TruPortal™

GEBRUIKERSHANDLEIDING VAN DE SOFTWARE

S/N 460820001C • REV 02.00 • ISS 02JAN13

Handelsmerken en octrooien

Interlogix, TruPortal, TruVision en logo's zijn handelsmerken van United Technologies.

Andere in dit document gebruikte handelsnamen kunnen handelsmerken of gedeponeerde handelsmerken zijn van de fabrikanten of leveranciers van de betreffende producten..

Fabrikant

UTC Fire &Security Americas Corporation, Inc.
791 Park of Commerce Blvd, Suite 100, Boca Raton, FL 33487 3630, USA

Geautoriseerde EU-productievertegenwoordiger:
UTC Fire & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Nederland

Versie.

Dit document is van toepassing op TruPortal versie 1.0.

Certificatie.

CE N4131

Volgens FCC-regels

Dit apparaat is in naleving met deel 15 van de FCC-regels. Werking wordt aan de volgende twee condities onderworpen: (1) dit apparaat mag geen schadelijke storing veroorzaken, en (2) dit apparaat moet elke ontvangen storing accepteren, inclusief storing die door ongewenste werking wordt veroorzaakt.

Klasse A: Deze apparatuur is getest en gevonden dat het, volgens deel 15 van de FCC-regels, aan de limieten voor een digitaal apparaat van Klasse A voldoet. Deze limieten zijn ontworpen om redelijke bescherming te bieden tegen schadelijke storing als het apparaat in een commerciële omgeving in werking wordt gesteld. Dit apparaat genereert, gebruikt en kan energie van radiofrequentie uitstralen en, wanneer niet volgens de instructiehandleiding geïnstalleerd en gebruikt, kan het schadelijke storing aan radiocommunicatie veroorzaken. Bediening van dit apparaat binnen een woongebied kan mogelijk schadelijke storing veroorzaken. In dit geval moet de gebruiker de storing op eigen kosten corrigeren.

Klasse B: Deze apparatuur is getest en bevonden dat deze, volgens deel 15 van de FCC-regels, aan de limieten voor een digitaal apparaat van Klasse B voldoet. Deze limieten zijn ontworpen om redelijke bescherming tegen schadelijke storing bij installatie in een woongebied te bieden. Dit apparaat genereert, gebruikt en kan energie van radiofrequentie uitstralen en, wanneer niet volgens de instructies geïnstalleerd en gebruikt, kan het schadelijke storing aan radiocommunicatie veroorzaken.

Er is geen garantie dat zich bij een bepaalde installatie geen storing zal voordoen. Als dit apparaat schadelijke storing aan radio- of televisieontvangst veroorzaakt, wat kan worden vastgesteld door het apparaat uit en weer in te schakelen, wordt de gebruiker aangeraden te proberen de storing volgens één of meerdere van de volgende maatregelen te corrigeren:

- richt de ontvangende antenne op een andere manier of verplaats deze;
- vergroot de afstand tussen het apparaat en de ontvanger;
- verbind het apparaat met een stopcontact van een ander circuit dan hetgeen waarop de ontvanger is aangesloten;

- raadpleeg de dealer of een ervaren radio-/tv-technicus voor hulp.

Volgens ACMA-regels

Opmerking! Dit is een Klasse A-product. In een woongebied kan dit product storing aan radio-ontvangst veroorzaken, in welk geval de gebruiker wordt vereist de juiste maatregelen te ondernemen.

Canada

Dit digitale apparaat van Klasse A voldoet aan de Canadese ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-0330 du Canada.

Richtlijnen Europese Unie

1**2004/108/EC (EMC-richtlijnen):** Hierbij verklaart UTC Fire & Security dat dit apparaat aan de essentiële vereisten en andere relevante voorwaarden van Richtlijn 2004/108/EC voldoet.

2002/96/EC (WEEE-richtlijn): Producten die van dit symbool zijn voorzien, kunnen binnen de Europese Unie niet als ongesorteerd, gemeentelijke afval worden verwijderd. Voor juist recyclen, dient u dit product naar uw lokale leverancier te retourneren, waar gelijkwaardige, nieuwe apparatuur wordt verkocht, of u dient het via de toegewezen verzamelpunten te verwijderen. Zie voor meer informatie: www.recyclethis.info.

2006/66/EC (batterijrichtlijnen): Dit product bevat een batterij die binnen de Europese Unie niet als ongesorteerd, gemeentelijke afval kan worden verwijderd. Zie de productdocumentatie voor specifieke informatie betreffende de batterij. De batterij is met dit symbool gemarkeerd, wat letters omvat die cadmium (Cd), lood (Pb) of kwik (Hg) aangeven. Retourneer de batterij naar uw leverancier of naar een toegewezen verzamelpunt voor juist recyclen. Zie voor meer informatie: www.recyclethis.info.

Contactinformatie

www.interlogix.com

Klantondersteuning

www.interlogix.com/customer-support

GNU openbare licenties

Linux Kernel 2.6.25, Pthreads, Larry DooLittle, Flex Builder, en Buildroot zijn onder de algemene openbare GNU-licentie, versie 2 gelicentieerd. Op http://www.gnu.org/licenses/gpl-2.0.html kan een kopie van de licentie worden verkregen.

YAFFS2 en GNU tar zijn onder de Algemene, openbare GNU-licentie, versie 3, gelicentieerd. Op http://www.gnu.org/licenses/gpl-3.0.html kan een kopie van de licentie worden verkregen.

uClibc, iClibc locale, GPG Gnu Privacy Guard, gpgme GnuPG Made Easy zijn onder de Minder algemene, openbare GNU-licentie, versie 3, gelicentieerd. Op http://www.gnu.org/licenses/gpl-3.0.html kan een kopie van de licentie worden verkregen.

OpenSSL, AstraFlex Components en LIGHTTPD zijn onder een Gewijzigde BSD-licentie gelicentieerd.

DEZE SOFTWARE WORDT DOOR DE AUTEURSRECHTHOUDERS EN CONTRIBUANTEN "ALS IS" GELEVERD EN ENIGE GARANTIES, EXPLICIET OF IMPLICIET, INCLUSIEF, MAAR NIET BEPERKT TOT DE IMPLICIETE GARANTIES VAN VERKOOPBAARHEID EN GESCHIKTHEID VOOR EEN BEPAALD DOELEINDE WORDEN AFGEWEZEN. DE AUTEURSRECHTEIGENAAR OF CONTRIBUANTEN ZIJN IN GEEN GEVAL AANSPRAKELIJK VOOR ENIGE DIRECTE, INDIRECTE, INCIDENTELE, SPECIALE, EXEMPLAIRE OF CONSEQUENTIËLE SCHADEN (INCLUSIEF, MAAR NIET BEPERKT TOT, AANBESTEDING VAN VERVANGENDE GOEDEREN OF SERVICES; VERLIES VAN GEBRUIK, GEGEVENS OF WINSTEN; OF BEDRIJFSONDERBREKING) DIE OP DE EEN OF ANDERE MANIER ZIJN VEROORZAAKT EN OP ENIGE THEORIE VAN AANSPRAKELIJKHEID, ZIJ HET IN EEN CONTRACT, STRIKTE AANSPRAKELIJKHEID, OF ONRECHTMATIGE DAAD (INCLUSIEF NALATIGHEID OF ANDERS) DIE ZICH OP ENIGE WIJZE UIT HET GEBRUIK VAN DIT SOFTWARE VOORDOET, ZELFS WANNEER OVER DE MOGELIJKHEID VAN EEN DERGELIJKE SCHADE GEADVISEERD.

CMockery en Google Protocol Buffers (C) zijn gelicentieerd onder de Apache-licentie, Versie 2.0 (de "Licentie")

U mag dit bestand niet gebruiken, tenzij in overeenkomst met de licentie. U kunt op http://www.apache.org/licenses/LICENSE-2.0 een kopie van de licentie verkrijgen

Tenzij door een toepasselijke wetgeving vereist, of schriftelijk overeengekomen, wordt de software, expliciet of impliciet, op basis van "ALS IS" onder licentie gedistribueerd, ZONDER ENIGE SOORT GARANTIES OF VOORWAARDEN. Zie de licentie voor de door onder de licentie specifieke taal heersende toestemmingen en beperkingen.

Flex-IFrame

Hierbij wordt, zonder enige kosten, toestemming verleend aan enige persoon die een kopie van deze Flex-IFrame-software en verwante documentatiebestanden (de "Software") verkrijgt, om de software zonder beperking, inclusief zonder beperking van de rechten om de software te gebruiken, kopiëren, wijzigen, samenvoegen, publiceren, distribueren, onder sublicentie te verspreiden en/of kopieën te verkopen en voor toestemming aan personen aan wie de software hiervoor is geleverd.

Google Protocol Buffers (C++) is onder de nieuwe BSD-licentie gelicenseerd.

DEZE SOFTWARE WORDT DOOR DE AUTEURSRECHTHOUDERS EN CONTRIBUANTEN "ALS IS" GELEVERD EN ENIGE GARANTIES, EXPLICIET OF IMPLICIET, INCLUSIEF, MAAR NIET BEPERKT TOT DE IMPLICIETE GARANTIES VAN VERKOOPBAARHEID EN GESCHIKTHEID VOOR EEN BEPAALD DOELEINDE WORDEN AFGEWEZEN. DE AUTEURSRECHTHOUDER OF CONTRIBUANTEN ZIJN IN GEEN GEVAL AANSPRAKELIJK VOOR ENIGE DIRECTE, INDIRECTE, INCIDENTELE, SPECIALE, EXEMPLAIRE OF CONSEQUENTIËLE SCHADEN (INCLUSIEF, MAAR NIET BEPERKT TOT, AANBESTEDING VAN VERVANGENDE GOEDEREN OF SERVICES; VERLIES VAN GEBRUIK, GEGEVENS OF WINSTEN; OF BEDRIJFSONDERBREKING) DIE OP DE EEN OF ANDERE MANIER ZIJN VEROORZAAKT EN OP ENIGE THEORIE VAN AANSPRAKELIJKHEID, ZIJ HET IN EEN CONTRACT, STRIKTE AANSPRAKELIJKHEID, OF ONRECHTMATIGE DAAD (INCLUSIEF NALATIGHEID OF ANDERS) DIE ZICH OP ENIGE WIJZE UIT HET GEBRUIK VAN DIT SOFTWARE VOORDOET, ZELFS WANNEER OVER DE MOGELIJKHEID VAN EEN DERGELIJKE SCHADE GEADVISEERD.

gSOAP is onder de openbare gSOAP-licentie (gemodificeerde MPL-licentie) gelicentieerd

DEZE SOFTWARE IN DIT PRODUCT WERD GEDEELTELIJK DOOR GENIVIA GELEVERD EN ENIGE GARANTIES, EXPLICIET OF IMPLICIET, INCLUSIEF, MAAR NIET BEPERKT TOT DE IMPLICIETE GARANTIES VAN VERKOOPBAARHEID EN GESCHIKTHEID VOOR EEN BEPAALD DOELEINDE WORDEN AFGEWEZEN. DE AUTEUR IS IN GEEN GEVAL AANSPRAKELIJK VOOR ENIGE DIRECTE, INDIRECTE, INCIDENTELE, SPECIALE, EXEMPLAIRE OF CONSEQUENTIËLE SCHADEN (INCLUSIEF, MAAR NIET BEPERKT TOT, AANBESTEDING VAN VERVANGENDE GOEDEREN OF SERVICES; VERLIES VAN GEBRUIK, GEGEVENS OF WINSTEN; OF BEDRIJFSONDERBREKING) DIE OP DE EEN OF ANDERE MANIER ZIJN VEROORZAAKT EN OP ENIGE THEORIE VAN AANSPRAKELIJKHEID, ZIJ HET IN EEN CONTRACT, STRIKTE AANSPRAKELIJKHEID, OF ONRECHTMATIGE DAAD (INCLUSIEF NALATIGHEID OF ANDERS) DIE ZICH OP ENIGE WIJZE UIT HET GEBRUIK VAN DEZE SOFTWARE VOORDOET, ZELFS WANNEER OVER DE MOGELIJKHEID VAN EEN DERGELIJKE SCHADE GEADVISEERD.

mini_httpd is onder de licentie voor Acme Labs Freeware gelicentieerd.

Herdistributie en gebruik in bron- en binaire vormen van mini_httpd, met of zonder modificatie, is toegestaan, mits aan de volgende voorwaarden wordt voldaan:

1. Herdistributies van de broncode moet de hierboven gegeven copyright-melding behouden, evenals de lijst met voorwaarden en de volgende disclaimer.
2. Herdistributies in binaire vorm moeten de hierboven gegeven copyright-melding, de lijst met voorwaarden en de volgende disclaimer in de met de distributie geleverde documentatie en/of andere materialen bevatten.

DEZE SOFTWARE WORDT DOOR DE AUTEUR EN CONTRIBUANTEN "ALS IS" GELEVERD EN ENIGE GARANTIES, EXPLICIET OF IMPLICIET, INCLUSIEF, MAAR NIET BEPERKT TOT DE IMPLICIETE GARANTIES VAN VERKOOPBAARHEID EN GESCHIKTHEID VOOR EEN BEPAALD DOELEINDE WORDEN AFGEWEZEN. DE AUTEUR OF CONTRIBUANTEN ZIJN IN GEEN GEVAL AANSPRAKELIJK VOOR ENIGE DIRECTE, INDIRECTE, INCIDENTELE, SPECIALE, EXEMPLAIRE OF CONSEQUENTIËLE SCHADEN (INCLUSIEF, MAAR NIET BEPERKT TOT, AANBESTEDING VAN VERVANGENDE GOEDEREN OF SERVICES; VERLIES VAN GEBRUIK, GEGEVENS OF WINSTEN; OF BEDRIJFSONDERBREKING) DIE OP DE EEN OF ANDERE MANIER ZIJN VEROORZAAKT EN OP ENIGE THEORIE VAN AANSPRAKELIJKHEID, ZIJ HET IN EEN CONTRACT, STRIKTE AANSPRAKELIJKHEID, OF ONRECHTMATIGE DAAD (INCLUSIEF NALATIGHEID OF ANDERS) DIE ZICH OP ENIGE WIJZE UIT HET GEBRUIK VAN DIT SOFTWARE VOORDOET, ZELFS WANNEER OVER DE MOGELIJKHEID VAN EEN DERGELIJKE SCHADE GEADVISEERD.

Apache log4Net is onder de Apache-licentie, versie 2.0 gelicentieerd.

Op http://logging.apache.org/log4net/license.html kan een kopie van de licentie worden verkregen.

Niet-Engelse versies van Interlogic-documenten worden als een service aan ons wereldwijde publiek aangeboden. Wij hebben een poging gedaan een nauwkeurige vertaling van de tekst te leveren, maar de officiële tekst is in het Engels en enige verschillen in de vertaling zijn niet bindend en hebben geen juridisch effect.

De in dit document beschreven software is onder een licentieovereenkomst geleverd en mag alleen volgens de voorwaarden van die overeenkomst worden gebruikt. Interlogix is een gedeponeerd handelsmerk van United Technologies.

Microsoft, Windows, Windows XP en Windows 7 zijn of gedeponeerde handelsmerken of handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen. Andere productnamen die in deze gebruikershandleiding worden genoemd, kunnen handelsmerken of gedeponeerde handelsmerken van hun respectievelijke bedrijven zijn en worden hierbij erkend.

De software die met dit product komt, bevat software met copyright dat onder de GPL is gelicentieerd. U kunt van ons de volledige Overeenkomstige broncode krijgen voor een periode van drie jaar vanaf onze laatste verzending van dit

product, wat niet eerder dan 30-08-2013 zal zijn, door een postwissel of cheque voor $5 naar het volgende adres te sturen:

Interlogix
1212 Pittsford-Victor Road
Pittsford, NY 14534-3820

Schrijf in de memoregel van uw betaling "bron voor TruPortal". U kunt ook op http://www.interlogix.com een kopie van de bron vinden. Deze aanbieding is geldig voor iedereen die deze informatie ontvangt.

HOOFDSTUK 1

Inleiding

De TruPortal Gebruikersinterface-software is ingenesteld op de TruPortal™ systeemcontroller. TruPortal laat u:

- op basis van door gebruikers gedefinieerde toegangsschema's voor tot 64 deuren de toegang bedienen
- schema's configureren zodat zij terugkerende vakanties omvatten
- tot 10.000 gebruikers en badges aan het systeem toevoegen
- gebeurtenissen extern bewaken en automatisch gebeurtenissen aan de overeenkomende video op TruVision-dvd recorders koppelen
- deuren extern openen, vergrendelen, uitsluiten en opheffen
- lezerschema's toevoegen om het systeem te helpen automatiseren
- anti-passback afdwingen
- lezersgroepen maken

Conventies die in deze documentatie worden gebruikt

De tekst in deze handleiding is opgemaakt zodat het gemakkelijker voor u is om te identificeren wat wordt beschreven.

- Waar een tem wordt gedefinieerd, wordt het wordt *cursief* weergegeven.
- Veldnamen worden **vetgedrukt** weergegeven.
- Menu's en menu-opties worden ***vetgedrukt cursief*** weergegeven. Alle menu-opties hebben sneltoetsen. Hiermee kunt u via het toetsenbord de menu-opties selecteren. De onderstreepte letter vertegenwoordigt de sneltoets voor die menu-optie. Sneltoetsen worden bijvoorbeeld als volgt geschreven: <Alt>, <C>.
- Knoppen van het toetsenbord worden tussen vierkante haakjes weergegeven. Bijvoorbeeld: <Tab>, <Ctrl>.
- Knopcombinaties van het toetsenbord worden op twee manieren geschreven:

  <Ctrl> + <Z> betekent de eerste toets ingedrukt houden en op de tweede drukken

  <Alt>, <C> betekent eerst de eerste knop indrukken en daarna op de tweede knop drukken
- Knoppen op het scherm worden tussen vierkante haakjes weergegeven, bijvoorbeeld: [Wijzigen], [Annuleren].

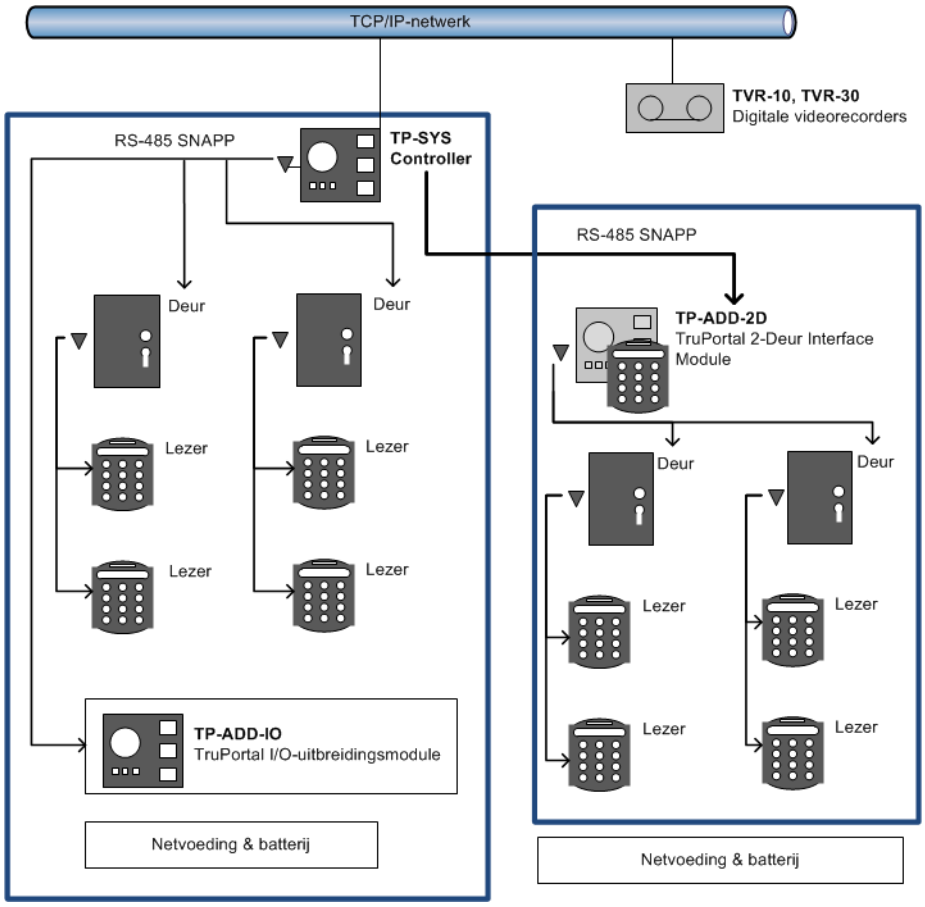
HOOFDSTUK 2

Configuratie TruPortal-hardware

Zodra de hardware-apparatuur voor TruPortal zijn geïnstalleerd, moet u de TruPortal-systeemcontroller configureren.

Gedetailleerde configuratie van optionele functies wordt vanuit de TruPortal-gebruikersinterface uitgevoerd. Voordat u de applicatie kunt activeren, moet de TruPortal-systeemcontroller op het netwerk worden aangesloten en moet het de ingangen, uitgangen, deuren en aangesloten lezers ontdekken en testen op juiste bekabeling en installatie.

TruPortal-systeemarchitectuur



Documenteer de fysieke locatie van elk apparaat volgens Serienummer

Terwijl elke deurconfiguratie (sloten, sensoren, lezers) wordt geïnstalleerd, geeft u voor elk een beschrijving en noteert u de serienummers van de apparaten die aan elke deur zijn verwant in een lijst. Dit helpt u later bij het benoemen van de apparaten, lezersgroepen en zones als u de apparaten in de TruPortal-gebruikersinterface configureert.

Beschrijving deur	Serienummers Nummers	Deurcontroller Serienummers	I/O-uitbreiding Serienummer	Gekoppelde camera
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			

Beschrijving deur	Serienummers Nummers	Deurcontroller Serienummers	I/O-uitbreiding Serienummer	Gekoppelde camera
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			
	In:			
	Uit:			

Zie **Configuratie TruPortal-software op pagina 9.**

Sluit de TruPortal-systeemcontroller aan op een LAN- of lokaal werkstation

Er zijn twee RJ-45 100BaseT ethernetbussen op de TruPortal-systeemcontroller. Een is configureerbaar en de ander is een vast IP (Internet Protocol)-adres. Raadpleeg de *TruPortal-systeemcontroller-snelgids* om de bussen te identificeren.

Als u rechtstreeks vanaf een lokaal client-werkstation op de controller bent aangesloten, gebruikt u de statische ethernetbus en een CAT-6-ethernetkabel om het op het werkstation aan te sluiten.

Als u de controller op een Local Area Network (LAN) aansluit, gebruikt u de configureerbare ethernetbus. Raadpleeg de netwerkbeheerder op locatie om de controller op de LAN aan te sluiten.

Opmerking: Als u meerder netwerkapparaten hebt die middels een switch of kleine router een enkel netwerkdrop gebruiken, dient u te verzekeren dat er niet meer dan één schakelaar of router tussen de controller en de netwerkdrop is.

Uw lokale client-werkstation configureren voor het bedienen van TruPortal

De TruPortal-gebruikersinterface bevindt zich op de TruPortal-systeemcontroller. Alles dat dus nodig is om de applicatie te activeren, is een internetbrowser op het lokale client-werkstation.

De Wizard ontdekking en installatie en de Import/Export-wizard worden echter vanaf een schijf op een lokaal werkstation geïnstalleerd om de nieuw geïnstalleerde hardware te configureren en te testen en om een bestaande personeelsdatabase (indien aanwezig) naar de controller te uploaden.

Microsoft .NET 4.0 Framework installeren

Het hulpprogramma van de TruPortal-software detecteert automatisch of de .NET software is geïnstalleerd en geeft naast de koppeling het woord "Geïnstalleerd" weer als het wordt gevonden.

1. Plaats de TruPortal-schijf in het CD/DVD-station van uw computer.

   Als alternatief, wanneer u de schijfafbeelding hebt gedownload en deze naar de vaste schijf van uw computer hebt uitgepakt, dubbelklikt u op de applicatie **start.hta** om het installatieprogramma te starten.
2. Klik op **.NET 4 Framework**.
3. Volg de instructies van het Microsoft .NET-installatieprogramma om de installatie te voltooien.

Installeer Bonjour-afdrukservices

Het hulpprogramma van de TruPortal-software detecteert automatisch of de Bonjour-software is geïnstalleerd en geeft naast de koppeling het woord "Geïnstalleerd" weer als het wordt gevonden.

1. Plaats de TruPortal-schijf in het CD/DVD-station van uw computer.

   Als alternatief, wanneer u de schijfafbeelding hebt gedownload en deze naar de vaste schijf van uw computer hebt uitgepakt, dubbelklikt u op de applicatie **start.hta** om het installatieprogramma te starten.
2. Klik op **Bonjour**.

   De installatie van de Bonjour-service gaat automatisch verder en wordt automatisch voltooid.

TruPortal-hardware ontdekken, configureren en testen

Opmerking: Voordat de TruPortal-systeemcontroller met de Wizard ontdekking en installatie kan worden ontdekt, moet het op het lokale netwerk worden aangesloten.

Hardware ontdekking en TruPortal-configuratie

1. Plaats de TruPortal-schijf in het CD/DVD-station van uw computer.

   Als alternatief, wanneer u de schijfafbeelding hebt gedownload en deze naar de vaste schijf van uw computer hebt uitgepakt, dubbelklikt u op de applicatie **start.hta** om het installatieprogramma te starten.
2. Klik op **Wizard ontdekking en installatie**.
3. Selecteer een **Taal** en klik op [Volgende].

   De wizard zoekt naar alle TruPortal-systeemcontrollers op het netwerk.
4. Selecteer uit de lijst de controller om te configureren en klik op [Volgende].
5. Typ het huidige wachtwoord van de **beheerder**.

   De standaard **gebruikersnaam** van de beheerder is “admin”

   Het standaard **wachtwoord** van de beheerder is “demo”
6. Kies een nieuw wachtwoord voor de beheerder.

BELANGRIJK: De beheerdersaccount heeft toegang tot alle aspecten van de TruPortal-configuratie. Standaard gebruikersnamen en wachtwoorden op hun plaats achterlaten is gevaarlijk. Iemand die bekend is met het product zal de standaardwaarden kennen.

7. Typ het wachtwoord in de velden **Nieuw wachtwoord** en **Wachtwoord bevestigen** en klik op [Volgende].
8. Wijzig de instellingen op het tabblad **Netwerkconfiguratie** zoals door de netwerkbeheerder op locatie wordt aangegeven.

   BELANGRIJK: Operatoren openen de TruPortal-gebruikersinterface door het IP-adres van de TruPortal-systeemcontroller in het adresveld van hun webbrowser te typen. Als het IP-adres van de controller dynamisch is, moeten de TruPortal-operatoren een virtuele URL of andere alias gebruiken voor toegang tot de controller. De feitelijke toewijzing van het IP-adres wordt namelijk door het netwerk gewijzigd en de operatoren zullen het niet kunnen vinden.

   BELANGRIJK: HTTPS wordt ten zeerste aangeraden. Dit veilige hypertext-protocol codeert de pakketten tussen de browsers van de gebruikers en de controller en voorkomt dat iemand gebruikersinformatie verzamelt door op het netwerkverkeer te spioneren. Er kunnen zich omstandigheden voordoen waarbij niet-veilig hypertext-protocol (HTTP) wordt vereist. Als de TruPortal-systeemcontroller bijvoorbeeld via een webproxy-server wordt geopend die geen HTTPS (SSL) ondersteunt, dan kan als enige optie HTTPS/SSL worden uitgeschakeld.

9. Klik op [Volgende].

   De wizard zal deurcontrollers en I/O-uitbreidingsmodules ontdekken die op de TruPortal-systeemcontroller zijn aangesloten.
10. Klik op [Met pc synchroniseren] om de juiste tijd op de controller in te stellen.
11. Selecteer de juiste **Algemene ingang EOL-overwakingen** om aan te geven hoe de sabotagecircuits en -sensoren op de deuren en lezers zijn bekabeld.
12. Voor elke hulpingang voor algemene doeleinden die is aangesloten:
    a. Selecteer een **modus**.
    b. Observeer de ingangen om vast te stellen dat zij werken en met de controller communiceren.
13. Voor elke hulpuitgang voor algemene doeleinden die is aangesloten:
    a. Klik op de pictogram naast de **Status** om de status te wijzigen.
    b. Observeer de uitgangen om vast te stellen dat zij werken en door de controller worden geactiveerd.
14. Selecteer voor elke deurcontroller het **Aantal deuren** die moeten worden bediend.
15. Voor elke deur:
    a. Selecteer de juiste **Modus** voor contact, verzoeken om circuits af te sluiten en te saboteren.
    b. Selecteer van de lijst **Deurcontrole** opdrachten om elke deur op juiste installatie en elektrische bekabeling te testen.
16. Klik op [Voltooien] als u alle apparaten hebt getest.

HOOFDSTUK 3

Configuratie TruPortal-software

TruPortal is ontworpen zodat, wanneer geconfigureerd, u snel personen en identificaties kunt toevoegen en verwijderen en toegang tot uw faciliteit kunt beheren. Tijdens de configuratie definieert u het volgende:

- De zones, deuren, identificatielezers, videobewaking, en hulp-beveiligingssystemen op uw locatie
- Toegangsniveaus nodig voor de diverse groepen personen die op uw locatie werken
- Toegangschema's voor gewone dagen en vakantiedagen
- Operatorrollen voor de mensen die beheer en bewaking uitvoeren voor de TruPortal

Dit hoofdstuk is sequentieel georganiseerd, waarbij taken in de volgorde zijn gerangschikt waarin zij moeten worden voltooid om de TruPortal-software te configureren.

1. **Update de firmware van de TruPortal-systeemcontroller**.
2. **Diagnostieken controleren**.
3. **De Datum en tijd instellen**.
4. **Een Beveiligingscertificaat maken**.
5. **Een Beveiligingscertificaat uploaden**.
6. **SSL/HTTPSinschakelen**.
7. **Locatiebeveiliging configureren**.
8. **Kaartformaat toevoegen**.
9. **Toewijzing betekenisvolle namen aan ontdekte hardware**.
10. **TruPortal configureren**.
11. Optioneel: **I/O-uitbreidingsmodules configureren**.
12. **Configuratie deurcontrollers**.
13. **Deuren configureren**.
14. **Lezers configureren**.
15. Optioneel: **Een DVR toevoegen**.
16. Optioneel: **Een videocamera toevoegen**.
17. Optioneel: **Koppel camera's aan Apparaten om video van gebeurtenissen volgen**.
18. Optioneel: **Een zone toevoegen**.
19. Optioneel: **Anti-passback configureren**.
20. Optioneel: **Lezers aan zones toewijzen**.
21. Optioneel: **Een vakantiegroep toevoegen**.
22. Optioneel: **Een schema toevoegen**.
23. Optioneel: **Een lezersgroep toevoegen**.
24. **Een toegangsniveau toevoegen**.
25. Optioneel: **Een operatorrol toevoegen**.
26. Optioneel: **Door gebruikers gedefinieerde velden toevoegen**.
27. Optioneel: **Planning gedrag deur en lezer**.
28. **Personen en identificaties van een CSV-bestand importeren**.
29. **Een back-up en een herstelpunt maken**.

Update de firmware van de TruPortal-systeemcontroller

1. Start uw internetbrowser.
2. Download de nieuwste update van de TruPortal firmware.
3. Meld u aan op TruPortal.
   a. Typ in de adresbalk van de browser het IP-adres voor TruPortal.
   b. Als u Internet Explorer gebruikt en een waarschuwing over het beveiligingscertificaat ontvangt, selecteert u **Naar deze website doorgaan (niet aangeraden)**.
   c. Typ uw **Gebruikersnaam**.
   d. Typ uw **Wachtwoord**.
   e. Selecteer een **Taal**.

f. Klik op [Aanmelden].

4. Selecteer ***Systeembeheer > Updates firmware***.
5. Klik op [Bladeren].
6. Navigeer naar en selecteer het update-bestand voor de firmware.
7. Klik op [Update].
8. Diagnostieken controleren

Verzeker dat zich geen problemen voordoen met de deuren, controllers en andere nieuw geïnstalleerde hardware. Hiervoor controleert u het TruPortal-scherm Diagnostieken.

Zie **Diagnostieken op pagina 67.**

De Datum en tijd instellen

TruPortal ondersteunt tijdsynchronisatie met een NTP-server. Deze optie houdt, wanneer ingeschakeld in zowel TruPortal als uw DVR, uw DVR(s) en TruPortal met de tijd gesynchroniseerd. Zonder dit kan de tijd van de TruPortal relatief ten opzichte van de tijd van de DVR afwijken en problemen veroorzaken of het onmogelijk maken om video op te halen die aan een toegangsgebeurtenis is verwant. De NTP-client probeert elk uur te synchroniseren.

Opmerking: TVR10 ondersteunt geen tijdsynchronisatie met een NTP-server.

Opmerking: Als de tijd van de TruPortal handmatig wordt veranderd om binnen één minuut voor de aanvang van een schema dat aan een deur is toegewezen, zal de geplande deurmodus per direct ingaan.

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Datum en tijd**.
3. Selecteer uw **tijdzone**.
4. Selecteer uw lokale **Datum en tijd**.
5. Optioneel: synchroniseer tijd:
   a. Selecteer [Met NTP-server synchroniseren].

      NTP-tijdsync vereist toegang vanaf het paneel tot de NTP-server via UDP-poort 123. Als deze poort niet toegankelijk is, wordt de tijd van het paneel niet met de NTP-server gesynchroniseerd en worden gebeurtenissen van "NTP sync mislukt" in een logboek opgenomen.
   b. Typ het IP-adres van de NTP-server.
   c. Klik op [Nu synchroniseren].

Configuratie Netwerkbeveiliging

Met het tabblad Netwerkconfiguratie van de pagina Systeeminstellingen kunt u een beveiligingscertificaat toewijzen en de netwerkeigenschappen, inclusief veilig bladeren, configureren voor TruPortal.

Een Beveiligingscertificaat maken

1. Selecteer ***Systeembeheer > Systeeminstellingen.***
2. Klik op het tabblad **Netwerkconfiguratie**.
3. Klik op de knop [Verzoek ondertekening certificaat maken].
   Het dialoogvenster Verzoek ondertekening certificaat verschijnt.
4. Typ de verzochte informatie en klik op [Genereren].
   De CSR-tekst verschijnt in het tekstvak, rechts van het dialoogventer.
5. Om een zelf-ondertekend certificaat te gebruiken:
   a. Klik op [Zelfondertekend certificaat installeren].
   b. Start de controller opnieuw op wanneer gevraagd.
6. Om een ondertekend certificaat te gebruiken:
   a. kopieer CSR-tekst en sla deze op naar een lokaal bestand om het naar een certificatenautoriteit van uw keuze te verzenden.
   b. Sluit het dialoogvenster Verzoek ondertekening certificaat.
   c. Zie **Een Beveiligingscertificaat uploaden op pagina 12.**

Een Beveiligingscertificaat uploaden

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Netwerkconfiguratie**.
3. Klik op de knop [Certificaat importeren]. Het dialoogvenster Upload certificaat verschijnt.
4. Klik op [Bestand selecteren].
5. Blader naar en selecteer het certificaatbestand.
6. Klik op [Openen].
7. Klik op [Uploaden].
8. Start de controller opnieuw op wanneer gevraagd.

SSL/HTTPSinschakelen

BELANGRIJK: Bediening van TruPortal zonder HTTPS-beveiliging wordt niet aangeraden. HTTPS codeert communicatie tussen TruPortal en uw client-browser om te verzekeren dat inbrekers uw communicaties niet kunnen opvangen en geen toegang tot de server kunnen verkrijgen.

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Netwerkconfiguratie**.
3. Klik op de knop [Configureren].
   Het eigenschappenblad Netwerkeigenschappen verschijnt.
4. Selecteer **HTTPS-verbinding inschakelen**.

Opmerking: Er kunnen zich omstandigheden voordoen waarbij niet-veilig hypertext-protocol (HTTP) wordt vereist. Als de TruPortal-systeemcontroller bijvoorbeeld via een webproxy-server wordt geopend die geen HTTPS (SSL) ondersteunt, dan kan als enige optie HTTPS/SSL worden uitgeschakeld.

Opmerking: Zorg dat u, vooral bij gebruik van Firefox of Chrome, na het in- of uitschakelen van HTTPS/SSL, het cachegeheugen van de browser wist.

Configuratie beveiliging

Met het tabblad Beveiliging van de pagina Systeeminstellingen kunt u bepaalde aspecten configureren die voor de fysieke beveiliging van uw faciliteit gelden. Netwerkbeveiliging wordt op het tabblad Netwerkconfiguratie behandeld.

Pincodes

TruPortal kan voor toegang met alleen een identificatie of met een identificatie en een Persoonlijk identificatienummer (PIN) worden geconfigureerd. Dit vereist dat mensen zowel een badge (identificatie) tonen en een pincode invoeren. Dit biedt aanvullende beveiliging door toegang met een gevonden of gestolen badge te vermijden. Lezers kunnen op basis van schema's op Alleen identificatie of Identificatie en pincode worden geconfigureerd. (Zie **Planning gedrag deur en lezer op pagina 39.**)

Maximum pincodelengte

Pincodes kunnen 4, 6 of 9 cijfers lang zijn.

Pincodepogingen

Hiermee kunnen personen het aantal pogingen instellen om hun pincodes juist in te voeren.

Tijdstip vergrendeling pincode

Als een persoon te vaak een onjuiste pincode invoert, wordt voor de door deze optie aangegeven tijdsperiode, de toegang tot die lezer voor het identificatie-ID geweigerd. Nadat de Tijd blokkering is verlopen, worden de toegangsmachtigingen voor het identificatie-ID hersteld.

Gedegradeerde modus deur

Identificatie-informatie wordt op de TruPortal-systeemcontroller opgeslagen. Als een deurcontroller communicatie met de controller verliest, kan het identificaties die bij de lezers zijn ingevoerd ten opzichte van de database die op de controller is opgeslagen, controleren. In zo'n geval moet de deurcontroller toegangsverzoeken beoordelen als iemand de faciliteit betreedt.

Ingang EOL-overwakingen

Deuren kunnen worden bekabeld om te detecteren of zij open of dicht zijn, evenals om geforceerde toegang en sabotage te detecteren. Van een dergelijke deur wordt gezegd dat deze wordt bewaakt. Van een deur zonder dergelijke detectiecircuits wordt gezegd dat deze onbewaakt is, zelfs als het een lezer met insteekslot of magnetisch slot heeft. Voor bewaakte deuren beschrijft deze optie het type weerstand(en) die wordt/worden gebruikt en hoe het circuit is bekabeld. Er zijn twee stroomtypes die door TruPortal worden bewaakt: circuits van 1.000 Ohm en van 4.700 Ohm. Deze kunnen met dubbele weerstanden worden bekabeld, of met een enkele weerstand in serie of parallel, relatief ten opzichte van de deursensor.

Locatiebeveiliging configureren

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Beveiliging**.
3. Selecteer een **Max pincodelengte**.

BELANGRIJK: Als een nieuwe Maximum pincodelengte wordt opgeslagen en er bestaan identificaties met pincodenummers die langer zijn dan de nieuwe maximum lengte, wordt een waarschuwingsprompt weergegeven die u zegt dat de

bestaande pincodenummers tot de nieuwe lengte worden verkort. Met de prompt kunt u met het opslaan doorgaan of de bewerking annuleren.

4. Selecteer het aantal **Pincodepogingen**.
5. Selecteer een **Tijdstip vergrendeling pincode**.
6. Selecteer een **Gedegradeerde modus deur**:
   - **Beperkt**: Helemaal geen toegang toegekend
   - **Locatiecode**: Toegang wordt gegeven wanneer de kaart met één van de formaten overeenkomt die op de pagina Kaartformaat wordt gedefinieerd en de locatiecode op de kaart overeenkomt met de locatiecode die voor het formatt is gedefinieerd.
   - **Alles**: Toegang wordt toegekend als de kaart overeenkomt met een van de formaten die op de pagina Kaartformaten wordt gedefinieerd
7. Selecteer een optie voor **Ingang EOL-overwakingen**.
8. Klik op [Wijzigingen accepteren].

Configuratie Kaartformaten

Identificaties (identificatiebadges) gebruikt voor elektronische toegangscontrole, slaan gegevens in diverse formaten op. Om de gegevens juist te kunnen lezen, moet aan uw configuratie het kaartformaat worden toegevoegd. Het identificatie-ID die op de kaart is opgeslagen, bevat een kaartnummer, een faciliteitscode en een uitgiftecode.

Kaartformaat toevoegen

1. Selecteer ***Systeembeheer> Kaartformaten***.
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Formaatnaam**.
4. Selecteer een **Formaattype**.
5. Typ, indien nodig, de **Faciliteitscode**.
6. Typ voor een aangepaste formaat, indien vereist, andere gegevens.
7. Klik op [Wijzigingen accepteren].

Kaartformaat verwijderen

1. Selecteer ***Systeembeheer> Kaartformaten***.
2. Selecteer de kaartformaat die u wilt verwijderen.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Standaard kaartformaten

TruPortal heeft standaard de volgende kaart-formaten geïnstalleerd:

- 37 Bit HID met faciliteit 40 (I10304)
- 37 Bit HID met faciliteit 50 (I10304)
- 37 Bit HID met faciliteit 60 (I10304)

- 4002 40 Bit (40 Bit CASI 4002)
- 26-Bit onbewerkt

Deze formaten kunnen worden verwijderd als u andere formaten moet toevoegen. TruPortal kan tot acht actieve kaartformaten ondersteunen.

Configuratie Apparaten

Na de hardware te installeren en te verbinden, zal de TruPortal-systeemcontroller automatisch alle downstream apparaten ontdekken en deze in een boomstructuur op de pagina Apparaten tonen. TruPortal zal generieke, opeenvolgende namen aan de apparaten die het detecteert, toewijzen. Deze namen moeten door betekenisvolle namen worden vervangen om bewaking van toegangsgebeurtenissen te helpen. Bijvoorbeeld, “Deurcontroller (3)” kan met “Hoofdlobby, deuren oostelijke muur” worden vervangen. Om op deze wijze apparatuur te hernoemen, hebt u van elk apparaat een record met het serienummer en de installatielocatie nodig.

Voor de configuratie van een apparaat is er meer dan alleen het wijzigen van namen nodig. Optioneel worden vanaf deze pagina ook ingangen en uitgangen, videobewaking en verlengde timers voor toegang van personen met handicaps geconfigureerd.

Opmerking: Zie **Configuratie Video-apparaten op pagina 24** om een videocamera of DVR aan te sluiten.

Toewijzing betekenisvolle namen aan ontdekte hardware

Voor een systeem met meer dan enkele apparaten wordt het aangeraden dat u deze taak voor alle apparaten voltooid voordat u met de gedetailleerde configuratie van de apparaten verder gaat. Dit helpt u om bij te houden waar de apparaten zich in de faciliteit bevinden terwijl u met de gedetailleerde vereisten doorgaat.

Voordat u met deze taak start, moet u de het schema van de locatieconfiguratie verkrijgen. Deze toont waar elk apparaat zich fysiek bevindt. Zie **Documenteer de fysieke locatie van elk apparaat volgens Serienummer op pagina 5.**

1. Selecteer ***Systeembeheer > Apparaten***.
2. Selecteer de TruPortal-systeemcontroller.
3. Typ een beschrijvende **Naam apparaat**.
4. Klik op [Wijzigingen accepteren].
5. Selecteer de eerste deurcontroller op de lijst.
6. Vergelijk het **Serienummer** met het installatieschema.
7. Typ een beschrijvende **Naam apparaat**.
8. Klik op [Wijzigingen accepteren].
9. Herhaal dit voor alle apparaten in de hiërarchie.

TruPortal configureren

TruPortal kan vier hulpingangen voor algemene doeleinden accepteren en twee uitgangsignalen voor algemene doeleinden, die handmatig moeten worden geactiveerd, aanleveren. De ingangen kunnen

voor accessoires zoals een bewegingsdetector in een kamer, of voor ingangen van andere systemen, zoals een brandalarmsysteem, worden gebruikt. Deze vertegenwoordigen optionele configuraties en moeten alleen na installatie worden ingeschakeld. Ingangen voor algemene doeleinden kunnen worden geconfigureerd om bij activering automatisch alle deuren te ontgrendelen, zoals in geval van een brandalarm of andere noodsituatie.

1. Selecteer ***Systeembeheer > Apparaten***.
2. Selecteer de TruPortal-systeemcontroller.
3. Klik op het tabblad **Algemeen**.
4. Selecteer een **Gekoppelde camera** als één die is geconfigureerd om de fysieke locatie van de controller te bewaken.
5. Klik op het tabblad **Ingangen**.
6. Voor elke hulpingang voor algemene doeleinden die is aangesloten:
   a. Selecteer **Ingeschakeld**.
   b. Typ een betekenisvolle naam.
   c. Selecteer het **type**.
   d. Optioneel: selecteer **Alle deuren ontgrendelen** als de ingang vanaf een alarm of noodsysteem afkomstig is.
   e. Optioneel: selecteer een **Gekoppelde camera** als er één met de ingang is verwant (bijvoorbeeld, een camera die met een bewegingsdetector in een kamer is verwant).
7. Klik op het tabblad **Uitgangen**.
8. Voor elke hulpuitgang voor algemene doeleinden die is aangesloten:
   a. Selecteer **Ingeschakeld**.
   b. Typ een betekenisvolle naam.
   c. Selecteer **Actief aan/uit** als het relais moet worden gevoed als de uitgang is uitgeschakeld. Anders dient u het keuzevak uit te schakelen.
   d. Optioneel: selecteer een **Gekoppelde camera** als er één met de uitgang is verwant.
9. Klik op [Wijzigingen accepteren].

TruPortal Ingangen en uitgangen

Ingangen en uitgangen zijn opties voor algemene doeleinden waarmee u TruPortal op uw vereisten kunt aanpassen. Eeningang kan bijvoorbeeld een signaal van een bewegingsdetector zijn. Een uitgang is een elektrische impuls van de TP-controller naar een of ander apparaat. Ingangen en uitgangen worden vanaf de pagina ***Ingangen/uitgangen> bewaken*** bewaakt en uitgangen kunnen vanaf die pagina handmatig worden geactiveerd.

Configuratie deurcontrollers

Deurcontrollers kunnen met maximaal vier lezers op twee deuren worden aangesloten. Elke deur kan twee lezers hebben, één voor toegang en één voor uitgang, vaak gebruikt met anti-passback.

1. Selecteer ***Systeembeheer > Apparaten***.
2. Vouw de structuur onder de TruPortal-systeemcontroller uit.
3. Selecteer de deurcontroller.
4. Selecteer het **aantal deuren** die op deze controller zijn aangesloten.
5. Optioneel: selecteer een **Gekoppelde camera** als een camera met het paneel van de deurcontroller is verwant.
6. Klik op [Wijzigingen accepteren].

Opmerking: Als alle deuren zijn geblokkeerd terwijl een nieuwe deurcontroller wordt toegevoegd, blijft de nieuwe deurcontroller ontgrendeld. Om te worden geblokkeerd, moet de blokkering van alle deuren opnieuw worden opgeheven waarna alle deuren weer worden geblokkeerd.

Deuren configureren

Elke deur moet voor het volgende worden geconfigureerd:

- de tijdsduur dat het ontgrendeld moet zijn als een geldige identificatie wordt getoond
- de tijdsduur dat het open moet worden gehouden voordat een alarm wordt geactiveerd
- het type insteekslot dat wordt gebruikt (standaardsloten of magnetische sloten)
- of een lezer alleen voor toegang of voor zowel toegang als uitgang wordt vereist
- de types gebeurtenissen en alarmen die door de deurcircuits worden bewaakt
- hulpingangen en relais, bijvoorbeeld, een deur die voor een automatische opener en een uitgebreid verzoek voor vertrek (RTE, request to exit) is geconfigureerd om toegang aan gehandicapte personen te bieden.

Deuren configureren

1. Selecteer ***Systeembeheer> Apparaten***.
2. Vouw de structuur onder de TP-controller uit.
3. Vouw de structuur onder de deurcontroller uit.
4. Selecteer de deur om te configureren.
5. Selecteer een **Normale toegangstijd**.
6. Optioneel: selecteer een **Verlengdetoegangstijd**.
7. Selecteer een **Tijd deur opengehouden**.
8. Optioneel: selecteer een **Verlengdetijd deur opengehouden**.
9. Selecteer een **Insteekslot deur**.
   - **Getimed ontgrendelen**
   - **Vergrendelen bij sluiting**
10. Optioneel: selecteer een **Gekoppelde camera** als een camera is geplaatst om de deur te bewaken.
11. Selecteer een **Toegangsmodus**.
12. Optioneel: Selecteer **Verzoek voor vertrek ingeschakeld** als de deur hiervoor is bekabeld.
13. Optioneel: selecteer willekeurige alarmen waarvoor de deur is bekabeld:
    - **Deur opengehouden**
    - **Deur geforceerd open**
    - **Sabotage**

14. Optioneel: als u op de deur een alarmlamp of claxon hebt bekabeld, selecteert u “Deur opgehouden/geforceerd” van de lijst **Aux-relais**.
15. Configureer de sensor-**ingangstypes** voor:
    - **Deurcontact**-sensor
    - **Verzoek tot vertrek**-knop of -sensor
    - **Hulp**ingang van de contactsensor voor het Uitgebreide verzoek tot vertrek of de magnetische vergrendeling
    - **Sabotage**circuit
16. Klik op [Wijzigingen accepteren].
17. Herhaal dit voor elke deur.

Configureer een deur voor Uitgeschakelde toegang

Elke keer dat deuren te lang open worden gehouden en als toegang wordt toegekend maar de deur wordt niet geopend, neemt TruPortal-gebeurtenissen op. Met een optionele alarmlamp of claxon kan TruPortal een fysiek alarm activeren als de deur wordt geforceerd of te lang wordt opengehouden.

Om aan de behoeften te voldoen van degenen die meer tijd nodig kunnen hebben om een deur te openen of te passeren, laat TruPortal u identificeren welke identificaties deze toestemming krijgen en u kunt een deur voor optionele functies, zoals een automatische deuropener en extra tijd om voor verzoek tot vertrek-sensoren, configureren. Dit wordt per identificatie uitgevoerd om de beveiliging van de locatie te verzekeren, omdat hoe langer een deur wordt opengehouden, des te gemakkelijker het is voor mensen om zonder een identificatie te tonen naar binnen te gaan. Zie **Een identificatie toevoegen op pagina 41.**

1. Selecteer ***Systeembeheer> Apparaten***.
2. Vouw de structuur onder de TP-controller uit.
3. Vouw de structuur onder de deurcontroller uit.
4. Selecteer de deur om te configureren.
5. Selecteer een **Normale toegangstijd**.
6. Selecteer een **Verlengdetoegangstijd**.

   Dis de hoeveelheid tijd dat de deur ontgrendeld blijft zodat de persoon het kan openen.
7. Selecteer een **Tijd deur opengehouden**.
8. Selecteer een **Verlengdetijd deur opengehouden**.

   Dis de hoeveelheid tijd dat de deur open kan blijven zodat de persoon het kan passeren.
9. Selecteer een **Insteekslot deur**.
   - **Getimed ontgrendelen**
   - **Vergrendelen bij sluiting**
10. Optioneel: selecteer een **Gekoppelde camera** als één is geplaatst om de deur te bewaken.
11. Selecteer een **Toegangsmodus**.
12. Optioneel: selecteer **Verzoek voor vertrek ingeschakeld** als de deur hiervoor is bekabeld.
13. Optioneel: selecteer willekeurige alarmen waarvoor de deur is bekabeld:
    - **Deur opengehouden**
    - **Deur geforceerd open**
    - **Sabotage**
14. Als de deur voor een deuropener is bekabeld:
    a. Selecteer “Verlengde RTE” van de lijst **Hulpingang**.
    b. Selecteer “**Deuropener**” uit de lijst **Aux-relais**.

c. Selecteer een **Aux-relais op tijd**.

15. Configureer de sensor-**ingangstypes** voor:
    - **Deurcontact**-sensor
    - **Verzoek tot vertrek**-knop of -sensor
    - **Hulp**ingang van de contactsensor voor het Uitgebreide verzoek tot vertrek of de magnetische vergrendeling
    - **Sabotage**circuit
16. Klik op [Wijzigingen accepteren].
17. Herhaal dit voor elke deur.

Configureer een deur voor magnetische sloten

• WAARSCHUWING! • Als u een deur met magnetische sloten configureert, is het belangrijk de optie "Kleefmagneet terugmeldcontact" te gebruiken om te vermijden dat deurmagneten voortijdig worden geactiveerd of dat de deur wordt dichtgeslagen, wat potentieel letsel kan veroorzaken.

1. Selecteer ***Systeembeheer> Apparaten***.
2. Vouw de structuur onder de TP-controller uit.
3. Vouw de structuur onder de deurcontroller uit.
4. Selecteer de deur om te configureren.
5. Selecteer een **Normale toegangstijd**.
6. Optioneel: selecteer een **Verlengdetoegangstijd**.
7. Selecteer een **Tijd deur opengehouden**.
8. Optioneel: selecteer een **Verlengdetijd deur opengehouden**.
9. Selecteer een **Insteekslot deur**:
    - **Getimed ontgrendelen**
    - **Vergrendelen bij sluiting**
10. Optioneel: selecteer een **Gekoppelde camera** als één is geplaatst om de deur te bewaken.
11. Selecteer een **Toegangsmodus**.
12. Optioneel: Selecteer **Verzoek voor vertrek ingeschakeld** als de deur hiervoor is bekabeld.
13. Optioneel: selecteer willekeurige alarmen waarvoor de deur is bekabeld:
    - **Deur opengehouden**
    - **Deur geforceerd open**
    - **Sabotage**
14. Selecteer “**Kleefmagneet terugmeldcontact**” van de lijst **Hulpingang**.
15. Optioneel: als u op de deur een alarmlamp of claxon hebt bekabeld, selecteert u “Deur opengehouden/geforceerd” van de lijst **Aux-relais**.
16. Configureer de sensor-**ingangstypes** voor:
    - **Deurcontact**-sensor
    - **Verzoek tot vertrek**-knop of -sensor
    - **Hulp**ingang van de contactsensor voor het Uitgebreide verzoek tot vertrek of de magnetische vergrendeling
    - **Sabotage**circuit
17. Klik op [Wijzigingen accepteren].
18. Herhaal dit voor elke deur.

Opties deurconfiguratie

Normale toegangstijd
Als door de lezer een geldige identificatie wordt gescand, wordt de deur voor de hier geselecteerde tijdsperiode ontgrendeld.

Verlengde toegangstijd toekennen
Als een geldige identificatie met de geselecteerde optie **Uitgebreide tijden voor aankloppen/ vasthouden** door de lezer wordt gescand, wordt de deur voor de hier geselecteerde tijdsperiode ontgrendeld. Hiermee kunt u uw systeem configureren zodat die in naleving van de wetgeving en reguleringen is die toegang door personen met handicaps voorschrijven.

Zie **Een identificatie toevoegen op pagina 41.**

Tijd deur opengehouden
Als door de lezer een geldige identificatie wordt gescand, wordt de deur voor deze geselecteerde tijdsperiode open gehouden. Als een deur langer dan dat wordt opengehouden en de optie **Deur opengehouden** is geselecteerd, wordt een gebeurtenis opgenomen.

Verlengde tijd deur opengehouden
Als een geldige identificatie met de geselecteerde optie **Uitgebreide tijden voor aankloppen/ vasthouden** door de lezer wordt gescand, wordt de deur voor de hier geselecteerde tijdsperiode opengehouden. Als een deur langer dan dat wordt opengehouden en de optie **Deur opengehouden** is geselecteerd, wordt een gebeurtenis opgenomen. Hiermee kunt u uw systeem configureren zodat in naleving van de wetgeving en reguleringen is die toegang door personen met handicaps voorschrijven.

Zie **Een identificatie toevoegen op pagina 41.**

Verzoek tot vertrek ingeschakeld
Als de deur voor geforceerd openen, of voor te lang opengehouden en sabotage wordt gealarmeerd, moet Verzoek tot vertrek samen met een van deze knoppen of een lezer worden gebruikt voor afsluiten, of een soort sensor die iemand detecteert die de deur van binnenuit benadert. Anders wordt een alarm voor geforceerde deur gegenereerd elke keer dat iemand vertrekt.

Insteekslot deur

Getimed ontgrendelen
Als toegang wordt toegekend, wordt de deur ontgrendeld en blijft het gedurende de tijdsperiode die in **Normale toegangstijd toekennen** wordt aangegeven, ontgrendeld.

Als de **Hulpingang** van de deur voor Kleefmagneet terugmeldcontact wordt geconfigureerd, blijft het aankloprelais actief totdat de magnetische contactsensor actief is, het deurcontact wordt gesloten en de ontgrendelingstijd van de deur is verlopen.

Vergrendelen bij sluiting
De deur wordt ontgrendeld zodra de toegang wordt toegekend en blijft ontgrendeld totdat de tijd verloopt die in **Normale toegangstijd** toekennen verloopt, of de deur is geopend en gesloten, ongeacht welk zich het eerst voordoet.

Als de **AUX-ingang** van de deur voor Kleefmagneet terugmeldcontact wordt geconfigureerd, blijft het aankloprelais, ongeacht de ontgrendelingstijd, actief totdat de magnetische contactsensor actief is of het deurcontact wordt gesloten.

Toegangsmodus

Alleen lezer in

De deur heeft een lezer om identificaties te scannen om toegang te verschaffen. Het vereist echter niet dat een persoon een identificatie presenteert om buiten te gaan.

Lezer in Lezer uit

De deur heeft lezers die zowel bij toegang als vertrek identificaties scant. Dit wordt voor configuraties van anti-passback vereist.

Alarm ingeschakeld

Deur opengehouden

Selecteer deze optie als de deur is bekabeld om het openen ervan te detecteren. Wanneer langer opengehouden dan de tijd die voor **Tijd deur opengehouden** is geselecteerd, wordt op de pagina Gebeurtenissen een gebeurtenis opgenomen.

Deur geforceerd open

Selecteer deze optie als de deur is bekabeld om geforceerde toegang te detecteren. Als een persoon de deur opent zonder een identificatie te tonen waaraan toegang is toegekend, wordt op de pagina Gebeurtenissen een gebeurtenis opgenomen. Als u wilt dat zich een fysiek alarm voordoet als de deur wordt geforceerd, dient u een alarmlamp of claxon te configureren die aan het **Aux-relais** is bekabeld.

Sabotage

Selecteer deze optie als de deur is bekabeld om sabotage te detecteren. Wanneer gesaboteerd, wordt op de pagina Gebeurtenissen een gebeurtenis opgenomen.

Aux-ingang

Geen

Geeft aan dat de ingang niet wordt gebruikt of bewaakt.

Verlengde RTE

Alleen bedoeld voor gebruik terwijl de optie Deuropener voor **Aux-relais** is geselecteerd.

Kleefmagneet terugmeldcontact

Bedoeld voor deuren die een magnetische vergrendeling in plaats van een insteekslot hebben. Dit detecteert de uitvoer van het magnetische slot die aangeeft dat de deur aan de magneet is gebonden. TruPortal zal de magneet niet activeren totdat de kleefsensor van de deur aangeeft dat de deur contact heeft gemaakt met de magneet en de contactsensor van de deur aangeeft dat de deur is gesloten. Dit voorkomt dat de magneet voortijdig wordt geactiveerd waardoor de deur dicht wordt geslagen.

Als “Getimede ontgrendeling” voor de **Insteekslot deur** wordt geselecteerd, blijft de magneet niet-actief totdat die tijd is verlopen. Het is echter nog steeds niet-actief totdat signalen van de magnetische kleefsensor en de contactsensor van de deur worden ontvangen. Dit geeft aan dat de deur is gesloten en aan de magneet kleeft.

Aux-relais

Geen

Geeft aan dat het relais niet wordt gebruikt of wordt geactiveerd.

Deur opengehouden/geforceerd

Deze optie wordt meestal gebruikt om het relais een fysiek alarm, zoals een sirene of lamp, te laten activeren als de deur wordt opengehouden, of gedwongen wordt geopend.

Deuropener
Meestal gebruikt met een deur die met een enkele lezer voor toegang is geconfigureerd en uitgerust is met een handmatige vrijgavebedrading voor Verzoek te vertrekken (RTE, Requested to Exit) en een drukknop voor een automatische opener voor verlengde RTE. De RTE-ingang ontgrendelt de deur voor de tijdsduur dat de handmatige vrijgave actief is zodat iemand normaal kan vertrekken. De Aux-ingang (Verlengde RTE) activeert het Aux-relais voor de aangegeven Aux-relais op tijd. Deze relais-uitvoer activeert een deuropener die automatisch ontgrendelt en opent de deur voor een persoon die hulp nodig heeft.

Deze instelling is alleen nuttig als **Aux-ingang** voor Verlengde RTE is geconfigureerd.

Ingangtypes

NO (normaal open)
De sensorschakelaar is normaal open.

NC (normaal gesloten):
De sensorschakelaar is normaal gesloten.

Niet overwaakt
Het circuit is niet met een continuïteitscircuit bekabeld om sabotage te detecteren.

Overwaakt
Het circuit is met een continuïteitscircuit bekabeld om sabotage te detecteren.

Lezers configureren

1. Selecteer ***Systeembeheer > Apparaten***.
2. Vouw de structuur onder de TruPortal-systeemcontroller uit.
3. Vouw de structuur onder de deurcontroller uit.
4. Vouw de structuur onder de deur uit.
5. Selecteer de lezer om te configureren.
6. Selecteer een **Toegangsmodus**.
   - **Alleen identificatie**
   - **Identificatie en pincode**
7. Selecteer een **Gekoppelde camera** als een camera is geplaatst om de deur en lezer te bewaken.
8. Klik op [Wijzigingen accepteren].
9. Herhaal dit voor andere lezers.

Opties lezer

Alleen identificatie
Een persoon hoeft alleen maar een geldige identificatie (ID-badge) te tonen om toegang te verkrijgen.

Identificatie en pincode
Een persoon moet een geldige identificatie presenteren en voert een Persoonlijk identificatienummer in om toegang te verkrijgen. Dit voorkomt dat iemand met een gestolen of gevonden identificatie toegang krijgt. Sommige faciliteiten gebruiken gedurende de dag **Alleen identificatie** en na werkuren, als de faciliteit leeg is **Identificatie en pincode**.

I/O-uitbreidingsmodules configureren

1. Selecteer ***Systeembeheer > Apparaten***.
2. De IO-uitbreiding selecteren.
3. Klik op het tabblad **Algemeen**.
4. Selecteer een **Gekoppelde camera** als er een camera is om de fysieke locatie van de controller te bewaken.
5. Selecteer **Sabotage-alarm ingeschakeld** als de afgesloten ruimte voor sabotagedetectie is bekabeld.
6. Klik op het tabblad **Ingangen**.
7. Voor elke hulpingang voor algemene doeleinden die is aangesloten:
   a. Selecteer **Ingeschakeld**.
   b. Typ een betekenisvolle naam.
   c. Selecteer het **type**.
   d. Optioneel: selecteer **Alle deuren ontgrendelen** als de ingang vanaf een alarm of noodsysteem afkomstig is.
   e. Optioneel: selecteer een **Gekoppelde camera** als er één met de ingang is verwant (bijvoorbeeld, een camera die met een bewegingsdetector in een kamer is verwant).
8. Voor elke hulpuitgang voor algemene doeleinden die is aangesloten:
   a. Selecteer **Ingeschakeld**.
   b. Typ een betekenisvolle naam.
   c. Selecteer **Actief aan/uit** als het relais moet worden gevoed als de uitgang is uitgeschakeld. Anders dient u het keuzevak uit te schakelen.
   d. Optioneel: selecteer een **Gekoppelde camera** als er één met de uitgang is verwant.
9. Klik op [Wijzigingen accepteren].

Configuratie Video-apparaten

TruPortal laat u videorecords van toegangsgebeurtenissen zien door de video te openen die op een TVR10 of TVR30 is opgenomen met de camera's die met de apparaten zijn verwant en die aan de TruPortal-systeemcontroller zijn verbonden. Als zich bij een apparaat een gebeurtenis voordoet, houdt TruPortal een record bij met de datum en tijd van de gebeurtenis. Als u aan dat apparaat een camera hebt gekoppeld, gebruikt TruPortal de datum en tijd van de gebeurtenis om een hyperlink naar de opgenomen video op de DVR te maken, waarmee de camera is verbonden.

Opmerking: TVR10 is verkrijgbaar in de Verenigde Staten en Europa, TVR30 is alleen verkrijgbaar in de Verenigde Staten.

Door een camera aan een apparaat te koppelen, kan TruPortal via de video die van de camera is opgenomen gedurende de tijd van de gebeurtenis, een gebeurtenis aan dat apparaat koppelen. TruPortal bedient de camera of DVR niet rechtstreeks, maar het gebruikt de informatie om de DVR de datum en tijd door te geven en aan te geven welke camera de video voor het afspelen heeft opgenomen.

Camera's voor videobewaking zijn één van de twee algemene types: een vaste camera of een camera die kan pannen, kantelen of in/uit-zoomen (PTZ). Met TruPortal kunt u PTZ-camera's bedienen als:

- U Internet Explorer als uw browser gebruikt

- U ActiveX en.NET 4.0 in uw browser hebt geïnstalleerd of ingeschakeld
- De camera is aan een TVR10 of TVR30 verbonden

Een DVR toevoegen

TruPortal kan op DVR's van het merk UTC Fire and Security TVR-10 en TVR-30 aangesloten worden. Deze moeten op de volgende firmwareniveaus zijn om te kunnen werken met TruPortal:

- TVR 30: 0617-0380-0625-6300 (of later)
- TVR 10: v2.3 versie100916 (of later)

Raadpleeg de TVR-documentatie voor instructies over hoe firmwareversies te controleren en bij te werken.

1. Selecteer ***Systeembeheer > Apparaten> Video-apparaten***.
2. Klik op [Toevoegen] en kies het juiste DVR-model.
3. Typ voor de DVR een beschrijvende naam in het veld **Naam apparaat**.
4. Typ het **IP-adres** van de DVR.
5. Typ de **gebruikersnaam** om op het apparaat aan te melden.
6. Typ het wachtwoord om op het apparaat aan te melden.
7. Klik op [Wijzigingen accepteren].
8. Klik hieronder op de koppeling **Configuratie en bediening webbrowser**om de verbinding te bevestigen en de configuratie van de camera's te controleren die op de DVR zijn aangesloten.

Een videocamera toevoegen

Voordat u deze taak uitvoert, moet u een TVR10- of TVR30-apparaat hebben toegevoegd aan TruPortal.

Opmerking: TVR10 is verkrijgbaar in de Verenigde Staten en Europa, TVR30 is alleen verkrijgbaar in de Verenigde Staten.

1. Selecteer ***Systeembeheer > Apparaten> Video-apparaten***.
2. Selecteer de DVR met de camera die moet worden toegevoegd.
3. Selecteer ***Toevoegen > Camera.***
4. Typ voor de camera een beschrijvende naam in het veld **Naam apparaat**.

   Bijvoorbeeld, “Camera hoofdlobby.”
5. Selecteer de juiste **DVR-ingang**.

   Dit is het kanaal op de DVR waarop de camera fysiek is aangesloten.
6. Selecteer een **Bandbreedte videostream**.

   Als u niet zeker bent betreffende de bandbreedte, meldt u zich aan via de webgebaseerde interface van de DVR en controleert u de instelling voor de camera.
7. Typ de gewenste **Tijdsduur afspelen gebeurtenis vooraf**.

   Dit is de tijdsduur die tot de gebeurtenis leidt die u bij het afspelen wilt zien. Een gebeurtenis van geforceerde deur wordt bijvoorbeeld in het systeem opgenomen als de deur geforceerd wordt geopend. De persoon die de deur forceerde heeft mogelijk de deur al enkele minuten, voordat hij/zij succesvol de deur geforceerd opende, kunnen saboteren.

Video-opmaken toevoegen

Een video-opmaak bepaalt hoeveel camera-ingangen u tegelijkertijd op uw computerscherm kunt controleren.

1. Selecteer ***Video-opmaken > bewaken.***
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Naam video-opmaak**.

   Als u bijvoorbeeld vier camera's hebt die over de zone van de laadsluis waken, kunt u een opmaak van 2x2 maken en het "Camera's laadsluis" noemen.
4. Selecteer een **Type video-opmaak**.
5. Selecteer voor elke cel van de opmaak een camera.
6. Klik op [Wijzigingen accepteren].

Koppel camera's aan Apparaten om video van gebeurtenissen volgen

Lezers genereren gebeurtenissen voor toegekende en geweigerde toegang. Als u dus een camera aan een lezer koppelt, hebt u van elke persoon die via die lezer toegang kreeg (of die de toegang werd geweigerd) een visueel record.

Deuren genereren gebeurtenissen wanneer zij geforceerd worden geopend, te lang open worden gehouden en bij tijdelijke ontgrendeling. Als u dus een camera aan een deur koppelt, hebt u van elk incident voor toegangsbeveiliging een record.

Hulpingangen en -uitgangen zijn optionele apparaten die met de TruPortal systeemcontroller of een TruPortal I/O-uitbreidingsmodule zijn verbonden. Om aan deze apparaten een camera te koppelen, moet u dit via het tabblad Ingang of Uitgang van de passende controller doen.

1. Sluit TruPortal aan (via uw TCP/IP-netwerk) op de DVR en camera.
   a. Zie **Een DVR toevoegen op pagina 25.**
   b. Zie **Een videocamera toevoegen op pagina 25.**
2. Selecteer ***Systeembeheer > Apparaten***.
3. Selecteer het apparaat van de structuur op de pagina Apparaten
4. Selecteer van de lijst **Gekoppelde camera** de passende camera.

Configuratie zones

Zones vertegenwoordigen de ruimten in het fysieke grondplan van uw faciliteit, vooral de ingangen en uitgangen van en naar deze ruimten. Door zones te definiëren, kunt u identificeren welke lezers naar deze ruimten leiden en welke lezers van deze ruimten naar naastliggende ruimten leiden. Zones worden gebruikt om de fysieke locatie van Personen binnen de faciliteit te volgen, die in het Roosterrapport kunnen worden gevonden, en voor het traceren van Anti-passback van identificaties.

Een zone toevoegen

Voordat u aan een zone lezers toewijst, moet u eerst de zone creëren.

1. Selecteer ***Toegangsbeheer > Zones > Zonedefinitie***.
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Zonenaam**.
4. Selecteer een optie voor **Automatische reset anti-passback**.

   Als u "Nooit" selecteert, moet u een APB-overtreding handmatig opnieuw instellen.
5. Klik op [Wijzigingen accepteren].

Lezers aan zones toewijzen

De toewijzing van lezers aan zones is wat zones in TruPortal definieert. TruPortal neemt op bij welke lezer een identificatie wordt gescand en op basis van de zonetoewijzing, meldt het bij welke zone de persoon met die identificatie moet zijn en welke lezers die persoon moet passeren voordat hij naar een andere zone gaat.

BELANGRIJK: Zorg dat de lezertoewijzingen juist zijn. Als TruPortal bij een lezer een identificatie detecteert die niet aansluit met de laatste lezer, dan wordt een anti-passbackovertreding geactiveerd. Als Lab A bijvoorbeeld aansluit op de hoofdgang en fysiek is ingesteld zodat Lezer 1 toegang toekent en Lezer 2 vertrek toekent, maar u hebt per ongeluk Lezer 3 als uitgang toegewezen, dan zal elke persoon die Lab A probeert te verlaten, een anti-passbackovertreding veroorzaken.

1. Selecteer ***Toegangsbeheer> Zones > Lezertoewijzingen***.
2. Voor elke lezer:
   a. Selecteer de **Van-zone**. Dit is de zone waar de lezer zich bevindt.
   b. Selecteer de **Naar-zone**. Dit is de zone die de persoon zal betreden zodra de lezer de identificatie heeft geaccepteerd.
   c. Selecteer **Anti-passback**:
      - **Geen**
      - **Soft**
      - **Hard**
3. Klik op [Wijzigingen accepteren].

Een zone verwijderen

Opmerking: De standaardzone kan niet worden verwijderd.

1. Selecteer ***Toegangsbeheer> Zones > Zonedefinitie***.
2. Selecteer de zone om te verwijderen.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Configuratie Anti-passback

Anti-passback vereist dat een identificatie wordt gebruikt om een zone te betreden of *te verlaten*. Op deze manier traceert TruPortal welk gebied momenteel wordt bezet door de identificatiehouder, bewaart het een record van bewegingen van personeel binnen beveiligde zones en voorkomt het doorgang naar zones die logisch onmogelijk zijn.

Als een persoon een identificatie gebruikt om een zone te betreden die voor Anti-passback is geconfigureerd, en de zone daarna verlaat (bijvoorbeeld via een deur die door een ander persoon open wordt gehouden), zal de TruPortal NGP-controller niet weten dat de persoon die specifieke zone heeft verlaten. Als resultaat, wanneer TruPortal voor krachtige dwang van anti-passback is geconfigureerd, voorkomt het dat die identificatie kan worden gebruikt om, inclusief de zonet verlaten zone, een andere zone te betreden totdat de locatie van de identificatie opnieuw op een standaard of neutrale zone is ingesteld.

Anti-passbackopties

Als een persoon een identificatie (ID-badge) toont om een zone te betreden, maar op de een of andere manier de zone zonder vertoning van het ID verlaat, dan doet zich een anti-passbackovertreding voor. De gebeurtenis wordt geactiveerd zodra de persoon een andere zone probeert te betreden die niet fysiek aan de laatst bekende zone van de persoon is verbonden.

Geen
Anti-passback wordt niet gebruikt.

Soft
Er wordt een gebeurtenis opgenomen als een identificatie anti-passback overtreedt.

Hard
De identificatie die de anti-passback overtreedt, wordt toegang tot alle zones geweigerd totdat de locatie van de identificatie opnieuw op een neutrale of standaardzone is ingesteld.

Anti-passback configureren

Om anti-passback te configureren, moet u aan TruPortal zones toevoegen die overeenkomen met de zones op uw locatie- of grondplan, lezers aan deze zones toewijzen en aan TruPortal identificaties toevoegen.

1. Zie **Een zone toevoegen op pagina 27.**
2. Zie **Lezers aan zones toewijzen op pagina 27.**
3. Zie **Een identificatie toevoegen op pagina 41.**

Opmerking: Via het deelvenster Identificatie van de pagina Personen (***Toegangsbeheer> Personen***) kunt u individuele identificaties uitsluiten van de bekrachtiging van anti-passback.

Vakantiegroepen maken

Vakanties zijn uitzonderingen in werkplekschema's. Voor deze dagen een vakantiegroep creëren, zorgt dat TruPortal het gewone schema op deze dagen opheft. Als u niet wilt dat een vakantie een bepaald schema opheft, moet u de vakantiegroep in dat schema opnemen.

Uw faciliteit kan bijvoorbeeld van elke maandag tot vrijdag open zijn, met uitzondering van bepaalde jaarlijkse vakanties als alleen huishoudelijk personeel en netwerkbeheerders toegang tot de faciliteit moeten hebben. Het huishoudelijke personeel kan uitgebreide reinigingswerkzaamheden uitvoeren als de faciliteit voor normaal werk is gesloten. De netwerkbeheerders kunnen vakanties gebruiken om uitgebreid onderhoud of upgrades uit te voeren die op een gewone werkdag storend kunnen zijn. Om aan deze behoeften te voldoen, maakt u voor deze dagen een vakantiegroep gedurende welke gewoon personeel zich niet op het werk aanmeldt. Daarna creëert u twee schema's en twee toegangsniveaus, één voor kantoorpersoneel en één voor ondersteuningspersoneel (huishoudelijke personeel en netwerkbeheerders). Plaats de vakantiegroep in het schema voor ondersteuningspersoneel, maar niet in het schema kantoorpersoneel. Als u het toegangsniveau voor ondersteuningspersoneel configureert, wijst u het schema van het ondersteuningspersoneel aan de lezers en lezersgroepen toe die door het ondersteuningspersoneel zullen worden gebruikt. Als u het toegangsniveau voor kantoorpersoneel configureert, wijst u het schema van het kantoorpersoneel aan de lezers en lezersgroepen toe die door het kantoorpersoneel zullen worden gebruikt.

Een vakantiegroep toevoegen

1. Selecteer ***Toegangsbeheer > Vakanties***.
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Naam vakantiegroep**.

   Een nieuw gecreëerde vakantiegroep heeft standaard één vakantie erin.

   a. Kies de datum en het patroon van de vakantie:
      - **Eenmaal**: een eenmalige gebeurtenis.
      - **Jaarlijks herhaald**: een gebeurtenis die zich elk jaar op dezelfde datum, zoals 25 december, voordoet.
      - **Aangepast**: een gebeurtenis die jaarlijks volgens een specifiek patroon wordt herhaald, zoals de laatste maandag van de maand.
4. Om aan de groep een vakantie toe te voegen, klikt u in het deelvenster met de vakantielijst op [Toevoegen] en herhaalt u stap a.
5. Klik op [Wijzigingen accepteren].

Een vakantie aan een vakantiegroep toevoegen

1. Selecteer ***Toegangsbeheer > Vakanties***.
2. Selecteer van de lijst met vakantiegroepen de vakantiegroep die u wilt wijzigen.
3. Een vakantie aan de groep toevoegen:
   a. Klik in het deelvenster vakantielijst op [Toevoegen].
   b. Kies de datum en het patroon van de vakantie:
      - **Eenmaal**: een eenmalige gebeurtenis.
      - **Jaarlijks herhaald**: een gebeurtenis die zich elk jaar op dezelfde datum, zoals 25 december, voordoet.
      - **Aangepast**: een gebeurtenis die jaarlijks volgens een specifiek patroon wordt herhaald, zoals de laatste maandag van de maand.
4. Klik op [Wijzigingen accepteren].

Vakantiegroep kopiëren

1. Selecteer ***Toegangsbeheer > Vakanties***.
2. Selecteer van de lijst met vakantiegroepen de vakantiegroep die u wilt kopiëren.
3. Klik op [Kopiëren].
4. Typ een beschrijvende naam in het veld **Naam vakantiegroep**.
5. Maak, indien nodig, veranderingen aan de vakanties in de gekopieerde groep.
6. Klik op [Wijzigingen accepteren].

Vakantiegroep verwijderen

Opmerking: Een vakantiegroep die in gebruik is, kan niet worden verwijderd.

1. Selecteer ***Toegangsbeheer > Vakanties***.
2. Selecteer van de lijst met vakantiegroepen de vakantiegroep die u wilt verwijderen.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Schema's maken

Schema's worden gebruikt om vast te stellen wanneer een persoon toegang toegekend krijgt bij een lezer of wanneer een deur automatisch zal vergrendelen of ontgrendelen. Schema's om de toegangstijden van lezers te bedienen worden via de pagina ***Toegangsbeheer> Toegangsniveaus*** toegewezen. Schema's om deurvergrendeling te bedienen, worden via de pagina ***Deuren> bewaken*** toegewezen.

TruPortal laat u tot 64 schema's creëren en omvat de volgende vooraf gedefinieerde schema's:

- Alle dagen 24/7
- Weekdagen 08:00-17:00
- Weekdagen 09:00-18:00
- Weekdagen 07:00:00-19:00

Opmerking: Schematijden worden in uren en minuten uitgedrukt en niet in seconden, maar starttijden van intervallen zijn relatief aan de start van de minuut (0 seconden) en eindtijden van de intervallen zijn relatief aan het einde van de minuut (59 seconden). Als u naar het vooraf gedefinieerde schema 24/7 kijkt, merkt u dat de starttijd 12:00 en de eindtijd 23:59 is. De starttijd is 12:00:00 en de eindtijd is 23:59:59 met, uitgedrukt in seconden, één seconde verschil. Een schema dat middernacht passeert, moet op deze manier worden ingesteld omdat als u de start- en eindtijd 12:00 invoerde, het schema maar 59 seconden actief zou zijn (van 12:00:00 tot 12:00:59).

Tijdintervallen

Een interval is de tijdsperiode gedurende welke een schema actief is. TruPortal-schema's kunnen aan meerdere intervallen worden toegewezen.

Als bijvoorbeeld uw reinigingspersoneel van het kantoor de etages op woensdagen wassen en stofzuigen, maar op de andere dagen van de week alleen de toiletten en afvalbakken reinigt, moeten zij op woensdag meer uren toegang krijgen dan op andere dagen van de week. In dit geval moet u voor woensdag één interval creëren en een andere interval voor de overige dagen van de week.

Een schema toevoegen

1. Selecteer ***Toegangsbeheer > Tijdschema's***.
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Naam schema**.
4. Maak intervallen voor het schema.
   a. Klik op het deelvenster Intervallenlijst op [Toevoegen] om extra intervallen te maken.
   b. Klik boven elke dag die u aan de interval wilt toevoegen, op het keuzevak.
   c. Typ waarden voor start- en eindtijden.
5. Klik op **Vakantiegroepen**.
6. Selecteer de vakantiegroepen die in dit schema zijn opgenomen.

Opmerking: Vakanties zijn uitzonderingen op normale toegangsschema's. Een vakantiegroep in een schema opnemen weerhoudt de vakantiegroep van het opheffen van dat schema. Als u bijvoorbeeld een vakantiegroep voor bankvakanties hebt gemaakt en uw kantoor is op die dagen gesloten, zult u voor het schema van het toegangsniveau voor uw kantoorwerknemers die vakantiegroep niet selecteren. Als uw verzendafdeling echter tijdens vakanties werkt, moet u de bankvakantiegroep voor het schema selecteren voor het toegangsniveau van de verzendingswerknemers en dus voorkomt u dat de bankvakantiegroep het verzendschema opheft.

7. Klik op [Wijzigingen accepteren].

Een interval aan een schema toevoegen

1. Selecteer ***Toegangsbeheer > Tijdschema's***.
2. Selecteer het schema dat moet worden gewijzigd.
3. Maak intervallen voor het schema.
   a. Klik op het deelvenster Intervallenlijst op [Toevoegen] om extra intervallen te maken.
   b. Klik boven elke dag die u aan de interval wilt toevoegen, op het keuzevak.
   c. Typ waarden voor start- en eindtijden.
4. Klik op [Wijzigingen accepteren].

Een interval van een schema verwijderen

1. Selecteer ***Toegangsbeheer > Tijdschema's***.
2. Selecteer het schema dat moet worden gewijzigd.
3. Selecteer het interval om te verwijderen.
4. Klik in het deelvenster intervallenlijst op [Verwijderen].
5. Klik op [Wijzigingen accepteren].

Een schema kopiëren

1. Selecteer ***Toegangsbeheer > Tijdschema's***.
2. Selecteer het schema dat moet worden gekopieerd.
3. Klik op [Kopiëren].
4. Typ een beschrijvende naam in het veld **Naam schema**.
5. Tijdintervallen toevoegen, verwijderen of wijzigen, indien nodig.
6. Klik op [Wijzigingen accepteren].

Een schema verwijderen

1. Selecteer ***Toegangsbeheer > Tijdschema's***.
2. Selecteer het schema om te verwijderen.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Lezergroepen maken

Lezersgroepen zijn nuttig als u in uw faciliteit een groot aantal lezers en deuren hebt. Met lezersgroepen kunt u verschillende lezers volgens algemene eigenschappen groeperen en deze als groep aan Toegangsniveaus toe wijzen. Bijvoorbeeld, alle lezers in de kelder van een gebouw kunnen aan een groep worden toegevoegd.

De groepering hoeft niet volgens de fysieke zone plaats te vinden. Een lezersgroep met de naam Huishouding kan bijvoorbeeld in een toegangsniveau worden gebruikt dat toegang tot alle beveiligde opslagruimten met reinigingsspullen toekent.

Lezersgroepen verschijnen op de pagina Toegangsniveaus zodat u met een enkele selectie aan alle lezers in een groep toegang kunt toekennen in plaats van dat lezer voor lezer te doen.

Een lezersgroep toevoegen

1. Selecteer ***Toegangsbeheer > Lezersgroepen***.
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Naam lezersgroep**.
4. Selecteer elke lezer in de groep.
5. Klik op [Wijzigingen accepteren].

Een lezersgroep kopiëren

1. Selecteer ***Toegangsbeheer > Lezersgroepen***.
2. Selecteer de lezersgroep om te kopiëren.
3. Klik op [Kopiëren].
4. Typ een beschrijvende naam in het veld **Naam lezersgroep**.
5. Voeg lezertoewijzingen naar behoefte toe of wijzig deze.
6. Klik op [Wijzigingen accepteren].

Een lezersgroep verwijderen

1. Selecteer ***Toegangsbeheer > Lezersgroepen***.
2. Selecteer de te verwijderen lezersgroep.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Toegangsniveaus kopiëren

Toegangsniveaus bepalen tot welke deuren een identificatie toegang heeft en wanneer. Als uw faciliteit bijvoorbeeld een kantoor en een magazijn heeft en kantoorwerkers niet in het magazijn mogen komen, dat creëert u een Toegangsniveau voor kantoorwerknemers die alleen de deuren binnen de kantoorzone omvat.

De pagina Toegangsniveaus wordt gebruikt om aan lezers en lezersgroepen schema's toe te wijzen. Daarna worden toegangsniveaus aan Identificaties toegewezen. Hierdoor wordt bepaald op welke dagen en tijdstippen en via welke lezers een gebruiker met die identificatie toegang tot dat toegangsniveau kan krijgen.

Een toegangsniveau toevoegen

1. Selecteer ***Toegangsbeheer***> ***Toegangsniveaus***.
2. Klik op [Toevoegen].
3. Typ een beschrijvende naam in het veld **Naam toegangsniveau**.
4. Selecteer de lezers en lezersgroepen om in dat toegangsniveau op te nemen.
5. Selecteer voor elke geselecteerde lezer een schema.
6. Klik op [Wijzigingen accepteren].

Een toegangsniveau kopiëren

Als u een groot aantal lezers hebt, kan het creëren van een nieuw toegangsniveau veel tijd in beslag nemen. Door een bestaand toegangsniveau te kopiëren, kunt u een gelijke configuratie hergebruiken en hoeft u alleen maar een paar wijzigingen aan te brengen die voor het nieuwe toegangsniveau zijn vereist.

1. Selecteer ***Toegangsbeheer*** > ***Toegangsniveaus***.
2. Klik op het toegangsniveau dat u wilt kopiëren.
3. Klik op [Kopiëren].
4. Typ een beschrijvende naam in het veld **Naam toegangsniveau**.
5. Maak enige benodigde wijzigingen aan de lezers en lezersgroepen in dat toegangsniveau.
6. Schakel het keuzevak uit naast lezers die u niet in dit toegangsniveau wilt opnemen.
7. Klik op [Wijzigingen accepteren].

Een toegangsniveau verwijderen

1. Selecteer ***Toegangsbeheer*** > ***Toegangsniveaus***.
2. Klik op het toegangsniveau dat u wilt verwijderen.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Operatorrollen configureren

Een operatorrol is een groepsbeleid voor machtigingen. Als u een persoon toevoegt en die persoon de mogelijkheid toekent om zich aan te melden en TruPortal te bedienen, dan kent u die operator bepaalde machtigingen toe om functies en gegevens te wijzigen, uit te voeren of gewoon te bekijken. In plaats van handmatig voor elke individuele operator toegang tot elke functie en alle gegevens te configureren, kunt u met de functie Operatorrol toegangsprivileges toewijzen die voor elk type operator algemeen zijn en op hun respectievelijke taakrollen zijn gebaseerd. TruPortal omvat vijf vooraf gedefinieerde rollen:

- **Alleen bekijken**
- **Bewaker**
- **Operator**
- **Dealer**
- **Beheerder**

De vijf vooraf gedefinieerde rollen kunnen niet worden verwijderd, maar vier ervan kunnen wel worden gewijzigd. U kunt ook aangepaste rollen maken. Aangepaste rollen kunnen worden verwijderd, maar niet als deze aan een gebruiker is toegewezen.

Een operatorrol toevoegen

1. Selecteer ***Systeembeheer > Operatorrollen***.
2. Klik op [Toevoegen].
3. Typ voor de rol een beschrijvende naam in het veld **Naam rol**.
4. Selecteer voor elke functie een **Machtiging**.
5. Klik op [Wijzigingen accepteren].

Een operatorrol wijzigen

Opmerking: De beheerdersrol kan niet worden gewijzigd.

1. Selecteer ***Systeembeheer > Operatorrollen***.
2. Typ voor de rol een beschrijvende naam in het veld **Naam rol** om het te hernoemen.
3. Wijzig, indien nodig, voor elke functie de **Machtiging**.
4. Klik op [Wijzigingen accepteren].

Een operatorrol kopiëren

Door een bestaande operatorrol te kopiëren, kunt u een gelijke configuratie hergebruiken en hoeft u alleen maar een paar wijzigingen aan te brengen die voor de nieuwe rol zijn vereist.

1. Selecteer ***Systeembeheer > Operatorrollen***.
2. Selecteer de rol die u wilt kopiëren.
3. Klik op [Kopiëren].
4. Typ voor de rol een beschrijvende naam in het veld **Naam rol**.
5. Wijzig, indien nodig, voor elke functie de **Machtiging**.
6. Klik op [Wijzigingen accepteren].

Een operatorrol verwijderen

Opmerking: De vijf vooraf gedefinieerde rollen kunnen niet worden verwijderd.

1. Selecteer ***Systeembeheer > Operatorrollen***.
2. Selecteer de rol die u wilt verwijderen.
3. Klik op [Verwijderen].
   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

Door gebruikers gedefinieerde velden configureren

Persoonsrecords in de TruPortal-database kunnen over verwante door gebruikers gedefinieerde velden beschikken. Hiermee kunt u persoonlijke gegevens over personeel invoeren, zoals het kenteken van het voertuig of het telefoonnummer thuis. Er moet een veld worden ingeschakeld dat op de pagina Personen moet verschijnen. Als u een veld uitschakelt, wordt het van de database verwijderd en gaan voor elk Persoonsrecord alle gegevens in dat veld verloren.

Elke database moet een manier hebben om het ene record van het andere te identificeren. Gezien sommige namen veel voorkomen, zal het niet helpen als u de achternamen van werknemers als een unieke identificatie van het databaserecord gebruikt. Daarom wijzen organisaties regelmatig een uniek identificatienummer toe aan elke werknemer of elk lid.

BELANGRIJK: Voor de beste resultaten met TruPortal moet u een persoonsrecord-ID, zoals een werknemersnummer, hebben, dat voor elk persoon in uw organisatie uniek is. Zonder elk record als uniek te kunnen identificeren, kunnen updates, import en export en andere onderhoudsacties van de database resulteren in wijzigingen die aan het verkeerde record worden uitgevoerd.

Als u door gebruikers gedefinieerde velden maakt, kunt u ze als beschermd toewijzen. Voor deze optie bepalen de instellingen of de door de gebruikers gedefinieerde velden binnen de geselecteerde functie Beschermd zichtbaar zijn of door diverse operatorrollen kunnen worden gewijzigd. Dit biedt een toegevoegd niveau van privacy voor gevoelige informatie, zoals telefoonnummers thuis. Als u bijvoorbeeld wilt dat gebruikers met de Operatorrol alle persoonlijke informatie kunnen zien en gebruikers met de Bewakersrol alleen niet-beschermde persoonlijke informatie kunnen zien, moet u de instellingen van de operatorrol wijzigen zoals in de volgende tabel wordt weergegeven:

Rol	Instelling van door gebruikers gedefinieerde velden	Instelling beschermde gebruikersvelden
Operator	Alleen bekijken	Alleen bekijken
Bewaker	Alleen bekijken	Geen

Door gebruikers gedefinieerde velden toevoegen

De door de gebruikers gedefinieerde velden maken deel uit van de Persoonsrecords in de TruPortal database. Er moet een veld worden ingeschakeld die op de pagina Personen moet verschijnen.

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Door gebruikers gedefinieerde velden**.
3. Voor elk veld:
   a. Selecteer **Ingeschakeld**.
   b. Typ een **Label**.
   c. Optioneel: selecteer **Vereist**.
   d. Optioneel: selecteer **Beschermd**.
4. Klik op [Wijzigingen accepteren].

Door gebruikers gedefinieerde velden opnieuw rangschikken

De door de gebruikers gedefinieerde velden maken deel uit van de Persoonsrecords in de TruPortal database. Er moet een veld worden ingeschakeld die op de pagina Personen moet verschijnen. Als u een veld uitschakelt, wordt het van de database verwijderd en gaan voor elk Persoonsrecord alle gegevens in dat veld verloren.

BELANGRIJK: Bewerk de veldlabels niet in een poging hun volgorde opnieuw te rangschikken. De gegevens zijn met het veld verwant en niet met het veldlabel. De wijziging van het label zal de volgorde niet wijzigen, maar het veroorzaakt echter dat de gegevens niet juist worden gelabeld.

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Door gebruikers gedefinieerde velden**.
3. Gebruik de Volgordepijlen om velden naar boven of beneden te verplaatsen.

   De volgorde van velden op dit tabblad komt overeen met de volgorde van velden op de pagina Personen.

Een door gebruikers gedefinieerd veld verwijderen

Er moet een veld worden ingeschakeld die op de pagina Personen moet verschijnen. Als u een veld uitschakelt, wordt het van de database verwijderd en gaan voor elk Persoonsrecord alle gegevens in dat veld verloren.

1. Selecteer ***Systeembeheer > Systeeminstellingen***.
2. Klik op het tabblad **Door gebruikers gedefinieerde velden**.
3. Schakel het keuzevak **Ingeschakeld** uit voor het veld en de gegevens die u wilt verwijderen.
4. Klik op [Wijzigingen accepteren].

Planning gedrag deur en lezer

Het tabblad Schemaweergave op de pagina Deuren wordt gebruikt om het standaardgedrag van een deur en lezer volgens een schema op te heffen. Tijdens werkuren wilt u misschien een publieke deur, zoals naar een showroom of kleinhandelzone, ontgrendelen. Na normale werkuren wilt u dat bepaalde lezers zowel een identificatie als een pincode vereisen (nuttig om toegang met verloren of gestolen identificatiekaarten te vermijden). U kunt de lezer dus configureren om standaard alleen een identificatie te verzoeken (***Systeembeheer > Apparaten***) en om na werkuren een identificatie en pincode te verzoeken (***Bewaking > Deuren > Schemaweergave***).

Opmerking: Verwar het gedrag van de deur en lezer niet met toegang. De pagina Toegangsniveaus wordt gebruikt om schema's aan lezers en lezersgroepen toe te wijzen. Daarna worden toegangsniveaus aan Identificaties toegewezen. Hierdoor wordt bepaald op welke dagen en tijdstippen en via welke lezers een gebruiker met die identificatie toegang tot dat toegangsniveau kan krijgen. De toegangsmodus, alleen identificatie of identificatie en pincode, is niet relevant voor het toegangsniveau. (Zie **Configuratie beveiliging op pagina 13.**)

1. Selecteer ***Deuren > bewaken***.
2. Klik op het tabblad **Schemaweergave**.
3. Voor elke deur- en lezercombinatie:
   a. Selecteer een **Schema**.
   b. Selecteer een **Schemamodus**.

      De Schemamodi voor deuren zijn:
      - **Ontgrendeld**
      - **Eerste kaart in**
      - **Vergrendeld**

      Voor lezers zijn de Schemamodi:
      - **Alleen identificatie**
      - **Identificatie en pincode**

Personen en identificaties van een CSV-bestand importeren

Met de Import/Export-wizard kunt u de velden van het bestand met door komma gescheiden waarden (CSV) aan de TruPortal-databasetabel toewijzen en de personen en identificaties importeren.

Opmerking: Een TruPortal-persoonsrecord bestaat uit door gebruikers gedefinieerde velden voor persoonlijke informatie, toegangsidentificaties (badge-ID, pincode, toegangsniveau) en optionele informatie over de gebruikersaccount om aanmelding op TruPortal toe te staan. Import en export van gegevens van een TruPortal gebruikersaccount wordt niet ondersteund. Alleen door gebruikers gedefinieerde persoonlijke gegevens en identificatiegegevens kunnen worden geïmporteerd en geëxporteerd.

Zie “Personen en identificaties van een CSV-bestand importeren” in de *Handleiding van de import/export-wizard voor TruPortal*.

Een back-up en een herstelpunt maken

In geval u het systeem naar de initiële bedrijfsstatus moet herstellen, is het belangrijk dat nadat u de configuratie van TruPortal hebt voltooid, u zowel een back-upbestand maakt die wordt opgeslagen op een lokale pc, als een herstelpunt (uw aangepaste instellingen opslaan) dat op de controller wordt opgeslagen.

Zie **Gegevensverlies voorkomen op pagina 57.**

HOOFDSTUK 4 *Toegang beheren*

U beheert wie toegang heeft tot uw faciliteit en TruPortal door:

- personen toe te voegen en te verwijderen
- identificaties toe te voegen, te deactiveren, te heractiveren en te verwijderen
- gebruikersaccounts toe te voegen en te verwijderen

Personen beheren

Elk persoon in uw organisatie kan toegang tot het gebouw en tot TruPortal hebben. Toegang tot de fysieke faciliteit wordt middels een identificatie gestuurd (algemeen een ID-badge genoemd). Toegang tot TruPortal wordt middels een gebruikersaccount gestuurd om op de controller aan te melden. Om de gebruikersaccounts en identificaties georganiseerd te houden, koppelt TruPortal beiden met één record voor elk persoon in uw organisatie. Dit individuele databaserecord wordt een "persoon" genoemd omdat het overeenkomt met een feitelijk persoon.

Het onderscheid tussen personen, identificaties en gebruikersaccounts is belangrijk. Ten eerste, iedereen die uw faciliteit moet betreden, heeft een identificatie nodig (een ID-badge met een gecodeerd nummer dat door TruPortal wordt herkend). Niet iedereen die de faciliteit moet betreden, heeft echter ook toegang tot TruPortal nodig met een gebruikersaccount. Ten tweede, alleen degenen die TruPortal besturen en beheren, hebben gebruikersaccounts nodig. Ten derde, in sommige gevallen bevinden TruPortal-operatoren zich buiten de locatie in een centraal station en vereisen daarom geen identificatie om de fysieke faciliteit te betreden. Zij hebben echter een gebruikersaccount.

Met de databaserecords, “personen,” in TruPortal kun u gemakkelijk identificaties en gebruikersaccounts van één record beheren in plaats van afzonderlijke databases voor systeemgebruikers en identificaties voor toegang tot de faciliteit te onderhouden.

Een persoon toevoegen

Weet u zeker dat u aan elk persoonsrecord een uniek identificatienummer van enige soort toewijst. Dit kan bijvoorbeeld een werknemersnummer zijn.

Zorg, voordat u personen toevoegt, dat u enige door gebruikers gedefinieerde velden die u nodig kunt hebben, configureert. Zie **Door gebruikers gedefinieerde velden toevoegen op pagina 38.**

1. Klik op ***Toegangsbeheer > Personen***.
2. Klik op [Toevoegen].
3. Typ een **Voornaam** en een **Achternaam**.
4. Klik op het tabblad **Details**.
5. Typ de verzochte informatie in de door de gebruiker gedefinieerde velden.
6. Als de persoon de TruPortal-software gebruikt, klikt u op het tabblad **Gebruikersaccount** en maakt u de account. Zie **Een gebruikersaccount toevoegen op pagina 44.**
7. Klik op [Wijzigingen accepteren].
8. Raadpleeg **Een identificatie toevoegen op pagina 41** als de persoon een identificatie nodig heeft voor toegang tot de fysieke faciliteit.

Een persoon verwijderen

TruPortal kan tot 10.000 persoonsrecords opslaan. Personen die echter geen toegang meer vereisen tot uw locatie of tot TruPortal, moeten van de database worden verwijderd.

Opmerking: Om in één batch een aantal personen te verwijderen, gebruikt u de Import/export-wizard.

1. Klik op ***Toegangsbeheer > Personen***.
2. Selecteer de persoon uit de lijst personen.
3. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
4. Klik op [Verwijderen].

ID-foto's van personen uploaden

Personen kunnen aan hun records een identificatiefoto hebben gekoppeld. Zodra een toegangsgebeurtenis zich voordoet waarbij de identificatie van de persoon is betrokken, verschijnt een miniatuurafbeelding van deze persoon.

Foto's worden tot een grootte van 10 Kb of minder beperkt.

1. Klik op ***Toegangsbeheer > Personen***.
2. Selecteer de persoon uit de lijst personen.
3. Klik op het pictogram van de ID-foto naast de naam van de persoon.

   Het dialoogvenster Foto uploaden verschijnt.
4. Klik op **Bestand selecteren**.

   Het dialoogvenster Bestand selecteren verschijnt.
5. Selecteer een foto om te uploaden en klik op **Openen**.
6. Klik op **Uploaden**.

7. Het dialoogvenster Bestand selecteren verdwijnt.
8. Klik op [Wijzigingen accepteren].

Opmerking: U kunt een ID-foto van een gebruiker met een bijgewerkte foto vervangen. Hiervoor klikt u op de bestaande foto en volgt u deze stappen.

Identificaties beheren

Iedereen die uw faciliteit moet betreden, heeft een identificatie nodig (een ID-badge met een gecodeerd nummer dat door TruPortal wordt herkend). Voordat u een identificatie kunt toewijzen, moet u eerst de persoon aan de database toevoegen. Zie **Een persoon toevoegen op pagina 40.**

Een identificatie toevoegen

Voordat u aan een persoon een identificatie kunt toevoegen, moet u eerst een record voor die persoon maken. Zie **Een persoon toevoegen op pagina 40.**

1. Selecteer ***Toegangsbeheer > Personen***.
2. Selecteer de persoon die de identificatie nodig heeft.
3. Klik op [Identificaties].
4. Klik op [Identificatie toevoegen].
5. Klik op het tabblad **Algemeen**.
6. Typ het **Identificatie-ID**.
7. Optioneel: typ de **PIN**-code.
8. Optioneel: selecteer **Uitgebreide tijden voor aankloppen/vasthouden gebruiken** als de persoon met deze identificatie extra tijd nodig heeft om de deuren te openen en te passeren.
9. Optioneel: selecteer **Vrijstelling anti-passback** als u anti-passback gebruikt en deze identificatie mag niet worden getraceerd.
10. Optioneel: selecteer een datum voor **Actief van** en **Actief tot** als de identificatie voor de geldigheid ervan een beperkte tijdsduur heeft.
11. Klik op het tabblad **Toegangsniveaus**.
12. Selecteer de toegangsniveaus die op deze identificatie van toepassing zijn.
13. Klik op [Wijzigingen accepteren].

USB-identificatielezers

RF IDeas produceert identificatiekaartlezers die op een computer kunnen worden aangesloten via USB. Deze apparaten kunnen worden gebruikt om de gegevens te lezen die op een ID-badge zijn opgeslagen en om de identificatie automatisch in het veld **Identificatie-ID** in te voeren. Dit kan een aanzienlijke tijdbesparing geven als u veel identificaties hebt die aan TruPortal moeten worden toegevoegd.

Deze apparaten moeten volgens de instructies van de fabrikant worden geïnstalleerd en geconfigureerd en als u identificaties met een faciliteitscode gebruikt, moeten de RF-lezers worden geconfigureerd om de faciliteitscode van de identificatiecode op de kaart te scheiden.

Een identificatie verwijderen

U hoeft geen identificatie te verwijderen om het gebruik ervan te vermijden. Als bijvoorbeeld een persoon een verloren identificatie meldt, kunt u deze zolang deactiveren zodat de persoon de tijd heeft om er naar te zoeken, in plaats van de identificatie onmiddellijk te verwijderen. Als de identificatie niet kan worden gevonden, dan kunt u de verloren identificatie verwijderen als de persoon om een nieuwe identificatie vraagt. Zie **Gebruik van een verloren of gestolen identificatie vermijden op pagina 43.**

1. Selecteer ***Toegangsbeheer > Personen***.
2. Selecteer de persoon met de identificatie die moet worden verwijderd.
3. Klik op [Identificaties].
4. Klik op de te verwijderen identificatie.
5. Klik op [Identificatie verwijderen].
6. Klik op [Verwijderen].

   Het dialoogvenster Item verwijderen verschijnt.
7. Klik op [Verwijderen].

Verloren of gestolen identificaties beheren

Als een persoon een verloren identificatie meldt, kunt u deze zolang deactiveren zodat de persoon de tijd heeft om er naar te zoeken, in plaats van de identificatie onmiddellijk te verwijderen. Als de identificatie niet kan worden gevonden, dan kunt u de verloren identificatie verwijderen als de persoon om een nieuwe identificatie vraagt.

Het deactiveren van een identificatie heeft nog een voordeel. Terwijl een ongeldige identificatie tijdens het scannen bij een lezer een gebeurtenis genereert, zal de gebeurtenis, als de identificatie nog aan een persoon is toegewezen, de persoon die een ongeldige identificatie probeerde te gebruiken, specifiek aanwijzen. Als videocamera's uw deur- en lezergebeurtenissen bewaken, moet u een afbeelding hebben van de persoon die de identificatie probeerde te gebruiken nadat deze als gestolen werd gemeld. Door in de Gebeurtenissendatabase naar de persoon te zoeken die de identificatie als verloren meldde, worden alle incidenten getoond die voor en na het tijdstip zijn opgetreden dat de identificatie als verloren werd gemeld, met die persoon zijn verwant. Op die manier kunt u een verband leggen tussen het slachtoffer van de diefstal en de inbreker.

Gebruik van een verloren of gestolen identificatie vermijden

Gebruik deze taak om een identificatie te deactiveren in plaats van deze te verwijderen.

1. Selecteer ***Toegangsbeheer > Personen***.
2. Selecteer de persoon met de identificatie die moet worden gedeactiveerd.
3. Klik op [Identificaties].
4. Klik op de te deactiveren identificatie.
5. Klik op het veld **Actief tot**.

   Het popup-venster Kalender verschijnt.
6. Selecteer een datum in het verleden.
7. Klik op [Wijzigingen accepteren].

Een gevonden identificatie herstellen

1. Selecteer ***Toegangsbeheer > Personen***.
2. Selecteer de persoon met de identificatie die moet worden gedeactiveerd.
3. Klik op [Identificaties].
4. Klik op de te heractiveren identificatie.
5. **Wis** het veld **Actief tot**.
6. Klik op [Wijzigingen accepteren].

Gebruikersaccounts beheren

Met gebruikersaccounts kunnen mensen zich aanmelden bij TruPortal. Een gebruikersaccount is, net als een identificatie, met een Persoonsdatabaserecord verwant. Een persoon hoeft echter geen gebruikersaccount te hebben om met een identificatie toegang te krijgen tot de faciliteit.

Een gebruikersaccount toevoegen

1. Meld u aan als beheerder of dealer. De andere operatorrollen hebben geen toestemming om gebruikeraccounts te wijzigen.
2. Selecteer ***Toegangsbeheer> Personen***.
3. Selecteer de persoon die moet worden gewijzigd.
4. Klik op het tabblad **Gebruikersccount**.
5. Selecteer **Kan aanmelden**.
6. Typ een **Gebruikersnaam**.
7. Klik op [Wachtwoord wijzigen].
8. Typ het nieuwe wachtwoord in de velden **Nieuw wachtwoord invoeren** en **Wachtwoord bevestigen**.
9. Klik op [OK].
10. Selecteer een **Rol**.
11. Klik op [Wijzigingen accepteren].

Een gebruikersnaam en wachtwoord wijzigen

1. Meld u aan als beheerder of dealer. De andere operatorrollen hebben geen toestemming om gebruikeraccounts te wijzigen.
2. Selecteer ***Toegangsbeheer> Personen***.
3. Selecteer de persoon die moet worden gewijzigd.
4. Klik op het tabblad **Gebruikersccount**.
5. Typ een nieuwe **Gebruikersnaam**.
6. Klik op [Wachtwoord wijzigen].
7. Typ het nieuwe wachtwoord in de velden **Nieuw wachtwoord invoeren** en **Wachtwoord bevestigen**.
8. Klik op [OK].
9. Klik op [Wijzigingen accepteren].

Een gebruikersaccount deactiveren

1. Meld u aan als beheerder of dealer. De andere operatorrollen hebben geen toestemming om gebruikeraccounts te wijzigen.
2. Selecteer ***Toegangsbeheer> Personen***.
3. Selecteer de persoon die moet worden gewijzigd.
4. Klik op het tabblad **Gebruikersccount**.
5. Schakel het keuzevak **Kan aanmelden** uit.
6. Klik op [Wijzigingen accepteren].

Rapporten

TruPortal heeft vijf vooraf gedefinieerde rapporten zodat u in de serverdatabase opgeslagen informatie kunt weergeven:

Toegangsgeschiedenis
Hiermee kunt u een overzicht van toegangspogingen weergeven volgens persoon, gefilterd op Datumbereik, Naam persoon (jokerteken), Lezer, Zone en Toekennen of Weigeren.

Identificatie
Hiermee kunt u een lijst van toegewezen identificaties weergeven, gefilterd op Naam persoon (jokerteken), Identificatie-ID (jokerteken), Toegangsniveaus, Actief of Niet-actief.

Toegang lezer
Hiermee kunt u een lijst van personen bekijken die toegang tot elke lezer hebben, gefilterd op Naam persoon (jokerteken), Lezer.

Presentie
Hiermee kunt u een lijst van personen bekijken volgens huidige zone of laatste lezer, gefilterd op Naam persoon (jokerteken), Zone, Lezer.

Rooster
Hiermee kunt u een lijst van alle personen in de database bekijken, gefilterd op Naam persoon (jokerteken) en Aanmeldingsrechten.

Opmerking: Rapporten worden in HTML-indeling, in een venster van een internetbrowser weergegeven. Het TruPortal-productlogo verschijnt in de hoek rechtsboven. Als u Internet Explorer 7 of ouder gebruikt, wordt deze afbeelding niet goed weergegeven. Dit is een beperking van oudere versies van Internet Explorer.

Naar personen zoeken

De Zoekfunctie filtert de database door de persoonsrecords in een lijst te plaatsen die een veld hebben dat overeenkomt met uw volledige of gedeeltelijke zoekopdracht.

Personen zoeken

1. Selecteer ***Toegangsbeheer > Personen***.
2. Klik op de knop **Zoeken** om te selecteren welk veld te zoeken.
3. Typ uw zoekterm.
4. Druk op <Enter>.

Een zoekopdracht annuleren

De zoekopdrachten blijven de database filteren, zelfs als u naar een ander pagina navigeert en naar de pagina Personen terugkeert en totdat u de zoekopdracht annuleert.

1. Selecteer ***Toegangsbeheer > Personen***.
2. Klik op de **X** om het zoekveld te wissen.

HOOFDSTUK 5 *Toegang bewaken*

Gedurende dagelijkse handelingen, bewaakt en bestuurt u de toegang tot de faciliteit door:

- gebeurtenissen te bekijken
- naar de video van de beveiligingscamera te kijken, als er camera's zijn geïnstalleerd
- naar behoefte gepland deurgedrag op te heffen om deuren te openen, te ontgrendelen, uit te sluiten of op te heffen
- op alarmen te reageren

Gebeurtenissen en alarmen

De pagina Gebeurtenissen toont een record over:

- toegangsproblemen
  - onbevoegde toegang
  - Anti-passbackovertredingen
  - Deuren die te lang zijn opengehouden
  - Gebruikers die zich aanmelden op TruPortal
- Statusberichten voor systeem en apparaat
  - Wijzigingen in systeemstatus, zoals updates voor de Tijd en Datum
  - Modus wijzigt voor gekoppelde apparaten
- Alarmen
  - Deursabotage
  - Deur geforceerd open
  - Systeemstoringen of -problemen

Elke gebeurtenis die met een apparaat is verwant die aan een camera is gekoppeld, heeft een videorecord van de gebeurtenis.

Laatste gebeurtenissen weergeven

De laatste gebeurtenissen worden in de linkerbenedenhoek van de pagina weergegeven. Als zich een gebeurtenis voordoet terwijl u op een andere pagina werkt, kunt u door met uw muiscursor over de gebeurtenis te bewegen, een overzicht van de gebeurtenis bekijken, inclusief een miniatuurfoto van de persoon die met de gebeurtenis is verwant.

Het popupvenster geeft de datum en tijd van de gebeurtenis weer, evenals een beschrijving van de gebeurtenis en de identificatie. Hieronder verschijnt de foto en naam van de persoon.

Meer gebeurtenissen laden

De weergave Gebeurtenissen wordt tot de meest recente gebeurtenissen beperkt. Om oudere gebeurtenissen dan de weergegeven gebeurtenissen weer te geven, moet u ze eerst vanaf de TruPortal naar de browser laden. De opdracht Meer gebeurtenissen laden zal de volgende 500 gebeurtenissen laden (of minder als er minder dan 500 zijn).

1. Selecteer ***Gebeurtenissen***.
2. Klik op de actieknop **Gebeurtenissen**.
3. Selecteer **Meer gebeurtenissen laden**.
4. Optioneel: klik op **Annuleren** wanneer dit verschijnt, om de handeling te stoppen.

Alle gebeurtenissen laden

De weergave Gebeurtenissen wordt tot de meest recente gebeurtenissen beperkt. Om oudere gebeurtenissen dan de weergegeven gebeurtenissen weer te geven, moet u ze eerst vanaf de TruPortal naar de browser laden. De opdracht Alle gebeurtenissen laden zal alle gebeurtenissen op uw controller naar uw browser laden. Het kan enkele minuten duren om te voltooien.

1. Selecteer ***Gebeurtenissen***.
2. Klik op de actieknop **Gebeurtenissen**.
3. Selecteer **Meer gebeurtenissen laden**.
4. Optioneel: klik op **Annuleren** wanneer dit verschijnt, om de handeling te stoppen.

Naar gebeurtenissen zoeken

Met de zoekfunctie kunt u de lijst weergegeven gebeurtenissen volgens één of meer facetten filteren.

1. Selecteer ***Gebeurtenissen***.
2. Klik op het pictogram **Filter** rechts op het scherm.
3. Typ de zoekcritera in de juiste velden.

   Hoe meer criteria u gebruikt, des te minder zoekresultaten.
4. Druk op <Enter>.

Gebeurtenissen exporteren

TruPortal kan tot 65.535 gebeurtenissen opslaan. Zodra deze limiet wordt bereikt, worden oudere gebeurtenissen zoals vereist verwijderd om ruimte te maken. Gebruik de opdracht Gebeurtenissen exporteren om een record van gebeurtenissen in een bestand op te slaan met een indeling van door komma gescheiden waarden (CSV).

1. Selecteer ***Gebeurtenissen***.

2. Klik op de actieknop **Gebeurtenissen**.
3. Selecteer **Gebeurtenissen exporteren**.
4. Kies de locatie op uw computer waar u het opgeslagen bestand wilt opslaan.
5. Typ een beschrijvende bestandnaam met de extensie .**csv**.
6. Klik op **Opslaan**.

Video van Gebeurtenissen

TruPortal kan van specifieke camera's de live (of opgenomen) video weergeven en opgenomen video's van gebeurtenissen met specifieke apparaten, zoals lezers en deuren, koppelen. Zie **Configuratie Video-apparaten op pagina 24.**

Op de pagina Gebeurtenissen worden koppelingen naar gebeurtenisspecifieke video's gevonden. Met de pagina Video kunt u de videotoevoer van één of meer camera's controleren.

Gebeurtenis video afspelen

Gebeurtenissen met verwante opgenomen video hebben een camerapictogram met hyperlink naast de Gebeurtenisbeschrijvnig op de pagina Gebeurtenissen.

AFBEELDING1. Pictogram Gebeurtenisvideo-camera

1. Selecteer ***Gebeurtenissen***.
2. Blader of zoek naar de gebeurtenis.
3. Klik op het pictogram Camera.
   Het deelvenster Details gebeurtenis verschijnt onder op de pagina.
4. Klik op [Gebeurtenisvideo afspelen]

Videobewaking

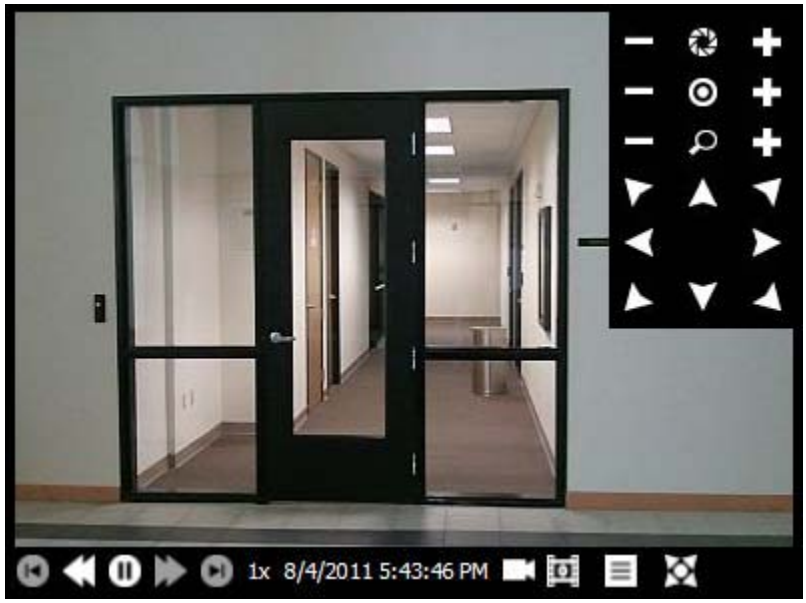
Terwijl u via het scherm Gebeurtenissen uw opgenomen video van gebeurtenissen die aan specifieke apparaten zijn gekoppeld, kunt weergeven, kunt u met de pagina Video de algemene locatiebeveiliging controleren. Als bijvoorbeeld een verdacht persoon op uw parkeerplaats rondhangt, zal dit geen gebeurtenis van deur of lezer activeren. Als u echter een camera hebt die de parkeerplaats overziet, zou u de persoon detecteren door naar die camera te kijken.

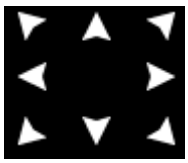
Voordat u live of opgenomen video controleert, moet u minsten één video-indeling toevoegen. Zie **Video-opmaken toevoegen op pagina 26.**

1. Selecteer ***Video >bewaking***.
2. Selecteer een **Opmaak**.
3. Om live video te bekijken, klikt u op de knop **Live**.
4. Om opgenomen video te bekijken, klikt u op de lijst **Afspelen** en selecteert u een optie.
5. Optioneel: om een camera met pannen-kantelen-in/uit-zoomen opnieuw te plaatsen, klikt u op de knop **PTZ** om de PTZ-besturingselementen te openen en aan te passen.

Referenties besturingselementen video

AFBEELDING2. TruPortal Besturingselementen videobewaking



Pictogram	Feature	Functie
	Irisbediening	opent of sluit de iris van de camera om deze op de hoeveelheid beschikbaar licht aan te passen
	Scherpstelbediening	past de scherpstelling van de afbeelding aan
	Zoombediening	past de zoom van de camera aan
	Pan- en kantelbediening	Verplaatst de camera in de richting(en) die door de respectievelijke pijl worden aangegeven
	Een stap achteruit-bediening	Verplaatst de opgenomen video één frame terug

Pictogram	Feature	Functie
	Achteruitbediening	Spoelt de video achteruit
	Pauzebediening	Pauzeert de videotoevoer (live of opgenomen)
	Vooruitbediening	Spoelt de opgenomen video snel vooruit
	Een stap vooruit-bediening	Verplaatst de opgenomen video één frame vooruit
	Live video-bediening	Schakelt van afspelen van opgenomen video over om live video weer te geven
	Afspeelbediening	Menuselectie van afspeelopties, van live tot enkele minuten in het verleden
	Presets-bediening	Verplaatst de camera snel naar de vooraf ingestelde locatie
	PTZ-bediening	Opent de besturingselementen Pannen, Kantelen, In/uit-zoomen (werkt alleen bij PTZ-camera's)

Deuren bedienen

De pagina **Deuren** toont de status van de deuren, de toegewezen lezers, recente gebeurtenissen aan die deuren en de toegewezen schema's. Met de pagina **Deuren** kunnen operatoren deuren vergrendelen, openen, opheffen en ontgrendelen.

Een deur openen

Gebruik de opdracht Deur openen om voor iemand zonder identificatie een deur te openen.

1. Selecteer ***Deuren > bewaken***.
2. Klik op het tabblad **Gebeurtenisweergave**.
3. Klik op de actieknop **Individuele deuropdrachten** voor de deur die u wilt openen.
4. Selecteer **Deur openen**.

Deurblokkering opheffen

Gebruik de opdracht Deurblokkering opheffen om de deur naar de normale bedrijfsmodus te retourneren nadat u deze hebt vergrendeld of uitgesloten.

1. Selecteer ***Deuren > bewaken***.
2. Klik op het tabblad **Gebeurtenisweergave**.
3. Klik op de actieknop **Individuele deuropdrachten** voor de deur waarvoor u de vergrendeling wilt opheffen.
4. Selecteer **Deurblokkering opheffen**.

Deur uitsluiten

Gebruik de opdracht Deur uitsluiten om te voorkomen dat er identificaties voor toegang tot de deur worden toegekend.

1. Selecteer ***Deuren > bewaken***.
2. Klik op het tabblad **Gebeurtenisweergave**.
3. Klik op de actieknop **Individuele deuropdrachten** voor de deur die u wilt uitsluiten.
4. Selecteer **Deur uitsluiten**.

Een deur ontgrendelen

Gebruik de opdracht Deur ontgrendelen om de beveiliging voor de deur op te heffen zodat iedereen zonder een geldige identificatie te tonen, kan binnenkomen en weggaan.

1. Selecteer ***Deuren > bewaken***.
2. Klik op het tabblad **Gebeurtenisweergave**.
3. Klik op de actieknop **Individuele deuropdrachten** voor de deur die u wilt ontgrendelen.
4. Selecteer **Deur ontgrendelen**.

Alle deurblokkeringen opheffen

Gebruik de opdracht Alle deurblokkeringen opheffen om alle deuren naar de normale bedrijfsmodus terug te brengen nadat u alle deuren hebt vergrendeld of uitgesloten.

1. Selecteer ***Deuren > bewaken***.
2. Klik bovenop de pagina op de actieknop **Algemene deuropdrachten**.
3. Selecteer **Alle deurblokkeringen opheffen**.

Alle deuren uitsluiten

Gebruik de opdracht Alle deuren uitsluiten om te voorkomen dat er identificaties voor toegang tot een deur worden toegekend.

1. Selecteer ***Deuren > bewaken***.
2. Klik bovenop de pagina op de actieknop **Algemene deuropdrachten**.
3. Selecteer **Alle deuren uitsluiten**.

Opmerking: Als alle deuren zijn geblokkeerd terwijl een nieuwe deurcontroller wordt toegevoegd, blijft de nieuwe deurcontroller ontgrendeld. Om te worden geblokkeerd, moet de

blokkering van alle deuren opnieuw worden opgeheven waarna alle deuren weer worden geblokkeerd.

Alle deuren ontgrendelen

Gebruik de opdracht Alle deuren ontgrendelen om de beveiliging voor de volledige locatie op te heffen zodat iedereen zonder een geldige identificatie te tonen, kan binnenkomen en weggaan.

1. Selecteer ***Deuren > bewaken***.
2. Klik bovenop de pagina op de actieknop **Algemene deuropdrachten**.
3. Selecteer **Alle deuren ontgrendelen**.

Menu's Deuropdrachten

Soms is het nodig om normaal gepland gedrag voor een specifieke deur, of voor de volledige locatie op te heffen. U wilt bijvoorbeeld een deur openen voor de persoon die een pakket komt afleveren. Tijdens een brandoefening zult u alle deuren ontgrendelen om de oefening te kunnen uitvoeren. In geval zich in de buurt van uw faciliteit een ramp of noodsituatie voordoet, moet u mogelijk alle deuren uitsluiten. U kunt vanaf het tabblad **Gebeurtenisweergave** op de pagina ***Deuren >bewaken*** individuele deuren bedienen. Met de algemene deuropdrachten kunt u met één klik de status van alle deuren op de locatie wijzigen.

Menu Algemene deuropdrachten

Opmerking: Na het ontgrendelen of uitsluiten van alle deuren moet u de opdracht **Alle deurvergrendelingen opheffen** gebruiken voordat u enige deur individueel probeert te bedienen.

Alle deuren blokkeren
Geeft alle sloten op de deuren vrij zodat vrije toegang en uittreding mogelijk is. Dit wordt als Gebeurtenis 14644 opgenomen. Na deze opdracht uit te geven, moet u van alle deuren de blokkering opheffen voordat u meteen een individuele deur kunt controleren.

Alle deuren uitsluiten
Vergrendelt alle deuren en negeert identificaties zodat niemand naar binnen of naar buiten kan. Dit wordt als Gebeurtenis 14646 opgenomen. Na deze opdracht uit te geven, moet u van alle deuren de blokkering opheffen voordat u meteen een individuele deur kunt controleren.

Alle deurvergrendelingen opheffen
Herstelt alle deuren naar hun normale status, tenzij een toegewezen ontgrendelings**ingang** actief is. Een ontgrendelingsingang wordt op de pagina ***Systeembeheer > Apparaten > Controller*** geconfigureerd.

Menu Individuele deuropdrachten

Deur openen
Ontgrendelt de deur voor de tijdsduur zoals in **Normale toegangstijd toekennen**, op de pagina ***Systeembeheer > Apparaten*** wordt aangegeven.

Deurvergrendeling opheffen
Herstelt de deur op basis van het schema naar standaardgedrag.

Deur uitsluiten
Vergrendelt de deuren en negeert identificaties zodat niemand naar binnen of naar buiten kan.

Deeur vergrendelen
Ontgrendelt het slot op de deur waardoor vrije toegang en uittreding mogelijk is, totdat u de deurstatus wijzigt, een lezerschema de deurstatus wijzigt of u een algemene opdracht ("alle deuren") uitvoert.

Tabblad Gebeurtenisweergave

Het tabblad **Gebeurtenisweergave** op de pagina ***Deuren> bewaken*** toont de meest recente gebeurtenis bij de deur en verwante lezers en de huidige status van elke deur en de lezers ervan. U kunt vanaf het tabblad **Gebeurtenisweergave** op de pagina ***Deuren >bewaken*** individuele deuren bedienen.

Tabblad Schemaweergave

Met het tabblad **Schemaweergave** op de pagina ***Deuren> bewaken*** kunt u het gedrag van een deur en lezer volgens schema's wijzigen, in plaats van handmatig zoals u op het tabblad **Gebeurtenisweergave** zou doen.

Als u bijvoorbeeld een klant-showroom hebt, wilt u de deur van de parkeerplaats naar de showroom gedurende de tijd dat het bedrijf gesloten is, vergrendeld hebben en ontgrendelen tijdens werkuren als een verkoper in de showroom is, zodat klanten gemakkelijk het gebouw kunnen betreden. In dit geval wilt u een deurschema voor 9:00 tot 17:00 selecteren en voor de **Planningsmodus** "Eerste kaart" kiezen als u de showroom alleen ontgrendeld wilt hebben nadat een verkoper een identificatie heeft gebruikt om de ruimte te betreden.

Schema
Selecteer van deze lijst een schema (schema's worden in ***Toegangsbeheer > Schema's*** gemaakt) om aan te geven wanneer de Planningsmodus actief moet zijn.

Planningsmodus (deur)

Selecteer in deze lijst een optie om voor de specifieke deur een gedrag tijdens het schema in te stellen.

Ontgrendeld
De deur wordt ontgrendeld en toegankelijk zonder gedurende het geselecteerde schema een identificatie te presenteren.

Eerste kaart in
de deur wordt aan het begin van het schema vergrendeld en blijft in deze status totdat de eerste geldige identificatie wordt doorgehaald. Op dat punt schakelt de deur over naar een ontgrendelde status.

Vergrendeld
De deur wordt vergrendeld en vereist dat tijdens het geselecteerde schema een geldige identificatie wordt ingevoerd.

Planningsmodus (lezer)

Selecteer van deze lijst een optie om voor de specifieke lezer een gedrag tijdens het schema in te stellen.

Alleen identificatie
Een persoon hoeft alleen maar een geldige identificatie (ID-badge) te tonen om toegang te verkrijgen.

Identificatie en pincode
Een persoon moet een geldige identificatie presenteren en voert een Persoonlijk identificatienummer in om toegang te verkrijgen. Dit voorkomt dat iemand met een gestolen of gevonden identificatie toegang krijgt. Sommige faciliteiten gebruiken gedurende de dag **Alleen identificatie** en na werkuren, als de faciliteit leeg is **Identificatie en pincode**.

Gedegradeerde modus deur

Identificatie-informatie wordt op de TruPortal-systeemcontroller opgeslagen. Als een deurcontroller niet met de controller kan communiceren om vast te stellen of toegang moet worden toegekend (bijv. slechte verbinding), dan werken de deuren op die deurcontroller in de gedegradeerde modus:

Beperkt
Helemaal geen toegang toegekend.

Locatiecode
Toegang wordt gegeven wanneer de kaart met één van de formaten overeenkomt die op de pagina ***Systeembeheer > Kaartformaten*** wordt gedefinieerd en de locatiecode op de kaart overeenkomt met de locatiecode die voor het formaat is gedefinieerd. Het identificatie-ID wordt niet overwaakt.

Alles
Toegang wordt toegekend als de kaart, ongeacht de sitelocatie of het identificatie-ID, overeenkomt met enkele van de formaten die op de pagina ***Systeembeheer > Kaartformaten*** zijn gedefinieerd.

Ingangen en uitgangen bewaken

Ingangen en uitgangen zijn opties voor algemene doeleinden waarmee u TruPortal op uw vereisten kunt aanpassen. Eeningang kan bijvoorbeeld een signaal van een bewegingsdetector zijn. Een uitgang is een elektrische impuls van de TP-controller naar een of ander apparaat. Ingangen en uitgangen worden vanaf de pagina ***Ingangen/uitgangen> bewaken*** bewaakt en uitgangen kunnen vanaf die pagina handmatig worden geactiveerd.

Een uitgang activeren of deactiveren

1. Selecteer ***Bewaking > Ingangen/uitgangen***.
2. Klik voor de uitgang op de knop Activeren/deactiveren.
   De status verandert van “Uit” naar “Aan,” of van “Aan” naar “Uit.”

Reset anti-passback

Anti-passback vereist dat een identificatie wordt gebruikt om een zone te betreden of te verlaten. Op deze manier traceert het systeem welk gebied momenteel wordt bezet door de identificatiehouder, bewaart het een record van bewegingen van personeel binnen beveiligde zones en voorkomt het doorgang naar zones die logisch onmogelijk zijn. Als een persoon een identificatie gebruikt om een zone te betreden die voor Anti-passback is geconfigureerd, en de zone daarna zonder identificatie verlaat (bijvoorbeeld via een deur die door een ander persoon open wordt gehouden), zal de TruPortal niet opnemen dat de persoon die specifieke zone heeft verlaten. Als resultaat, als TruPortal voor

krachtige dwang van anti-passback is geconfigureerd, voorkomt het dat die identificatie kan worden gebruikt om, inclusief de zo juist verlaten zone, een andere zone te betreden totdat de locatie van de identificatie opnieuw op een standaard of neutrale zone is ingesteld.

1. Selecteer ***Bewaking > Reset anti-passback***.
2. Om alle personen opnieuw in te stellen:
   a. Klik op [Alles opnieuw instellen].
   b. Selecteer een zone van de lijst.
3. Om geselecteerde personen opnieuw in te stellen:
   a. Selecteer een bereik van personen door op de eerste naam in de lijst te klikken, <Shift> ingedrukt te houden en op de laatste persoon te klikken. Het bereik van namen wordt gemarkeerd.
   b. Selecteer personen door op de eerste gewenste naam te klikken, <Ctrl> ingedrukt te houden en op andere namen te klikken om ze te selecteren.
   c. Klik op [Geselecteerd opnieuw instellen].
   d. Selecteer een zone van de lijst.

HOOFDSTUK 6 *Onderhoud*

Enkele eenvoudige onderhoudsactiviteiten verzekeren dat uw TruPortal-systeem efficiënt werkt, met minimale problemen en zonder onderbreking van de service. Deze omvatten het maken van back-ups van de database, de configuratie-instellingen van de controller en het bijwerken van de firmware (de TruPortal Gebruikersinterface-software die op de TruPortal-systeemcontroller is geïnstalleerd).

Meld u aan op TruPortal

1. Start uw internetbrowser.
2. Meld u aan op TruPortal.
   a. Typ in de adresbalk van de browser het IP-adres voor TruPortal.
   b. Als u Internet Explorer gebruikt en een waarschuwing over het beveiligingscertificaat ontvangt, selecteert u **Naar deze website doorgaan (niet aangeraden)**.
   c. Typ uw **Gebruikersnaam**.
   d. Typ uw **Wachtwoord**.
   e. Selecteer een **Taal**.
   f. Klik op [Aanmelden].

Gegevensverlies voorkomen

Periodieke back-up van uw TruPortal-database wordt ten zeerste aangeraden om snel herstel te verzekeren van uw beveiligingsvereisten na een ramp. TruPortal slaat back-ups op uw lokale computer op zodat u een kopie hebt die zich niet op de controller bevindt. Het back-upbestand is gecodeerd. Het back-upbestand omvat alle records en instellingen die u in TruPortal kunt configureren, met uitzondering van:

- Instellingen netwerkconfiguratie
- Statussen van deur/lezer die handmatig via de pagina Deur worden ingesteld.

Een back-up maken

1. Meld u aan op TruPortal.
2. Selecteer ***Systeembeheer > Back-up/hertel database***.
3. Klik op [Back-upbestand downloaden].
   Het dialoogvenster Back-up database verschijnt.
4. Klik op [Back-upbestand downloaden].
5. Selecteer een locatie voor het bestand.
6. Klik op [Opslaan].

Van een back-up herstellen

BELANGRIJK: Tijdens een back-upherstel wordt de database overgeschreven en alle wijzigingen die sinds de datum van de back-up zijn aangebracht, gaan verloren.

1. Meld u aan op TruPortal.
2. Selecteer ***Systeembeheer > Back-up/hertel database***.
3. Klik op [Bladeren].
4. Navigeer naar het back-upbestand.
5. Selecteer het bestand en klik op [Openen].
6. Klik op [Back-upbestand uploaden].

Aangepaste instellingen opslaan en herstellen

In tegenstelling tot een back-up worden aangepaste instellingen op de TruPortal-systeemcontroller opgeslagen. Het bestand voor aangepaste instellingen omvat alle instellingen en gegevens. Dit is net als een aangepaste standaardstatus. In plaats van de controller terug naar de standaard fabrieksstatus in te stellen, die dan volgens uw specifieke vereisten opnieuw moet worden geconfigureerd, kunt u uw basis-locatieconfiguratie als een aangepaste instelling opslaan en deze, indien nodig, opnieuw instellen.

Aangepaste instellingen opslaan

Deze taak maakt een bestand met al uw huidige TruPortal gegevens- en configuratie-instellingen die op de TruPortal-systeemcontroller zijn opgeslagen.

1. Selecteer ***Systeembeheer > Instellingen opslaan/resetten.***
2. Selecteer **Aangepaste instellingen opslaan**.
3. Typ uw **Gebruikersnaam**.
4. Typ uw **Wachtwoord**
5. Typ de beveiligingszin, precies zoals weergegeven (hoofdlettergevoelig).
6. Klik op **Aangepaste instellingen opslaan**.

Aangepaste instellingen herstellen

BELANGRIJK: Door deze functie te gebruiken, worden alle instellingen en gegevens in TruPortal gewist en worden alle instellingen die in het aangepaste instellingenbestand zijn opgeslagen, opnieuw ingesteld. Weet u zeker dat u een huidige back-up hebt voordat de aangepaste instellingen worden hersteld.

BELANGRIJK: Na het herstellen van de aangepaste instellingen, wordt de controller opnieuw gestart. Gedurende deze periode is deze maar enkele minuten offline. Daarom kan deze functie beter worden gebruikt tijdens perioden met weinig tot geen toegangsactiviteiten. Anders worden identificatiehouders gedwongen te wachten met het verkrijgen van toegang als u geen **Degradatiemodus deur** hebt geconfigureerd waarmee toegang kan worden toegestaan terwijl de controller offline is.

1. Selecteer ***Systeembeheer > Instellingen opslaan/resetten.***
2. Selecteer **Aangepaste instellingen herstellen**.
3. Typ uw **Gebruikersnaam**.
4. Typ uw **Wachtwoord**
5. Typ de beveiligingszin, precies zoals weergegeven (hoofdlettergevoelig).
6. Klik op **Aangepaste instellingen herstellen**.

   Het volgende waarschuwingsbericht verschijnt: “Het apparaat is opnieuw aan het opstarten" en er wordt een voortgangsbalk weergegeven.

   Als de voortgangsbalk wordt voltooid, gaat de server offline en geeft uw browser de standaardpagina weer als het geen verbinding kan maken met een webadres.
7. Wis het cachegeheugen van uw browser. (Druk in Internet Explorer 8+ op <Ctrl>+<Shift>+<Delete>.)

Fabrieksinstellingen opnieuw instellen

BELANGRIJK: Door deze functie te gebruiken, worden alle instellingen en gegevens in TruPortal gewist en wordt deze opnieuw naar de fabrieksstandaarden ingesteld. Weet u zeker dat u een huidige back-up hebt voordat u het systeem opnieuw instelt.

1. Selecteer ***Systeembeheer > Instellingen opslaan/resetten***.
2. Selecteer **Fabrieksinstellingen opnieuw instellen**.
3. Typ uw **Gebruikersnaam**.
4. Typ uw **Wachtwoord**.
5. Typ de beveiligingszin, precies zoals weergegeven (hoofdlettergevoelig).
6. Klik op **Fabrieksinstellingen opnieuw instellen**.

   Het volgende waarschuwingsbericht verschijnt: “Het apparaat is opnieuw aan het opstarten" en er wordt een voortgangsbalk weergegeven.

   Als de voortgangsbalk wordt voltooid, gaat de server offline en geeft uw browser de standaardpagina weer als het geen verbinding kan maken met een webadres.
7. Wis het cachegeheugen van uw browser. (Druk in Internet Explorer 8+ op <Ctrl>+<Shift>+<Delete>.)

   Als de server weer online komt, wordt het Acceptatieformulier softwarelicentie eindgebruiker weergegeven.

8. Klik op **Accepteren**.

Updates firmware

De TruPortal-software bevindt zich op de circuitkaart van de controller zelf. Op de controller worden periodieke software-updates toegepast middels de functie Updates firmware.

1. Start uw internetbrowser.
2. Download de nieuwste update van de TruPortal firmware.
3. Meld u aan op TruPortal.
   a. Typ in de adresbalk van de browser het IP-adres voor TruPortal.
   b. Als u Internet Explorer gebruikt en een waarschuwing over het beveiligingscertificaat ontvangt, selecteert u **Naar deze website doorgaan (niet aangeraden)**.
   c. Typ uw **Gebruikersnaam**.
   d. Typ uw **Wachtwoord**.
   e. Selecteer een **Taal**.
   f. Klik op [Aanmelden].
4. Selecteer ***Systeembeheer > Updates firmware***.
5. Klik op [Bladeren].
6. Navigeer naar en selecteer het update-bestand voor de firmware.
7. Klik op [Update].

Start de TruPortal-systeemcontroller opnieuw op

1. Selecteer ***Systeembeheer> Apparaten***.
2. Selecteer de controller uit de apparatenlijst.
3. Klik op [Controller opnieuw starten].

Pagina Systeeminstellingen

De pagina Systeeminstellingen is in vijf tabbladen verdeeld. Het tabblad Systeeminformatie wordt standaard weergegeven.

Tabblad Systeeminformatie

Dit tabblad is alleen maar informatief en geeft de revisie van de applicatie-firmware weer; Firmwarerevisie gebruikersinterface en Firmwarerevisie kernel. De applicatie- en firmware gebruikersinterface moeten hetzelfde zijn.

Gebruik deze versie-informatie voor technische ondersteuning en om vast te stellen of u naar een nieuwere versie van de firmware moet bijwerken.

Tabblad Datum en tijd

De datum en tijd worden gebruikt om de gebeurtenissen met de video te synchroniseren en om gepland gedrag van een deur en lezer te implementeren.

Opmerking: Als u de tijd handmatig wilt wijzigen naar minder dan één minuut van een geplande periode, of de NTP-functie doet dit automatisch, dan zal het schema onmiddellijk in werking treden en niet op het moment van de toegewezen minuut.

Zie **De Datum en tijd instellen op pagina 11.**

Tabblad Netwerkconfiguratie

Dit tabblad toont de netwerkinstellingen voor TruPortal. Vanaf dit tabblad kunt u een beveiligingscertificaat voor een beveiligingscertificaat for secure hypertext transfer protocol (https) maken, een beveiligingscertificaat importeren en het Internet protocol (IP)-adres, subnetmasker, standaard gateway en domain name server (DNS) configureren, zoals door de specifieke instellingen van het locatienetwerk wordt vereist.

Zie **Configuratie Netwerkbeveiliging op pagina 11.**

Tabblad Beveiliging

Met het tabblad Beveiliging van de pagina Systeeminstellingen kunt u bepaalde aspecten configureren die voor de fysieke beveiliging van uw faciliteit gelden. Netwerkbeveiliging wordt op het tabblad Netwerkconfiguratie behandeld.

Zie **Configuratie beveiliging op pagina 13.**

Tabblad Door gebruikers gedefinieerde velden

Met dit tabblad kunt u aangepaste velden voor persoonsrecords maken, om op het scherm hun volgorde te rangschikken en om velden met gevoelige informatie te beschermen.

Persoonsrecords in de TruPortal-database kunnen over verwante door gebruikers gedefinieerde velden beschikken. Hiermee kunt u persoonlijke gegevens over personeel invoeren, zoals het kenteken van het voertuig of het telefoonnummer thuis. Er moet een veld worden ingeschakeld dat op de pagina Personen moet verschijnen. Als u een veld uitschakelt, wordt het van de database verwijderd en gaan voor elk Persoonsrecord alle gegevens in dat veld verloren.

Zie **Door gebruikers gedefinieerde velden configureren op pagina 37.**

Overzicht kaartformaten

Voordat een identificatie kan worden herkend, moet TruPortal worden geconfigureerd om de kaartformaat, dit is de manier waarop de gegevens op de ID-badge zijn ingedeeld, te herkennen.

TruPortal is vooraf voor 16 populaire, commerciële kaartformaten geconfigureerd en ondersteunt gelijktijdig tot acht actieve kaartformaten. Als de kaartformaat die u gebruikt, niet in de lijst voorkomt, kunt u deze als een aangepast type toevoegen.

Onbewerkte formaten

Een onbewerkte kaartformaten omvat geen faciliteitscode. In plaats daarvan behandelt het alle gegevensbits op de kaart als onderdeel van de toegangsidentificatie. Identificatiekaarten met onbewerkt formaat zijn gemakkelijker te configureren dan kaarten met faciliteitscodes en zijn daarom toegevoegd.

Veel standaard-kaartformaten omvatten een faciliteitscode als onderdeel van het identificatie-ID. Hierdoor is grotere perfectie mogelijk tijdens het configureren van de locatiebeveiliging. Het voegt echter ook complexiteit aan de configuratie toe. Als u bijvoorbeeld een faciliteitscode gebruikt en een deur gaat over in gedegradeerde modus omdat deze niet met TruPortal kan communiceren, dan kan de deur worden geconfigureerd zodat deze open gaat als bij de lezer een kaart met een geldige faciliteitscode wordt gescand. Dit is omdat de deurcontroller niet de gehele persoonsdatabase kan opslaan. Het kan echter wel de faciliteitscode opslaan.

HOOFDSTUK 7 *Probleemoplossend*

Het cachegeheugen van de internetbrowser wissen

Door het cachegeheugen te wissen en uw browser opnieuw te starten kan veel problemen, zoals een plotseling vreemd gedrag in de TruPortal-software, oplossen. Specifieke stappen verschillen volgens het model en de versie van de browser.

1. Meld u af van TruPortal en keer terug naar uw startpagina.
2. Wis de geschiedenis en het cachegeheugen van uw browser.
3. Sluit en open uw browser opnieuw.
4. Meld u aan op TruPortal.

Opmerking: Zorg dat u, vooral bij gebruik van Firefox of Chrome, na het in- of uitschakelen van HTTPS/SSL, het cachegeheugen van de browser wist.

Schermvereisten

De TruPortal-applicatie werkt in een internetbrowser. Voor optimale weergave moet u:

- Internet Explorer 8+ gebruiken
- Open het venster van de browser in volledig scherm (om bladeren te vermijden is een minimum breedte van minstens 1024 pixels nodig)
- Stel uw schermresolutie in op een breedte van minimum 1024 pixels

Systeemcapaciteiten en -beperkingen

Attribuut	TP-
Aantal personen	10,000
Aantal unieke identificaties	10,000
Identificaties per persoon	5
Toegangsniveaus	64
Toegangsniveaus per identificatie	8
Schema's	64
Tijdintervallen per schema	6
Vakantiegroepen per schema	8
Vakantiegroepen	8
Vakanties per vakantiegroep	32
Vakanties (totaal)	255
Zones	64
Lezersgroepen	64
Operatorrollen	32
Door gebruikers gedefinieerde velden	10
Video-opmaak	64
Kaartformaten	8
Aantal bewaarde gebeurtenissen in gebeurtenissenlogboek	65,000
Deuren/lezers	
Aantal deuren (basiskaart en dubbele deurcontrollers) met lezers in/Aantal deuren met lezers in en uit	64 / 32
TP-ADD-2D-BRD Dubbele deur-bedieningsmodule(inclusief ingebouwd)	32
Lezers (totaal)	64
Ingangen/uitgangen	
Totaal aantal systeemingangen (inclusief TruPortal-systeemcontroller)	132
Totaal aantal systeemuitgangen (inclusief TruPortal-systeemcontroller)	66
Totaal aantal TP-ADD-IO of TP-ADD-IO-BRD invoegtoepassingen voor uitbreiding van ingang/ uitgang	8
DVR/Camera's	
DVR's	4
Camera's per DVR	
TVR10 (EMEA & VS)	4
TVR30 (Alleen VS)	16
Camera's (maximum)	64

Attribuut	TP-
Ethernetpoorten (totaal/ondersteund)	2/1
RS-485 SNAPP-buspoorten	4

Opmerking: TVR10 is verkrijgbaar in de Verenigde Staten en Europa, TVR30 is alleen verkrijgbaar in de Verenigde Staten.

Overzicht van Vooraf gedefinieerde operatorrollen

Machtigingsniveaus:

- **Geen**: De operator kan deze pagina niet openen of weergeven
- **Beeld**: De operator kan de pagina of gegevens zien, maar kan geen wijzigingen of opdrachten uitvoeren.
- **Modificatie/uitvoeren**: De operator kan instellingen wijzigen of opdrachten uitvoeren

Machtiging	Machtigings niveaus	Beheerder	Operator	Bewaker	Alleen bekijken	Dealer
Toegangs-niveaus	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Reset anti-passback	Geen, Beeld, Uitvoeren	Uitvoeren	Uitvoeren	Uitvoeren	Beeld	Uitvoeren
Zones	Geen, Beeld, Modificatie	Modificatie	Beeld	Beeld	Beeld	Modificatie
Back-up maken van de database	Geen, Uitvoeren	Uitvoeren	Uitvoeren	Geen	Geen	Uitvoeren
PTZ-besturing camera	Geen, Uitvoeren	Uitvoeren	Uitvoeren	Uitvoeren	Geen	Geen
Kaart-formaten	Geen, Beeld, Modificatie	Modificatie	Beeld	Geen	Geen	Modificatie
Identificaties	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Geen	Modificatie
Datum en tijd	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Apparaten	Geen, Beeld, Modificatie	Modificatie	Beeld	Beeld	Beeld	Modificatie
Diagnosti-eken	Geen, Beeld	Beeld	Beeld	Beeld	Beeld	Beeld
Deuren	Geen, Beeld, Uitvoeren	Uitvoeren	Uitvoeren	Uitvoeren	Beeld	Uitvoeren
Gebeur-tenissen	Geen, Beeld	Beeld	Beeld	Beeld	Beeld	Beeld

Machtiging	Machtigings niveaus	Beheerder	Operator	Bewaker	Alleen bekijken	Dealer
Updates firmware	Geen, Uitvoeren	Uitvoeren	Geen	Geen	Geen	Uitvoeren
Vakanties	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Ingang/ uitgang	Geen, Beeld, Uitvoeren	Uitvoeren	Uitvoeren	Uitvoeren	Beeld	Uitvoeren
Netwerkconfi guratie	Geen, Beeld, Modificatie	Modificatie	Beeld	Beeld	Beeld	Modificatie
Operator-rollen	Geen, Beeld, Modificatie	Modificatie	Beeld	Beeld	Beeld	Beeld
Personen	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Beschermde gebruikers-velden	Geen, Beeld, Modificatie	Modificatie	Geen	Geen	Geen	Geen
Lezers-groepen	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Rapporten	Geen, Uitvoeren	Uitvoeren	Uitvoeren	Uitvoeren	Uitvoe-ren	Uitvoeren
Instellingen opnieuw instellen	Geen, Uitvoeren	Uitvoeren	Geen	Geen	Geen	Uitvoeren
Database terugzetten	Geen, Uitvoeren	Uitvoeren	Geen	Geen	Geen	Uitvoeren
Schema's	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Veiligheid	Geen, Beeld, Modificatie	Modificatie	Beeld	Beeld	Beeld	Modificatie
Systeem-informatie	Geen, Beeld	Beeld	Beeld	Beeld	Beeld	Beeld
Gebruikersac counts	Geen, Beeld, Modificatie	Modificatie	Beeld	Geen	Geen	Modificatie
Door gebruikers gedefi-nieerde velden	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie
Video	Geen, Beeld	Beeld	Beeld	Beeld	Beeld	Geen
Video-opmaken	Geen, Beeld, Modificatie	Modificatie	Modificatie	Beeld	Beeld	Modificatie

Diagnostieken

TruPortal levert informatieve diagnostieken; er zijn geen acties die u kunt uitvoeren om specifieke diagnostische tests uit te voeren. De pagina Diagnostieken heeft visuele indicatoren voor algemeen storingsmodi die helpen problemen te identificeren en op te lossen. Alle informatie wordt op het moment van aanmelding en elke minuut daarna ondervraagd. U kunt de gegevens handmatig vernieuwen door op [Vernieuwen] te klikken. De pagina geeft de laatste keer weer dat het scherm werd bijgewerkt.

Opmerking: De TruPortal-systeemcontroller kan geen nauwkeurige lezing weergeven voor de gelijkstroom als het systeem door een gelijkstroombron wordt aangedreven. De informatie over gelijkstroom wordt alleen weergegeven als de TruPortal-systeemcontroller wisselstroom heeft.

Diagnostisch	Waarde weergeven	Status
AC-voeding	OK | Brownout | Fout	INF = OK WRN = Brownout ERR = Fout
DC-voeding	Spanning, stroom	INF >= 10,0 VWRN < 10,0 V WRN = Overbelasting stroom
Back-upbatterij	Spanning, Stroom, Laden | Ontladen	INF >= 11,7 VWRN < 11.7 V ERR < 11,4 V, Geen batterij
Batterij geheugen	Spanning	INF >= 2,3 V WRN < 2.3 V ERR < 2.0 V
Zekeringen	OK | *Naam zekering,…*	INF = Alles OK ERR = Wanneer iets niet OK is
Controller	OK | *Problemen*,…	INF = OK WRN = Wanneer niet OK
Modules	OK | *Probleem ModuleName*,…	INF = Alles OK WRN = Wanneer sabotage ERR = Wanneer offline

Diagnostisch	Waarde weergeven	Status
Deuren	OK | *Probleem DoorName*,…	INF = Alles OK WRN = Wanneer vastgehouden, gedwongen, sabotage ERR - Wanneer offline
Digitale ingangen	OK | *Probleem InputName*,…	INF = Alles OK WRN = Wanneer sabotage ERR - Wanneer offline
Actieve tijdsduur	Laatste tijd opnieuw starten, dagen actief	INF = Altijd
Gem CPU-belasting	1 m, 5 m, 15 m	INF 15 m < 0,80 WRN 15 m >= 0,80 ERR 15 m >= 0,95
Geheugengebruik	Gebruikt, Totaal	INF < 95% WRN >= 95% ERR = 100%
Hoofdopslag	Procent	INF < 90% WRN >= 90% ERR = 100%
Afbeeldingen & back-upopslag	Gebruikt, Totaal	INF < 50% WRN >= 50% ERR >= 95%
ADP-kaarten	Gebruikt, Totaal	INF = Altijd
Deuren	Gebruikt, Totaal	INF = Altijd
Lezers	Gebruikt, Totaal	INF = Altijd
EIO-kaarten	Gebruikt, Totaal	INF = Altijd
Ingangen	Gebruikt, Totaal	INF = Altijd
Uitgangen	Gebruikt, Totaal	INF = Altijd
DVR's	Gebruikt, Totaal	INF = Altijd
Camera's	Gebruikt, Totaal	INF = Altijd
Persoon	Gebruikt, Totaal	INF = Altijd
Identificaties	Gebruikt, Totaal	INF = Altijd
Toegangsniveaus	Gebruikt, Totaal	INF - Altijd
Schema's	Gebruikt, Totaal	INF - Altijd
Vakantiegroepen	Gebruikt, Totaal	INF - Altijd
Vakanties	Gebruikt, Totaal	INF = Altijd

Diagnostisch	Waarde weergeven	Status
Zones	Gebruikt, Totaal	INF = Altijd
Lezersgroepen	Gebruikt, Totaal	INF = Altijd
Operatorrollen	Gebruikt, Totaal	INF = Altijd
Video-opmaken	Gebruikt, Totaal	INF = Altijd
Kaartformaten	Gebruikt, Totaal	INF = Altijd

Zekeringen

De zekeringen beschermen Gelijkstroom die door de kaart van de TruPortal-systeemcontroller wordt geleverd om door externe randapparatuur te worden gebruikt.

Zekering	+V	0V
Aux 1	CN3.1	CN3.2
Aux 2	CN3.3	CN3.4
Deurcontroller	CN10.2 CN17.2	CN11.4 CN18.4
Aux-ingang	CN21.1	CN21.3 CN22.2

Hardware-probleemstatussen

Hardware-items kunnen de volgende problemen vertonen:

Controller

- Sabotage

Modules

- Offline
- Sabotage

Deuren

- Offline
- Geforceerd
- Vastgehouden
- RTE-sabotage
- Onrechtmatige wijziging deurcontact
- Sabotage aux deur
- Deur sabotage

Digitale ingang:

- Offline
- Sabotage

Fout, Waarschuwing en Gebeurtenisberichten

Sabotagestatussen

De TruPortal-systeemcontroller kan geen onderscheid maken welke van de vier deuringangen in sabotagestatus is als het sabotagegebeurtenissen in het logboek opneemt. Op de pagina Diagnostieken, of via de Installatiewizard te gebruiken, kan de real-time status van ingangen tijdens sabotage worden bekeken.

Voedings- en batterijgebeurtenissen

TruPortal Systeemcontroller schakelt uit bij batterijvermogen

Als de controller alleen op batterijvermogen werkt en de batterijspanning daalt onder 10,2V dan wordt de controller uitgeschakeld totdat de wisselstroom wordt hersteld.

Zie **Back-upbatterij gebeurtenissen op pagina 71.**

AC-voedingsgebeurtenissen

Gebeurteniscode	Gebeurtenis beschrijving
Gebeurtenis 14626	AC-voeding storing
Gebeurtenis 14627	AC-voeding hersteld

Opmerking: De TruPortal-systeemcontroller kan geen nauwkeurige lezing weergeven voor de gelijkstroom als het systeem door een gelijkstroombron wordt aangedreven. De informatie over gelijkstroom wordt alleen weergegeven als de TruPortal-systeemcontroller wisselstroom heeft.

Back-upbatterij gebeurtenissen

Back-upbatterij gebeurtenissen doen zich voor als de spanning van de back-upbatterij onder bepaalde drempels valt.

Gebeurtenis-code	Gebeurtenis beschrijving	Oorzaak
Gebeurtenis 14612	Back-upbatterij kritiek	Spanning valt onder 11,4 V, of stijgt boven 10,2 V
Gebeurtenis 14613	Back-upbatterij afgebroken	Spanning valt onder 10,2V, of stijgt boven 9,0V
Gebeurtenis 14624	Back-upbatterij leeg	Spanning valt onder 11.7V, of stijgt boven 11.4V
Gebeurtenis 14625	Back-upbatterij hersteld	Spanning stijgt boven 11,7 V
Gebeurtenis 14649	Back-upbatterij niet gedetecteerd	Spanning valt onder 9,0 V

Opmerking: Als het systeem exclusief vanaf de back-upbatterij wordt gevoed, zal het systeem bij 10,2 V uitschakelen en zullen de gebeurtenissen Afgebroken en Niet gedetecteerd niet worden gegenereerd.

Geheugenbatterij gebeurtenis

Gebeurteniscode	Gebeurtenis beschrijving
Gebeurtenis 14618	Geheugen back-upbatterij leeg

Gebeurtenissen zekering

Gebeurteniscode	Gebeurtenis beschrijving
Gebeurtenis 14651	Zekering doorgeslagen
Gebeurtenis 14652	Zekering hersteld

Gebeurtenissen apparaat

Gebeurteniscode	Gebeurtenis beschrijving	Apparaat
Gebeurtenis 4105	Apparaatcommunicaties mislukt	Deurcontroller, I/O-uitbreiding
Gebeurtenis 4106	Apparaatcommunicaties hersteld	Deurcontroller, I/O-uitbreiding
Gebeurtenis 4107	Sabotage-alarm*	Controller,Deurcontroller, I/O-uitbreiding
Gebeurtenis 14622	Systeemprobleem	Controller
Gebeurtenis 14623	Systeem hersteld	Controller
Gebeurtenis 14628	Apparaat mislukt	Controller
Gebeurtenis 14629	Apparaat hersteld	Controller
Gebeurtenis 14643	Sabotage-alarm hersteld*	Controller,Deurcontroller, I/O-uitbreiding

* Niet van toepassing bij ingebouwde deurcontroller

Apparaatcommunicaties mislukt/hersteld
Gebruikt om communicatiefouten met downstream apparaten aan te geven. Doet zich voor als SNAPP-buscommunicaties met een geconfigureerd downstream-apparaat verloren gaat of wordt verkregen. Apparaat zal altijd aangeven welke module is aangetast.

Apparaat mislukt/hersteld
Gebruikt om algemene problemen met downstream apparaten aan te geven. Doet zich voor als van een sabotage-ingang van een apparaat de status verandert (inclusief Sabotage extern/muur, maar geen Deursabotage), of als een VBUS-communicatiefout wordt gedetecteerd. Apparaat geeft altijd controller aan. Voor sabotagegebeurtenissen is er voor het apparaat een overeenkomende sabotagegebeurtenis. Voor VBUS-foutgebeurtenissen bestaat geen manier om te melden bij welk apparaat de VBUS-fout zich voordeed. Er is dus een overeenkomende gebeurtenis om aan te geven bij welk apparaat de VBUS-fout zich voordeed.

Systeemstoring/hersteld
Gebruikt om algemene problemen met het systeem aan te geven. Doet zich voor als **Sabotage extern/muur** van status verandert. **Apparaat** geeft altijd de controller aan. Deze gebeurtenis kan in de toekomst worden gebruikt om andere probleemcondities te identificeren.

Sabotagegebeurtenissen deur

Gebeurteniscode	Gebeurtenis beschrijving
Gebeurtenis 14633	Sabotage deur hersteld
Gebeurtenis 14632	Sabotage-alarm deur

Sabotage-alarm deur/hersteld
Gebruikt om sabotageconditie op een van de vier deuringangen aan te geven - DR, RTE, TR, AUX. De gebeurtenis van het sabotage-alarm wordt gegenereerd als op een van de ingangen een sabotageconditie wordt waargenomen, of als TR actief is. Totdat alle sabotagecondities zijn

opgelost worden geen aanvullende gebeurtenissen van sabotage-alarm voor RTE, TR en AUX gegenereerd. Voor DR worden echter aanvullende gebeurtenissen van sabotage-alarm gegenereerd terwijl andere sabotagecondities nog bestaan. De gebeurtenis voor sabotageherstel wordt alleen gegenereerd als de sabotageconditie op alle vier de ingangen is opgelost en TR niet-actief is.

Gebeurtenissen hulpingang

Gebeurteniscode	Gebeurtenis beschrijving
Gebeurtenis 14640	Ingang actief
Gebeurtenis 14641	Ingang sabotage-alarm
Gebeurtenis 14642	Ingang niet-actief
Gebeurtenis 4170	Ingang uitgeschakeld

Gebeurtenissen hulpuitgang

Gebeurteniscode	Gebeurtenis beschrijving
Gebeurtenis 10240	Uitgang aan
Gebeurtenis 11264	Uitgang uit

Waarschuwing "Objecten zijn gewijzigd"

Van tijd tot tijd zal het cachegeheugen van uw lokale browser niet gesynchroniseerd zijn met TruPortal. Als dit gebeurt, wordt de interface uitgeschakeld en verschijnt het waarschuwingsbericht.

Klik op de tekst van de waarschuwing om de pagina opnieuw te laden.

“NTP Sync mislukt” Gebeurtenis

NTP-tijdsync vereist toegang vanaf het paneel tot de NTP-server via UDP-poort 123. Als deze poort niet toegankelijk is, wordt de tijd van het paneel niet met de NTP-server gesynchroniseerd en worden gebeurtenissen van "NTP sync mislukt" in een logboek opgenomen.

Videospeler Active X fouten

Geen actieve videoverbindingen

Dit bericht verschijnt op de pagina ***Video> bewaking*** en het deelvenster Details gebeurtenis van de pagina ***Gebeurtenissen***.

Het bericht betekent een van het volgende:

- een camera is niet geconfigureerd
- de TruPortal-applicatie heeft de communicatie verloren met een aangesloten DVR
- de ActiveX-besturing die nodig is om video te kijken, is niet geïnstalleerd of is verouderd

Opmerking: Video kan alleen op Internet Explorer worden bekeken.

Als het foutbericht wordt weergegeven terwijl u op een camerapictogram naast een gebeurtenis klikt:

1. Klik op [Gebeurtenisvideo afspelen]
2. wordt de video weergegeven of de ActiveX-besturing wordt geïnstalleerd.
3. Als geen van beiden gebeurt en het bericht aanhoudt, dient u te controleren of de DVR en de camera werken:
   a. Zie **Configuratie Video-apparaten op pagina 24.**
   b. Zie **Koppel camera's aan Apparaten om video van gebeurtenissen volgen op pagina 26.**.

Als het foutbericht wordt weergegeven terwijl u *Video> bewaking* selecteert:

1. dubbelklikt u op het deelvenster van de video die het foutbericht weergeeft.
2. Als de video niet verschijnt:
   a. Selecteer ***Video-opmaken >bewaking***.
   b. Selecteer de video-opmaak die u aan het bekijken was.
   c. Zorg dat voor elke vervolgkeuzelijst in elk deelvenster in de video-opmaak de juiste camera wordt gekozen.
3. Als de juiste camera niet in de lijst wordt weergegeven, dient u te controleren of de camera aan de pagina Apparaten is toegevoegd en functioneert:
   a. Zie **Configuratie Video-apparaten op pagina 24.**
   b. Zie **Een videocamera toevoegen op pagina 25.**
   c. Zie **Video-opmaken toevoegen op pagina 26.**

Internetbrowser kan Aanmeldingspagina niet laden

Na te hebben gewisseld tussen veilig (HTTPS) en normaal hypertext-protocol (HTTP), merkt u mogelijk dat Firefox of Chrome de aanmeldingspagina van de TruPortal-systeemcontroller niet laadt.

Zie **Het cachegeheugen van de internetbrowser wissen op pagina 63.**

Verklarende woordenlijst

Toegangsniveau
Eén of meer lezer/schema-combinaties die worden gebruikt om toegang tot hardware door één of meer kaarthouders te bedienen. Toegangsniveaus kunnen aan actieve badges worden toegewezen om te definiëren tot welke lezers een badge toegang heeft en op welke tijdstippen.

ANSI
Afkorting voor het American National Standards Institute (Amerikaanse nationale instituut voor standaarden). Dit is een vrijwilligersorganisatie die standaarden voor de computerindustrie creëert.

APB
Kort voor anti-passback. De preventie van toegang verkrijgende badge in een toegangscontrolesysteem als de badge onlangs toegang heeft gekregen tot dezelfde lezer of zone (getimede APB) of niet wordt gezien als in de juiste huidige zone te zijn die nodig is om toegang tot de nieuwe zone te verkrijgen (Zone-APB). Het is, eenvoudig gesteld, een methode om de toegangs- en uitgangsacties van een kaarthouder te bewaken om te verzekeren dat die persoon de kaart niet aan een andere persoon heeft overgedragen om toegang te krijgen.

Zone APB
Zones worden door lezers gedefinieerd via welke toegang of uitgang tot deze zones wordt verkregen. De huidige Zone een Badge die zich binnen bevindt, is opgenomen. Als een badge via een gegeven lezer toegang probeert te verkrijgen tot een gegeven zone, wordt deze toegang geweigerd als deze niet wordt opgenomen als momenteel in de zone zijnde en de gegeven lezer op verlaten is geconfigureerd.

Kaarttype
Categoriseert kaart coderende technologieën, zoals Magnetisch, Wiegand, Smart Card, Eerste toegang, enz.

DHCP
Afkorting voor Dynamic Host Configuration Protocol. Een communicatieprotocol waarmee netwerkbeheerders centraal de toewijzing van internet-protocoladressen in een netwerk van organisaties kunnen beheren en automatiseren.

Deurcontact
Een tweedelig apparaat dat door een kaart-toegangssysteem wordt gebruikt om aan te geven of een deur open of gesloten is. Meestal wordt één onderdeel op de deur en het andere onderdeel in gelijke positie op het deurkozijn gemonteerd.

Deurhouder

Een apparaat die een deur in de geopende positie houdt totdat het van het systeem de instructie krijgt de status te wijzigen.

Insteekslot

Een elektrisch en/of magnetisch apparaat dat wordt gebruikt om een deur in vergrendelde positie te houden. Om een insteekslot te openen wordt enige vorm van elektrische lading vereist die vanaf een apparaat zoals een kaartlezer wordt geïnitieerd.

Ethernet

Een netwerkstandaard van LAN-communicatie via een coaxiale of twisted pair-kabel. IEEE 802.3 is de Ethernetstandaard. Er bestaan de volgende verschillende types ethernet: 10 Mbps (Mega (miljoen) bits per seconde); 100 Mbps; 1 Gbps (Giga (miljard) bits per seconde)

Faciliteitscode

Een optioneel badgeveld die een locatie op unieke wijze identificeert. Wiegand-kaartleveranciers leveren meestal de faciliteitscode en slaan deze in de kaarten op. Voor andere kaarten wordt de faciliteitscode door de gebruiker gedefinieerd. Een kaartlezer kan in de modus Alleen faciliteitscode worden gezet, waarna de faciliteitscode vereist wordt om toegang te kunnen geven.

HTTP

Afkorting voor Hyper Text Transfer Protocol. HTTP definieert hoe berichten worden opgemaakt en verzonden en het controleert welke acties in reactie op diverse opdrachten moeten worden ondernomen door webservers en browsers.

IP

Afkorting voor Internet Protocol. Geeft de opmaak aan voor pakketten en het adressenschema op een netwerk.

IP-adres

Een identificatienummer voor een computer op een TCP/IP-netwerk. De opmaak van een IP-adres bestaat uit een numeriek adres van 32 bit, dat als vier cijfers, gescheiden door punten, wordt geschreven. Elk nummer kan nul tot 255 zijn. Bijvoorbeeld, 1.120.4.72 kan een IP-adres zijn.

IP-camera

Een digitale videocamera die rechtstreeks verbinding maakt via zijn eigen IP-adres met het netwerk en die de capaciteit heeft om met standaard communicatieprotocollen, zoals TCP/IP, beelden te verzenden. Een IP-camera hoeft niet met een pc of een videokaart te worden verbonden.

LAN

Afkorting voor Local Area Network. Koppeling van persoonlijke computers binnen een beperkt gebied, met kabels met hoge prestaties zodat de gebruikers informatie kunnen uitwisselen, randapparatuur kunnen delen en gebruik kunnen maken van een massieve secundaire opslageenheid, een bestandsserver genoemd.

LDAP

Afkorting voor Lightweight Directory Access Protocol (lichtgewicht toegangsprotocol directory), LDAP is een softwareprotocol dat algemeen wordt gebruikt om met servers te communiceren die informatie, inclusief digitale certificaten, opslaan. Hiermee kan iedereen organisaties,

personen of andere hulpbronnen zoals bestanden en apparaten in een netwerk, het publieke internet of een bedrijfsintranet, zoeken. Een verbinding met een LDAP-server kan ongecodeerd zijn, of met SSL zijn gecodeerd.

National Television Standards Committee

Algemeen naar verwezen als NTSC is dit het algemene televisie videosignaal dat in de Verenigde Staten en Japan wordt gebruikt.

Niet overwaakt

Een deur of afgesloten ruimte die niet met een continuïteitscircuit is bedraad om sabotage te detecteren.

Overwaakt

Een deur of afgesloten ruimte die met een continuïteitscircuit is bedraad om sabotage te detecteren.

PAL

Een videostandaard die in Europa, Australië en Nieuw-Zeeland wordt gebruikt. PAL-video zendt elke 1/25 seconde 625 lijnen uit.

Pincode

Afkorting voor persoonlijk identificatienummer, een nummer die meestal met een persoon is verwant en voor toegangscontrole wordt gebruikt

PTZ

Afkorting voor pannen-kantelen-in/uit-zoomen (Pan-Tilt-Zoom). Een functie op camera's die via computerbesturing kunnen pannen, kantelen en in- en uitzoomen. Met PTZ is een groter weergavegebied mogelijk voor een camera door deze in verschillende richtingen te draaien.

Router

Een intelligente 'hub' die het mogelijk maakt om meerdere sub-netten samen te verbinden om hulpbronnen en gegevens te delen

SNMP

Afkorting voor Simple Network Management Protocol (eenvoudig protocol voor netwerkbeheer). Een methode om diverse stukken hardware, bijvoorbeeld een printer, die op een netwerk zijn aangesloten, te beheren.

SSL

Afkorting voor Secure Sockets Layer, een algemeen protocol voor authenticatie en gecodeerde communicatie op het internet. SSL wordt voor communicatie met beide webservers (HTTPS) en and LDAP-servers gebruikt.

Subnet

Een groep computers die dezelfde netwerkeigenschappen en netwerkhulpbronnen delen

TCP/IP

Afkorting voor Transmission Control Protocol/Internet Protocol. Een suite van communicatieprotocollen die worden gebruikt om hosts op het internet met elkaar te verbinden.

TCP/IP-poort

Elk proces dat met een ander proces wil communiceren, identificeert zichzelf middels één of meer poorten t.o.v. de TCP/IP-protocolsuite. Een poort is een nummer van 16-bit, gebruikt door het host-tot-host-protocol om te identificeren naar welk protocol op hoger niveau of applicatieprogramma (proces) het inkomende berichten moet leveren.

URL

Afkorting voor Uniform Resource Locator (uniforme hulpbronzoeker). Een URL is het adres van een hulpbron, of bestand, dat op een TCP/IP-netwerk zoals het internet beschikbaar is.

Wiegand

Een technologie voor toegangscontrole die kaarten gebruikt waarbij magnetisch geladen wolfraamdraden in repen zijn gesneden en verticaal in kolommen zijn geplaatst.

Wizard

Een hulpprogramma dat als richtlijn wordt gebruikt om stapsgewijs door een proces te werken.

Index

D

E

F

G

T

U

V

W

Z