Elke controller moet worden uitgerust met een back-up accu om ervoor te zorgen dat de controller en de connectoren blijven werken tijdens stroomuitval. {Niet van toepassing als er geen back-up accu geplaatst wordt}
		1. De back-up accu wordt gemonitord door het systeem en geeft de huidige status van de back-up accu weer in de gebruikersinterface.
	4. **ALGEMENE EISEN VOOR COMMUNICATIE**
11. De software controller dient verbonden te worden aan het lokale TCP/IP netwerk.
	1. Er wordt een lokale link verstrekt waarop de software toegankelijk moet zijn op elke computer binnen hetzelfde netwerk.
	2. Indien nodig wordt een remote link gegenereerd waarvoor de software toegankelijk moet zijn op elke computer met een internetverbinding, op voorwaarde dat de software controller ook internettoegang heeft.
	3. Communicatie tussen de software en de software controller verloopt via een beveiligde https-verbinding, versleuteld met SSL.
	4. De software dient door een client bereikbaar zijn via een DNS naam.
12. Deurcontrollers dienen aangesloten te worden op het lokale TCP/IP-netwerk.
	1. Controllers dienen gebruik te maken van IPv6 link-local.
	2. Deurcontrollers dienen te communiceren met de software controller.
	3. Deurcontrollers dienen te over het netwerk te communiceren met andere deurcontrollers (peer to peer).
	4. Deurcontrollers dienen automatisch gedetecteerd te worden door de software controller
13. Camera's dienen aangesloten te worden op het lokale TCP/IP-netwerk.
	1. Camera's dienen gebruik te maken van IPv6 link-local.
	2. Camera's communiceren met de software controller voor configuratie en gebruik.
	3. Camera's communiceren de videobeelden direct naar de client waardoor de bandbreedte vereisten op het netwerk worden verminderd.
	4. De lokaal opgeslagen videobeelden op de camera en de communicatie van en naar de camera zal voorzien zijn van een encryptie
		1. De encryptiesleutel is alleen bekend door het systeem en hoeft niet door de gebruiker ingevoerd te worden.
14. Camera, video en configuratie moeten met een wachtwoord worden beveiligd.
	* 1. Camera’s worden automatisch ontdekt met behulp van ONVIF Profile detectie.
		2. Camera’s communiceren met een videocontroller.
15. De camera's dienen verbonden te worden aan het lokale TCP/IP netwerk.
	1. De camera's worden handmatig toegevoegd doormiddel van het RTSP-adres.
	2. De camera's dienen te communiceren met een video controller.
16. Lezers dienen aangesloten te worden op een controller.
	1. Per lezer wordt een enkele 22 AWG, 4-aderige twisted pair kabel gebruikt.
		1. Aan de lezer zit standaard 5 meter aangegoten kabel.
		2. De kabeltype om de kabel mee te verengen dient een 22 AWG, 4-aderige twisted pair kabel gebruikt.
		3. De lezer kabel kan verlengd worden tot maximaal 100 meter.
	2. De lezers worden automatisch gedetecteerd door de deurcontroller.
	3. Iedere deurcontroller ondersteund minimaal 2 kaartlezers
17. De desktoplezer wordt verbonden met de client PC.
	1. De desktoplezer wordt gebruikt om kaartgegevens toe te voegen aan de software via de Client PC.
	2. De desktoplezer wordt doormiddel van een mini USB naar USB A kabel verbonden aan de client PC.
	3. De desktoplezer dient Plug and Play te zijn en er is geen driver nodig.
18. Alle deurcontrollers die op het netwerk aangesloten worden dienen IPv6 te ondersteunen voor automatische detectie en plug-and-play-functionaliteit.
19. Alle gebruikte camera's zijn voorzien van 2 videostream. Een Hoofdstream met hoge resolutie en een substream met lage resolutie. De substream wordt gebruikt om netwerkbandbreedte te besparen bij het streamen van meerdere videostreams.
20. Het systeem maakt gebruik van standaard netwerkprotocollen om installatie op bedrijfsnetwerken mogelijk te maken.

**2.1                FABRIKANTEN**

1. Fabrikant: Paxton {Verwijder indien nodig}
	1. E-mailadres: {Verwijder opties die niet vereist zijn}
		1. {UK} [support@paxton.co.uk]
		2. {FR} [support@paxtonaccess.fr]
		3. {US} [supportUS@paxton-access.com]
		4. {DE} [verkauf@paxton-gmbh.de]
		5. {NL} [support@paxton-benelux.com]
	2. Telefoonnummer:
		1. {UK} [01273 811011]
		2. {FR} [01 57 32 93 56]
		3. {US} [877.438.7298]
		4. {DE} [0251 2080 6900]
		5. {NL} [076 3333 999]
	3. Skype:
		1. {UK} [Paxton.support]
		2. {FR} [Paxton.benelux.support]
		3. {US} [usaPaxton.support]
		4. {DE} [Paxton.gmbh.support]
2. Vervangingen: niet toegestaan. {Verwijder indien nodig}
3. De componenten van het systeem zullen verkrijgbaar zijn bij dezelfde fabrikant om compatibiliteit van producten te garanderen.
4. Componenten bestaan ​​uit:
5. Systeemsoftware. De fabrikant zal het software-engineeringspersoneel in dienst hebben dat de code voor het systeem schrijft en beheert en zal alle vereiste licenties onderhouden.
6. Deurcontrollers. De fabrikant zal deurcontrollers en videocontrollers leveren voor een plug-and-play-oplossing om een ​​gebouw en deuren te beveiligen.
7. Lezers. De fabrikant zal Proximity-lezers, keypads en vandaalbestendige varianten leveren voor het identificeren en toegang geven van een gebruiker.
8. Tokens/credentials. De fabrikant heeft verschillende kaarten en tags beschikbaar voor het project.
9. Camera's. De fabrikant levert zijn eigen assortiment plug-and-play, 4K beveiligingscamera’s. De camera's zullen verkrijgbaar zijn in verschillende modellen.
10. Deurintercom. Mocht dit nu of op een later tijdstip nodig zijn, dan zal de fabrikant plug-and-play binnen- en buitenposten leveren om bezoeker te laten communiceren doormiddel van een spreek luisterverbinding met een gebruiker van het systeem. Het intercomsysteem zal worden geïntegreerd op een nieuw of bestaand systeem.
11. Draadloze deurbeslagen. Mocht het nu of op een later tijdstip nodig zijn, dan zal de fabrikant draadloze deurklinken leveren voor toegangscontroleoplossingen waar een bedrade oplossing niet haalbaar is. De draadloze deurkruk kan op elk moment en in elke hoeveelheid worden toegevoegd aan het systeem.
12. Vervangingsbeperkingen

1. Geen vervanging

* 1. **SPECIFIEKE VEREISTEN VOOR TOKENS**
1. De fabrikant van het systeem moet Paxton HiTag2 125KHz-tokens kunnen leveren.
	1. De geleverde kaarten of tags bevatten een authenticatiemethode om het kopiëren en ongeoorloofd gebruik van tokens te ontmoedigen.
	2. **SPECIFIEKE VEREISTEN VOOR {PAXTON10} SERVER**
2. Functies
	1. Bewaar de systeemdatabase op een centrale locatie.
	2. De software is geïnstalleerd op krachtige hardware die geleverd wordt door de fabrikant
	3. De fabrikant zorgt voor een USB-opslagapparaat voor externe back-ups van de database.
		1. Deze wordt zonder extra kosten geleverd.
		2. De capaciteit van het USB-opslagapparaat moet minimaal 32 GB zijn.
		3. Database back-ups worden automatisch gemaakt.
	4. 4. De Software Controller werkt plug-and-play.
	5. 5. De server zal alle wijzigingen communiceren naar alle andere apparaten in het systeem.
	6. 6. De software om het systeem te beheren moet vooraf op de server zijn geïnstalleerd.
		1. De software is toegankelijk vanaf elk client op hetzelfde netwerk.
3. Installatie

1. De software controller zal plug-and-play zijn.

2. Na installatie is geen verdere configuratie met de hardware vereist.

1. De database wordt bewaard op de software controller en bevat de volgende items.
	1. Gebruikers
		1. Naam
		2. Emailadres
		3. Geldig van/geldig tot datum
		4. Profielfoto
		5. Groepen
		6. Bevoegdheden
		7. Gebruikersvelden
		8. Gebruikersvoorkeuren
	2. Rapporten

a. Een overzicht van alle systeem en toegangsgebeurtenissen

* 1. Dashboards
	2. Plattegronden
	3. Apparaten

a. Naam

b. Hardware mapping

c. Configuratie

d. Groepen

e. Bevoegdheden

* 1. 6. Regels
		1. Specifieke Regels
		2. Bevoegdheden
		3. Tijdschema's
		4. Roll Call Rapport
		5. Anti-Passback configuratie
1. Software Controller specificatie
	1. De software controller in voorzien van minimaal een Intel core i3
	2. De software controller in voorzien van minimaal 8GB RAM-geheugen.
		1. Het RAM-geheugen is DDR3.
	3. De software controller is voorzien van interne harde schijf voor de opslag van de database

a. De harde schijf is een Solid State Drive (SSD)

b. De harde schijf heeft een opslagcapaciteit van minstens 60GB

4. De software Controller is voorzien van een Intel® HD

1. Adapter
	1. De software controller wordt gevoed doormiddel van 19volt, 65 watt AC-DC adapter.

a. De Adapter wordt geleverd zonder extra kosten.

* 1. De software controller zal voorzien zijn van maximaal 25 Watt.
	2. De software controller zal een spanningssensor bevatten.
	3. De software controller is ACPI-compliant.
1. Temperatuur

1. De software controller moet voldoen aan de vereiste temperatuurnormen voor een intern product.

* + 1. De software controller moet betrouwbaar werken binnen het temperatuurbereik van 0°C tot +50°C.
1. Behuizing
	1. Het ontwerp van de behuizing is stijlvol en modern.
	2. De behuizing is gemaakt van aluminium en kunststof.
	3. Er zullen geen zichtbare bevestigingen zichtbaar zijn.
	4. Het artikel is verkrijgbaar in het zwart.
2. Afmetingen.
	1. De afmetingen van de server mogen niet groter zijn dan:
		1. Een breedte van 179mm
		2. Een hoogte van 36.5mm
		3. Een diepte van 182.9mm
	2. **SPECIFIEKE EISEN VOOR {PAXTON10} DEURCONTROLLER**

{Verwijder indien nodig}

1. Functies
	1. De deurcontroller is geschikt voor het aansturen van één toegangspunt.
	2. De deurcontroller kan de deur opensturen binnen ingestelde tijden door middel van een tijdschema.
	3. De deurcontroller slaat de database lokaal op in het ingebouwde geheugen, zodat toegang verleend wordt wanneer de deurcontroller offline is
	4. Het is mogelijk om op de deurcontroller extra connectoren aan te sluiten door middel van de connectorpoort op de deurcontroller.
	5. De deurcontroller bepaalt zelfstandig of een gebruiker toegang krijgt tot een deur of geweigerd wordt.
	6. Het is mogelijk om een back-up accu aan te sluiten op de deurcontroller.
		1. Tijdens een stroomstoring zal de deurcontroller gedurende een periode blijven functioneren.
		2. De deurcontroller toont de status van de back-up accu in de gebruikersinterface.
	7. De database blijft op de deurcontroller bewaard tijdens een stroomuitval.
	8. De deurcontroller is voorzien van verwijderbare schroefconnectoren voor een probleemloze installatie.
2. Installatie
	1. De software controller zal plug-and-play zijn.
	2. Na installatie is geen verdere configuratie met de hardware vereist.
3. Visueel
	1. De controller is voorzien van een duidelijk aansluit label met kleurcoderingen voor de lezers, exit buttons en uitgangen voor een probleemloze installatie.
	2. De controller is voorzien van LED-status lampjes om de status van de verschillende in- en uitgangen weer te geven. Ook is er een LED-status lamp voorzien voor de TCP/IP communicatie.
4. Voeding
	1. De deurcontroller wordt van stroom voorzien doormiddel van;
		1. Power over Ethernet+ (PoE+) via de Power over Ethernet.
		2. Een 12v 2A voeding.
	2. Het stroomverbruik in rust is niet hoger dan 3.0W
	3. Het maximale stroomverbruik is niet hoger dan 5.6W
	4. De controller wordt voorzien van een 12V back-up accu.
5. Temperatuur

1. De deurcontroller voldoet aan de vereiste temperatuurnormen voor een intern product.

a. De controller zal betrouwbaar werken binnen het temperatuurbereik van 0°C tot +45°C.

1. Behuizing
	1. De controller kan geleverd worden in een behuizing die geschikt is voor montage aan een muur
	2. De behuizing is beschikbaar in de kleur wit
	3. De deurcontroller is voorzien van verwijderbare schroefconnectoren voor een probleemloze installatie
2. Afmetingen
	1. De afmetingen van de controller in behuizing mogen niet groter zijn dan.
		1. Een breedte van 236mm
		2. Een hoogte van 322mm
		3. Een diepte van 77mm
3. Aansluitingen
	1. De deurcontroller is voorzien van verschillende aansluitingen om één ​​enkel toegangspunt te bedienen en te beveiligen. De volgende aansluitingen zijn beschikbaar:
		1. 1 x aangedreven slotuitgang

De slotuitgang levert de spanning om een ​​enkel elektrisch slot te beveiligen en te bedienen.

De slotuitgang levert 1A op 12V DC.

De slotuitgang moet configureerbaar zijn voor een arbeidsstroom of ruststroom slot.

* + 1. 1x deurcontact.

Het deurcontact laat de deurstatus zien van een toegangspunt.

* + 1. 1 x exit-knop

Met een exit-knop is het mogelijk om een deur vrij te openen zonder een kaart of tag

De exit knop is voorzien van 12V ledverlichting voor een visuele indicatie of de deur geopend is.

De exit-knop kan worden uitgezet in de software om te voorkomen dat toegang wordt verkregen via hardware sabotage.

* + 1. 2x relais

Elk relais is voorzien van N.O. en N.C.-contacten.

Relaiscontacten moeten spanningsvrij zijn.

Elk relais moet een weerstandsbelasting van ten minste 2A @ 30V DC kunnen schakelen.

Een relais kan worden geconfigureerd als een alarmuitgang.

Een relais kan worden geconfigureerd als een slotuitgang.

 Een relais kan worden gebruikt voor andere apparaten dan het beveiligde toegangspunt

* + 1. 2 x lezer poorten

Het is mogelijk om een ​​combinatie van Proximity-lezers, keypad-Proximity-lezers en vandalismebestendige lezers te gebruiken.

De randapparatuur van de lezer levert gegevens en stroom aan alle aangesloten lezers

De lezer poort accepteert verschillende data types van verschillende type kaarten of tags met verschillende lengte kaartnummers. De lezer poort accepteert de verschillende datatypes;

1. PIN

2. Code

3. Kaartserienummer

4. Bluetooth credential ID

De lezer poort geeft de huidige status weer aan de gebruiker die de lezer gebruikt. Doormiddel van een LED op de lezer en een pieptoon.

De lezer poort voorziet voldoende spanning om de aangesloten lezer te laten functioneren.

Naast het openen van een deur kan een lezer gebruikt worden om andere apparaten aan te sturen.

* + 1. 1 X vrije ingang
1. (!) De vrije ingang kan gebruikt worden als exit knop ingang
2. De vrije ingang kan gebruikt worden om een externe voeding te monitoren
3. De vrije ingang kan gebruikt worden voor andere apparaten om de status voor deze apparaten te monitoren
	1. Het is mogelijk om iedere aansluiting van een deurcontroller te mappen voor gebruik met verschillende apparaten
	2. De deurcontroller is voorzien van een connector poort
4. De aangesloten connectoren communiceren met het systeem via de deurcontroller
5. De deurcontroller voorziet spanning voor de aangesloten connectoren.
	1. De deurcontroller is voorzien van een potentiaal vrije sabotage ingang.
6. Het systeem genereert een alarm gebeurtenis wanneer de behuizing geopend is.
	1. De deurcontroller is voorzien van aansluitingen van een back-up accu.
7. Een 12V DC 7Ah back-up accu kan geïnstalleerd worden.
8. De controller monitort de back up accu status.
	1. **SPECIFIEKE EISEN VOOR {PAXTON10} VIDEOCONTROLLER**{Verwijder indien nodig}
9. Functies
	1. De video controller is geschikt voor het aansturen van één toegangspunt.
	2. De video controller kan de deur opensturen binnen ingestelde tijden door middel van een tijdschema.
	3. De videocontroller zorgt voor de verwerking en opslag van minimaal 4 netwerkcamera's.
	4. De videocontroller moet ten minste 2 videostreams van elke camera verwerken en opnemen, naast een regelmatig periodiek QCIF-beeld. De verwerkingsverantwoordelijke voorziet het systeem van:
		1. Een videostream met hoge resolutie, tot 4K resolutie bij 20 FPS
		2. Een videostream met lage resolutie, tot 640 x 480 resolutie bij 15 FPS
		3. Een QCIF-beeld met lage resolutie, opgenomen met 1 FPS
	5. De videocontroller heeft een aansluiting voor 2 harde schijven.
	6. De deurcontroller slaat de database lokaal op in het ingebouwde geheugen, zodat toegang verleend wordt wanneer de deurcontroller offline is
	7. Het is mogelijk om op de videocontroller extra connectoren aan te sluiten door middel van de connectorpoort op de deurcontroller.
	8. De videocontroller bepaalt zelfstandig of een gebruiker toegang krijgt tot een deur of geweigerd wordt.
	9. Het is mogelijk om een back-up accu aan te sluiten op de videocontroller.
		1. Tijdens een stroomstoring zal de videocontroller gedurende een periode blijven functioneren.
		2. De videocontroller toont de status van de back-up accu in de gebruikersinterface.
	10. De database blijft op de videocontroller bewaard tijdens een stroomuitval.
	11. De videocontroller is voorzien van verwijderbare schroefconnectoren voor een probleemloze installatie
10. Installatie

1. De videocontroller zal plug-and-play zijn.

2. Na installatie is geen verdere configuratie met de hardware vereist.

1. Visueel
	1. De videocontroller is voorzien van een duidelijk aansluit label met kleurcoderingen voor de lezers, exit buttons en uitgangen voor een probleemloze installatie.
	2. De videocontroller is voorzien van LED-status lampjes om de status van de verschillende in- en uitgangen weer te geven. Ook is er een LED-status lamp voorzien voor de TCP/IP communicatie.
2. Voeding
	1. De videocontroller wordt van stroom voorzien doormiddel van;
		1. Power over Ethernet+ (PoE+) via de Power over Ethernet splitte.
		2. Een 12v 4A voeding.
	2. Het stroomverbruik in rust is niet hoger dan 3.9W
	3. Het maximale stroomverbruik is niet hoger dan 8.3W
	4. Er is een mogelijkheid om zelf een 12 Volt Accu te gebruiken
3. Temperatuur
	1. De Controller moet voldoen aan de vereiste temperatuurnormen
		1. De controller zal werken binnen het temperatuurbereik van (0°C tot +45°C).
4. Behuizing
	1. Behuizing voor wandmontage is beschikbaar.
	2. De behuizing zal wit van kleur zijn
	3. De controller moet verwijderbare connectoren bevatten om de installatie en de uitwisseling van kaarten indien nodig te vergemakkelijken. Voor het aansluiten van de aansluitpunten is geen speciaal gereedschap nodig.
5. Afmetingen
	1. De afmetingen van de Controller, indien geplaatst, mogen niet groter zijn dan:
		1. Een breedte van 275 mm
		2. Een hoogte van 320 mm
		3. Een diepte van 70 mm
6. H. Randapparatuur
	1. De controller levert de randapparatuur om één toegangspunt te besturen en te beveiligen. De volgende aansluitpunten zijn beschikbaar:
		1. 1x slotuitgang

De slotuitgang zal de kracht leveren om een slot te beveiligen en te controleren

De slotuitgang levert 1A

De slotuitgang moet configureerbaar zijn als een normally-open of een normally-close slot

* + 1. Deurcontact

Het deurcontact signaleert de open/gesloten status van het toegangspunt

* + 1. 1 x aangedreven exit-knop

Een exit-knop zorgt voor vrij verkeer door het toegangspunt

De randapparatuur voor de exit-knop moet 12V-uitvoer leveren voor visuele indicatie en feedback bij de exit-knop.

Het randapparaat met de exit-knop kan worden uitgeschakeld in de systeemsoftware als het niet wordt gebruikt, om te voorkomen dat toegang wordt verkregen via hardware sabotage.

* + 1. 2x relais

Elk relais moet worden voorzien van N.O. en N.C.-contacten.

Relaiscontacten zijn spanningsvrij.

Elk relais moet een weerstandsbelasting van ten minste 2A @ 30V DC kunnen schakelen.

Een relais kan worden geconfigureerd als alarmuitgang

Een relais kan naast een toegangspunt ook voor andere doeleinden gebruikt worden.

* + 1. 2x lezer poorten

Het is mogelijk om een combinatie van proximity-lezers, keypad-proximity-lezers en vandalismebestendige lezers te gebruiken.

De randapparatuur van de lezer levert gegevens en voeding aan alle aangesloten lezers.

Het randapparaat van de lezer is niet beperkt tot een vaste gegevensinvoer, maar accepteert in plaats daarvan gegevens die worden gelezen van een verscheidenheid aan tokentypen met verschillende lengtes, inclusief maar niet beperkt tot het volgende:

Pin

Code

Token-ID

Bluetooth-referentie-ID

(iv) Het randapparaat van de lezer geeft de huidige statussen weer die relevant zijn voor het te bedienen apparaat om feedback te geven aan de tokenhouder in de vorm van een LED en een luidspreker.

(v) De Het randapparaat van de lezer moet het vermogen leveren dat de lezer nodig heeft om te werken.

(vi) Een lezer kan naast het beveiligde toegangspunt ook met andere apparaten gebruikt worden.

* + 1. 1x digitale ingang

Een digitale ingang kan worden geconfigureerd als een exit-knop

Een digitale ingang kan worden geconfigureerd om een externe PSU te bewaken

Een digitale ingang kan worden gebruikt voor andere apparaten dan het beveiligde toegangspunt

* 1. Het is mogelijk om elk randapparaat toe te wijzen aan verschillende apparaten of aangepaste functionaliteit te geven.
	2. De controller heeft twee SATA-aansluitingen voor het aansluiten van externe harde schijven.
		1. De controller moet een aangedreven MOLEX-uitgang leveren
		2. De controller biedt 2 SATA-aansluitingen
		3. De controller neemt video op naar de schijven met behulp van de RAID 1-configuratie.
	3. De controller biedt een connectorpoort.
		1. Connectoren communiceren met het systeem via de controller.
		2. De controller levert PoE aan de connectoren.
	4. De controller zal een spanningsvrije sabotageschakelaar leveren.
	5. Het systeem genereert een alarmgebeurtenis wanneer een sabotage wordt geactiveerd.
	6. De controller zorgt voor batterijaansluitingen.
	7. Er kan een 12V DC 7Ah accu worden geplaatst.
	8. De controller houdt de stand en de lading van de batterij bij.

**2.6                SPECIFIEKE VEREISTEN VOOR [PAXTON10] ALARMCONNECTOR**

1. Functies
	1. De connector maakt de controle en bewaking van een inbraakalarm mogelijk.
	2. De connector moet de bewaking van een brandalarm mogelijk maken."
	3. De connector is klein en compact, voor installatie in een bestaande alarmpaneel.
	4. De connector is voorzien van een statussignalering
	5. De connector heeft afneembare aansluitingen voor snel en probleemloos onderhoud.
2. Communicatie
	1. De connector bevat een TCP/IP-interface voor netwerkcommunicatie rechtstreeks naar het verwerkingsbord (controller) via een RJ45-connector. Add-on modules zijn niet goedgekeurd.
3. Voeding
	1. Het item werkt op gelijkstroom geleverd door de controller.
		1. Er is geen extra stroombron nodig.
		2. De data en voeding gebruiken dezelfde kabel.
	2. De spanning is 30V.
	3. Stroomverbruik tijdens inactiviteit mag niet hoger zijn dan 0,6 W.
4. Aansluitweergave
	1. Randapparatuur wordt duidelijk en intuïtief weergegeven.
		1. De aansluiting wordt weergegeven
	2. Het artikel bevat LED's voor het opsporen van fouten.
	3. De volgende perifere staten moeten worden aangegeven:

a. relais status

b. input status

* 1. Een LED geeft aan wanneer het item wordt gevoed.
1. Temperatuur
	1. De bedrijfstemperatuur is tussen 0°C en 55°C.
2. Behuizing

1. Het item moet klein en compact zijn, zodat het kan worden geïnstalleerd in de bestaande behuizing die wordt gebruikt voor het betreffende alarm.

1. Afmetingen

1. De afmetingen van de I/O-connector mogen niet groter zijn dan:

* + 1. Een breedte van (51 mm)
		2. Een hoogte van (68 mm)
		3. Een diepte van (34 mm)
1. Randapparatuur
	1. De alarmconnector moet een enkel bestuurbaar relais bevatten.
		1. Elk relais is voorzien van een COM, N.O. en N.C.-contacten.
		2. Relaiscontacten moeten spanningsvrij zijn.
		3. Elk relais moet een belasting kunnen schakelen van ten minste:

(i) 2A @ 24V DC

(ii) 0,5A @ 125V AC

* + 1. Elk relais behoudt zijn status wanneer de alarmconnector stroom verliest.
		2. De relaisfunctionaliteit kan worden geconfigureerd in de toegangscontrolesoftware die bij het systeem wordt geleverd.
	1. De alarmconnector moet 2 digitale ingangen bevatten.
		1. Elke ingang bestaat uit 2 aansluitklemmen.
		2. Elke ingang moet minimaal 14V kunnen weerstaan.
		3. De begin- en eindwaarde die het systeem aan elke status zal koppelen, zijn:

Laag: < 0,8 V

Hoog: > 3,0V

* + 1. Elke ingang kan worden geconfigureerd om een trigger- en actieregel te activeren om geautomatiseerde triggers en acties uit te voeren.
	1. De alarmconnector bevat geen sabotageschakelaar-ingang.
		1. . De alarmconnector moet worden geïnstalleerd in de behuizing van een alarmpaneel of een andere connector, waarvan de eigen sabotage moet zijn voorzien.
		2. Het moet mogelijk zijn om een reserve-ingang op de alarmconnector of een andere connector te gebruiken om alarmgebeurtenissen binnen het systeem te genereren als een sabotage-ingang vereist is.

**2.7                SPECIFIEKE VEREISTEN VOOR [PAXTON10] WIRELESS CONNECTOR**{Verwijder indien nodig - Draadloze connector vereist voor PaxLock}

1. Functies
2. De Wireless Connector zorgt voor communicatie met draadloze deurbeslagen.
3. De Wireless Connector zorgt voor communicatie met Z-Wave-apparaten.
4. Er kunnen drie Paxton10 Wireless Connectoren in serie worden aangesloten vanaf één controller.
5. De Wireless Connector is voorzien van een led status.
6. Communicatie
7. De connector bevat een TCP/IP-interface voor netwerkcommunicatie rechtstreeks naar het verwerkingsbord (controller) via een RJ45-connector. Add-on modules zijn niet goedgekeurd.
8. De connector bevat een Bluetooth-interface voor communicatie met elektronische deurbeslagen.
	* 1. De connector communiceert via Bluetooth Low Energy (BLE) 2,4 GHz
9. Voeding
10. Het item werkt op gelijkstroom geleverd door de controller.
	1. Er is geen extra stroombron nodig.
	2. De data en voeding gebruiken dezelfde kabel.
11. De bedrijfsspanning is 30V.
12. Het stroomverbruik bij inactiviteit mag niet hoger zijn dan 0,7 W.
13. Het stroomverbruik tijdens Bluetooth-activiteit mag niet hoger zijn dan 0,8 W.
14. Aansluitweergave
	1. De Wireles Connector heeft een led status weergave.
		1. Gezondheid en communicatie
		2. Bluetooth activiteit
		3. Z-Wave activiteit
15. Temperatuur
	1. Het artikel moet betrouwbaar werken binnen het temperatuurbereik van (0°C tot +45°C).
16. Behuizing
	1. Door zijn moderne en compacte uiterlijk is de Paxton10 Wireless Connector speciaal ontworpen voor zichtbare montage aan de muur of onder het plafond.
	2. De behuizing is wit.
	3. Het artikel moet geschikt zijn voor montage:
		1. Op een muur
		2. Aan een plafond
		3. Op een gipsplaat
		4. Op een achterplaat
17. Afmetingen
	1. De afmetingen van de connector mogen niet groter zijn dan:
	2. Een breedte van 164 mm
	3. Een hoogte van 163 mm
	4. Een diepte van 34 mm
18. Randapparatuur
	1. De Wireless Connector bevat een RS485-poort voor doorlussen naar extra connectoren.
		1. Er kunnen maximaal 3 connectoren worden door-gelust vanaf één controller (maximaal 100 meter tussen 2 Wireless Connectors)
		2. Voeding en communicatie moeten in serie worden geschakeld.

**2.8   SPECIFIEKE VEREISTEN VOOR [PAXTON10] CAMERA'S**

1. Functies
	1. Alle camera's zullen een resolutie vanaf 4K kunnen weergeven.
	2. Alle camera's moeten ultralichtsensoren bevatten voor opnamen bij weinig licht.
	3. IR-bereik van camera's moet minimaal 30 meter zijn.
	4. Alle camera's hebben ingebouwde opslag voor directe opname op de camera (edge-opslag).
	5. Alle camera's moeten audio kunnen opnemen.
	6. Elke camera voorziet het systeem van meerdere videostreams van verschillende kwaliteit:
		1. Een videostream met hoge resolutie, tot 4K resolutie bij 20 FPS
		2. Een videostream met lage resolutie, tot 640 x 480 resolutie bij 15 FPS
		3. C. Een QCIF-beeld met lage resolutie, opgenomen met 1 FPS
	7. Video wordt alleen opgenomen wanneer beweging wordt gedetecteerd, waardoor de opslagefficiëntie wordt gemaximaliseerd en videobeelden van niet-betrokken scènes worden geminimaliseerd.
	8. De fabrikant levert 4 cameravarianten:
		1. Mini Bullet camera
		2. Mini Dome camera
		3. Vari-focal Bullet camera
		4. Vari-focal Dome camera
	9. All camera’s zijn plug-and-play.
	10. Alle camera's communiceren via een IP-netwerk.
	11. Alle gegevens blijven behouden tijdens stroomuitval.
2. Communicatie
	1. De camera verwerkt en neemt zijn eigen video op, zonder dat er voortdurend communicatie met een externe videorecorder nodig is.
	2. De camera communiceert met de software controller en clients via TCP/IP.
	3. De maximale videobandbreedte kan worden geconfigureerd om te voldoen aan de vereisten van het netwerk.
3. Gebruikersinteractie
	1. Alle camera's zijn plug-and-play.
		1. Camera's nemen standaard 1080p op met 20 FPS.
		2. Standaard nemen camera's videobeelden op in hun interne opslag.
	2. De volgende cameraparameters kunnen worden geconfigureerd:
		1. Videorotatie
		2. Videostandaard (PAL/ NTSC)
		3. Video resolutie
		4. Frame rate (FPS)
		5. Maximale bit snelheid (Kbps)
	3. Voor de varifocale camera's is de volgende aanvullende configuratie beschikbaar:
	4. Brandpuntsafstand
	5. De volgende video-opname-instellingen kunnen worden geconfigureerd:
		1. Video-opslaglocatie

Intern – opslaan op camera

Extern – opslaan naar netwerklocatie (externe nas)

* + 1. Video-opslagperiode/ Video automatisch verwijderen na een bepaalde tijdsperiode.
	1. Na installatie is geen verdere interactie met de hardware vereist.
1. Voeding
	1. Elke camera wordt gevoed met PoE.
	2. Het maximale stroomverbruik van een camera mag niet hoger zijn dan 15 W.
2. Temperatuur
	1. Elke camera moet voldoen aan de vereiste temperatuurnormen voor een extern product.
		1. De camera moet betrouwbaar werken binnen het temperatuurbereik van -30°C tot +60°C
3. Behuizing
	1. Elke camera moet geschikt zijn voor montage:
		1. Aan de muur
		2. Tegen het plafond
	2. Elke camera moet vandaalbestendig zijn volgens IK10.
		1. Volledige metalen behuizing
	3. Elke camera moet weerbestendig zijn volgens IP67.
4. Afmetingen
	1. De afmetingen van de Mini Bullet-camera’s mogen niet groter zijn dan:
		1. Een breedte van 70 mm
		2. Een hoogte van 68 mm
		3. Een diepte van 171 mm
	2. De afmetingen van de Mini Dome-camera’s mogen niet groter zijn dan:
		1. Een diameter van 111 mm
		2. Een diepte van 82,4 mm
	3. De afmetingen van de varifocale bullet-camera’s mogen niet groter zijn dan:
		1. Een diameter van 144,13 mm
		2. Een diepte van 332,73 mm
	4. De afmetingen van de varifocale dome-camera’s mogen niet groter zijn dan:
		1. Een diameter van 153,4 mm
		2. Een diepte van 133,1 mm
5. Randapparatuur
	1. Iedere camera is voorzien een geheugenkaartsleuf voor video opslag
		1. De camera biedt ondersteuning voor de volgende geheugenkaarten:

(i) Micro SD

(ii) Micro SDHC

(iii) Micro SDXC

* + 1. De camera biedt ondersteuning voor SD-kaarten tot een capaciteit van 256GB
		2. De schrijfsnelheid is minimaal 25 MB/s
		3. De leessnelheid is minimaal 95 MB/s

**2.9               Specifieke vereisten voor de [PAXTON10] SOFTWARE**

1. Gebruikersinterface
	1. De software wordt gehost op een software controller
	2. De software is bereikbaar vanaf iedere PC met netwerktoegang.
	3. Er is geen software-installatie benodigd op een client werkstation.
	4. De software is kosteloos beschikbaar
	5. De fabrikant van de software stelt kosteloos updates voor de software beschikbaar.
	6. De software is voorzien van alle functies om een toegangscontrole systeem te configureren en beheren
	7. De software biedt alle functies die nodig zijn voor het beheer van een video managementsysteem
2. Remote toegang
	1. Het is mogelijk om overal ter wereld toegang te krijgen tot de software met een internetverbinding.
	2. Het is mogelijk om softwaregebruikers rechten te geven om toegang te krijgen tot de software op afstand.
3. Vereisten voor clientwerkstations
	1. De toegang tot de software is mogelijk vanaf elke PC of apparaat met de nieuwste versie van:
		1. Google Chrome
		2. Apple Safari
	2. De toegang tot de software is mogelijk vanaf iedere tablet of smartphone met een app.
		1. De app is beschikbaar voor de volgende besturingssystemen

IOS

Android

* + 1. De app is kosteloos beschikbaar
1. Weergave
	1. De software biedt een duidelijke en eenvoudige gebruikersinterface
	2. Het menu dient overal in de software toegankelijk te zijn om snel naar andere delen van de software te navigeren.
	3. De taakbalk bovenaan in de software biedt handige snelkoppelingen

a. Het is mogelijk om de taakbalk te verbergen om meer schermruimte beschikbaar te hebben

b. Om de eenvoud te behouden, wordt de taakbalk gevuld snelkoppelingen die relevant zijn voor het menu waar u zich in bevindt.

* 1. Het is mogelijk om de weergave van de items aan te passen
		1. Grote pictogrammen, ideaal voor apparaten met touchscreen. Afbeeldingen van gebruikers en andere items worden weergegeven bij het bekijken
		2. Details, alle items worden in een lijst weergeven zodat meer informatie van een item getoond wordt.
	2. Hoe de software wordt bekeken, wordt voor elke softwaregebruiker opgeslagen, zodat zijn indeling- en lay-outvoorkeur iedere keer dat hij of zij inlogt hetzelfde zijn.
1. Interactie
	1. Het is mogelijk om de software met een touchscreen te bedienen
	2. Het is mogelijk om de software op mobiele apparaten te gebruiken.
	3. Er worden tooltips getoond in de software die uitleg geven over de verschillende softwarefuncties.
2. Groeperen
	1. De software biedt een eenvoudige maar effectieve methode voor het organiseren van verschillende items in de software.
	2. Het is mogelijk om te groeperen op afdelingsniveau of gebouwniveau
3. Gegevensbeheer
	1. De software biedt de mogelijkheid om te voldoen aan de regelgeving over gegevensbescherming.
	2. Alle softwaregebruikers worden gedwongen een sterk wachtwoord aan te maken.
	3. De software biedt de mogelijkheid om:
		1. Gebruikers verwijderen
		2. Rapporten verwijderen
		3. Gebeurtenissen verwijderen
		4. Verwijder gebeurtenissen automatisch na een bepaalde periode
		5. Videobeelden verwijderen
		6. Verwijder videobeelden automatisch na een bepaalde periode
4. Taal

1. De software is beschikbaar in de volgende talen

* 1. Nederlands
	2. Engels (UK)
	3. Engels (US)
	4. Frans
	5. Duits
	6. Spaans
1. Hulp en support
	1. De software biedt hulp aan softwaregebruikers in de vorm van tooltips, wizards, video's en documentatie.
		1. Wizards begeleiden gebruikers door specifieke taken, waardoor de gebruiker de mogelijkheid krijgt om zijn taak te voltooien terwijl hij de stappen leert die nodig zijn.
		2. Video's bieden instructies en ondersteunende informatie om taken uit te voeren en delen van de gebruikersinterface te verkennen.
		3. De documentatie moet bestaan ​​uit gebruikershandleidingen, instructies en datasheets.
		4. Tooltips zijn beschikbaar wanneer u met de cursor over menu items en opties staat.

(i) Indien beschikbaar, zullen tooltips een link bevatten die de gebruiker naar verdere informatie leidt.

* 1. Een ingebouwde helptool stelt de gebruiker in staat de benodigde ondersteuningsinformatie te vinden.

a. De helptool moet toegankelijk zijn vanaf alle locaties in de software.

1. Release notes
	1. Wanneer er een software-update beschikbaar is, worden er release notes getoond aan de gebruiker
	2. De release notes informeren de gebruiker over wat de software update bevat en alle andere belangrijke informatie met betrekking tot de update.

**2.10               Specifieke vereisten voor [PAXTON10] softwarefuncties**

1. Gebruikers
	1. Gebruikers worden met behulp van de software aan het systeem toegevoegd.
		1. Er moeten minimaal 50.000 gebruikers kunnen worden aangemaakt.
		2. Het is mogelijk om minimaal 50.000 unieke credentials aan gebruikers toe te wijzen.
	2. Aan gebruikers worden bevoegdheden toegewezen om te bepalen wat elke individuele gebruiker kan doen, configureren of bekijken.
		1. Gebruikers hebben alleen toegang tot deuren, en controle over apparaten die binnen de bevoegdheid vallen die aan de gebruiker is toegewezen.
		2. Gebruikers moeten kunnen inloggen op de software en items kunnen bekijken/wijzigen die binnen de aan hen toegewezen software bevoegdheden vallen.
	3. Elke gebruiker moet invoervelden bevatten waarin gebruikersgegevens kunnen worden opgeslagen.
		1. De volgende velden zijn standaard beschikbaar:

E-mailadres

Geldig van datum

Geldig tot datum

* + 1. Indien nodig kunnen er extra velden toegevoegd worden om aanvullende informatie vast te leggen:

Mobiel nummer

Kenteken

Adres 1

Adres 2

Plaats

Nederlands

Postcode

* + 1. Het is mogelijk om aangepaste invoervelden te creëren waarbij het bovenstaande niet de gegevens dekt die voor elke gebruiker wordt opgeslagen. Een label dat moet worden weergegeven en het gegevenstype van de gegevens die moet worden ingevoerd/opgeslagen, moet selecteerbaar zijn. De volgende soorten gegevens worden ondersteund:

Aanvinkhokje

Datum

E-mail

Nummer

Tekst

* 1. Het is mogelijk om voor iedere gebruiker een profielfoto te uploaden
		1. Elke gebruikersrecord moet een persoons silhouet als standaardafbeelding hebben.
		2. Het is mogelijk om voor iedere gebruiker een profielfoto te uploaden
		3. Met de software kunnen afbeeldingen tot 4 MB worden geüpload bij een gebruiker.
		4. Minimaal worden de volgende afbeeldingsformaten ondersteund:

JPEG

JPG

GIF

PNG

* + 1. Het moet mogelijk zijn om de geüploade afbeelding binnen de software te bewerken. Het volgende moet minimaal kunnen worden bereikt:

Snij de geüploade afbeelding bij.

Plaats een rand rond de geüploade afbeelding.

Voeg een schaduw toe aan de geüploade afbeelding.

* + 1. De afbeelding wordt gebruikt:

Als een manier om een ​​gebruiker te identificeren

Als een methode om gebruikers te zoeken

In plattegronden om een ​​gebruiker te koppelen aan toegangscontrole gebeurtenissen

In videorapporten om een ​​gebruiker te koppelen aan toegangsgebeurtenissen

In dashboards voor het identificeren van een gebruiker

In een aanwezigheidsrapport als visuele bevestiging

* 1. Het moet mogelijk zijn om credentials aan een gebruiker toe te wijzen.
		1. De volgende typen credentials worden ondersteund:

Wachtwoord

Tag of kaart

Smart credential

PIN

* + 1. Wachtwoorden zijn vereist voor een gebruiker om toegang te krijgen tot de software.

Gebruikers mogen slechts één wachtwoord hebben.

Wachtwoorden moeten door de gebruiker worden aangemaakt wanneer hij voor de eerste keer probeert in te loggen.

De software zal afdwingen dat het wachtwoord dien te voldoen aan een aantal vereisten.

Het wachtwoord dient te voldoen aan de volgende vereisten:

Bevat minimaal 7 tekens.

Bevat ten minste 3 verschillende tekentypen: hoofdletters/ kleine letters / cijfers / leestekens

* + 1. Credentials zijn vereist voor een gebruiker om toegang te krijgen tot en controle te hebben over deuren en apparaten op een systeem.

Het is mogelijk om meerdere credentials aan elke gebruiker toe te wijzen.

credentials worden aan het systeem toegevoegd door middel van:

Een desktoplezer geleverd door de fabrikant van de software.

Een toegang geweigerd gebeurtenis

Er worden meerdere soorten credentials ondersteund. Het moet voor gebruikers mogelijk zijn een type te selecteren en de credential een naam te geven voor bruikbaarheid en herkenbaarheid.

Elk credentialtype wordt onderscheiden door een unieke afbeelding.

Het is mogelijk een credential als verloren te markeren, waardoor alle toegangsrechten voor die credential worden verwijderd, terwijl de gebruiker actief kan blijven met andere credentials.

* + 1. Met smart credentials kunnen gebruikers hun smartphone of tablet gebruiken om toegang te krijgen tot en controle te krijgen over deuren en apparaten op een systeem.

Het is mogelijk om aan elke gebruiker meerdere smart credentials toe te wijzen.

Smart credentials zullen door middel van een app op een smart device worden opgeslagen

De volgende mobiele besturingssystemen worden ondersteund:

Android

IOS

Smart credentials zijn gratis te verstrekken en te gebruiken.

Smart credentials worden via e-mail vanuit de software verstrekt.

De e-mail met de smart credentials bevat instructies, een downloadlink en een unieke registratie-code voor de geadresseerde gebruiker.

De registratie-code is slechts geldig voor één apparaat.

 Het zal mogelijk zijn om een smart credential als verloren te markeren, waardoor alle toegangsrechten van die smart credential worden verwijderd, terwijl de gebruiker andere credentials kan blijven gebruiken.

Het is mogelijk om een extra verificatie te vereisen bij gebruik van smart credentials. Wanneer verificatie vereist is, moet een gebruiker zichzelf authentiseren met behulp van:

Vingerafdruk, met behulp van de ingebouwde biometrische lezer van hun smart device

Toegangscode of patroon (Android), met behulp van de ingebouwde schermbeveiliging van het smart device

Het moet mogelijk zijn een tijdschema in te voeren voor wanneer biometrisch verificatie ingeschakeld moet zijn.

* + 1. Pincodes bieden een manier om een ​​gebruiker te identificeren zonder een fysieke kaart of tag.

Gebruikers mogen slechts één pincode hebben.

De lengte van de pincode moet in de software worden geconfigureerd om aan de beveiligingsvereisten van het project te voldoen.

Het systeem genereert een keypad hacker alarmgebeurtenis wanneer meerdere mislukte invoerpogingen worden gedaan bij een toetsenbordlezer, waardoor bescherming wordt geboden tegen hackers en ongeautoriseerde toegangspogingen.

* + 1. Het is mogelijk om van een gebruiker een combinatie van inloggegevens te eisen, zoals een kaart + pincode, voor extra veiligheid
	1. Het moet mogelijk zijn een gebruiker te blokkeren.
		1. Door een gebruiker te blokkeren wordt de toegang en controle over alle deuren en apparaten verwijderd.
		2. Het blokkeren van een gebruiker zal de toegang tot de software blokkeren
		3. Het is mogelijk om de blokkering van een gebruiker op te heffen om al zijn eerdere bevoegdheden te herstellen.
1. Apparaten
	1. Hardware wordt weergegeven en geconfigureerd als software-onderdelen, ook wel ‘apparaten’ genoemd.
	2. De software ondersteunt de volgende typen apparaten.
		1. Toegangspunt
		2. Uitgang
		3. Ingang
		4. Inbraakalarm
		5. Brandalarm
		6. Camera
		7. Videocontroller
	3. Het gemaakte softwareapparaat moet kunnen worden gekoppeld aan de hardware die aan het systeem is toegevoegd.
		1. De configuratie van het apparaat zal invloed hebben op de werking van de hardware.
	4. Voor deuren moet de volgende configuratie mogelijk zijn:
		1. Werkingsmodus:
			1. Tijd gestuurd. De deur wordt ontgrendeld voor de ingestelde tijd bij het aanbieden van een credential
			2. Toggle. De deur wordt geopend bij het aanbieden van een credential en blijft open tot er nogmaals een credential wordt aangeboden
		2. Deur open tijd, dit bepaalt hoelang de deur ontgrendeld blijft wanneer het in de tijdgestuurde modus is ingesteld.
		3. Open deur gedurende het tijdschema, de deur wordt geopend volgens het ingestelde tijdschema
		4. Lezer-LED, hiermee kan de LED op de lezer in- of uitgeschakeld worden
		5. Lezer Pieptoon, hiermee kan de pieptoon van de lezer in- of uitgeschakeld worden.
		6. Geef gebruikers altijd toegang om het gebied te verlaten, hiermee kan een gebruiker altijd naar buiten ook wanneer hij of zij geen bevoegdheid heeft.
		7. Werkingsmodus, configureer met welke credential type de deur geopend kan worden
		8. Bluetooth mode, configureer de werkingsmodus voor de smart credentials
		9. Alarmen:
			1. Deur te lang open
			2. Deur geforceerd.
			3. Voedingswegval
		10. Camera's, die camerabeelden koppelen aan gebeurtenissen met betrekking tot het toegangspunt.
	5. Schakelbare apparaten moeten de volgende configuratie bieden:
		1. Werkingsmodus:
			1. Tijd gestuurd, het apparaat wordt ingeschakeld voor de ingestelde tijd bij het aanbieden van een credential
			2. Toggle, het apparaat wordt ingeschakeld bij het aanbieden van een credential en blijft aan tot er nogmaals een credential wordt aangeboden
			3. Puls, het apparaat wordt voor 1 seconden ingeschakeld
		2. Inschakeltijd, geeft aan hoelang het apparaat wordt ingeschakeld
		3. Gedurende tijdschema, het apparaat wordt ingeschakeld volgens het ingestelde tijdschema
		4. Lezer-LED, hiermee kan de LED op de lezer in- of uitgeschakeld worden
		5. Lezer pieptoon, hiermee kan de pieptoon van de lezer in- of uitgeschakeld worden.
		6. Geef gebruikers altijd toestemming om het apparaat uit te schakelen, hiermee kan een gebruiker altijd het apparaat uit schakelen
		7. Werkingsmodus, configureer met welke credential type het apparaat geschakeld kan worden
		8. Bluetooth mode, configureer de werkingsmodus voor de smart credentials
		9. Camera's, die camerabeelden koppelen aan gebeurtenissen met betrekking tot het apparaat.
	6. Ingangen moeten de volgende configuratie bieden:
		1. Gebeurtenissen, hier kan ingesteld worden welke type gebeurtenis er gegenereerd moet worden bij de status verandering van het apparaat.
		2. Camera's, die camerabeelden koppelen aan gebeurtenissen van het apparaat.
		3. Inbraakalarm apparaten moeten de volgende configuratie opties bieden:
		4. Geef aan bij welke ingang-status het inbraakalarm is ingeschakeld
		5. Geef aan bij welke ingang-status het inbraakalarm is uitgeschakeld
		6. De puls duur om het inbraakalarm te schakelen
		7. Deuren, deuren die niet kunnen worden geopend terwijl het alarm is ingeschakeld is
		8. Uitschakelen, deuren waar het inbraaksysteem kan worden uitgeschakeld
		9. Lezer-LED, hiermee kan de LED op de lezer in- of uitgeschakeld worden
		10. Lezer Pieptoon, hiermee kan de pieptoon van de lezer in- of uitgeschakeld worden.
		11. Werkingsmodus, configureer met welke credential type het apparaat geschakeld kan worden
		12. Bluetooth mode, configureer de werkingsmodus voor de smart credentials
		13. Camera's, die camerabeelden koppelen aan gebeurtenissen met betrekking tot het apparaat.
		14. Brandalarm apparaten moeten de volgende configuratie opties bieden:
		15. Geef aan bij welke ingang-status het brandalarm actief is
		16. Deuren, Deuren die moeten ontgrendelen wanneer het brandmeldsysteem in alarm is.
		17. Camera's, die camerabeelden koppelen aan gebeurtenissen met betrekking tot het apparaat.
	7. Camera's en Videocontrollers moeten de volgende configuratie opties bieden:
		1. Opname, configureer wanneer de camera beeld opneemt
		2. Opslaglocatie, biedt de mogelijkheid om de opslaglocatie te kiezen zodat beelden op een netwerkschijf kunnen worden opgenomen
		3. Opslagperiode voor video, verwijder automatisch de videobeelden na een ingesteld aantal dagen
		4. Beeldrotatie, draai het beeld links of rechtsom (Alleen voor Paxton10 camera's)
		5. In/uit zoomen, laat de camera in- of uitzoomen (Alleen Paxton10 vari-focal camera's)
		6. Videokwaliteit, biedt de mogelijkheid om de resolutie, bitrate en framerate in te stellen om de videokwaliteit aan te passen
		7. Een preview van de camera wordt getoond tijdens de configuratie

Apparaten, koppel apparaten in het beeld van de camera, zodat videobeelden van de camera gekoppeld worden aan de gebeurtenissen van de geselecteerde apparaten.

1. Rapporten
	1. Gebeurtenisrapporten worden gebruikt om systeemactiviteit weer te geven.
	2. Gebeurtenissen worden gegenereerd voor, maar niet beperkt tot:
		1. Geldige Credential gelezen
		2. Onbekende credential gelezen (onbekende credential, geen geldige bevoegdheid of gemarkeerd als verloren)
		3. Deur ontgrendeld/vergrendeld
		4. Apparaat in- of uitgeschakeld
		5. Status wijziging van een ingang
		6. Deuralarmen (deur geforceerd, deur te lang open, sabotage)
		7. Inbraakalarm ingeschakeld/uitgeschakeld
		8. Inbraakalarm in alarm
		9. Brandalarm in alarm
		10. Systeemgebeurtenissen (hardware online/offline, servergebeurtenissen)
		11. Softwaregebeurtenissen (persoon/apparaat gewijzigd)
	3. Het is mogelijk gebeurtenissen te filteren op basis van de volgende filters:

a. De gebruiker waarop de gebeurtenis betrekking heeft.

b. Het apparaat waarop de gebeurtenis betrekking heeft.

c. Het tijdstip waarop de gebeurtenis plaatsvond.

d. Het type gebeurtenis (referentie lezen/ alarm/ systeem/ software)

e. Zijn videobeelden gekoppeld

* 1. Er bestaat een selectie van standaardrapporten om veel voorkomende informatie weer te geven, waaronder de volgende rapporten:
		1. Alle gebeurtenissen
		2. Alle gebeurtenissen afgelopen week
		3. Alle gebeurtenissen deze week
		4. Alle gebeurtenissen vandaag
		5. Alle gebeurtenissen gisteren
		6. Verlopen credentials
		7. Eerste en laatste gebeurtenissen
		8. Laatst bekende positie
		9. Lijst van alle gebruikers
		10. Verloren credentials
		11. Bevoegdheden
		12. Laatst bekende positie
		13. Ongebruikte credentials
		14. Wie is erbinnen geweest vandaag
	2. Het is voor gebruikers mogelijk om custom rapporten te maken.
	3. Het volgende is mogelijk in de gebeurtenis rapporten:
		1. Bekijk een videobeeld dat gekoppeld is aan een gebeurtenis
		2. Bekijk het profiel van de persoon waarop een gebeurtenis betrekking heeft.
		3. Bevestig een alarm en maak een notitie bij de alarm gebeurtenis.
		4. Voeg een credential toe aan het systeem vanuit een toegang geweigerd gebeurtenis.
		5. Markeer een gebruiker als veilig of vermist in een aanwezigheidsrapport.
	4. De gebeurtenissen die in een rapport worden weergegeven, worden gefilterd om alleen de gebeurtenissen weer te geven waarvoor de kijker software bevoegdheid heeft om ze in te zien.
1. Videorapporten
	1. Videorapporten worden gebruikt om live en opgenomen video weer te geven die is opgenomen door camera's in het systeem.
	2. Videorapporten moeten schaalbaar zijn en weergave bieden van 1 camera, tot maximaal 20 camera's.
		1. De weergave wordt dynamisch aangepast om een ​​optimale weergave van het aantal camera's in het rapport te bieden.
		2. De weergave van de videostream wordt aangepast op basis van het aantal camera's dat momenteel wordt weergegeven op het scherm, waardoor het bandbreedtegebruik van het netwerk wordt geoptimaliseerd.
	3. Het is mogelijk om gebeurtenissen binnen een videorapport te bekijken.
		1. De gebeurtenissen moeten vooraf worden gefilterd om alleen de gebeurtenissen weer te geven die betrekking hebben op de apparaten die door de camera's in het rapport kunnen worden gezien.
		2. Het moet mogelijk zijn om de getoonde gebeurtenissen te filteren.
		3. Apparaat gerelateerde gebeurtenissen en gebruikersgegevens worden waar nodig als overlay op de videobeelden weergegeven.
	4. Er zijn minimaal de volgende afspeelopties beschikbaar, waaronder:
		1. Play/ Pauze
		2. Afspeelsnelheid aanpassen
		3. 15 seconden terugspringen
		4. Ga naar live video
		5. Tijdlijn met scrub functie
	5. Er is bediening beschikbaar voor cameraweergave, waaronder:
		1. Volume dempen/opheffen
		2. Cameranaam tonen/verbergen
		3. Cameratijd tonen/verbergen
		4. Deze instellingen hebben geen invloed op de camera of de video-opname, ze hebben alleen invloed op het afspelen en bekijken van videobeelden voor de huidige client.
	6. Het moet mogelijk zijn een videofragment naar een netwerklocatie te exporteren.
		1. De periode voor export wordt geïdentificeerd met behulp van een eenvoudige en grafische gebruikersinterface.
		2. Standaard wordt een videoclip van 5 minuten geselecteerd.

De minimale clipduur bedraagt ​​1 minuut.

De maximale clipduur bedraagt ​​30 minuten.

* + 1. De geëxporteerde clip bevat audio.
		2. De videoclip wordt gedownload in MP4-formaat.
	1. Het moet mogelijk zijn om een ​​moment opname van een videobeeld naar een netwerklocatie te exporteren.
		1. Het systeem biedt een selectie van momentopnamen rond de geselecteerde tijd.
		2. De momentopname wordt gedownload in JPEG-formaat.
	2. Het is mogelijk een video opnamen te bookmarks voor toekomstig gebruik.
		1. Het moet mogelijk zijn om een ​​bookmark een naam of beschrijving te geven.
		2. Bookmarks moeten duidelijk herkenbaar zijn op de videotijdlijn.
		3. Bookmarks worden automatisch verwijderd wanneer video wordt verwijderd.
		4. Er moeten bedieningselementen beschikbaar zijn waarmee u eenvoudig door alle bookmarks kunt navigeren.
		5. Er geldt geen limiet voor het aantal bookmarks dat kan worden aangemaakt.
	3. Smart search is beschikbaar voor het zoeken naar beweging in opgenomen video.
		1. Met smart search kunnen gebruikers gemakkelijk lokaliseren wanneer een item is verplaatst of wanneer er activiteit heeft plaatsgevonden.
		2. Een gebruiker kan gebieden over meerdere videostreams markeren met smart search, waarbij de videostreams worden doorzocht op wanneer er beweging heeft plaatsgevonden in de gemarkeerde gebieden.
	4. Met digitale zoom kunnen gebruikers inzoomen op een videostream om aanvullende details te bekijken.
		1. Bij het inzoomen op een videostream schakelt het systeem over naar de stream met de hoogste resolutie die beschikbaar is voor de opgegeven camera.
		2. Digitale zoom heeft geen invloed op de opname van de video of de weergave voor andere gebruikers.
		3. Digitale zoom is beschikbaar via schermbediening, scrollwiel en aanraakscherm.
	5. Volledig scherm en pop-up weergave voor vergrote weergave met meer details.

a. Het moet mogelijk zijn om elke camera afzonderlijk op volledig scherm of in een pop-up te plaatsen.

b. Bij weergave op volledig scherm of in een pop-up schakelt het systeem over naar de stream met de hoogste resolutie die beschikbaar is voor de opgegeven camera.

* 1. Er geldt geen limiet voor het aantal videorapporten dat kan worden gemaakt.
	2. Het bekijken van een videorapport moet zodanig in te stellen zijn ​​dat elke softwaregebruiker alleen de videobeelden kan bekijken die hij/zij mag zien.
1. Dashboards
	1. Dashboards bieden een aanpasbare gebruikersinterface waar diverse widgets in geplaatst kunnen worden zodat de weergave voldoet aan de wensen van de klant.
	2. Dashboards bestaan ​​uit een combinatie van de volgende widgets:
		1. Gebeurtenissen

Wanneer een gebeurtenissenwidget aan een dashboard wordt toegevoegd, worden alle systeemgebeurtenissen en -activiteiten weergegeven.

Het moet mogelijk zijn om de gebeurtenissenwidget te filteren zodat alleen specifieke gebeurtenissen worden weergegeven.

* + 1. Systeem alarmen

Wanneer de widget systeem alarmen aan een dashboard wordt toegevoegd, kunnen de systeem alarmen weergegeven worden in een dashboard.

Het moet mogelijk zijn om de widget te configureren om alarmen voor specifieke apparaten of alarmtypen te tonen.

De widget geeft informatie over de meest recente alarmgebeurtenissen.

Het moet mogelijk zijn videobeelden van een alarmgebeurtenis te bekijken.

* + 1. Status alarmsystemen

Wanneer de widget status alarmsystemen aan een dashboard wordt toegevoegd, wordt de huidige status van geselecteerde brandalarmen of inbraakalarmen getoond.

* + 1. Video

De videowidget voegt videocamera's toe aan een dashboard, waardoor live en opgenomen videobeelden bekeken kunnen worden.

Elke videowidget biedt weergave van de video van één camera.

De volgende bedieningselementen worden ondersteund wanneer de videobeelden in een dashboard worden bekeken:

Volledig scherm/ pop-up

Wijzig de afspeelsnelheid

15 seconden terugspringen

Live video bekijken

Tijdlijn met scrub functie

Digitale zoom

Exporteer videobeeld

Exporteer snapshot

Toon/verberg cameranaam

Toon/verberg cameratijd

Dempen/opheffen audio

* + 1. Soft buttons

Met Soft buttons is het mogelijk om voor ingestelde acties uit te voeren met een druk op de knop

Soft buttons worden op een centrale locatie aangemaakt en beheerd

De weergave van een soft button kan worden aangepast en het is duidelijk zichtbaar wanneer er op een soft button is geklikt

In één widget kunnen meerdere soft buttons toegevoegd worden

* + 1. Gebruikersverificatie

Wanneer een gebruikersverificatie aan een dashboard wordt toegevoegd, worden de afbeelding en details van elke gebruiker weergegeven wanneer deze een credential heeft aangeboden bij een deur.

De gebruikersverificatie widget geeft de afbeelding van een gebruiker weer wanneer de gebruiker een credential aanbiedt bij een deur.

De gebruikersverificatie widget geeft de gegevens van een gebruiker weer wanneer de gebruiker een credential aanbiedt.

De widget kan worden geconfigureerd op welk apparaat of toegangspunt moet worden gecontroleerd en welke gebeurtenissen moeten worden getoond.

Het is mogelijk om de videobeelden van de gebeurtenissen te bekijken.

* + 1. Plattegronden

Wanneer de plattegrond widget aan een dashboard wordt toegevoegd biedt de widget een grafische weergave van de locatie.

De widget toont een plattegrond vanuit het systeem

De plattegrond wordt gemaakt en beheerd in een speciaal daarvoor bestemd menu in de software.

De widget maakt navigatie naar andere plattegronden mogelijk.

De widget biedt de volgende functionaliteit en interactie:

* + 1. Wie is erbinnen geweest

De widget biedt een overzicht van gebruikers die op de huidige dag binnen zijn geweest

De widget toont de volgende gegevens

Gebruikersnaam

Gebruikersgroep of afdeling

Datum en tijd

Locatie waar de gebeurtenis plaatsvindt

* + 1. Weer

Een weerwidget geeft een weersvoorspelling voor een specifieke locatie.

In de widget is het mogelijk om de locatie voor het weer rapport op te zoeken.

* 1. Dashboards bestaan ​​uit 1 tot 16 widgets.
	2. De widgets en de grootte kunnen geconfigureerd worden.
	3. Er geldt geen limiet voor het aantal dashboards dat kan worden gemaakt.
	4. Dashboards moeten zodanig worden toegestaan ​​dat elke softwaregebruiker alleen de dashboards bekijkt die geschikt zijn voor zijn of haar taken en rol.
1. Plattegronden
	1. Plattegronden bieden een grafische weergave van de locatie.
	2. Het is mogelijk een afbeelding te uploaden om als plattegrond te gebruiken.

Met de software kunnen afbeeldingen van maximaal 4 MB worden geüpload.

Minimaal worden de volgende afbeeldingsformaten ondersteund:

JPEG

JPG

GIF

PNG

Het moet mogelijk zijn om de geüploade afbeelding binnen de software bij te snijden.

* 1. Apparaten worden toegevoegd aan een plattegrond om deze vanaf een plattegrond te monitoren en bedienen
		1. Apparaat pictogrammen geven de huidige status van het apparaat aan door van kleur te veranderen en te knipperen.
		2. Apparaat pictogrammen geven gebeurtenissen weer die verband houden met het apparaat zodra deze zich voordoen.
		3. Het moet mogelijk zijn om het apparaat te bedienen of de deur te ontgrendelen.
		4. Het moet mogelijk zijn om de videobeelden van een camera te bekijken vanaf een plattegrond.
	2. Aan een plattegrond worden navigatiepictogrammen toegevoegd om naar andere plattegronden te navigeren, waardoor navigatie tussen verschillende locaties of meerdere verdiepingen van een gebouw mogelijk wordt.
		1. Wanneer erop wordt geklikt, zullen navigatiepictogrammen de gebruiker naar volgende plattegrond leiden.
		2. Navigatiepictogrammen moeten gebeurtenis pictogrammen weergeven die gebeurtenissen vertegenwoordigen die plaatsvinden op apparaten op de gekoppelde plattegrond.
		3. De overgang die wordt gebruikt bij het wisselen van plattegronden houdt verband met de navigatieknop die gebruikt wordt. Dit wil zeggen als de navigatie knop naar links gebruikt wordt dan is de overgang ook naar links.
	3. Er kunnen soft buttons aan de plattegrond worden toegevoegd om voor gedefinieerde acties uit te voeren

a. De soft buttons zijn configureerbaar door de gebruiker om verschillende acties uit te voeren.

b. Soft buttons worden op een centrale locatie aangemaakt en beheerd

c. De weergave van een soft button kan worden aangepast en het is duidelijk zichtbaar wanneer er op een soft button is geklikt

* 1. Alarmgebieden moeten worden toegevoegd aan een plattegrond om belangrijke gebeurtenissen te tonen.
		1. Alarmgebieden moeten alarmgebeurtenissen voor geselecteerde apparaten weergeven, zoals het afgaan van een inbraakalarm.
		2. Alarmgebieden moeten een deel of het geheel van een plattegrond markeren om de gebruiker te waarschuwen van een alarm gebeurtenis.
		3. Het moet voor een gebruiker mogelijk zijn om het gebied te definiëren dat het alarm vertegenwoordigt.
	2. Er moeten labels aan een plattegrond worden toegevoegd om gebruikersinstructies en gebiedstitels te tonen.
		1. Labels zijn eenvoudige tekst labels die aanvullende informatie en opmerkingen bij een plattegrond kunnen geven.
	3. Een plattegrond moet in 2D en 3D zichtbaar zijn.

a. In 3D moet het mogelijk zijn om de plattegrond te roteren.

1. Bevoegdheden
	1. Bevoegdheden worden gebruikt om de gebruikerstoegang tot apparaten te beheren
	2. Er geldt geen limiet voor het aantal bevoegdheden dat kan worden aangemaakt.
	3. Het moet mogelijk zijn om gebruikers aan meerdere bevoegdheden toe te wijzen.
	4. Het moet mogelijk zijn om apparaten aan meerdere bevoegdheden toe te wijzen.
	5. Het moet mogelijk zijn om tijdschema's toe te wijzen aan meerdere gebouwbevoegdheden.
	6. Een gebruiker heeft alleen toegang tot een apparaat als dit in een bevoegdheid is gecombineerd met een actief tijdschema.
2. Software bevoegdheden
	1. Softwarebevoegdheden worden gebruikt om de gebruikerstoegang tot de software te beheren.
	2. Er geldt geen limiet voor het aantal softwarebevoegdheden dat kan worden aangemaakt.
	3. Het moet mogelijk zijn om gebruikers aan meerdere softwarebevoegdheden toe te wijzen.
	4. Het moet mogelijk zijn om verschillende bevoegdheden voor elke softwareonderdeel te selecteren. De volgende niveaus zijn mogelijk:
		1. Volledig – toegang om te maken/wijzigen/verwijderen
		2. Lezen – toegang tot bekijken
		3. Gebeurtenissen – toegang om gebeurtenissen te bekijken
	5. Een gebruiker heeft alleen toegang tot de software als deze is toegevoegd in een softwarebevoegdheid
		1. Een gebruiker heeft alleen toegang tot de softwareonderdelen die zijn gespecificeerd in de softwarebevoegdheid
	6. De volgende softwareonderdelen zijn individueel toe te wijzen in de bevoegdheid:
		1. Dashboards of gespecificeerde groepen dashboards
		2. Rapporten of gespecificeerde groepen rapporten
		3. Plattegronden of gespecificeerde groepen plattegronden
		4. Mensen of specifieke groepen mensen
		5. Regels, of gespecificeerde groepen regels
		6. Apparaten of gespecificeerde groepen apparaten
		7. Hardware beheren
		8. Opties
		9. Software gebeurtenissen
		10. Hardware gebeurtenissen
		11. Remote toegang
3. Tijdschema's
	1. Tijdschema's worden gebruikt om verschillende functionaliteiten binnen het systeem voor verschillende tijdstippen van de dag of dagen van de week mogelijk te maken.
	2. Er geldt geen limiet voor het aantal tijdsschema's dat kan worden aangemaakt.
	3. Het is mogelijk om in één tijdschema een ander tijdschema toe te wijzen voor minimaal 28 dagen.
	4. Specifieke dagen worden gebruikt om unieke functionaliteit voor bepaalde dagen te bieden.
		1. Er geldt geen limiet voor het aantal specifieke dagen dat kan worden aangemaakt.
		2. Het is mogelijk om voor specifieke dagen een ander tijdschema toe te wijzen.
		3. Als er specifieke dagen voorkomen, worden de tijdschema's overschreven door de tijdschema's die voor de specifieke dag zijn gedefinieerd.
	5. De lay-out moet grafisch en gebruiksvriendelijk zijn en tijdschema's kunnen gemaakt worden door te klikken en slepen op de geselecteerde tijden.
4. Triggers en Acties
	1. Trigger- en actieregels zorgen voor aangepaste functionaliteit binnen het systeem, triggers en acties vooraf ingestelde regels die een bepaalde actie uitvoeren.
	2. De software maakt het mogelijk trigger- en actieregels te creëren om specifieke functionaliteiten binnen het systeem aan te maken
	3. Er geldt geen limiet voor het aantal trigger- en actieregels dat kan worden gemaakt.
	4. Het moet mogelijk zijn een actie uit te voeren wanneer een geselecteerde trigger optreedt. De lijst met triggers omvat, maar is niet beperkt tot:
		1. Geldige credential gelezen
		2. Ongeldige credential gelezen
		3. Ingang geopend
		4. Ingang gesloten
		5. Status verandering van ingang
		6. Exit verzoek
		7. Deur geforceerd open alarm
		8. Deur te lang open alarm
		9. Inbraak systeem ingeschakeld
		10. Inbraak systeem uitgeschakeld
		11. Inbraak systeem in alarm
		12. Brandmeldsysteem in alarm
		13. Aan het begin van een tijdschema
		14. Aan het eind van een tijdschema
		15. Soft button ingedrukt
	5. Het moet mogelijk zijn om te voorwaarden toe te voegen wanneer een regel wordt uitgevoerd door de status van andere apparaten op het systeem. De lijst met beperkingen omvat, maar is niet beperkt tot:

a. Invoer hoog

b. Invoerlaag

c. Inbraakalarm Ingeschakeld

d. Inbraakalarm Uitgeschakeld

e. Inbraakalarm actief

f. Inbraakalarm inactief

g. Brandalarm actief

h. Brandalarm inactief

i. Toegangspunt geopend

j. Toegangspunt gesloten

k. Uitgang aan

l. Uitgang uit

* 1. Wanneer er een trigger plaats vindt en aan alle beperkingen is voldaan, kunnen er meerdere acties plaatsvinden. De lijst met acties omvat, maar is niet beperkt tot:
		1. Toegangspunt ontgrendelen
		2. Toegangspunt vergrendelen
		3. Toggle een toegangspunt
		4. Apparaat inschakelen
		5. Apparaat uitschakelen
		6. Apparaat Toggle
		7. Inschakelen inbraakalarm
		8. Uitschakelen inbraakalarm
		9. Voer het Roll Call-rapport uit
	2. Er mag geen limiet zijn aan het aantal triggers, beperkingen en acties waaruit een regel kan bestaan.
1. Anti-Passback
	1. Anti-passbackregels bieden de mogelijkheid om opeenvolgende toegangspogingen te monitoren en te beperken.
	2. Er zijn 2 soorten anti-passback beschikbaar:
	3. Het zal mogelijk zijn om de mensen te specificeren die onderworpen zijn aan een anti-passbackregel.
	4. Het moet mogelijk zijn om de toegangspunten te specificeren waarop een anti-passbackregel van toepassing is.
		1. Traditionele Anti-Passback

Zodra een gebruiker via een van de gedefinieerde in-lezer is binnengekomen, kan hij of zij niet opnieuw naar binnen totdat de credential op de uitlezer wordt aangeboden.

Automatisch resetten van Anti-Passback moet mogelijk zijn, waarbij alle in/uit-statussen elke dag op een bepaald tijdstip worden gereset.

* + 1. Tijd gestuurde Anti-Passback

Zodra een gebruiker via een van de gedefinieerde in-lezers is binnengekomen, kan deze gedurende een bepaalde periode niet opnieuw binnenkomen met dezelfde tag.

Het is mogelijk om gebruikers binnen deze periode opnieuw toegang te geven als wordt gezien dat deze de locatie verlaten hebben.

* 1. Er zijn 2 soorten toegangsbeperkingen:

a. Harde Anti-Passback – als u niet aan de regel voldoet, wordt de toegang van de gebruiker ontzegd.

b. Softe Anti-Passback – als u zich niet aan de regel houdt, wordt toegang verleend volgens de machtigingen van de gebruiker, terwijl er een gebeurtenis wordt gegenereerd om beheerders op de hoogte te stellen van de overtreding.

* 1. Er geldt geen limiet voor het aantal Anti-Passback regels dat kan worden gemaakt.
1. Roll Call
	1. De software biedt Roll Call-functionaliteit.
	2. Roll Call-regels moeten worden gebruikt om de Roll Call-functionaliteit te configureren.

a. Elke regel definieert de toegangspunten waaruit een gebied bestaat.

b. Elke regel definieert de lezers die zich op elk verzamelpunt voor het gebied bevinden.

* 1. Roll Call-rapporten worden gebruikt om alle gebruikers in een gebied te vermelden op het moment dat rapporten worden gegenereerd.
		1. Het rapport wordt gegenereerd volgens de configuratie van een individuele Roll Call Rapport.
		2. Het moet mogelijk zijn het genereren van een appèlrapport in geval van een noodsituatie te automatiseren.
		3. Het moet mogelijk zijn om bij het genereren automatisch een Roll Call Rapport te e-mailen.
	2. Het Roll Call Rapport moet in de software kunnen worden bekeken.
	3. Het Roll Call Rapport vermeldt:
		1. Overzicht van alle gebruikers binnen een gebied.
		2. Gebruikersinformatie, inclusief naam, e-mailadres en alle informatie die voor gebruikers is opgeslagen.
		3. Gebruikersafbeelding.
		4. Laatst bekende locatie van elke gebruiker.
		5. Ontbrekende/veilige status

Gebruikers kunnen in het rapport als veilig worden gemarkeerd.

Gebruikers kunnen zichzelf als veilig markeren door hun token aan een aangewezen verzamellezer te presenteren.

* 1. Alleen gebruikers waarvan bekend is dat ze zich in een gebied bevinden, worden in het rapport opgenomen wanneer dit wordt gegenereerd.
		1. Het rapport moet elke dag op een bepaald tijdstip kunnen worden gewist.
		2. Het moet mogelijk zijn om gebruikers uit het rapport te verwijderen nadat ze gedurende een bepaalde tijd inactief zijn geweest.
1. Hardware beheer
	1. Hardware wordt aan de software toegewezen door middel van eenvoudig klikken en slepen.
	2. Hardware wordt op een centrale locatie beheerd.
	3. De software rapporteert details van alle verbonden hardware, waaronder:
2. Type hardware
3. Serienummer of uniek ID
4. Subset
5. IP-adres
6. Batterij status
7. Firmware versie
8. Online status
	1. Hardware beheer is toegestaan ​​voor geselecteerde softwaregebruikers.
	2. Het toewijzen van hardware randapparatuur aan apparaten moet flexibel en veelzijdig zijn, waardoor apparaten kunnen bestaan ​​uit meerdere componenten van een aantal hardware
9. Het moet mogelijk zijn om elk uitgangs-relais te koppelen aaneen:

Vergrendeling voor een toegangspunt

Alarm voor een toegangspunt

Gecontroleerde uitvoer voor een apparaat

Inbraakalarm inschakelen

1. Het moet mogelijk zijn om elk digitaal ingangsrandapparaat te koppelen aan een:

Exit knop voor een toegangspunt

Deurcontact voor een toegangspunt

Digitale ingang voor een apparaat

Alarm inschakel status voor een inbraakalarm

Alarm actieve status voor een inbraakalarm

Alarm actieve status voor een brandalarm

1. Het moet mogelijk zijn om elke lezer te koppelen aaneen:
	* + 1. Toegangspunt om de toegang te controleren en te beperken
			2. Controleerbaar apparaat om het gebruik te controleren en te beperken
			3. Inbraakalarm om het in-/uitschakelen te controleren en te beperken.
2. Controleapparaat
	1. De software maakt het mogelijk de hardware op afstand vanuit de software te besturen.
	2. Vanuit de software is minimaal het volgende mogelijk:
3. Ontgrendel een toegangspunt
4. Schakel de status van een bestuurbaar apparaat in/uit/schakel deze in
5. Een inbraakalarm in/-uitschakelen
	1. Softwaregebruikers mogen uitsluitend toegang hebben tot het op afstand bedienen van de apparaten die zij zouden kunnen bedienen als zij hun credential aan een lezer hebben gepresenteerd.
6. Toegang op afstand
	1. De software is overal toegankelijk waar een internetverbinding aanwezig is.
7. Het moet mogelijk zijn deze functie in of uit te schakelen.
8. Het moet mogelijk zijn om het inloggen op afstand te beperken tot elke groep of elk individu.
	1. Bij toegang op afstand is geen software-installatie of complexe handmatige adressering vereist.
	2. Bij toegang op afstand is de gebruikersinterface identiek aan bij lokale toegang.
9. Startpagina
10. Een startpagina biedt gebruikers een centrale plek waar ze hun systeem kunnen bekijken en beheren.
11. De startpagina biedt toegang tot:
12. Het toevoegen van nieuwe apparaten aan het systeem aanmaken
13. Favorieten.
14. De startpagina geeft een samenvatting van het systeem en zijn activiteiten, waaronder:
15. Overzicht
	* + 1. Aantal actieve gebruikers
			2. Totaal aantal gebruikers
			3. Totaal aantal apparaten
16. Meldingen
	* + 1. Aantal onbevestigde alarmgebeurtenissen
			2. Aantal offline apparaten
			3. Aantal ingelogde gebruikers
17. Systeemactiviteit

(i)          Grafiek van toegangsgebeurtenissen per dag, gedurende de afgelopen zeven dagen

1. Favorieten
2. De software biedt elke softwaregebruiker een aanpasbaar menulint voor bedienings- en navigatiesnelkoppelingen.
3. Het moet voor een gebruiker mogelijk zijn om het volgende aan het favorietenlint toe te voegen:
4. Links – om snel naar delen van de software te navigeren.
5. Acties – voor het uitvoeren van de standaardactie van een apparaat.
6. Het moet voor een gebruiker mogelijk zijn om snelkoppelingen en acties op het lint van de favoriet te plaatsen.

a. Dit wordt gepresenteerd in een grafische drag-and-drop-interface.

1. Gebruikers hebben de mogelijkheid om standaard een specifiek softwaregebied te openen wanneer ze inloggen.
2. Alle favorieten en opties worden per gebruiker opgeslagen, zodat elke softwaregebruiker zijn eigen gepersonaliseerde favorieten en instellingen kan hebben.
3. Gebruikers importeren
4. Het moet mogelijk zijn om gebruikersgegevens in het systeem te importeren.
5. De volgende bestandsformaten worden ondersteund:
	1. .xlsx
	2. .xls
	3. .csv
	4. .text
	5. .txt
6. De gebruiker kan een voorbeeld van de gegevens bekijken voordat de import plaatsvindt.
7. Deurintercom Systeem
8. De software ondersteunt een intercomstation dat toegang kan verlenen vanaf een externe monitor en/of een geïntegreerde toegangscontrolelezer.
	* 1. De software rapporteert gebeurtenissen vanuit het intercomsysteem.
		2. De software levert de toegangspuntconfiguratie die bij het intercomsysteem wordt gebruikt.
		3. Het buitenpostpaneel wordt automatisch door het systeem gedetecteerd.
9. Het intercomsysteem moet aan de volgende criteria voldoen:
	* 1. De kaartlezer zit in de buitenpost ingebouwd en is visueel gemaakt met een afbeelding op de buitenpost, zodat de gebruiker weet waar deze zijn credential moet aanbieden.
		2. Er wordt een Lcd-scherm gebruikt om bewoners weer te geven en deze op te roepen, waarna er een audio-video oproep tot stand komt. Er kunnen maximaal 1000 namen worden weergegeven.
		3. Zodra het communicatiekanaal open is, kan de medewerker de bezoeker bekijken via de binnenpost. In de buitenpost is een interne camera opgenomen.
		4. Alle communicatie, audio, video en stroom zullen via één enkele kabel verbonden zijn via TCP/IP en Power-over-Ethernet, met behulp van IPV6-technologie.
		5. De binnenpost moet zijn voorzien van een monitor om te zien wie er bij de ingang staat.
		6. De binnenpost kan de communicatie met het buitenpost starten en een aankondiging doen of video te bekijken, en de deur ontgrendelen.
		7. Er kunnen maximaal 100 panelen ​​en maximaal 1000 binnenposten worden aangesloten op een systeem.
		8. Er zit standaard een ingebouwde low-light camera in het intercompaneel, die in het paneel is geplaatst om schade als gevolg van vandalisme te voorkomen.
		9. Er moet een reeks LED's worden opgenomen nabij de camera om bezoekers te verlichten voor nachtelijk zicht.
		10. Als er slechts één intercomstation en één monitor op het systeem zijn aangesloten, is er geen configuratie vereist.
		11. Voor de intercom panelen en binnenposten hoeft geen IP-adres te worden geconfigureerd. Alle panelen en monitoren binnen hetzelfde LAN zullen elkaar automatisch detecteren bij het opstarten.
		12. Als er een toetsenbord aanwezig is op het apparaat, moet toets met nummer vijf een reliëf hebben voor aanraakreferentie.
		13. Het Intercompaneel heeft geen externe voeding nodig maar wordt gevoed via PoE.
		14. Er moet een inbouwbehuizing beschikbaar zijn.
		15. Elke smartphone, computer en tablet kan worden gebruikt met het Entry-systeem met behulp van SIP Compatibiliteit en een industriestandaard SIP-server (session initiatie protocol).

**2.11             SPECIFIEKE EISEN VOOR DESKTOPLEZER**

1. Kenmerken
	1. De desktoplezer moet het toewijzen van credentials aan gebruikers vergemakkelijken.
	2. De desktoplezer moet meerdere typen en formaten proximity credentials lezen.
	3. De desktoplezer identificeert credentials die al aan gebruikers zijn toegewezen.
	4. De desktoplezer elimineert de noodzaak om het nummer van elk token te kennen.
	5. In systemen met meerdere client-pc's moet het systeem meerdere desktoplezers kunnen ondersteunen.
	6. De desktoplezer zal een uniek ID van elk gepresenteerde credential weergeven.
	7. De desktoplezer zal een unieke ID uit verschillende kaartformaten en lengtes weergeven.
2. Gebruikers handeling:
	1. De desktoplezer is een gebruiksvriendelijk apparaat.
		1. Wanneer een niet-toegewezen credential wordt gepresenteerd, zal de toegangscontrole-software automatisch het gebruikersscherm creëren voor het invoeren van gebruikersinformatie en andere beveiligingsinstellingen.
		2. Wanneer de beheerder van de software zich al in een gebruikersveld bevindt en een niet-toegewezen credential wordt gepresenteerd, zal de software de optie weergeven om de credential aan de huidige gebruiker toe te voegen.
		3. Wanneer een bestaande credential aan de desktoplezer wordt gepresenteerd, haalt de software automatisch de gebruikersgegevens op die aan die credential is gekoppeld en geeft deze weer. Als er meerdere credentials aan de desbetreffende gebruiker zijn toegewezen, zal de software deze credentials markeren.
	2. De Desktoplezer is Plug & Play.
3. Proximity lezer
	1. Het artikel moet een proximity-lezer bevatten.
		1. Minimaal wordt de volgende tokentechnologie ondersteund:
			1. Paxton HiTag2 125KHz
			2. HID 125KHz
			3. EM4100/02
			4. EM4200
			5. Sony FeliCa Lite-S
			6. MIFARE 1K
			7. MIFARE 4K
			8. MIFARE Ultralight/ C
			9. MIFARE DESFire/ EV1
			10. MIFARE Mini
		2. Alle bovengenoemde kaart technologie wordt gelijktijdig ondersteund.
		3. De volgende kaartformaten worden ondersteund:
			1. ISO Kaart
			2. Proximity clamshell kaarten
			3. Tags
			4. Proxidisc
			5. Proximity Horloge tags
			6. Handsfree kaart
4. Voeding
	1. De desktoplezer wordt gevoed via USB.
5. Communicatie
	1. De desktoplezer moet via een USB-poort worden aangesloten op een PC waarop de software geïnstalleerd is.
6. Weergave
	1. De desktoplezer zal een stijlvolle LED weergave bevatten.
	2. De LED's op de desktoplezer geven de volgende statussen aan:
		1. De desktoplezer staat aan, klaar voor gebruik
		2. Credential wordt gelezen
7. Temperatuur
	1. Het artikel moet voldoen aan de vereiste temperatuurnormen.
		1. De desktoplezer werkt betrouwbaar binnen het temperatuurbereik van 0 °C tot 49 °C (32 °F tot 120 °F)
8. Behuizing
	1. De desktoplezer zal er stijlvol en modern uitzien.
	2. De desktoplezer zal ook beschikbaar zijn in een zwarte uitvoering
9. Afmetingen
	1. De afmetingen van de Proximity desktoplezer mogen niet groter zijn dan:
		1. Een breedte van 115mm (4.5")
		2. Een hoogte van 19mm (0.7")
		3. Een diepte van 75mm (3")

**EINDE VAN SECTIE**

*MIFARE®, MIFARE® Classic, DESFire®, MIFARE® Plus en MIFARE® Ultralight C zijn handelsmerken van NXP B.V.*

*FeliCa® is een geregistreerd handelsmerk van Sony Corporation.*

*HID is een geregistreerd handelsmerk van HID Global Corporation.*

*Intel® is een geregistreerd handelsmerk van Intel Corporation.*

*Microsoft en Windows zijn geregistreerde handelsmerken van Microsoft Corporation.*

*Bluetooth is een geregistreerd handelsmerk van Bluetooth SIG.*