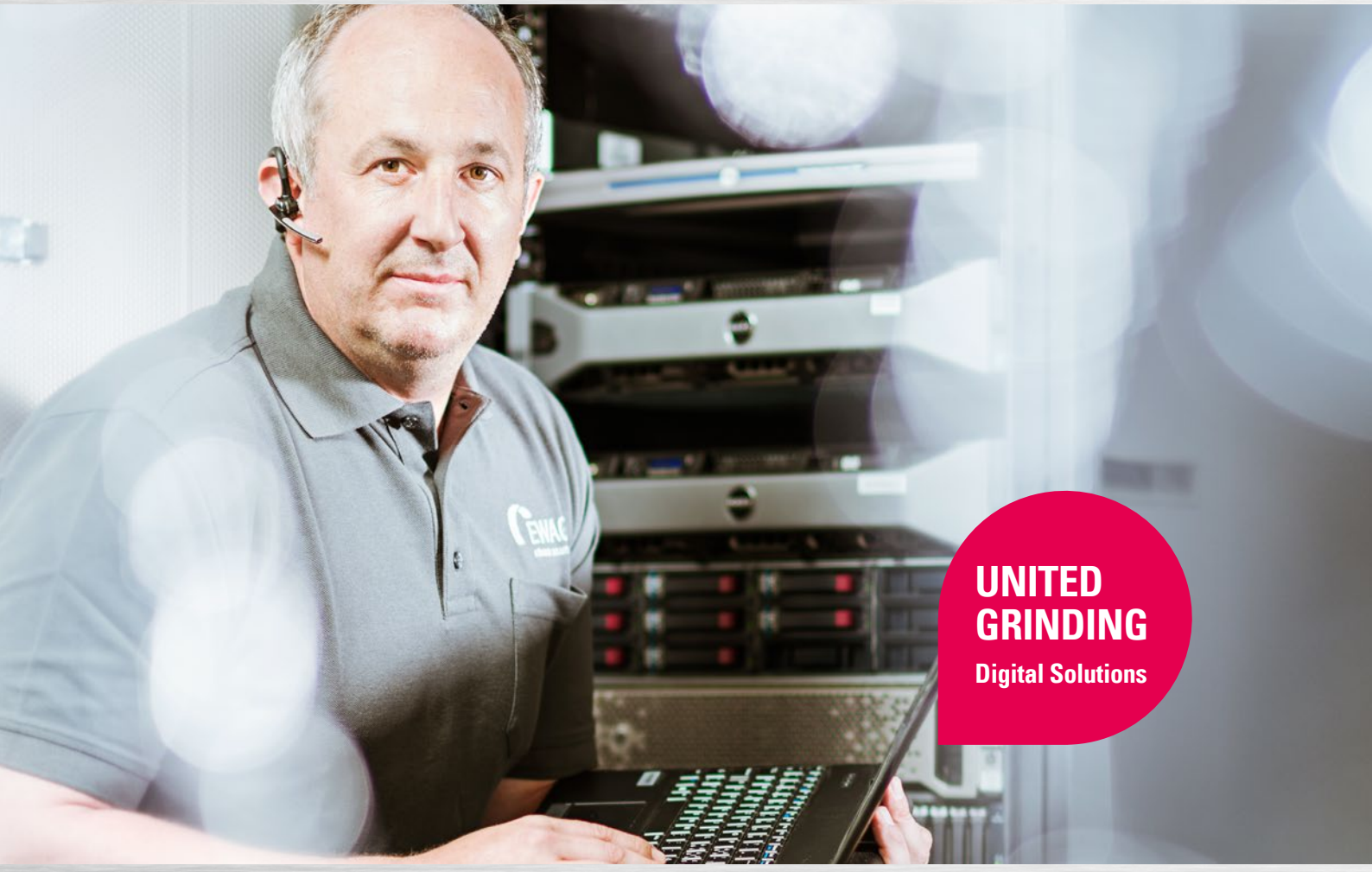


IT security
Your data in safe hands

The most important feature of Internet-based connections is safety.

With UNITED GRINDING Digital Solutions, online access to your machine or system is always quick and secure. Remote maintenance takes place on invitation by the customer only, i.e. the connection is exclusively established with UNITED GRINDING at your initiation.

UNITED GRINDING

As the customer you simply trigger a service request with a mouse-click. A corresponding service ticket appears immediately in the UNITED GRINDING Service Cockpit.

The connection from UNITED GRINDING to your machine is only enabled through the service request you have triggered.

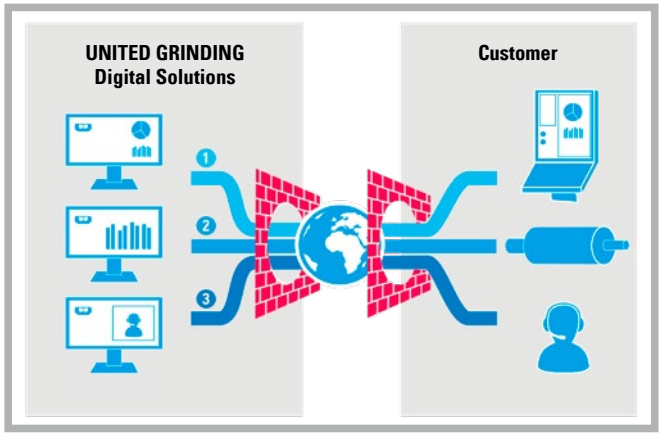
Advantage of reconnection
The connection always originates with you. In the event of a service case, you decide if and when you want to allow remote access to your machine. This means that you (the customer) do not need to make any adjustments or modifications to your security provisions.

This makes our service quick and secure

Once an outgoing connection has been established, communication is enabled in both directions. The tunnel services used here are encrypted as per symmetric AES 256 Bit and SSL with Public Key RSA 2048 Bit. All of the tasks relevant for the customer care employee at UNITED GRINDING during remote access, e.g. data transmission, remote diagnosis or remote programming, are completed in compliance with the respective permissions level via the tunnel services.

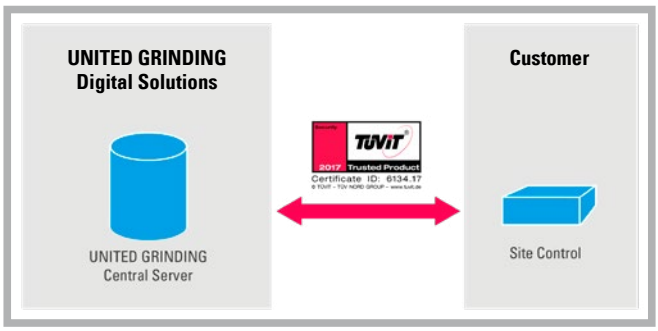
UNITED GRINDING Digital Solutions always set up a secure connection between the Service Cockpit on our side and the Site Control on your machine so that data can be read out by Site Control and checked.

Your benefit: high performance and maximum security.



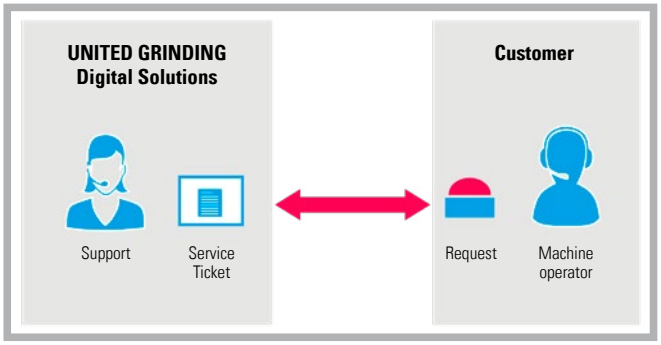
Secure connection

It is vital that connections via the Internet are secure. This is particularly true in a production environment, where the operator of a machine wants to know that the highly sensitive machine data is reliably protected against third-party access. The software used by UNITED GRINDING Digital Solutions has the «Trusted Product»-certificate (TÜViT). This certificate means that the software has been tested in terms of technical safety requirements, architecture and design, and development process and has undergone a weakness analysis and penetration test.



Trouble-shooting

The secure and quick connection with customer machines throughout the world is the basis for efficient trouble-shooting. At your service request, the qualified customer care technician at UNITED GRINDING can access your machine by reconnecting and solve your problems, for example by reading in new data, installing updates or carrying out remote maintenance or changing parameters.



UNITED GRINDING Digital Solutions: Your advantages

- Each connection is established directly and exclusively between you (the customer) and UNITED GRINDING.
- Connections are always limited in terms of time, i.e. they are temporary.
- An exchange takes place exclusively at your initiative and only on precisely defined machines and/or functions.
- Encryption of tunnel services comply with the symmetric AES 256 Bit and SSL with Public Key RSA 2048 Bit (minimum standard: AES with at least 192 key length and TLS 1.2 or higher).
- Identification of each user via personal user name and password. Blocking of the account after a defined number of attempts.
- Secure remote access is based on technical and organisational measures. Risk analysis, inventory-taking, regular function checks, requirements/standards, patch process as well as the evaluation of logs are the standard in UNITED GRINDING software solutions.

UNITED GRINDING Digital Solutions – Q & A

Who decides who can access your plant network and what they can do there?
The management of user rights as well as control over access is always in your hands. Only the respective qualified and authenticated people can connect.

In detail
As a production company, you have to carefully check whenever your systems and machines are accessed remotely and need to be able to prevent access as required. Each user is given a specific login and password. In the event of an unauthorized connection attempt, a black-list mechanism blocks the IP address or user that has initiated the connection request automatically for a limited period of time. Role-specific TLS-(SSL-) certificates are used for the authentication process.

UNITED GRINDING Digital Solutions provide a group and role-based authentication concept. Dynamic port approval and decoupling of the networks prevents malware from accessing your machine.

How can I check what has been done on the system remotely?
All of the processes carried out by UNITED GRINDING Digital Solutions are logged consistently.

In detail
- All service request processes are logged and archived.
- All completed service requests are saved in your system record.
- The use of functions that require Admin rights are logged on your on-site system. The log entries in the so-called prolog files all have a signature and therefore cannot be manipulated unnoticed.

Do I have to open my Firewall for incoming connections?
No. You do not need any incoming connections.

In detail
The key characteristic of UNITED GRINDING Digital Solutions is the structured set-up and disconnection of TLS-secured TCP connections. Connections between the Site Control and our Server are always initiated by Site Control and are therefore, in terms of the Firewall, outgoing connections. This means that no incoming open ports are required. The outgoing TLS (formerly SSL) connection communicates only through one port (standard is 443) and can also be directed via a Web-Proxy-Server. The communication between our Service Cockpit and your Site Control takes place via a tunnel connection following a service request.

A major advantage of the safety technology at UNITED GRINDING Digital Solutions in comparison with classic VPN solutions is the restrictive port management. While all ports have to be opened for the entire connection period in conventional VPN solutions, UNITED GRINDING Digital Solutions opens ports only as required: When end-to-end application tunnels are started, e.g. via Remote Desk programs or SPS programming tools, only those ports relevant to the application are activated for these tunnels - and consequently only for the time during which they are actually being used. You therefore only grant access that is actually required for the specific service case. The UNITED GRINDING Digital Solutions safety technology is used throughout the expansive functions of the UNITED GRINDING Digital Solutions Conference Centre: For secure communication with the technician, we provide video calls, chats, whiteboards including photo-functionality and a VNC conference.

What data do UNITED GRINDING get from me and are the data encrypted?
In the event of remote service, only your connection data are transmitted by default to UNITED GRINDING. The communication between our server and Site Control takes place securely and is encrypted.

In detail
The reconnection takes place through a tunnel, which is not set up until you trigger a service request. This means: If a machine is fitted with a UNITED GRINDING Digital Solutions Customer Cockpit, the entire communication is secured by certificate-based encryption. Data that is also logged by UNITED GRINDING affects only the actual connections, i.e. data such as the access time and connection duration, IP address of the accessing party, etc.

This data are recorded in the log files and transported to our server. Without your consent, sensitive machine data will not leave your company.

Further information

How to set up UNITED GRINDING Digital Solutions safely and easily in your network.
UNITED GRINDING Digital Solutions is based on the Java programming language and consists of software components with a distributed architecture and low resource requirements.

Your machine is equipped with a UNITED GRINDING Digital Solutions Site Control Box.

In detail
The Site Control Box is hardware and serves as the server for the Customer Cockpit. The Customer Cockpit is the graphic user interface for accessing your machine and, even without connecting to our server, provides many useful functions for your machine.

The pre-configured hardware solution UNITED GRINDING Digital Solutions Site Control Box with pre-installed software is installed in the electrical enclosure of your machine and subsequently connected to the machine network.

The UNITED GRINDING Digital Solutions Site Control Box Industrial is a electrical enclosure compatible Industrial PC with secure CentOSLinux-Distribution.

UNITED GRINDING

Any questions? Please contact us.

Secure your individual offer now.
Call us, we would be happy to support you.

Mägerle AG Maschinenfabrik
Fehraltorf, Schweiz
Tel. +41 43 355 66 00
customercare@maegerle.com

Blohm Jung GmbH
Hamburg, Deutschland
Tel. +49 40 7250 02
customercare-hh@blohmjung.com

Blohm Jung GmbH
Göppingen, Deutschland
Tel. +49 7161 612 0
customercare-gp@blohmjung.com

Fritz Studer AG
Thun, Schweiz
Tel. +41 33 439 11 11
info@studer.com

Schaudt Mikrosa GmbH
Leipzig, Deutschland
Tel. +49 341 49 71 123
customercare@schaudtmikrosa.com

Walter Maschinenbau GmbH
Tübingen, Deutschland
Tel. +49 7071 9393 0
customercare@walter-machines.com

Ewag AG
Etziken, Schweiz
Tel. +41 32 613 31 31
customercare@ewag.com

United Grinding North America, Inc.
Miamisburg (Ohio), USA
Tel. +1 937 847 1234
customercare@grinding.com

United Grinding India GmbH
Bangalore, Indien
Tel. +91 80 3025 7600
customercare@grinding.in.ch

United Grinding (Shanghai) Ltd.
Shanghai, China
Tel. +86 21 3958 7333
customercare@grinding.cn