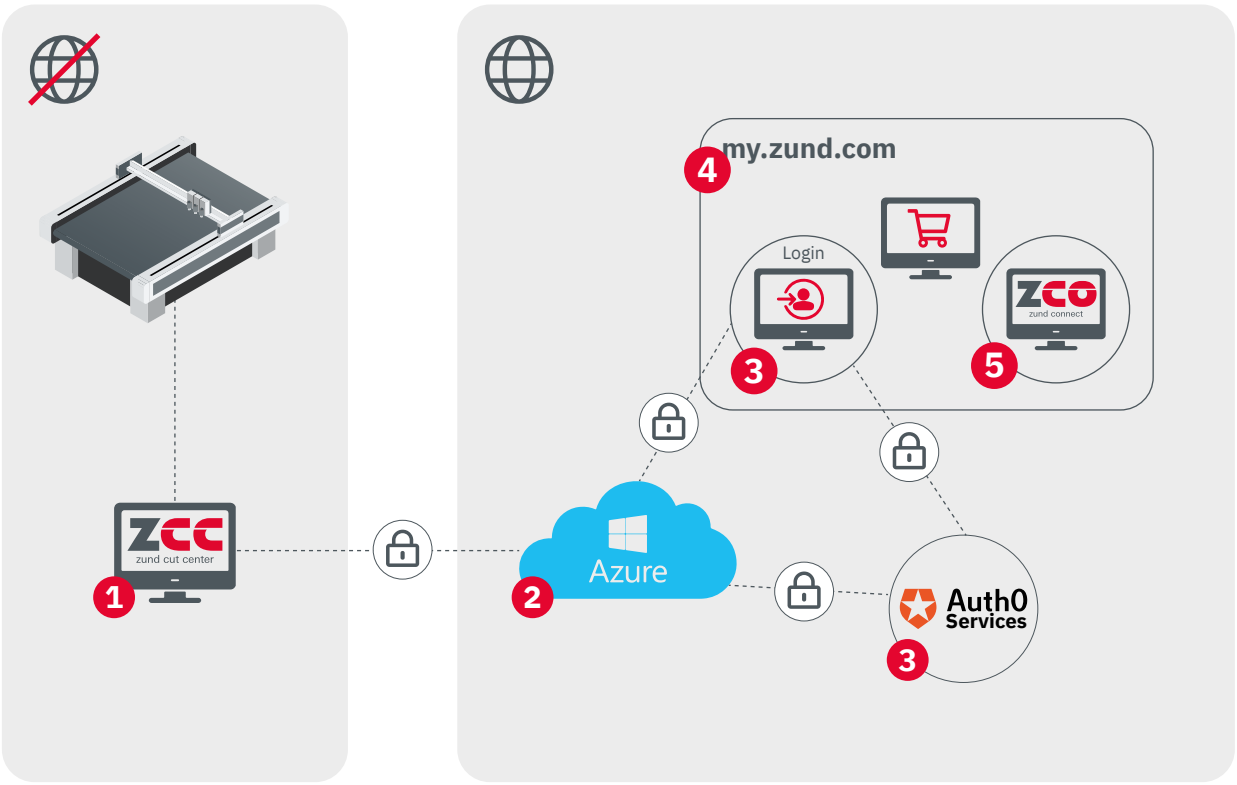
Sécurité des données - Zünd Connect

Il est garanti par l'utilisation de normes et de composants de sécurité éprouvés que les données et les accès jouissent d'une sécurité élevée. Cela protège les données d'une utilisation malveillante en dehors de la politique de confidentialité. De même, les données sont protégées ainsi de la meilleure manière possible contre une destruction volontaire par des tiers. Elles sont exclusivement envoyées par Cutter dans le Cloud. Il n'y a aucun accès depuis le Cloud au Cutter.



Chaque connexion est sécurisée avec TLS 1.2 (Transport Layer Security) selon RFC 5246.

Sub-System 1 : Fonctionnement du Cutter
Avec l'installation du Zünd Cut Center (ZCC), un proxy IdO est installé pour Zünd Connect. L'utilisateur doit explicitement accepter l'installation du proxy. Ce proxy tourne comme service Windows en arrière-plan et inclut une mémoire intermédiaire locale des données. Des données qui ne peuvent pas être transférées directement sont enregistrées sur un disque dur protégé contre les défaillances dans cette mémoire intermédiaire. Cela peut être le cas par exemple lorsque la connexion au Hub IdO est provisoirement interrompue.
Le proxy communique avec le Hub IdO via AMQP :5671 et https :443 par le biais d'une connexion cryptée TLS1.2. L'authentification passe par une clé univoque qui est générée à l'installation.

Sub-System 2 : Azure Cloud
Les données sont enregistrées et traitées dans une instance dédiée de Microsoft Azure Cloud. Cela assurer que la mise à jour de sécurité la plus actuelle de Microsoft est faite et garantit une stabilité et une sécurité élevées.
Tous les accès de base de données backend sont protégés par mot de passe. Les mots de passe utilisés à cet effet sont protégés dans un Key Vault prévu spécialement à cet effet dans Azure Cloud. Les accès aux données du tableau de bord dans le Backend sont uniquement possibles avec le jeton d'accès temporaire généré à la connexion de l'utilisateur.

Sub-System 3 : Authentification de l'utilisateur
Pour que l'utilisateur puisse utiliser Zünd Connect, il doit se connecter au moyen de son identifiant et du mot de passe sous My Zünd. Zünd mise pour l'inscription, la connexion et la restauration du mot de passe sur la solution de tiers éprouvée et sûr d'Auth0 pour garantir les normes de sécurité les plus strictes.

Sub-System 4: my.zund.com
Zünd Connect est intégré dans My Zünd, le portail client de Zünd. Il existe ainsi une connexion de l'utilisateur valide à l'échelle du portail.

Sub-System 5 : Zünd Connect
Les tableaux de bord peuvent être visualisés depuis tout ordinateur de bureau avec un navigateur Internet actuel. Pour ce faire, le navigateur Internet doit être en mesure d'afficher des pages Internet basées sur http.

Hostnames ZundConnectProxy

Log data, via HTTPS (port 443)
dc.services.visualstudio.com

File upload (e.g. support report, .zcc-Files), via HTTPS (port 443)
zuend-iot-prod-hub.azure-devices.net
fileprodstore.blob.core.windows.net

Device provisioning (during the installation), via HTTPS (port 443)
zuend-iot-prod-cert-fn.azurewebsites.net

Events, via AMQP (port 5671)
zuend-iot-prod-hub.azure.devices.net

06/2024

Zünd Systemtechnik AG
Industriestrasse 8 | CH-9450 Altstätten | T +41 71 554 81 00 | info@zund.com | www.zund.com

ZÜND
swiss cutting systems