

MANUAL

UniLock Web-Adgangseditor

Pro.nr.: PCS125-20

Rev.: 2023-10-11

Intro information

Web-Adgangseditor giver fjernkontrol og overvågning via en tovejs højsikret webforbindelse. Web-Adgangseditor kan anvendes på pc, tablet og telefon i webbrowser og som App.

Indhold

1. Beskrivelse	2
1.1 Generel beskrivelse	2
2. Netværksforbindelse	3
2.1 Lokalt netværk.....	3
2.2 Internet/eksternt netværk.....	3
3. Opsætning.....	4
3.1 Webserver	5
3.2 Web-Adgangseditor.....	8
3.3 Login.....	8
4. Installation på pc og telefon	9
4.1 PC	9
4.2 Telefon og tablet.....	9
5. Grafisk overvågning.....	10

1. Beskrivelse

1.1 Generel beskrivelse

The screenshots illustrate the Web-Adgangseditor interface, which is used for managing access control systems. The interface is divided into several main sections:

- Delte undtagelser styring (Shared Exemptions Management):** A table listing exemptions with columns for 'Delt undtagelse' (Shared exemption), 'Aktiv' (Active), 'Handlinger' (Actions), and 'Beskrivelse' (Description). Examples include 'Aktiver fri adgang til elevator' (Activate free access to elevator) and 'Booking af Hal' (Booking of Hall).
- Grafisk overvågning (Graphic Monitoring):** A floor plan diagram showing various rooms and areas, including 'Køkken' (Kitchen), 'Kantine' (Canteen), 'Tilf.' (Toilet), 'Kontor' (Office), 'Kontorfløj nord' (Office wing north), 'Kontorfløj syd' (Office wing south), 'Lager' (Warehouse), 'Lagerindgang' (Warehouse entrance), 'Shopsplan' (Shopping plan), 'Personaleindgang' (Staff entrance), 'Pladeværksted' (Plate workshop), 'Markedskammer' (Market room), 'Indgangs parti' (Entrance part), and 'Hovedindgang' (Main entrance). The diagram includes status indicators for 'DAS TV' and 'DAS'.
- K-punkts styring (K-point Control):** A table showing the status of various points, including 'Herrings bagder' (Herrings back door), 'Herrings hoveddør' (Herrings main door), 'Herrings lager' (Herrings warehouse), 'Hovedindgang' (Main entrance), 'Indgang vest' (Entrance west), 'Kantine' (Canteen), 'Kantinekontor' (Canteen office), 'Kontorfløj nord' (Office wing north), 'Kontorfløj syd' (Office wing south), 'Lager' (Warehouse), 'Lagerkontor' (Warehouse office), 'Odense bagder' (Odense back door), 'Odense hoveddør' (Odense main door), and 'Parkeringskælder' (Parking basement).
- Personer (Persons):** A list of users with search and filter options. The 'Birgitte Nielsen' profile is highlighted, showing details such as 'Fødselsdato' (Date of birth), 'Telefonnummer' (Phone number), 'E-mail', 'Adresse', and 'By'.
- Tyverialarm styring (Burglar Alarm Management):** A table showing the status of various alarm points, including 'Fællesområde' (Common area), 'Herrings bagder' (Herrings back door), 'Herrings hoveddør' (Herrings main door), 'Herrings lager' (Herrings warehouse), 'Kantine' (Canteen), 'Kantinekontor' (Canteen office), 'Kontorfløj nord' (Office wing north), 'Kontorfløj syd' (Office wing south), 'Lager' (Warehouse), 'Lagerkontor' (Warehouse office), 'Odense' (Odense), and 'Vejle bader' (Vejle bathroom).

Anvendelse

Web-Adgangseditor giver fjernadministration, fjernkontrol og overvågning på pc, tablet og telefon via en tovejs højsikret webforbindelse.

Driftsovervågning giver mulighed for at se status på k-punkter, DAS og delte undtagelser.

Fjernkontrol giver:

- Oplåsning/låsning af k-punkter (døre).
- Tilkobling/tidsforskuet tilkobling og frakobling af DAS (tyverialarmer).
- Aktivering/deaktivering af delte undtagelser (scenarier).

På plantegninger kan man have grafisk overvågning af status på hver indgang og udgang for hver k-punkt, status for DAS og fjernstyring af både oplåsning/låsning og DAS.

Beskrivelse

Forbindelsen er sikret med HTTPS og login er sikret jævnfør OAuth 2.0.

Web-Adgangseditor kan installeres som app på mobilplatforme (Apple, Android mv.) og som program på pc.

2. Netværksforbindelse

I dette afsnit beskrives de netværksmæssige tilføjelser der skal foretages for at klienter kan forbinde til Web-Adgangseditor.

Det anbefales at installations-pc altid har samme IP adresse, hvilket typisk indstilles i netværkets DHCP server eller blot ved at give installations-pc'ens netkort en fast IP adresse frem for at anvende DHCP.

2.1 Lokalt netværk

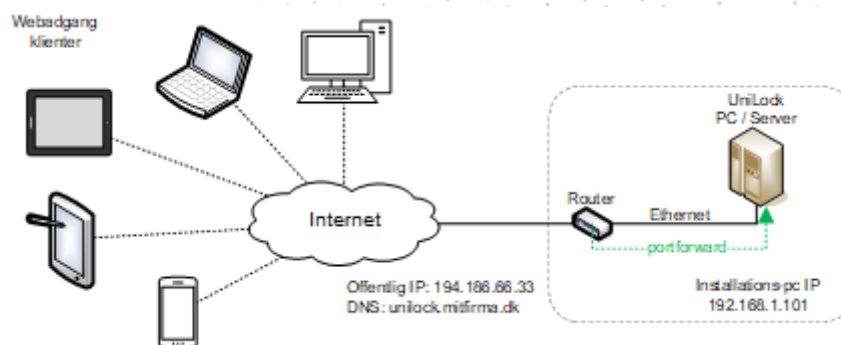
Forbindelse til Web-Adgangseditor fra klienter på det lokale netværk kan ske blot ved at åbne sin webbrowser og indtaste installationspc'ens IP adresse eller hostnavn.

2.2 Internet/eksternt netværk

Forbindelse til Web-Adgangseditor fra klienter på eksterne netværk, som fx internettet, kan ske efter at der er lavet portforwarding i routere mellem det eksterne netværk og UniLock installations-pc/-server.

I nedenstående eksempel tilføjes en portforwarding i Router til installations-pc'ens ip-adresse på Webserver porten (default 443). Hvis portforwarding fra port 80 er aktiveret i Webserver eller integritonen med Let's Encrypt anvendes, tilføjes også en portforwarding til port.

Bemærk at samme portnumre skal anvendes i UniLock Webserver og Router portforwarding af hensyn til tekniske redirects. Altså konfigureres UniLock til at anvende port 80 og 443, så skal portforward laves fra offentlig port 80 til installations pc port 80 og ligeledes for port 443.



Forbindelse til Web-Adgangseditor fra klienter på eksterne netværk kan ske blot ved at åbne sin webbrowser og indtaste det offentlige DNS-navn eller den offentlige IP adresse. Det anbefales at anvende et offentligt DNS-navn, da sikkerhedscertifikater kun kan udstedes til DNS-navne.

Har man en offentlig fast ip-adresse kan denne fx registreres hos Punktum dk (tidligere DKHostmaster) til at peger på en DNS udbyder. Hos DNS udbyderen kan man oprette sin DNS A-record og CNAME. Den offentlige IP adresse kan findes ved at åbne www.whatismyip.com fra installations-pc.

Har man en offentlig ikke-fast ip-adresse kan man anvende en Dynamisk DNS service som fx DynDNS til at vedligeholde sammenhængen mellem sin dynamisk ip-adresse og sit offentlige DNS-navn.

3. Opsætning

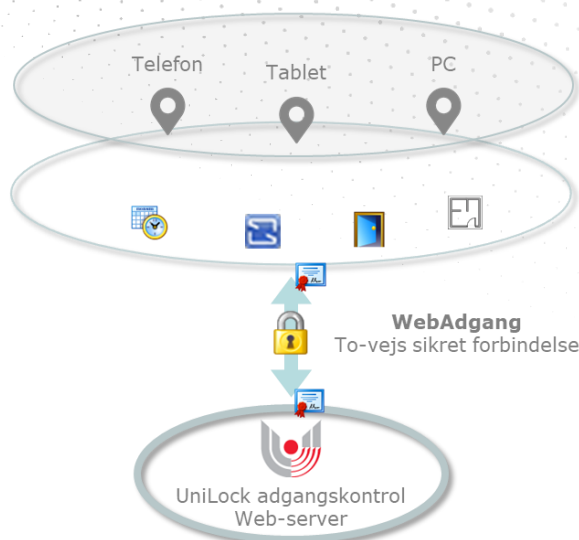
Web-Adgangseditor er hosted i den indbyggede Webserver i UniLock PollerService. Webserveren skal således køre før Web-Adgangseditor kan aktiveres.

Muligheder:

- ✓ Døre oplås/lås
- ✓ Tyverialarmer tilkobl/frakobl
- ✓ Tyverialarmer tidsforskydning
- ✓ Undtagelser aktiver/deaktiver
- ✓ Driftsovervågning
- ✓ Plantegninger

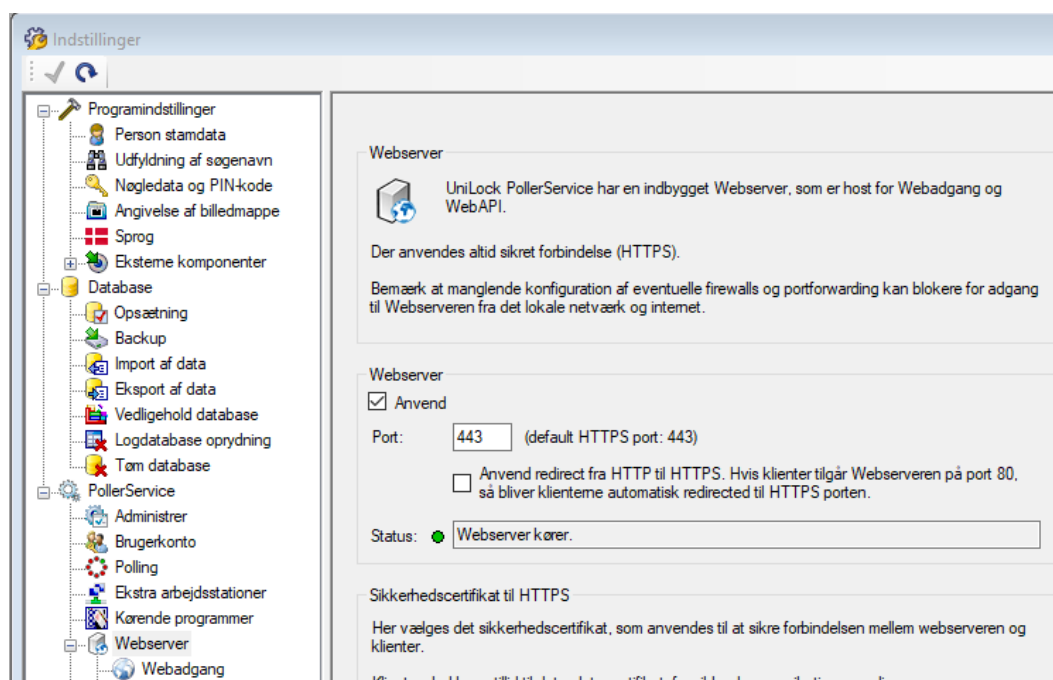
Teknik:

- ✓ Adgang med App / browser
- ✓ Sikret forbindelse
- ✓ Sikret login



3.1 Webserver

Opsætning af Webserver foretages i UniLock Adgangseditor: [Indstillinger], [PollerService], [Webserver].



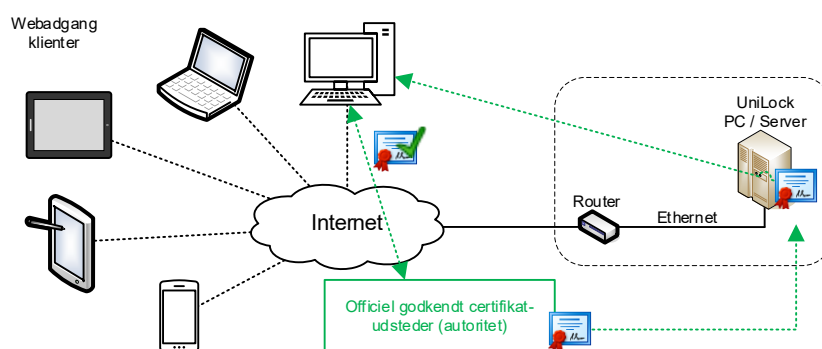
Når UniLock Webserveren aktiveres, forsøger UniLock at åbne de nødvendige porte på installations-pc i Windows Firewall. Anvendes anden firewall skal man manuelt oprette regler i denne firewall, så UniLock kan lytte på de nødvendige porte.

Sikkerhedscertifikat til HTTPS

UniLock Webserver anvender krypteret forbindelse (HTTPS), hvilket kræver et standard sikkerhedscertifikat.

HTTPS er en krypteret protokol til at sikre at afsender og modtager kan kommunikere uden at andre kan lytte med (man-in-the-middle angreb).

Sikring opnås ved at afsender (Webserver) afleverer et sikkerhedscertifikat, udstedt af et officiel godkendt certificeringsfirma, til modtagere (klienter), så modtagere kan have tillid til at afsender er den rigtige.



Klienters programmer (webbrowser mv.) godkender automatisk at kommunikation er sikret så snart tillid er på plads, ellers vil programmerne typisk advare eller blokere afsenderen indtil modtageren manuelt godkender.

I Webserveren kan man vælge et sikkerhedscertifikat fra installations-pc eller bruge integrationen med det godkendte certificeringsfirma Let's Encrypt til at udstede og vedligeholde sit sikkerhedscertifikat.

Sikkerhedscertifikat til HTTPS

Her vælges det sikkerhedscertifikat, som anvendes til at sikre forbindelsen mellem webserveren og klienter.

Klienter skal have tillid til det valgte certifikat, for sikker kommunikation er mulig.
Det anbefales at anvende et certifikat, som er udstedt af en officiel godkendt certificerings-autoritet, da klienter automatisk vil have tillid til dette certifikat. Et officielt godkendt certifikat udleveres typisk af IT-afdelingen eller oprettes og vedligeholdes gennem tredjeparts-service som fx "Let's Encrypt".

Vælg certifikat:

Udsteder:

Udløbsdato:

Primær domænenavn:

Domænenavne:

Certifikattype:

Certifikat - Fra installation

Listen af valgbare certifikater hentes fra installations-pc.
Certifikat import/eksport udføres af en meget IT-kyndig i Windows Certificate Manager.
Anvendes et certifikat, som ikke er udstedt af en officiel certificerings-autoritet, skal der skabes tillid til certifikatet på hver enkelt klient.

Til testformål kan et UniLock SelfSigned Certifikat anvendes:

Fra installations-pc kan certifikat til kryptering vælges ud fra de certifikater som har privat nøglen tilgængelig og placeret i [Windows Certificate Store], [Local Machine], [Personal].

UniLock genererer automatisk alarmer ved certifikatfejl og snarlig udløb af certifikat.

Bemærk at integrationen med Let's Encrypt kræver at UniLock Webserveren er alene om både port 80 og Webserver-porten, og at begge porte er portforwarded fra internettet til installations-pc.

3.2 Web-Adgangseditor

Web-Adgangseditor er en indbygget hjemmeside, som muliggør fjernbetjening og overvågning af en række funktioner i UniLock.

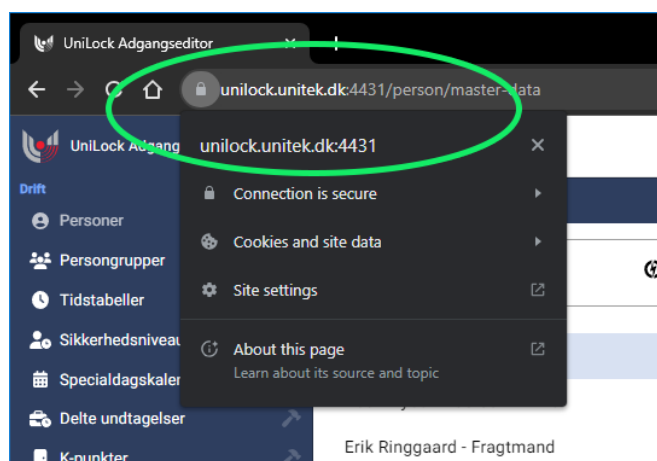
Opsætning af Web-Adgangseditor foretages i UniLock Adgangseditor: [Indstillinger], [PollerService], [Webserver], [Web-Adgangseditor].

Web-Adgangseditor indeholder som standard:

- Oversigt over k-punkter (døre) med mulighed for fjernstyring.
- Oversigt over DAS (tyverialarmer) med mulighed for fjernstyring.
- Oversigt over delte undtagelser med mulighed for fjernbetjening.
- Eksempel på bygningstegning med dynamisk ikoner for overblik og fjernbetjening.

Derudover er det muligt at tilføje egne sider.

Når Webbrowser og Web-Adgangseditor er aktiveret kan tillid kontrolleres i webbrowser som fx Google Chrome ved at trykke på hængelåsen:



3.3 Login

UniLock operatører kan logge ind i Web-Adgangseditor med brugernavn og adgangskode, som også anvendes til deres operatørlogin i UniLock Adgangseditor.

To-faktor login kan aktiveres efter opsætning af mail-server for udsendelse af to-faktor kode til operatøren mailadresse.

Operatøren kan logge ind når operatørrettigheden til Web-Adgangseditor er givet. De forskellige funktioner i Web-Adgangseditor kan betjenes, når de respektive operatørrettigheder er givet. Se nærmere i den overordnede manual til pc-programmet.

For de sikkerheds-interesserede er login bygget på et certificeret OpenID Connect provider library (IdentityServer3¹) som benytter:

- OpenID Connect Dynamic Client Registration 1.0
- OAuth 2.0 Dynamic Client Registration Protocol (rfc7591)
- OAuth 2.0 Dynamic Client Registration Management Protocol (rfc7592)

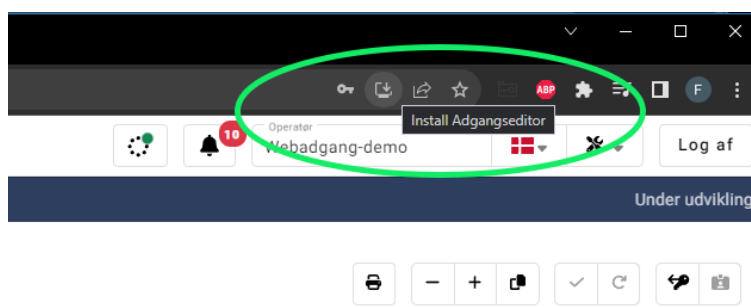
4. Installation på pc og telefon

Web-Adgangseditor kan installeres på pc, tablet og telefon. Web-Adgangseditor åbnes første gang i en webbrowser ved at indtaste DNS-navnet (webadresse) eller den offentlige IP adresse.

Installation fra webbrowser er mulig når der er tillid til Web-Adgangseditor sikkerhedscertifikat, se denne manuals afsnit 3.1 Webserver.

4.1 PC

Web-Adgangseditor installeres fra webbrowser som fx Google Chrome ved at trykke på knappen [+], [Install UniLock Web-Adgangseditor]:



På pc bliver Web-Adgangseditor installeret som et standard program.

4.2 Telefon og tablet

Når Web-Adgangseditor er åbnet vises automatisk "Føj til startskærm". På mobilplatforme bliver Web-Adgangseditor installeret som en standard App.

Evt. manuel installation på Android udføres i webbrowser, [Menu], [Føj til startskærm].

Evt. manuel installation på Apple udføres i Safari, [Menu], [Føj til hjemmeskærm].

¹ <https://github.com/IdentityServer/IdentityServer3>

5. Grafisk overvågning

På basis af en bygningstegning giver Grafisk overvågning et hurtigt samlet overblik over hele installationens aktuelle driftstilstand, så overvågning bliver en overskuelig og lettilgængelig opgave.



Der kan opbygges forskellige sider, hvor operatøren kan vælge mellem siderne i menuen øverst til venstre på siden eller indsætte navigationsikoner.

Dynamiske ikoner

Grafisk overvågning består af et baggrundsbillede, hvorpå aktuel status for døre, DAS, tyverialarmer, indgange og udgange vises ved hjælp af dynamiske ikoner, der frit kan placeres på baggrundsbilledet.

Online overblik ved hjælp af en almindelig webbrowser

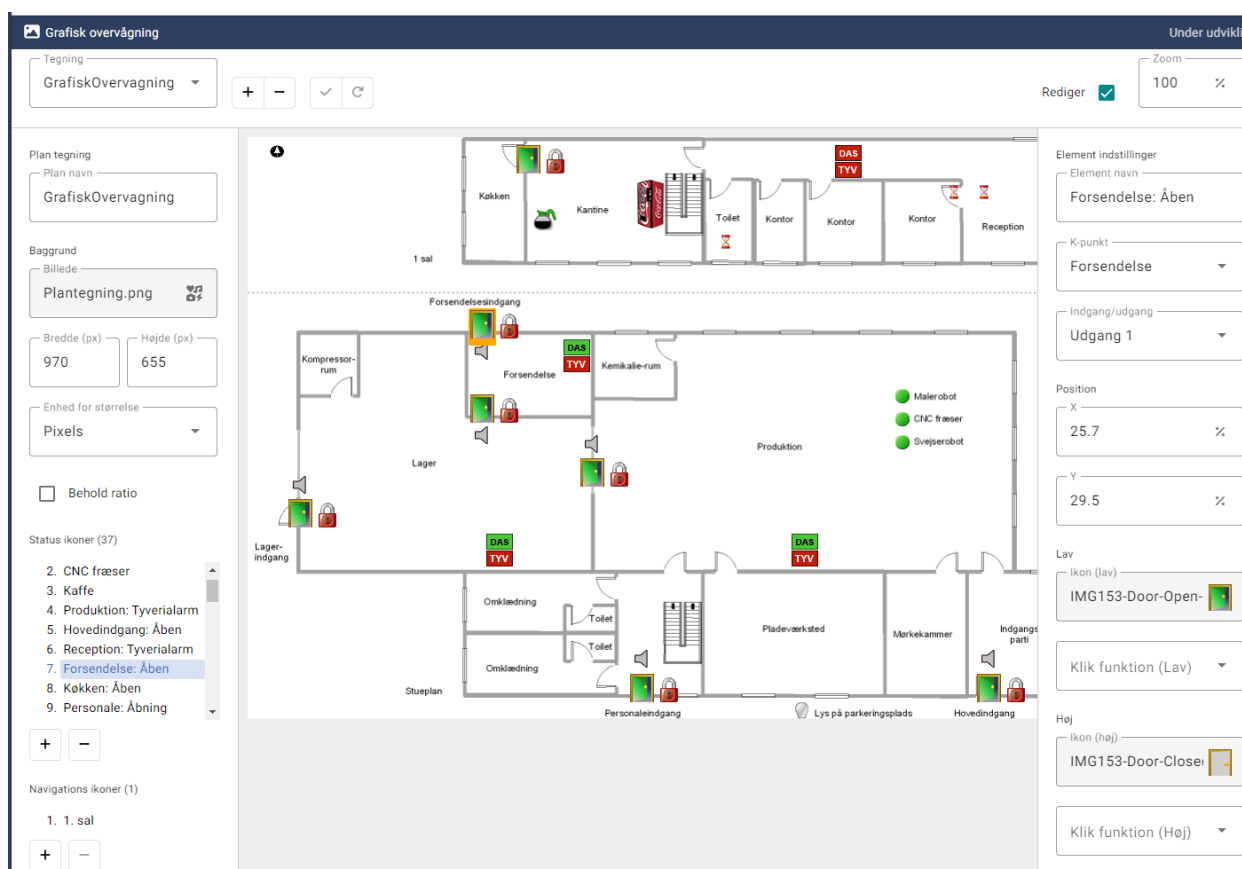
Grafisk overvågning er indbygget i hjemmesiden for Web-Adgangseditor. Web-Adgangseditor henter løbende aktuelle statusinformationer fra systemets indbyggede Webserver og præsenterer status informationerne for operatøren i form af dynamiske ikoner på baggrundsbilledet.

Fjernkontrol

Med et klik på k-punktets ikoner er det muligt at oplåse/låse døren og tilkoble eller frakoble tyverialarmen.

Konfiguration

Da Grafisk overvågning er baseret på en eller flere bygningstegninger over den pågældende installation, kræves der følgelig tilpasning til den aktuelle installation. Redigering foretages ved at aktivere [Rediger] i øverste højre hjørne.



Ny plantegning tilføjes ved at trykke [+]

Egne billeder (baggrunde/ikoner) tilføjes til ved at vælge baggrund/ikon, hvorefter man kan tilføje nye billeder til databasens billedbibliotek.

Status for døre, DAS, tyverialarmer, indgange og udgange, der kræver operatørens opmærksomhed, gives et ikon, som frit placeres på baggrundsbilledet. Der kan tilføjes kommandoer til hvert ikon, således at man med museklik kan: oplåse/låse, tilkoble DAS og frakoble DAS.