Experts in
Flexible Feeding Systems

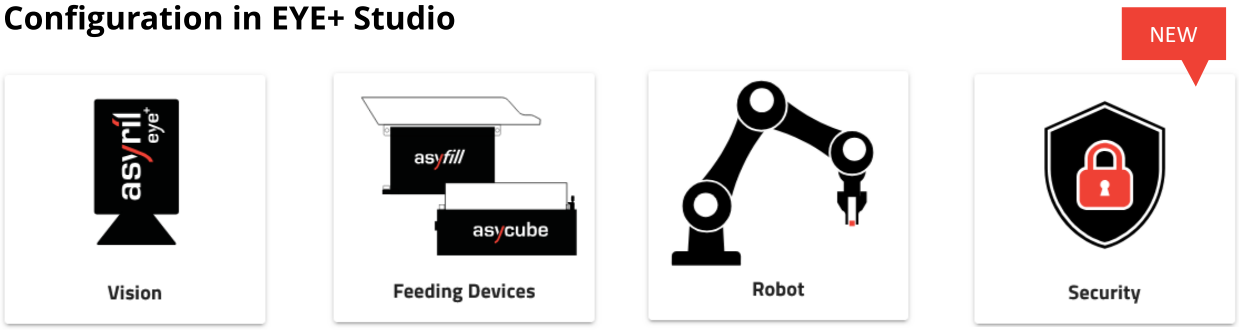
How to ensure enhanced security and user protection in a web-based interface: Introducing HTTPS certificates and user access control

In today's digital age, security is paramount. As businesses increasingly rely on web interfaces, the need for robust security measures has never been so important. In response to this situation, the latest product enhancements of EYE+ smart control system focus on two critical areas:

- Secure connections via HTTPS certificates
- Stringent user access control (UAC)

Part of the new “Security” section in EYE+ Studio, these features do not only safeguard your access to Asyril’s web interface and data. They are also paving the way for future product compliance with newly announced cybersecurity regulations. It includes the Cyber Resilience Act (CRA) that will outline minimum security requirements to consider, both on products and Asyril’s security competences as a company, in the perspective of CE-Marks as of mid 2027 (EU expectations).

Configuration in EYE+ Studio



The importance of secure connections

What is HTTPS?

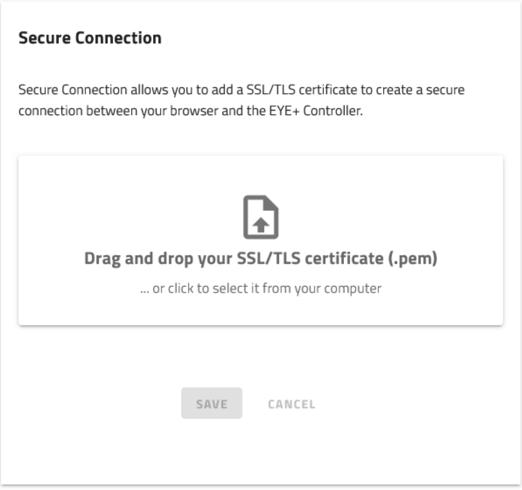
Hypertext Transfer Protocol Secure (HTTPS) is an extension of HTTP. It uses an encryption to secure data transfer between a user's browser and the server, preventing eavesdropping.

Benefits of HTTPS certificates

1. **Data integrity:** HTTPS prevents data from being tampered with during transfer.
2. **Confidentiality:** Encryption ensures that only intended recipients can read the data.
3. **Authentication:** HTTPS verifies that users are communicating with the intended website.

HTTPS in EYE+ smart control system

We simplified the process of enabling HTTPS on the EYE+ platform, allowing users to upload HTTPS certificates generated by their IT departments. This ensures that data transfers between EYE+ Studio and users are encrypted and secured, providing peace of mind and compliance with regulatory standards. Enabling this feature and adding an SSL/TLS certificate will typically encrypt the password you enter via the user access control to access EYE+ Studio. You are then sure that nobody can read this password and unintentionally give access to other users connected to your company network.



Secure Connection

Secure Connection allows you to add a SSL/TLS certificate to create a secure connection between your browser and the EYE+ Controller.

Drag and drop your SSL/TLS certificate (.pem)

... or click to select it from your computer

SSL/TLS certificates are not topics that all companies are aware of. Asyril wants to make sure that each user of EYE+ smart control system can benefit from this secure feature. We explain how these certificates work and how to generate them. Further information can be found in the chapter “Knowledge database” of the EYE+ user manual.

User access control: protecting your interface

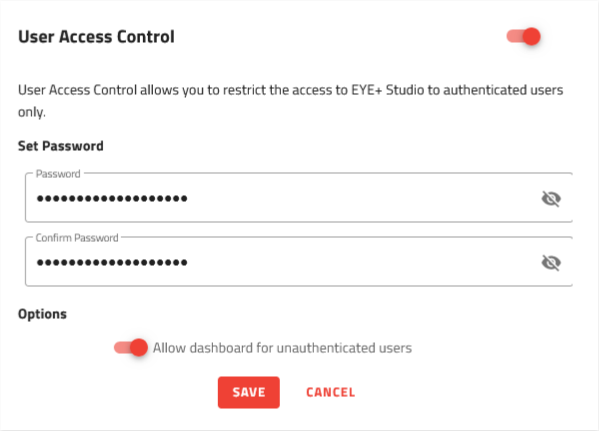
Even if the EYE+ smart control system does not require a direct connection to the company network, unauthorized access is a significant threat to any system. By restricting access to authorized users only, Asyril can prevent malicious activities and ensure that sensitive data remains secure.

Benefits of EYE+ user access control

1. **Password protection:** Users can set a strong password to protect the user interface (UI).
2. **User authentication:** Only authenticated users can access the system, reducing the risk of unauthorized access.
3. **Access levels:** Authenticated users can be granted access to the dashboard, ensuring that they only have access to necessary information during production.

Enable user access control in EYE+

EYE+ Studio provides step-by-step instructions to guide the users through the configuration of the user access control. This feature allows you to either protect the complete interface via a **single password** defined by the user, or to only give access to the dashboard to operators who monitor different metrics during the production.



User Access Control

User Access Control allows you to restrict the access to EYE+ Studio to authenticated users only.

Set Password

Password: ••••••••••••••••••

Confirm Password: ••••••••••••••••••

Options

Allow dashboard for unauthenticated users

How to use the user access control according to your needs?

The user access control feature in EYE+ can be used to protect the user interface against unqualified persons, but also to prevent malicious users to penetrate the system and break critical elements to the production. For example, by editing a recipe or modifying system settings, enabling the secure connection via HTTPS certificate before typing a password is typically a good practice to ensure an encryption of the password. Defining a strong password will also reduce the risks of giving unintentional access to malicious people. To help users to ensure security, good practices of password definition are included in the EYE+ user manual.

Secure your system today and stay ahead in the digital security landscape

The introduction of HTTPS certificates and EYE+ user access control features mark a significant step forward in the direction of security. By protecting communications between the EYE+ controller and EYE+ Studio, restricting access to authorized users, and documenting cybersecurity good practices, Asyril provides a secure and reliable web interface for customers.

The security of our users has been considered since the inception of the product, typically by carefully selecting Asyril's suppliers both for software, hardware, and securing third party involvement, to avoid any repercussions on customer's facilities. The images acquired by EYE+ are being kept strictly on the machine network and the machine does not need to be connected to the cloud apart for remote maintenance purposes.

Cyber threat landscape is rapidly evolving and requires compliance with regulations such as the Cyber Resilience Act (CRA) that is becoming increasingly vital for many industries. By mid 2027, it will even become mandatory for maintaining the CE-Marks. Asyril is taking a proactive approach to meet CRA criteria, focusing on protecting our customers from any cybersecurity issues. Our R&D team constantly aligns our product portfolio with these regulations and follows a clear roadmap to ensure that our customers are also prepared well in advance. If you have any cybersecurity requirements, please feel free to contact us through our technical centers.

For more information on how to use EYE+ security features, please refer to Asyril's online documentation, update your EYE+ smart control system or experience it yourself via EYE+ simulation.

EYE+ documentation: https://doc.eyeplus.asyril.com/en/5.0/index.html

EYE+ simulation: https://register.eyeplus.asyril.com/

Switzerland - HQ
info@asyril.com
+41 26 420 42 42

US – Subsidiary
info.us@asyril.com
+1 612 294-6886

Japan – Subsidiary
info.jp@asyril.com
+81 (45) 479-9393

Germany – Subsidiary
info.de@asyril.com
+49 781 12552870

Singapore – Subsidiary
info.sg@asyril.com
+65 98361678

www.asyril.com