



ASSA ABLOY Access[®]

ASSA ABLOY
Opening Solutions

Teknisk brochure

Experience a safer
and more open world

Indholdsfortegnelse

- 3. ASSA ABLOY Access® - Generel beskrivelse
- 4. ASSA ABLOY Access® SaaS
- 5. Funktioner
- 6. Arkitektur og netværksdiagram
- 8. Datasikkerhet og GDPR
- 10. ABLOY PULSE®
- 11. ABLOY CUMULUS®
- 12. Læsere/opdateringsenheder
- 14. Systemkrav
- 14. Krav til kundens internetforbindelse

ASSA ABLOY Access®

Generel beskrivelse

Access er en cloudbaseret adgangskontrol-software, der tilbyder nøgle- og mobiladgangskontrol i én og samme platform.

Access kan bruges til at styre forskellige låseprodukter, fx ABLOY PULSE og ABLOY CUMULUS.

For at administrere systemet er der brug for en internetforbindelse og en enhed med en webbrowser. Access-softwaren leveres kun som en service, hvilket betyder, at det ikke er muligt at få den som en separat installation på kundens server. ABLOY er ansvarlig for udvikling, vedligeholdelse og opdateringer af Access.

Brugernavn og adgangskode er nødvendige for at logge ind på Access. Der kræves ingen separat systemidentifikation. Access gør det muligt at administrere flere systemer med samme login.

Softwaren er i øjeblikket tilgængelig på engelsk, finsk, svensk, norsk, dansk og fransk.



ASSA ABLOY Access

SaaS-indhold (Software as a Service)

ASSA ABLOY Access SaaS er hostet på en Amazon Web Services (AWS)-platform. Tjenesten bruger et AWS-datacenter i Irland, hvor Access softwaren fungerer i to forskellige tilgængelighedszoner.

Amazon Web Services (AWS) har ISO27001-, ISO27017-, ISO27018- og SOC1-SOC3-certificeringer. Mere information findes på Amazon Clouds hjemmeside på aws.amazon.com/compliance.

Infrastrukturen er baseret på AWS' princip om høj tilgængelighed, hvor hver instans har en aktiv og en passiv server. Dette giver mulighed for hurtig genopretning efter problemer og vedligeholdelse i overførselstilstand mellem servere.





Funktioner

1. Tilgængelighed og brugervenlighed

- Muliggør systemadministration uafhængigt af tid og sted ved hjælp af en computer
- Automatiske softwareopdateringer, sikkerhedsopdateringer og sikkerhedskopier
- Grundlæggende brug af softwaren kræver ikke softwareinstallationer (bortset fra bordkoderen)

2. Login

- Et brugernavn og en adgangskode er nødvendige for at administrere systemet (uden en separat fysisk programmeringsidentifikator)
- Det er muligt at administrere flere systemer

3. Design af system, brugere og produkter

- Tilføjelse og redigering af bygninger, etager og plantegninger
- Oprettelse og redigering af produkter og brugeroplysninger
- Udlevering og tilbagelevering af nøgler med mulighed for at udskrive udleveringskvittering
- Håndtering af låse og læsere ved hjælp af plantegninger

4. Import af massedata

- Import af produkter, nøgler, personer og adgangsrettigheder ved hjælp af Excel-skabeloner

5. Administration af adgange

- Oprettelse, ændring og sletning af adgangsrettigheder
- Administrering af nøglers gyldighedsperioder
- Håndtering af mistede nøgler
- Administration af adgangsgupper og adgangsprofiler
- Håndtering af adgangskoder
- Eksport af låseskema i Excel-format

6. Hændelseslog

- Indsamling og visning af hændelseslog for nøgler, låse og opdateringslæsere (tilvalg)
- Hændelseslog indsamles automatisk via opdateringslæserne

7. Roller som systemadministrator

- Angiv, hvilke funktioner i låsesystemet administratoren har tilladelse til at udføre
- Funktionerne vises i softwaren afhængigt af den rolle, administratoren har fået tildelt

8. Brugervenlig brugerinterface

- Dashboard med statistik over låsesystemet
- Logisk menustruktur
- Responsivt webdesign

9. Generelle systemindstillinger

- Indstilling af gyldighedsperiode for nøgler
- Indstilling af lagringstid for logfiler
- Skabeloner til udleveringskvitteringer på flere sprog

ASSA ABLOY Access arkitektur og netværksdiagram

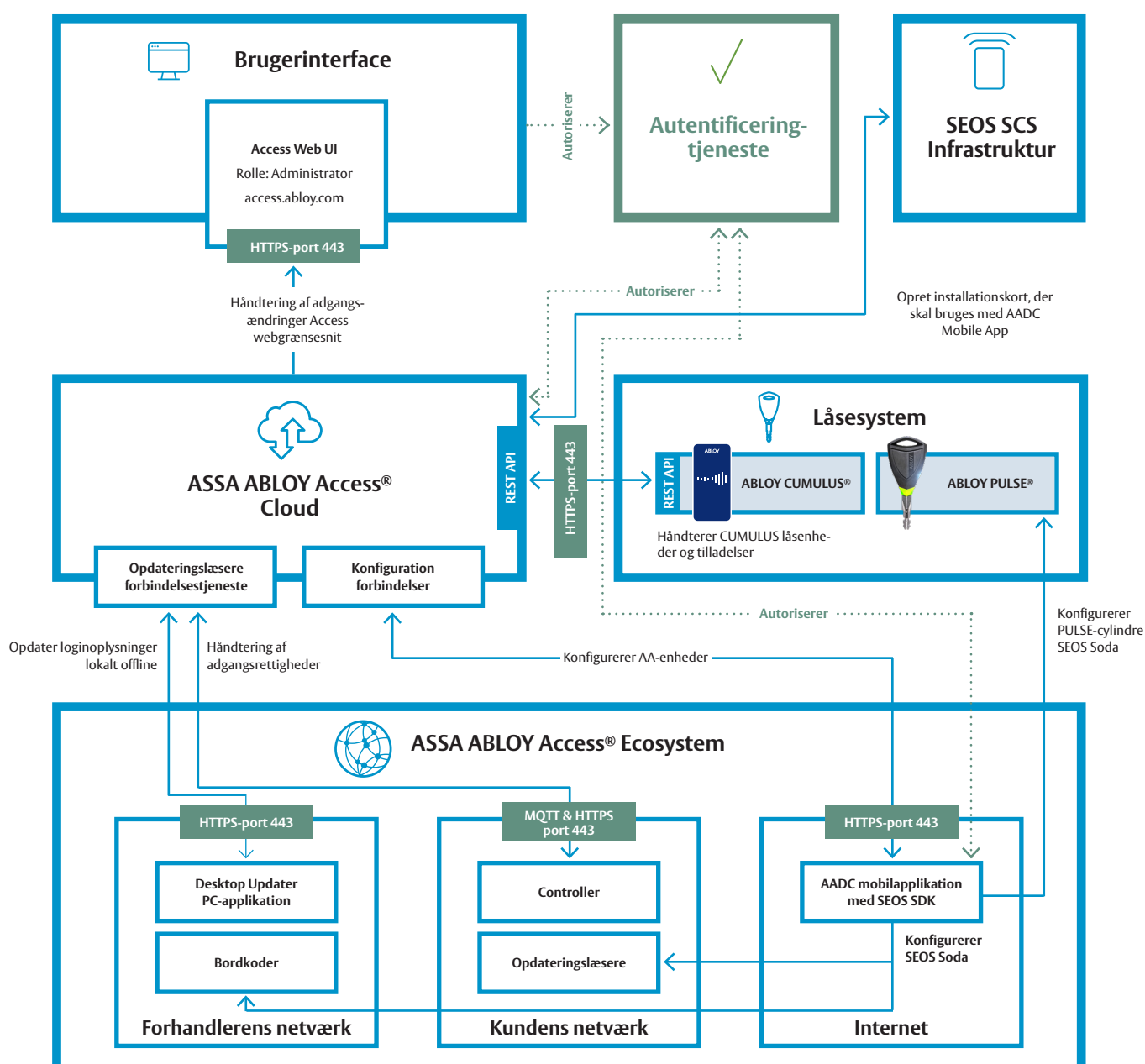
Access Cloud er opbygget ved hjælp af mikrotjenester i Amazon Web Services og er hostet af AWS i Irland. AWS' infrastrukturdyagram vises senere i dokumentet som reference. Alle forbindelser er krypterede og kører i enten HTTPS eller MQTTS.

Bordkoderens PC-applikation og dørcontroller kan placeres i henholdsvis forhandlerens og kundens netværk. Dørcontrolleren kommunikerer med Access Cloud ved hjælp af krypteret MQTT-protokol på port

443 og bruger HTTPS som backup-metode. Access Cloud har en REST API, der muliggør integration med tredjeparter for at udvide funktionaliteten. For eksempel bruger det nøglefri låsesystem, ABLOY Cumulus, denne REST API.

Diagrammet nedenfor beskriver Access-økosystemet og -netværket med de vigtigste systemkomponenter og deres relationer.

ASSA ABLOY Access



Opdatering af bordkoder

Nødvendige URL'er som Desktop Updater skal have adgang til:

- access.assaabloy.com
- europe1.system-manager.assaabloy.com
- accentra.abloy.com
- accentra.assaabloy.com

Alle køres i port 443 HTTPS TCP.

Controller

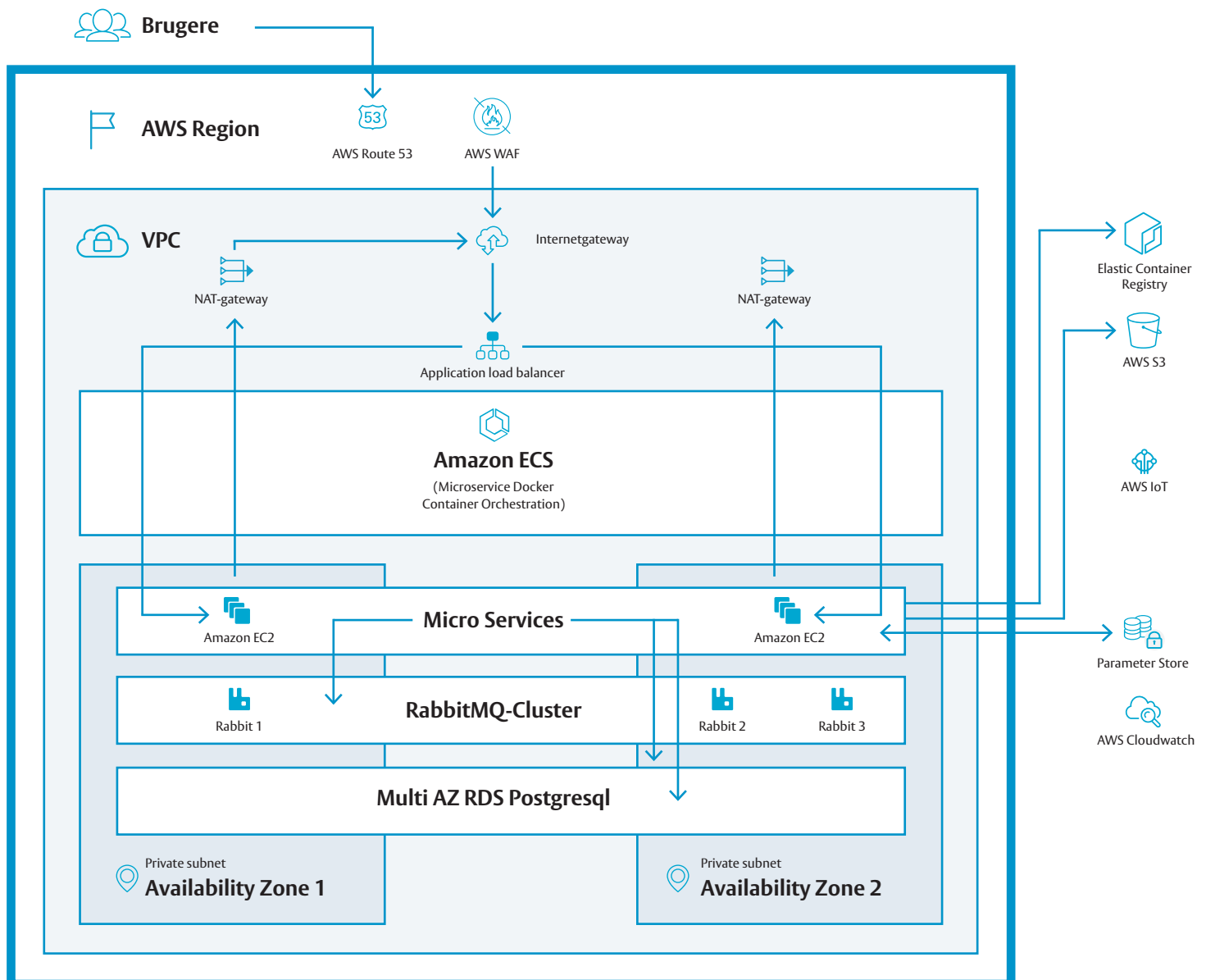
Controlleren kan konfigureres med statiske IP-adresser eller bruges med DHCP-server. Controlleren skal have følgende protokoller og porte samt URL'er, der er tilgængelige via firewallen.

- MQTT og HTTPS-port 443
- NTP-port 123
- DNS-port 53
- Access til følgende URL'er er tilgængelig:
 - access.assaabloy.com/*
 - accentra.abloy.com/*
 - accentra.assaabloy.com/*
 - rocketfw.s3-eu-west-1.amazonaws.com/*
(bruges til opdateringer af firmware)
 - a2118gv0vua4gp-ats.iot.eu-west-1.amazonaws.com
(adresse til MQTT-broker)

* henviser til alle sub-URL'er under det samme domæne.

Diagram over AWS infrastruktur

- Region - Irland
- WAF - Firewall til webapplikationer
- Køres i AWS EC2-instanser
- Loadbalancere til applikationer
- Database i RDS PostgreSQL
- Køhåndtering sker vha. RabbitMQ



Datasikkerhed og GDPR

Sikkerhed for datakommunikation

ASSA ABLOY Access' infrastruktur er bygget på en offentlig cloud-plattform (Amazon Web Services). Access har en separat privat sky og avancerede firewall-regler og adgangskontrol, der begrænser adgangen udefra og inde fra netværket til kun at omfatte betroede kilder.

Adgang til servere er begrænset til funktions- og supportteammedlemmer og til skrivebeskyttet adgang. Alle licenshavere har gennemgået et baggrundstjek baseret på ASSA ABLOYs sikkerhedspolitik, og adgangsrettighederne gennemgås to gange om året.

Kommunikationen mellem alle tjenester og enheder er beskyttet af HTTPS og ved at bruge TLS-mekanismen til at validere servercertifikater.

I PULSE-systemet er datakommunikationen og den datapakke, den indeholder, krypteret separat, hvilket gør systemet ekstremt sikkert.

Følgende tabel beskriver mekanismen til sikring af kommunikation mellem ASSA ABLOY Access og fysiske enheder.

Service	Ekstern enhed/applikation	Protokol og sikkerhedsmekanisme
Access	ABLOY PULSE mobil applikation	Applikationen fungerer som en HTTPS-klient. Applikationen sikrer kommunikationen med den rigtige tjeneste med et certifikat og bruger et adgangstoken (OAuth) til at autentificere sig over for tjenesten.
Access	Internet browser	Applikationen fungerer som en HTTPS-klient. Applikationen sikrer kommunikationen med den rigtige tjeneste med et certifikat og bruger et adgangstoken (OAuth) til at autentificere sig over for tjenesten. Kommunikationen er beskyttet ved hjælp af HTTPS-protokollen. Browseren er ansvarlig for at validere servercertifikatet, der leveres af Access.
Access	Opdateringslæser	Der bruges MQTT med TLS- og HTTPS-beskyttelse til datakommunikation. Den faste softwaren sikrer kommunikation med den korrekte tjeneste ved hjælp af et certifikat. Opdatering af følsomme data i læserens hukommelse er beskyttet af SeoS-kryptering.
Access	Bordkoder / PC-software	Der anvendes HTTPS-beskyttelse til datakommunikation. Programmet sikrer kommunikationen med den korrekte tjeneste ved hjælp af et certifikat.
CUMULUS	CUMULUS Applikationer og låseenheder	Hver driftsenhed registreres i CUMULUS-økosystemet og modtager et certifikat, som bruges til at kommunikere sikkert med CUMULUS-backend og med låseenheden.
CUMULUS	Integration	Al integration mellem Access og CUMULUS er sikker og foregår via API'er.

Datasikkerhed

ASSA ABLOY Opening Solutions (AAOS) er en del af ASSA ABLOY-koncernen. I overensstemmelse med ASSA ABLOYs regler for god forretningsskik forpligter vi os til at drive vores forretning i overensstemmelse med bedste etiske praksis og til at overholde gældende love. AAOS er forpligtet til løbende at gennemgå sine processer og retningslinjer.

I ASSA ABLOY Access systemet er AAOS altid databasehandler. AAOS behandler kun personoplysninger på vegne af kunden. AAOS behandler aldrig personoplysninger til andre formål end dem, der er angivet af kunden. Slutkunden er den dataansvarlige, der har gemt dataene i systemet.

Ved udviklingen af Access-systemet følger vi princippet om indbygget integritet og foretager konsekvensanalyser af datasikkerheden.

ASSA ABLOY koncernen mener, at det er vigtigt at afsløre sårbarheder for at forbedre kvaliteten af vores produkter og tjenester, sikkerheden for vores kunder, der er afhængige af dem, og bevidstheden om deres valg for at bevare deres specifikke interesser. ASSA ABLOY værdsætter viden fra sikkerhedsforskere og byder information og samarbejde med dem velkommen.

Du kan finde flere oplysninger og politikken på ASSA ABLOYs produktsikkerhedssider.

Vi er forpligtet til at følge den bedste praksis i Secure Software Development Life Cycle (SSDLC) for at sikre, at alt udvikles med sikkerhed i tankerne. SSDLC bruges til at identificere og afbøde potentielle sikkerhedsproblemer og -trusler under udviklingen, så slutproduktet er sikkert som standard.

Datalagring

De databaser, der bruges i Access, sikkerhedskopieres hver sjette time og gemmes i en separat tjeneste i AWS. Sikkerhedskopierne gemmes i 30 dage.

Access indsamler logfiler på applikationsniveau over systemaktivitet. Følsomme oplysninger som fx adgangskoder gemmes ikke i logdataene.

Logopbevaring varierer mellem tjenesterne, men den længste opbevaringsperiode er 30 dage. På samme måde administreres og gennemgås logfiler relateret til infrastruktur af tjenesteudviklingsteamet. Kun autoriseret personale har adgang til lagring af logfiler, og visningerne registreres også i logfilerne. Infrastrukturrelaterede logs opbevares i to uger.





ABLOY PULSE®

Generel beskrivelse

ABLOY PULSE er et avanceret låse- og adgangskontrolsystem, som kan betragtes som et økosystem, hvor nøgler og låse kommunikerer med hinanden.

Økosystemet dækker kundernes låsebehov, herunder adgangsstyring og låseløsninger. Cylindre, hængelåse og møbellåse, RFID-læsere og nøgler kan kobles til systemet. Systemet administreres med ASSA ABLOY Access software.





ABLOY CUMULUS®

Generel beskrivelse

ABLOY CUMULUS er et nøglefrit låsesystem, der giver nem adgang ved hjælp af en mobil enhed i stedet for en fysisk nøgle eller nøglebrikker. Mobiltelefonen bærer autorisationen til at åbne en bestemt enhed i stedet for at definere autorisationen i selve låsen og sørger for at hente logfiler fra låsene til skyen.

Låseenheder kan bruges med mobiltelefonen, selv uden online-forbindelse, når adgangsnøglerne indlæses på mobilen under online-brug, før offline-låsen åbnes.

CUMULUS-porteføljen omfatter mobilnøgler, hænge-låse, nøglerør, controllere, svinghåndtag og firmware. Låseenhederne integreres med digitale værktøjer, der giver pålidelig og problemfri funktionalitet sammen med adgangskontrolsystemet. CUMULUS integreres med ASSA ABLOY Access, og adgangsauctorisationer administreres via Access Web UI.

Online opdateringslæser

Opdateringsenheden er det centrale element i PULSE-systemet. Opdateringslæseren består af en dørcontroller og en RFID-læser, der er tilsluttet denne. Dørcontrolleren er forbundet med Access via internettet, hvilket gør fjernstyring af system en mulighed.

Opdateringsæseren gør det muligt at ændre nøglernes adgangsrettigheder og opdatere nøglernes data. Brugernes nøgler overfører også data fra låsene til softwaren, uden at en administrator behøver at besøge ejendommen.

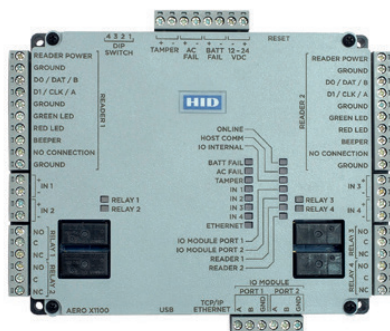
Opdateringslæseren kan også bruges til at styre en dør, elevator eller port, der er forbundet med controlleren. I princippet kan den bruges til at styre enhver

relæstyret enhed. Controllerens hukommelse gemmer systemets adgangsrettigheder i krypteret form, så døren kan bruges, selv om forbindelsen til cloud-tjenesten ikke fungerer.

Systemet kan bestå af en eller flere opdateringslæsere. Controlleren kan tilsluttes to læsere og bruges til at styre en eller to døre. Controlleren er kompatibelt med PULSE Signo 20- og 20K-læsere. Selv hvis internetforbindelsen afbrydes, kan op til 1.000 tidligere adgangs-hændelser og 20.000 nøglerettigheder gemmes i hukommelsen.

Tekniske specifikationer for dørcontroller

Indgangsspænding	12 til 24V DC +/- 10%
Ethernet-kommunikation	10 BaseT/100Base-TX
Strømforsyning til læsere	12 Vdc +/- 10% reguleret, max 500 mA per læser
Driftstemperatur	0 til 70°C
Dimension	6,46" x 5,51" x 1,02" (164 mm x 140 mm x 26 mm)
Vægt	352 g
Support til læsere	Maks. 2 læsere





Tekniske specifikationer for læseren

	Signo 20	Signo 20K
Farve	Sort med sølvfarvet bundplade	
Driftsspænding	12V DC	
Tastatur	Nej	Ja (2x6 layout)
Mål (B x L x D)	45 mm x 121,5 mm x 19,5 mm	45 mm x 121,5 mm x 21,5 mm
Miljømæssig klassificering	UL294 udendørs og indendørs klassificeret, IP65	
Sendefrekvens	125 kHz, 13,56 MHz, og 2,4 GHz	
Drifttemperatur og luftfugtighed	-35° C til +66° C 0 % til 95 % ikke-kondenserende	





Systemkrav til computer

- Den anbefalede browser til Access softwaren er Google Chrome, som officielt er fuldt understøttet. Mozilla Firefox og Microsoft Edge er også blevet testet og har vist sig at fungere, selv om de ikke officielt anbefales.
- Hvis du bruger de andre browsere, vil nogle funktioner måske ikke virke efter hensigten.
- Internet Explorer anbefales ikke.



Krav til internetforbindelse

Access controlleren kommunikerer med Access via en internetforbindelse. De mest almindelige internetforbindelser, der er tilgængelige fra operatører, er velegnede som internetforbindelse.

Den anbefalede internat hastighed er mindst 10 Mbit/s. Hvis du bruger en mobil bredbåndsforbindelse, anbefales et abonnement med ubegrænset dataoverførsel.

Afhængigt af netværksinfrastrukturen tilsluttes controlleren til routeren eller switchen vha. et netværkskabel med RJ45-stik. Controlleren henter automatisk IP-adressen og andre nødvendige netværksindstillinger fra DHCP-tjenesten på netværket. Hvis der ikke er nogen DHCP-tjeneste på netværket, kan netværket konfigureres manuelt.

Controlleren holder kontakt med Access, hvor de foretagne ændringer kan opdateres til nøglen med en forsinkelse på ca. 10 sekunder (afhængigt af internet-

forbindelsens hastighed og belastningen på serveren).

Controlleren kan selv beslutte, om døren skal åbnes. Afbrydelse af netværket forhindrer således ikke døren i at blive brugt, hvis nøglen er programmeret i systemet, og hvis nøglen har adgangsrettigheder til den dør, der styres af controlleren. Men når netværksforbindelsen afbrydes, kan nøgledataene ikke opdateres til Access, og nøglen kan heller ikke opdateres med ændrede adgangsrettigheder.

I princippet er der ikke behov for separate firewall-regler for controllerens datakommunikation, da dataoverførslen sker fra det interne netværk til internettet. I firewalls autoriseres returpakker normalt automatisk. Firewallen og de nødvendige netværksindstillinger kan verificeres af netværksadministratoren. Controlleren skal have adgang til det offentlige internet via TCP 443-porten.



ASSA ABLOY

ASSA ABLOY koncernen er global markedsleder inden for adgangsløsninger. Koncernen opererer på globalt plan med 52.000 medarbejdere og en omsætning på 11,4 milliarder euro.

Koncernen er førende inden for områder som effektive adgangsløsninger, sikre identiteter og indgangsautomatisering. ASSA ABLOYs innovationer leverer sikker, tryk og praktisk adgang til fysiske og digitale lokationer. Hver dag hjælper vi milliarder af mennesker med at opleve en mere åben verden.

ASSA ABLOY Opening Solutions Denmark A/S
Borupvang 5D
2750 Ballerup

Tfl. +45 4454 44 54
info.dk.openingsolutions@assaabloy.com

assaabloy.dk