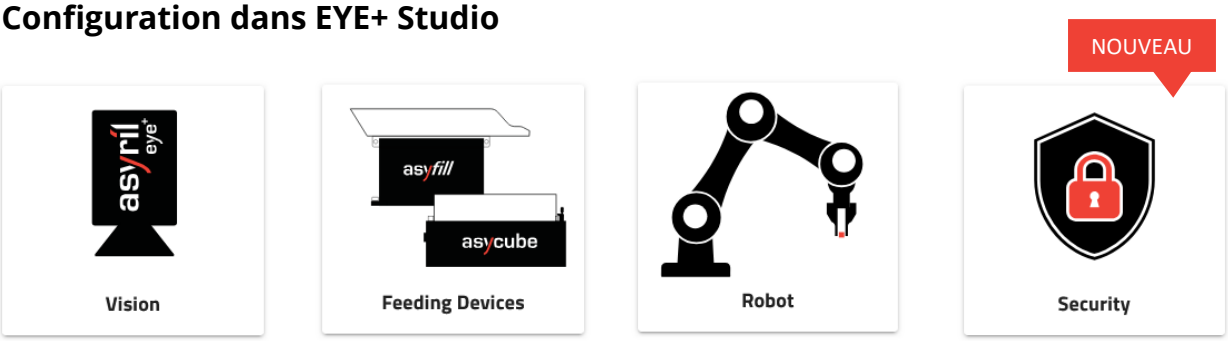
Comment assurer une sécurité renforcée et la protection des utilisateurs dans une interface web: Certificats HTTPS et contrôle d'accès utilisateur

Dans le monde numérique d'aujourd'hui, la sécurité est primordiale. Les entreprises faisant de plus en plus appel à des interfaces web, le besoin de mesures de sécurité robustes n'a jamais été aussi important. En réponse à cette évolution, des améliorations ont été apportées au système de contrôle intelligent EYE+ dans deux domaines clé:

- Connexions sécurisées au moyen de certificats HTTPS
- Contrôle d'accès utilisateur strict

Intégrées à la nouvelle section « Sécurité » d'EYE+ Studio, ces fonctionnalités protègent non seulement votre accès à l'interface web et aux données d'Asyril, mais permettront également de garantir la conformité des produits avec les nouvelles normes de cybersécurité récemment annoncées. Celles-ci comprennent notamment le règlement sur la cyberrésilience (Cyber Resilience Act, CRA) qui définira les exigences minimales en matière de sécurité applicables aux produits et aux compétences d'Asyril en tant qu'entreprise en vue de l'obtention du marquage CE à compter du milieu de l'année 2027 (exigences de l'UE).

Configuration dans EYE+ Studio



Importance des connexions sécurisées

Qu'est-ce que le protocole HTTPS?

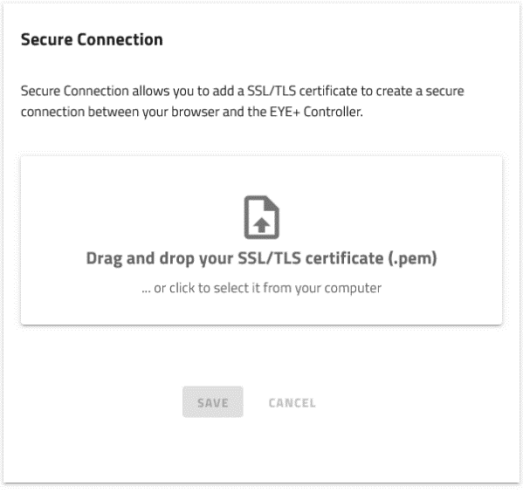
Le protocole de transfert hypertextuel sécurisé (Hypertext Transfer Protocol Secure, HTTPS) est une extension du protocole HTTP. Il utilise un cryptage pour sécuriser le transfert de données entre le navigateur de l'utilisateur et le serveur, empêchant ainsi toute écoute de la communication.

Avantages des certificats HTTPS

1. **Intégrité des données:** Le protocole HTTPS empêche la manipulation des données pendant le transfert.
2. **Confidentialité:** Le cryptage garantit que seuls les destinataires souhaités peuvent lire les données.
3. **Authentification:** Le protocole HTTPS vérifie que les utilisateurs communiquent bien avec le site web souhaité.

HTTPS dans le système de contrôle intelligent EYE+

Nous avons simplifié le processus de mise en œuvre du protocole HTTPS sur la plateforme EYE+, permettant ainsi aux utilisateurs d'utiliser des certificats HTTPS générés par leurs services informatiques. Les transferts de données entre EYE+ Studio et les utilisateurs sont ainsi chiffrés et sécurisés pour un travail en toute sérénité dans le respect des normes réglementaires. L'activation de cette fonctionnalité et l'ajout d'un certificat SSL/TLS permettent par exemple de crypter le mot de passe que vous entrez via le contrôle d'accès utilisateur pour accéder à EYE+ Studio. Vous avez alors la certitude que personne ne peut lire ce mot de passe et donner involontairement accès à d'autres utilisateurs connectés à votre réseau d'entreprise.



Toutes les entreprises ne sont pas familières avec les certificats SSL/TLS. Asyril tient à s'assurer que chaque utilisateur du système de contrôle intelligent EYE+ puisse bénéficier de cette fonctionnalité sécurisée. Nous expliquons donc le fonctionnement de ces certificats et comment les générer. De plus amples informations à ce sujet sont disponibles dans le chapitre « Base de connaissances » du manuel d'utilisation EYE+.

Contrôle d’accès utilisateur: protégez votre interface

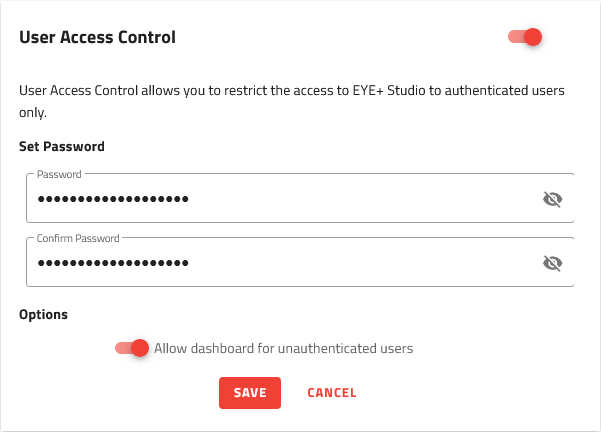
Même si le système de contrôle intelligent EYE+ ne nécessite pas une connexion directe au réseau d'entreprise, l'accès non autorisé est une menace importante pour tout système. En limitant l'accès aux seuls utilisateurs autorisés, Asyril peut prévenir les activités malveillantes et assurer que les données sensibles restent sécurisées.

Avantages du contrôle d’accès utilisateur EYE+

1. **Protection par mot de passe:** Les utilisateurs peuvent définir un mot de passe sûr pour protéger l'interface utilisateur.
2. **Authentification de l'utilisateur:** Seuls les utilisateurs authentifiés peuvent accéder au système, ce qui réduit le risque d'accès non autorisé.
3. **Niveaux d'accès:** Un accès au tableau de bord peut être accordé aux utilisateurs authentifiés, ce qui garantit qu'ils n'ont accès qu'aux informations nécessaires pendant la production.

Activer le contrôle d’accès utilisateur dans EYE+

EYE+ Studio fournit des instructions étape par étape pour guider les utilisateurs dans la configuration du contrôle d'accès utilisateur. Cette fonctionnalité vous permet soit de protéger l'ensemble de l'interface par un **mot de passe unique** défini par l'utilisateur, soit de donner accès uniquement au tableau de bord aux opérateurs qui supervisent différents paramètres en cours de production.



Comment utiliser le contrôle d’accès utilisateur en fonction de vos besoins

La fonction de contrôle d'accès utilisateur EYE+ peut être utilisée pour empêcher que des personnes non qualifiées n'accèdent à l'interface utilisateur, mais aussi pour prévenir toute intrusion malveillante dans le système et la perturbation d'éléments essentiels à la production comme la modification d'une recette ou des paramètres du système. La mise en place d'une connexion sécurisée à l'aide d'un certificat HTTPS avant de saisir un mot de passe est par exemple recommandé afin de garantir le cryptage du mot de passe. La définition d'un mot de passe sûr permet également de réduire les risques de donner involontairement accès à des personnes malveillantes. Dans le but d’aider les utilisateurs à garantir la sécurité du système, le guide de l'utilisateur EYE+ contient des recommandations concernant la définition d'un mot de passe sûr.

Sécurisez votre système dès aujourd'hui et gardez une longueur d'avance en matière de sécurité numérique

L'introduction des certificats HTTPS et des fonctions de contrôle d'accès utilisateur EYE+ marque une étape importante dans le domaine de la sécurité. Grâce à la protection de la communication entre le contrôleur EYE+ et EYE+ Studio, à la limitation de l'accès aux utilisateurs autorisés et à la définition de bonnes pratiques en matière de cybersécurité, Asyril fournit une interface web sûre et fiable à ses clients.

La sécurité de nos utilisateurs a été prise en compte dès la création du produit, notamment par une sélection minutieuse de nos fournisseurs de logiciels et de matériel, ainsi qu'en s'assurant de l'implication de prestataires tiers, afin d'éviter toute répercussion sur les installations de nos clients. Les images acquises par EYE+ sont conservées strictement sur le réseau de la machine et celle-ci n'a pas besoin d'être connectée au cloud, hormis à des fins de maintenance à distance.

Le contexte des cybermenaces évolue rapidement et exige de se conformer à des réglementations, telles que la loi sur la cyberrésilience (Cyber Resilience Act, CRA), qui deviennent de plus en plus vitales pour de nombreux secteurs d'activité. D'ici à la mi-2027, le respect de cette réglementation deviendra même obligatoire pour le maintien du marquage CE. Asyril adopte une approche proactive pour répondre aux critères du CRA en mettant l'accent sur la protection de ses clients contre tout problème de cybersécurité. Notre équipe R&D ajuste constamment notre gamme de produits à ces réglementations et suit une feuille de route claire pour s'assurer que nos clients soient également préparés bien à l'avance. Si vous avez des exigences particulières en matière de cybersécurité, n'hésitez pas à nous contacter par l'intermédiaire de nos centres techniques.

Pour plus d'informations sur l'utilisation des fonctions de sécurité d'EYE+, veuillez consulter la documentation en ligne d'Asyril et mettre à jour votre système de contrôle intelligent EYE+. Vous pouvez également découvrir nos produits par vous-même grâce à la simulation EYE+.

Documentation EYE+: https://doc.eyeplus.asyril.com/fr/5.0/index.html

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

Suisse - Siège

info@asyril.com

+41 26 420 42 42

USA - Filiale

info.us@asyril.com

+1 612 294-6886

Japon - Filiale

info.jp@asyril.com

+81 (45) 479-9393

Allemagne - Filiale

info.de@asyril.com

+49 781 12552870

Singapour - Filiale

info.sg@asyril.com

+65 98361678