

MANUAL

UniLock Web Access-editor

Project No.: PCS125-20

Revision.: 2026-08-13

Introduction

The Web Access Editor provides remote control and monitoring via a highly secure two-way web connection. It can be used on PCs, tablets and mobile phones through a web browser or installed as an application.

Indhold

- 1. Description2
 - 1.1 General Description2
- 2. Network connection.....3
 - 2.1 Local network3
 - 2.2 Internet/external network3
- 3. Setup4
 - 3.1 Webserver5
 - 3.2 Web Access-editor8
 - 3.3 Operator login8
 - 3.4 Operator privileges.....9
- 4. Installation at pc and smartphone9
 - 4.1 PC9
 - 4.2 Phone and tablet.....9
- 5. Graphical monitoring10

1. Description

1.1 General Description

The screenshots illustrate the Unitek Web Access Editor interface, which is used for remote administration, control, and monitoring of access systems. The interface is divided into several main sections:

- Delte undtagelser styring (Deleted exceptions management):** A table showing active exceptions with columns for 'Delt undtagelse' (Deleted exception), 'Aktiv' (Active), 'Handlinger' (Actions), and 'Beskrivelse' (Description). Examples include 'Aktiver fri adgang til elevator' and 'Booking af Hal'.
- Grafisk overvågning (Graphic monitoring):** A floor plan diagram showing the layout of a facility with various rooms and access points. Rooms are color-coded and labeled, such as 'Køkken', 'Kantine', 'Toilet', 'Kontor', 'Lager', 'Produktion', 'Pladeværksted', and 'Markedskammer'.
- K-punkts styring (K-point control):** A table showing the status of access points. Columns include 'Navn' (Name), 'Online status', 'Derovervågnings status' (Monitoring status), and 'Derfor status' (Reason status). Examples include 'Herring bagder', 'Herring hoveddør', 'Herring lager', 'Hovedindgang', 'Indgang vest', 'Kantine', 'Kantinekontor', 'Kontorfløj nord', 'Kontorfløj syd', 'Lager', 'Lagerkontor', 'Odense bagder', 'Odense hoveddør', and 'Parkeringskælder'.
- Personer (Persons):** A screen for managing personnel. It includes a search bar and a list of personnel. The 'Birgitte Nielsen' profile is highlighted, showing details such as 'Fødselsdato' (Date of birth), 'Telefonnummer' (Phone number), 'E-mail', 'Adresse', and 'Borgerdefineret nr.' (Municipal ID number).
- Tyverialarm styring (Burglar alarm management):** A screen for managing burglar alarm settings. It includes a search bar and a list of alarm zones. Examples include 'Fællesområde', 'Herring bagder', 'Herring hoveddør', 'Herring lager', 'Kantine', 'Kantinekontor', 'Kontorfløj nord', 'Kontorfløj syd', 'Lager', 'Lagerkontor', 'Odense', and 'Vejle baader'.

Usage

The Web Access Editor provides remote administration, remote control and monitoring by a two-way highly secure connection.

Operational monitoring allows users to view the status of access points (doors), intruder alarm systems (IAS/DAS) and shared exceptions.

Remote control enables:

- Locking and unlocking of doors
- Arming / delayed arming and disarming of intrusion systems
- Activation / deactivation of shared exceptions (scenarios)

Floor plans can display graphical monitoring of inputs, outputs, doors, shared exception, intrusion system and remote operation functions.

Description

The connection is protected with HTTPS and authentication is secured in accordance with OAuth 2.0. The application can be installed on mobile platforms such as Apple iOS and Android, and as a desktop application on PCs.

2. Network connection

This section describes the network-related additions required to enable clients to connect to the Web Access-Editor.

It is recommended that the installation PC always has the same IP address; this is typically configured via the network's DHCP server or simply by assigning a static IP address to the installation PC's network card instead of using DHCP.

2.1 Local network

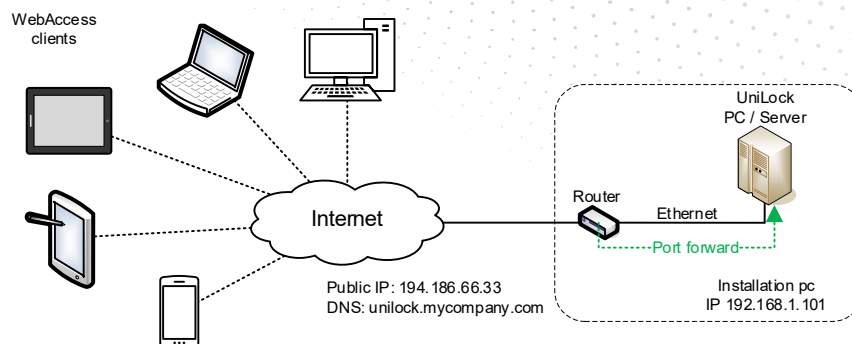
Clients on the local network can connect by entering the installation PC IP address or host name in a browser.

2.2 Internet/external network

Access from external networks such as the Internet requires router port forwarding to the UniLock installation PC or server.

In the example below, a port forwarding rule is added to the router, directing traffic to the installation PC's IP address on the web server port (default 443). If port forwarding from port 80 is enabled on the web server, or if Let's Encrypt integration is used, a port forwarding rule for that port is also added.

Please note that the same port numbers must be used in the UniLock web server and for router port forwarding to ensure technical redirects work correctly. In other words, if UniLock is configured to use ports 80 and 443, port forwarding must be set up from public port 80 to port 80 on the installation PC, and likewise for port 443.



Clients on external networks can connect to the Web Access Editor simply by opening a web browser and entering the public DNS name or public IP address. It is recommended to use a public DNS name, as security certificates can only be issued for DNS names.

If you have a public static IP address, it can be registered with Punktum dk (formerly DKHostmaster), for example, to point to a DNS provider. You can then create your DNS A-record and CNAME with the DNS provider. The public IP address can be found by visiting www.whatismyip.com from the installation PC.

If you have a public, non-static IP address, you can use a dynamic DNS service (such as DynDNS) to maintain the link between your dynamic IP address and your public DNS name.

3. Setup

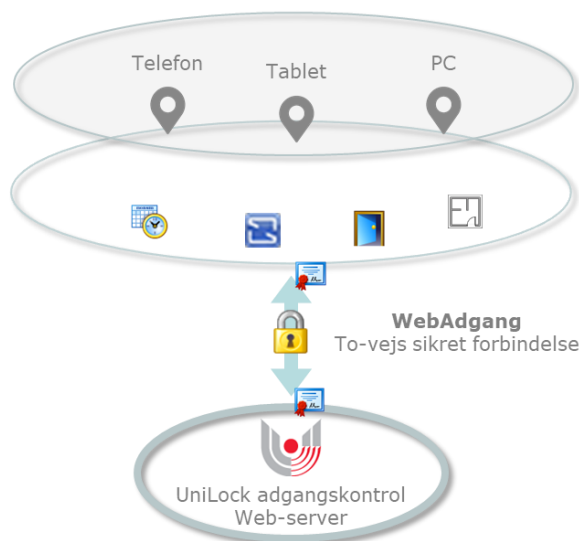
The Web Access-Editor is hosted by the built-in web server in the UniLock PollerService. Consequently, the web server must be running before the Web Access-Editor can be activated.

Muligheder:

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

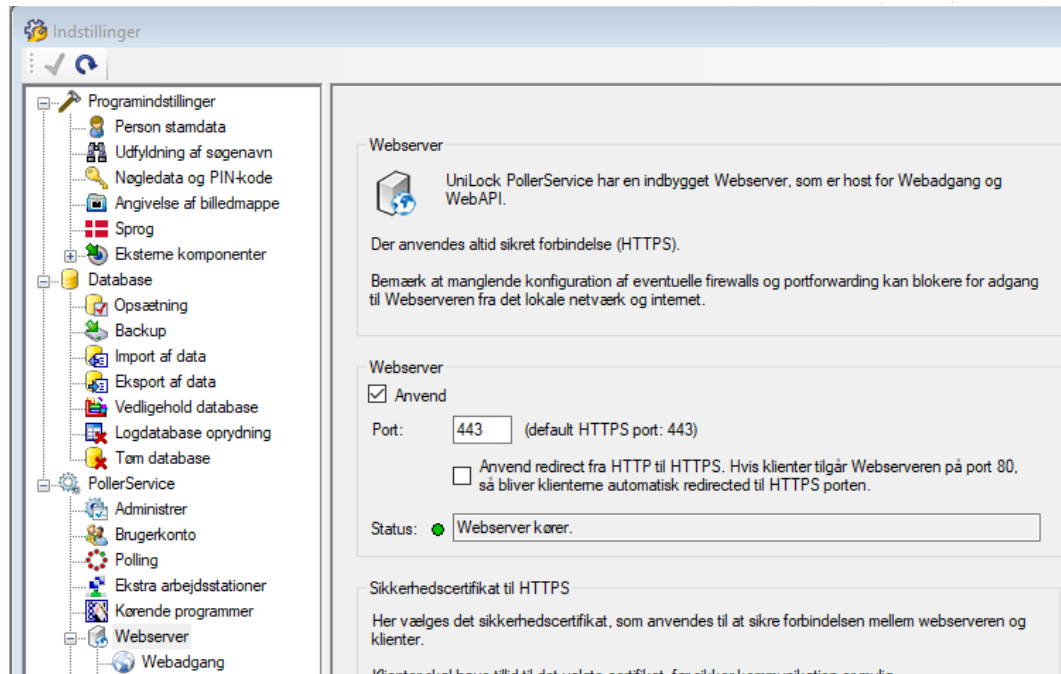
Teknik:

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



3.1 Webserver

Web server setup is performed in the UniLock Access Editor: [Settings], [PollerService], [Webserver].



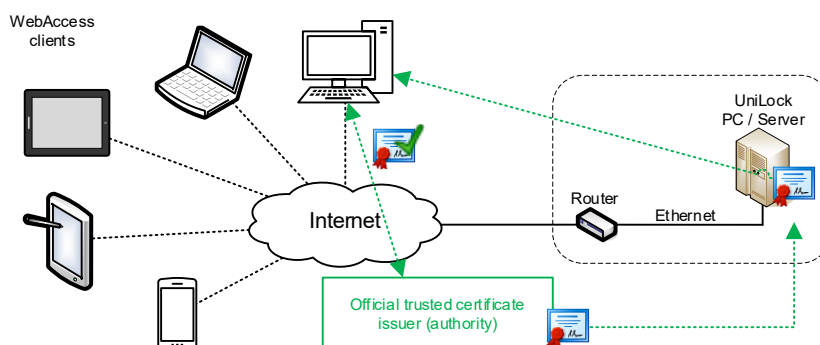
When the UniLock Web Server is activated, UniLock attempts to open the necessary ports in the Windows Firewall on the installation PC. If a different firewall is used, you must manually create rules in that firewall to allow UniLock to listen on the required ports.

Security certificate for HTTPS

The UniLock Webserver uses an encrypted connection (HTTPS), which requires a standard security certificate.

HTTPS is an encrypted protocol that ensures the sender and receiver can communicate without others eavesdropping (man-in-the-middle attacks).

Security is achieved by the sender (web server) providing a security certificate (issued by an officially approved certification authority) to the recipients (clients), enabling them to trust that the sender is legitimate.



Client applications (web browsers, etc.) automatically accept that communication is secure once trust has been established; otherwise, the applications will typically issue a warning or block the sender until the recipient manually grants approval.

In the web server, you can select a security certificate from the installation PC or use the integration with the approved certification authority Let's Encrypt to issue and maintain your security certificate.

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:

From the installation PC, the encryption certificate can be selected from the certificates that have the private key available and are located in [Windows Certificate Store], [Local Machine], [Personal].

UniLock automatically generates alarms for certificate errors and imminent certificate expiration.

Please note that the integration with Let's Encrypt requires the UniLock Web Server to have exclusive use of both port 80 and the web server port, and for both ports to be forwarded from the internet to the installation PC.

3.2 Web Access-editor

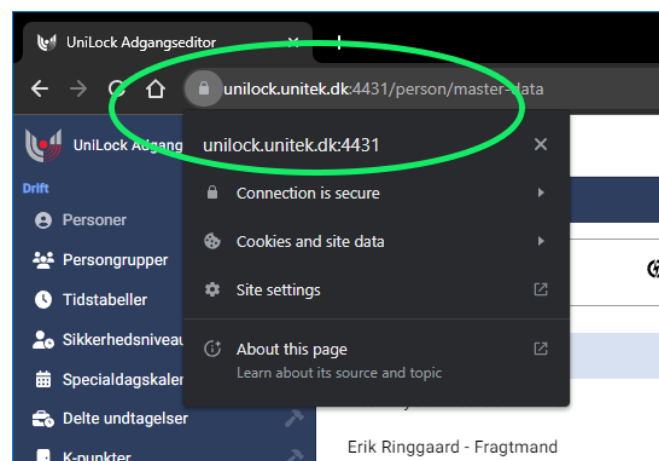
The Web Access-Editor is a built-in web interface that enables remote control and monitoring of a range of UniLock functions.

The Web Access Editor is set up within the UniLock Access Editor: [Settings], [PollerService], [Web Server], [Web Access Editor].

By default, the Web Access Editor includes:

- Overview of control points (doors) with remote control capability
- Overview of DAS (intrusion system) with remote control capability
- Overview of shared exceptions with remote control capability
- Example of a building layout with dynamic icons for an overview and remote control
- Navigation across building layout to provide a layered experience

When the Web Browser and Web Access Editor are enabled, trust can be verified in a web browser such as Google Chrome by clicking the padlock icon:



3.3 Operator login

UniLock operators can log in to the Web Access-Editor using the username and password also used for their operator login in the UniLock Access Editor.

Two-factor login can be enabled after setting up a mail server to send the two-factor code to the operator's email address.

Microsoft Entra access rules (MFA, Geo-fencing ect.) can be include by adding integration for Entra.

For those interested in security, the login is built on a certified OpenID Connect provider library (IdentityServer3) that utilizes:

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

- OAuth 2.0 Dynamic Client Registration Management Protocol (rfc7592)

3.4 Operator privileges

The operator can log in once the operator privilege for the Web Access-Editor has been granted.

The display of menu items and the ability to use functions are controlled by the respective operator privileges.

For more details on operator privileges, please refer to the main manual for the PC program.

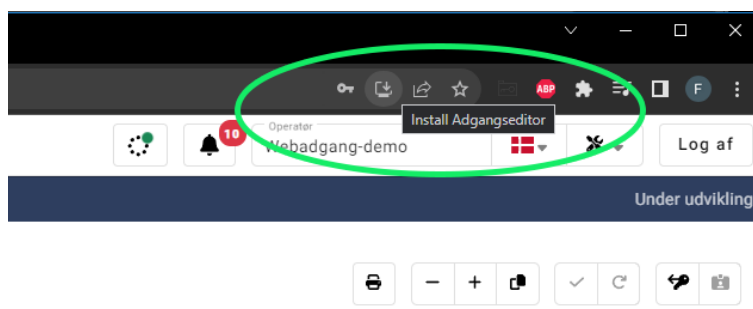
4. Installation at pc and smartphone

The Web Access Editor can be installed on a PC, tablet, or phone. The Web Access Editor is opened for the first time in a web browser by entering the DNS name (web address) or the public IP address.

Installation from a web browser is possible when the Web Access Editor security certificate is trusted; see this section of this manual. 3.1 Webserver.

4.1 PC

The Web Access Editor is installed from a web browser, such as Google Chrome, by clicking the [+] button, [Install UniLock Web Access Editor]:



On a PC, the Web Access-Editor is installed as a standard Windows App.

4.2 Phone and tablet

When the Web Access Editor is opened, "Add to Home Screen" appears automatically. On mobile platforms, the Web Access Editor is installed as a standard app.

If necessary, manual installation on Android is performed via the web browser: [Menu], [Add to Home screen].

If necessary, manual installation on Apple devices is performed in Safari via [Menu] > [Add to Home Screen].

5. Graphical monitoring

Based on a building layout, Graphical Monitoring provides a quick, comprehensive overview of the entire installation's current operating status, making monitoring a manageable and easily accessible task.



Various pages can be created, allowing the operator to select pages from the menu in the top-left corner or use navigation icons.

Dynamic icons

Graphical monitoring consists of a background image displaying the current status of doors, DAS, intrusion system, inputs, outputs and shared exceptions using dynamic icons that can be freely positioned on the background image.

Online overview using a standard web browser

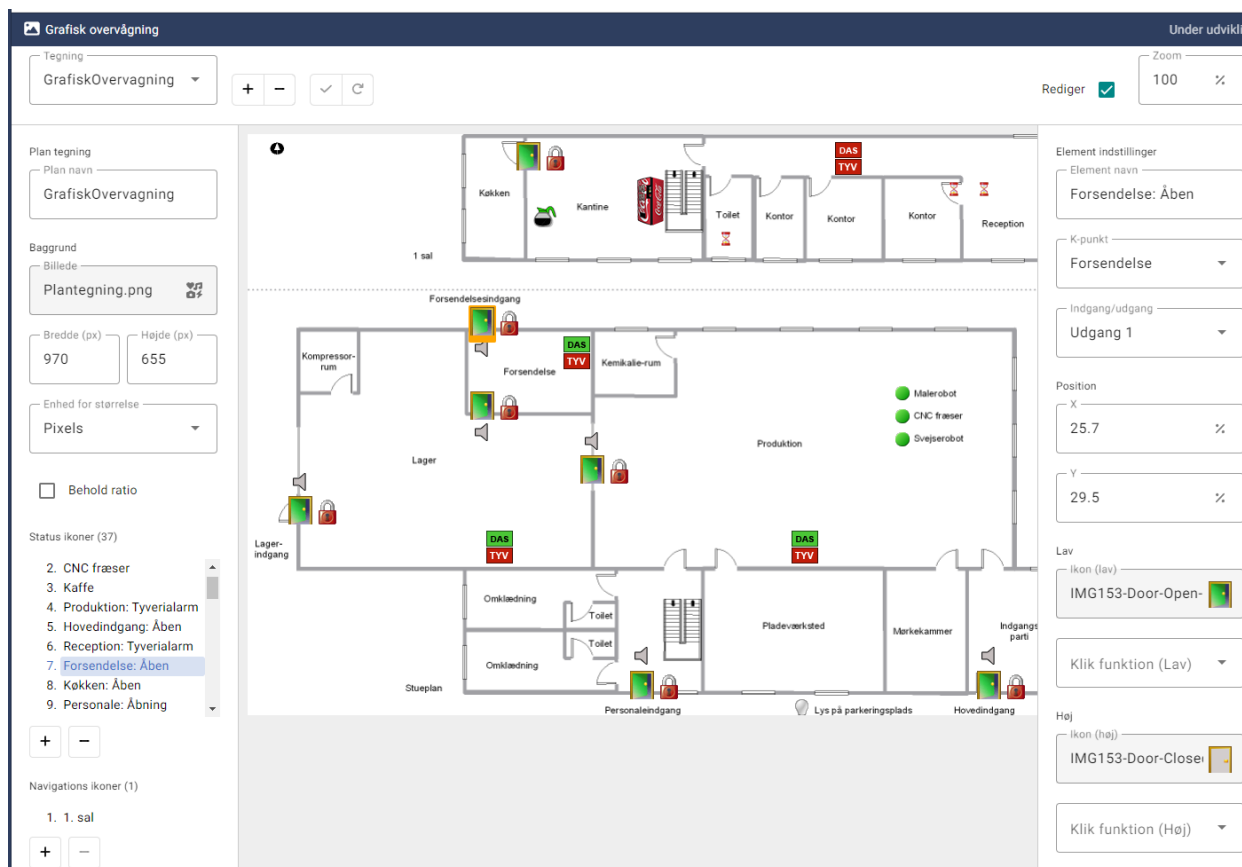
Graphical monitoring is built into the Web Access-Editor website. The Web Access-Editor continuously retrieves current status information from the system's built-in web server and presents this information to the operator in the form of dynamic icons on the background image.

Remote control

By clicking the icons at the k-point, it is possible to unlock or lock the door, arm or disarm the intrusion system and control shared exceptions.

Configuration

Since the graphical monitoring feature is based on one or more building drawings of the installation in question, it must be adapted to the specific installation. Editing is performed by selecting [Edit] in the top right corner.



Add a new floor plan by pressing [+].

You can add your own images (backgrounds/icons) by selecting the background or icon, after which you can add new images to the database's image library.

Items requiring operator attention (such as doors, DAS, burglar alarms, and inputs and outputs) are represented by icons that can be freely positioned on the background image. Commands can be assigned to each icon, enabling actions such as unlocking/locking and arming/disarming the DAS via mouse clicks.