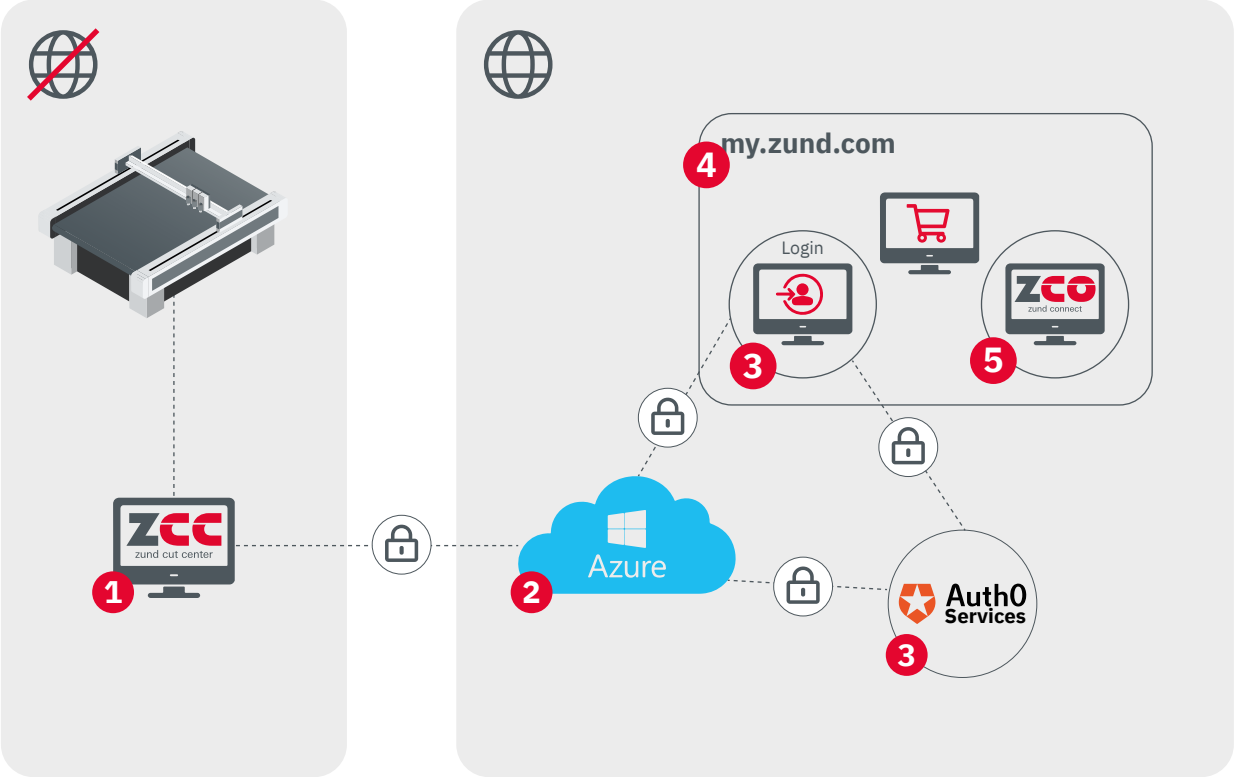
# Seguridad de los datos: Zünd Connect

**El uso y la aplicación de estándares y componentes de seguridad de eficacia probada garantizan que los datos y los accesos gocen de un alto nivel de protección. De este modo, se protegen los datos contra una utilización maliciosa que incumpla la Directiva europea en materia de protección de datos. Asimismo, los datos se protegen de la mejor forma posible frente a la destrucción intencionada de terceras personas. Los datos se envían a la nube exclusivamente desde la mesa de corte. No puede accederse a la mesa de corte desde la nube.**




Todas las conexiones se protegen con el protocolo TLS 1.2 (Transport Layer Security) conforme al estándar RFC 5246.

**Subsistema 1: funcionamiento de la mesa de corte**
Al instalar Zünd Cut Center (ZCC), también se instala un proxy IoT para Zünd Connect. El usuario debe aceptar la instalación del proxy de manera explícita. Este proxy se ejecuta en segundo plano como servicio de Windows y contiene una memoria local caché de datos. Los datos del disco duro que no puedan enviarse de inmediato se almacenan en la memoria caché a prueba de fallos. Esto puede suceder, por ejemplo, cuando la conexión al centro de IoT está interrumpido temporalmente.
El proxy se comunica con el centro de IoT mediante AMQP :5671 y https :443 a través de una conexión cifrada TLS1.2. La autenticación tiene lugar mediante una clave única que se genera durante la instalación.

**Subsistema 2: nube de Azure**
Los datos se almacenan y procesan en una instancia específica de la nube de Microsoft Azure. Esto garantiza en todo momento que se ejecutarán las últimas actualizaciones de seguridad de Microsoft y asegura un alto nivel de seguridad y estabilidad.
Todos los accesos a las bases de datos de la interfaz back-end están protegidos con contraseña. Las contraseñas utilizadas para ello están protegidas en un almacén de claves de la nube de Azure, previsto para tal fin. Solo es posible acceder a los datos de la interfaz back-end desde el panel utilizando los token temporales de acceso, que se generan cuando el usuario inicia sesión.

**Subsistema 3: autenticación del usuario**
Para que el usuario pueda usar Zünd Connect, deberá iniciar sesión utilizando su nombre de usuario y contraseña. Zünd emplea Auth0, una solución segura de un tercer proveedor, para el registro, el inicio de sesión y la recuperación de contraseñas garantizando el cumplimiento de los más estrictos estándares de seguridad.

**Subsistema 4: my.zund.com**
Zünd Connect está integrado en el portal de clientes My Zünd. Así, los usuarios pueden realizar un inicio de sesión válido en el portal.

**Subsistema 5: Zünd Connect**
La eficiencia de la producción, las pérdidas de producción y su origen, así como la visión general de la guillotina, pueden consultarse desde cualquier ordenador de sobremesa con un navegador web actualizado.

### 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