

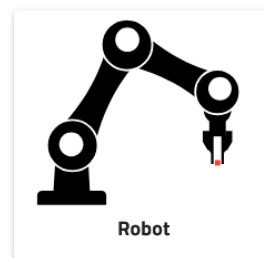
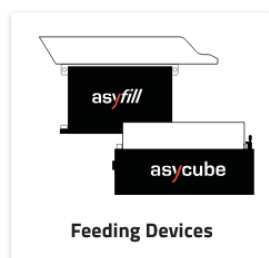
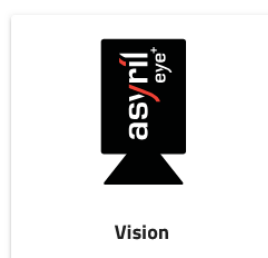
Verstärkte Sicherheit und Benutzerschutz in einer Webschnittstelle: Einführung von HTTPS-Zertifikaten und Benutzerzugriffskontrolle

Im heutigen digitalen Zeitalter ist Sicherheit wichtiger denn je. Da Unternehmen zunehmend auf Webschnittstellen setzen, ist der Bedarf an robusten Sicherheitsmassnahmen so hoch wie nie zuvor. Als Reaktion auf diese Entwicklung wurde das EYE+ Smart Control System in zwei entscheidenden Bereichen verbessert:

- Sichere Verbindungen mit HTTPS-Zertifikaten
- Strikte Benutzerzugriffskontrolle

Diese Funktionen sind Teil des neuen Abschnitts «Sicherheit» in EYE+ Studio und schützen nicht nur Ihren Zugriff auf die Weboberfläche und die Daten von Asyril, sondern ebnen auch den Weg für die Konformität des Produkts mit den neu angekündigten Cybersicherheitsvorschriften. Diese umfassen insbesondere den Cyber Resilience Act (CRA), der Mindestanforderungen an die Sicherheit festlegt, die sowohl für Produkte als auch in Bezug auf die Sicherheitskompetenzen von Asyril als Unternehmen im Hinblick auf die Vergabe von CE-Kennzeichnungen ab Mitte 2027 zu berücksichtigen sind (EU-Anforderungen).

Konfiguration in EYE+ Studio



Die Bedeutung sicherer Verbindungen

Was ist HTTPS?

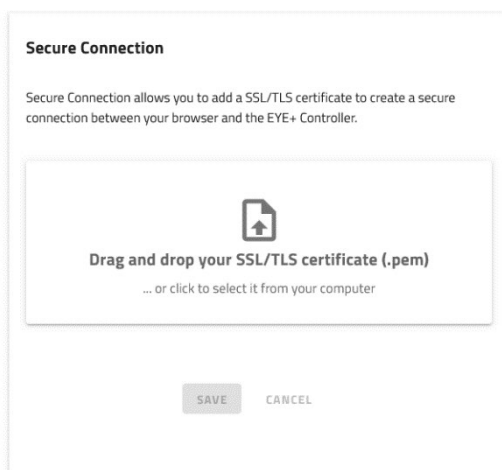
Das sichere Hypertext-Übertragungsprotokoll (Hypertext Transfer Protocol Secure, HTTPS) ist eine Erweiterung von HTTP. Es verwendet eine Verschlüsselung, um Daten zwischen dem Browser eines Benutzers und dem Server geschützt und abhörsicher zu übermitteln.

Vorzüge von HTTPS-Zertifikaten

- 1. Datenintegrität:** HTTPS verhindert, dass Daten während der Übertragung manipuliert werden.
- 2. Vertraulichkeit:** Die Verschlüsselung stellt sicher, dass nur die beabsichtigten Empfänger die Daten lesen können.
- 3. Authentifizierung:** HTTPS stellt sicher, dass die Benutzer tatsächlich mit der beabsichtigten Website kommunizieren.

HTTPS im EYE+ Smart Control System

Wir haben den Prozess zur Implementierung von HTTPS auf der EYE+ Plattform vereinfacht, sodass Benutzer HTTPS-Zertifikate hochladen können, die von ihren IT-Abteilungen generiert wurden. Dadurch wird sichergestellt, dass die Datenübertragung zwischen EYE+ Studio und den Benutzern verschlüsselt und sicher ist, sodass Sie unbesorgt arbeiten können und zugleich die Einhaltung geltender Vorschriften gewährleistet ist. Die Aktivierung dieser Funktion und das Hinzufügen eines SSL/TLS-Zertifikats ermöglicht z. B. die Verschlüsselung des Passworts, das Sie über die Benutzerzugriffskontrolle für den Zugriff auf EYE+ Studio eingeben. So können Sie sicher sein, dass niemand dieses Passwort lesen und unbeabsichtigt anderen Benutzern, die mit Ihrem Firmennetzwerk verbunden sind, Zugriff gewähren kann.



Nicht alle Unternehmen sind mit SSL/TLS-Zertifikaten vertraut. Asyril möchte sicherstellen, dass alle Benutzer des EYE+ Smart Control Systems von dieser sicheren Funktion profitieren können. Wir erklären deshalb, wie diese Zertifikate funktionieren und wie sie erstellt werden. Weitere Informationen finden Sie im Kapitel «Wissensdatenbank» des EYE+ Benutzerhandbuchs.

Benutzerzugriffskontrolle: Schützen Sie Ihre Schnittstelle

Auch wenn das EYE+ Smart Control System keine direkte Verbindung zum Firmennetzwerk erfordert, stellt der unbefugte Zugriff eine erhebliche Bedrohung für jedes System dar. Durch die Beschränkung des Zugriffs auf befugte Benutzer kann Asyril böswillige Aktivitäten verhindern und die Sicherheit sensibler Daten gewährleisten.

Vorzüge der EYE+ Benutzerzugriffskontrolle

- 1. Passwortschutz:** Benutzer können zum Schutz der Benutzeroberfläche ein starkes Passwort festlegen.
- 2. Benutzerauthentifizierung:** Nur authentifizierte Benutzer können auf das System zugreifen, wodurch das Risiko eines unbefugten Zugriffs verringert wird.
- 3. Zugriffsstufen:** Authentifizierten Benutzern kann Zugriff auf das Dashboard gewährt werden, wodurch sichergestellt wird, dass sie während der Produktion nur auf die erforderlichen Informationen zugreifen können.

Benutzerzugriffskontrolle in EYE+ aktivieren

EYE+ Studio bietet eine Schritt-für-Schritt-Anleitung, welche die Benutzer durch die Konfiguration der Benutzerzugriffskontrolle führt. Mit dieser Funktion können Sie entweder die gesamte Benutzeroberfläche durch **ein einziges**, benutzerdefiniertes **Passwort** schützen oder Benutzern, die während der Produktion verschiedene Parameter überwachen, ausschliesslich Zugriff auf das Dashboard gewähren.

The screenshot shows the 'User Access Control' configuration window. At the top, there is a toggle switch labeled 'User Access Control' which is currently turned on (red). Below this, a text box explains: 'User Access Control allows you to restrict the access to EYE+ Studio to authenticated users only.' The 'Set Password' section contains two input fields: 'Password' and 'Confirm Password', both with masked characters (dots) and a toggle for visibility. The 'Options' section has a toggle switch labeled 'Allow dashboard for unauthenticated users' which is currently turned off. At the bottom right, there are 'SAVE' and 'CANCEL' buttons.

Stellen Sie die Benutzerzugriffskontrolle entsprechend Ihren Bedürfnissen ein

Die Benutzerzugriffskontrolle von EYE+ kann verwendet werden, um unqualifizierten Personen den Zugriff auf die Benutzeroberfläche zu verwehren, aber auch um böswillige Eingriffe in das System und die Störung von produktionsrelevanten Elementen wie die Änderung eines Rezepts oder der Systemeinstellungen zu verhindern. Das Einrichten einer sicheren Verbindung mit einem HTTPS-Zertifikat vor der Eingabe eines Passworts wird beispielsweise empfohlen, um die Verschlüsselung des Passworts zu gewährleisten. Das Festlegen eines sicheren Passworts verringert auch das Risiko, dass böswilligen Personen unbeabsichtigt Zugang gewährt wird. Das EYE+ Benutzerhandbuch enthält zur Unterstützung der Benutzer bei der Aufrechterhaltung der Sicherheit Empfehlungen für die Festlegung eines sicheren Passworts.

Schützen Sie jetzt Ihr System und bleiben Sie in Bezug auf digitale Sicherheit einen Schritt voraus

Die Einführung von HTTPS-Zertifikaten und der EYE+ Benutzerzugriffskontrolle stellt einen bedeutenden Schritt hin zu mehr Sicherheit dar. Durch den Schutz der Kommunikation zwischen dem EYE+ Controller und EYE+ Studio, die Beschränkung des Zugriffs auf autorisierte Benutzer und die Beschreibung guter Praktiken im Bereich der Cybersicherheit bietet Asyril seinen Kunden eine sichere und zuverlässige Webschnittstelle.

Die Sicherheit unserer Benutzer war von Anfang an Teil der Produktentwicklung, insbesondere durch die sorgfältige Auswahl unserer Software- und Hardwarelieferanten und die Einbeziehung von Drittunternehmen, um jeglichen Auswirkungen auf die Einrichtungen unserer Kunden vorzubeugen. Die von EYE+ aufgenommenen Bilder werden ausschliesslich im Maschinennetzwerk gespeichert und die Maschine muss ausser zu Fernwartungszwecken nicht mit der Cloud verbunden werden.

Die Cyber-Bedrohungslandschaft verändert sich rasch, was die Einhaltung von Vorschriften wie dem Cyber Resilience Act (CRA) erfordert, die für viele Wirtschaftszweige immer wichtiger werden. Ab Mitte 2027 ist die Einhaltung dieser Vorschriften sogar eine Voraussetzung für die Vergabe der CE-Kennzeichnung. Asyril verfolgt einen proaktiven Ansatz, um die CRA-Kriterien zu erfüllen und seine Kunden vor jeglichen Cyber-Sicherheitsproblemen zu schützen. Unser F&E-Team stimmt unser Produktangebot ständig auf diese Vorschriften ab und verfolgt eine klare Strategie, um sicherzustellen, dass auch unsere Kunden rechtzeitig vorbereitet sind. Wenn Sie besondere Anforderungen an die Cybersicherheit haben, können Sie sich gerne über unsere technischen Zentren an uns wenden.

Für weitere Informationen zur Nutzung der EYE+ Sicherheitsfunktionen lesen Sie bitte die Online-Dokumentation von Asyril, aktualisieren Sie Ihr EYE+ Smart Control System oder überzeugen Sie sich selbst anhand der EYE+ Simulation.

EYE+ Dokumentation: <https://doc.eyepius.asyril.com/de/5.0/index.html>

EYE+ Simulation: <https://register.eyepius.asyril.com/>

asyril



Schweiz - Hauptsitz

info@asyril.com

+41 26 420 42 42

USA - Niederlassung

info.us@asyril.com

+1 612 294-6886

Japan - Niederlassung

info.jp@asyril.com

+81 (45) 479-9393

Deutschland - Niederlassung

info.de@asyril.com

+49 781 12552870

Singapur - Niederlassung

info.sg@asyril.com

+65 98361678