Sécurité informatique
Vos données entre de bonnes mains

La sécurité est l'élément majeur des connexions basées sur l'internet.

UNITED GRINDING Digital Solutions™ autorise l'accès en ligne à votre machine ou votre installation de manièresûre et rapide. La télémaintenance est toujours exécutée sur invitation du client, c'est-à-dire que vous êtes toujours le seul à pouvoir établir la connexion directement avec UNITED GRINDING.

UNITED GRINDING

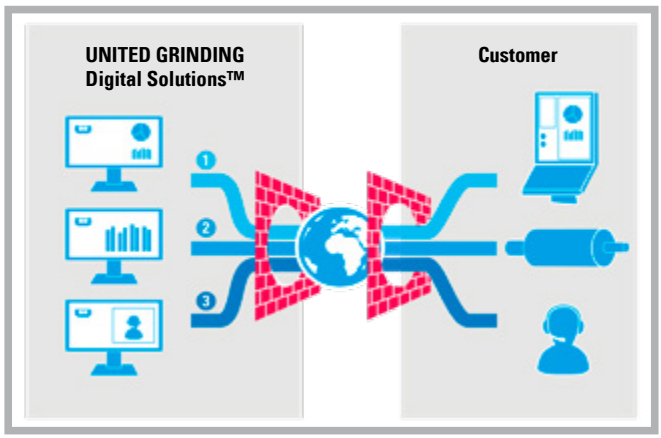
En tant que client, vous pouvez déclencher une demande d'intervention (Service Request) par un seul clic de souris. Un « Service Ticket » correspondant s'affiche immédiatement dans le « Service Cockpit » UNITED GRINDING.
La connexion de UNITED GRINDING avec votre machine ne sera établie que si vous êtes l'initiateur de la demande d'intervention.

Avantage de la connexion en retour
Vous êtes toujours à l'origine de l'établissement de la connexion. Dans une demande d'intervention, c'est vous qui décidez si vous octroyez l'accès à distance à votre machine et à quel moment. De votre côté (c'est-à-dire du côté client), vous n'avez pas besoin de procéder à des ajustements ou modifications.

Notre offre est ainsi rapide et sûre

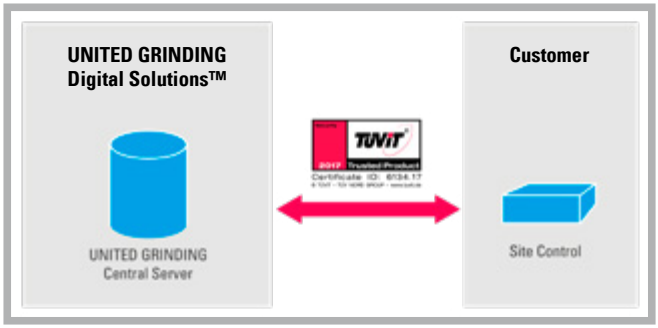
Dès que la connexion sortante a été établie avec succès, la communication dans les deux sens est possible. Les services de tunnelisation utilisés à cet effet sont sécurisés par l'algorithme de chiffrement symétrique AES 256 bits et par SSL avec la clé publique RSA 2048 bits. Ces services de tunnelisation permettent aux membres du service d'assistance Customer Care de UNITED GRINDING d'effectuer les tâches nécessaires pendant une opération de télémaintenance (transfert des données, diagnostic ou programmation à distance) avec l'autorisation d'accès en ligne correspondante.
Dans tous les cas, UNITED GRINDING Digital Solutions™ établit une une connexion sécurisée entre le Service Cockpit du côté UNITED GRINDING et le Site Control du côté de votre machine, de sorte que la commande peut lire les données et les traiter.

L'avantage pour vous : haute performance et sécurité maximale.



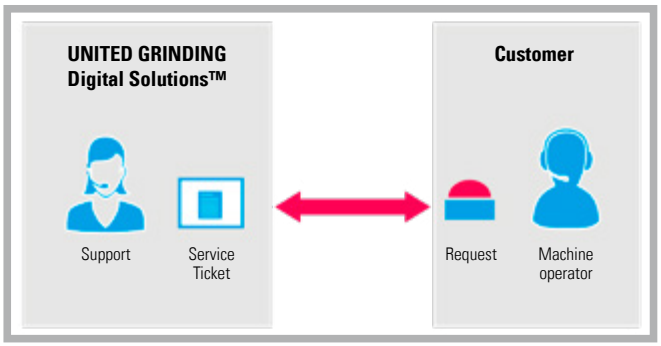
Connexion sécurisée

Le maître-mot des connexions Internet est : sécurité. C'est particulièrement vrai dans un environnement de production où l'exploitant d'une machine veut savoir si ses données extrêmement sensibles sont protégées à tout moment des accès non autorisés, de manière fiable. Le logiciel utilisé par UNITED GRINDING Digital Solutions™ possède une certification « Trusted Product » (certificat de confiance délivré par l'organisme de certification TÜViT). L'attribution de ce certificat est associée notamment à la réalisation d'un contrôle des exigences de sécurité techniques, de l'architecture, de la conception, du processus de développement, ainsi qu'à une analyse des points faibles et des tests de pénétration.



Dépannage

La connexion sécurisée et rapide aux machines des clients dans le monde entier est la base même d'un service de dépannage efficace. À partir de votre demande d'intervention, un technicien qualifié du service Customer Care de UNITED GRINDING peut accéder à votre machine via une connexion en retour et peut ainsi résoudre des problèmes, tels que saisir de nouvelles données, effectuer des mises à jour, exécuter une télémaintenance ou modifier des paramètres.



UNITED GRINDING Digital Solutions™: Vos avantages

- Chaque connexion est établie directement et exclusivement entre vous (le client) et UNITED GRINDING Group.
- Les connexions établies sont toujours limitées dans le temps, c'est-à-dire temporaires.
- Vous êtes le seul à pouvoir initier un échange de données et dans tous les cas, il se déroule toujours sur des machines et/ou des fonctions définies de manière précise.
- Chiffrement des services de tunnelisation par chiffrement symétrique AES 256 bits et SSL avec clé publique RSA 2048 bits (standard minimum : AES avec longueur de clé d'au moins 192 bits et TLS 1.2 ou version supérieure).
- Identification de chaque utilisateur via un nom d'utilisateur et un mot de passe spécifiques. Blocage du compte après un nombre défini de tentatives infructueuses.
- Un accès sécurisé à la télémaintenance s'appuie sur des mesures techniques mais aussi organisationnelles. Analyse des risques, établissement d'inventaires, vérification régulière du bon état de fonctionnement, directives/normes, procédure de patch correctif et évaluation des fichiers journaux, telles sont les prestations fournies en standard par la solution logicielle de UNITED GRINDING.

UNITED GRINDING Digital Solutions™ – Questions et réponses

Qui décide qui peut accéder au réseau de votre atelier et quelles opérations peuvent y être effectuées ?
Vous êtes en charge à tout moment de la gestion des droits des utilisateurs et du contrôle des accès. Seules des personnes autorisées et authentifiées doivent pouvoir se connecter.

Dans le détail
En tant qu'entreprise productrice, vous devez pouvoir contrôler précisément chaque accès à distance à vos installations et machines et, si nécessaire, être en mesure de mettre fin à un accès à tout moment. Chaque utilisateur reçoit un identifiant de connexion et un mot de passe spécifiques. Après des tentatives de connexion non autorisées, un mécanisme de liste noire bloque automatiquement et temporairement l'adresse IP ou l'utilisateur à l'origine de la demande et/ou tentative de connexion. Des certificats TLS (SSL) spécifiques à chaque rôle sont utilisés pour l'authentification des utilisateurs.

UNITED GRINDING Digital Solutions™ offre un concept d'autorisation basé sur les notions de groupe et de rôle. La validation dynamique des ports et le découplage des réseaux empêchent l'accès de logiciels malveillants à votre machine.

Comment savoir ce qui a été fait à distance sur mon installation ?
Toutes les opérations effectuées par UNITED GRINDING Digital Solutions font l'objet de rapports complets.

Dans le détail
- Les opérations effectuées dans le contexte d'une demande d'intervention sont journalisées et archivées.
- Toutes les demandes d'intervention clôturées sont enregistrées dans le dossier de votre installation.
- L'utilisation de fonctions exigeant un rôle d'administrateur fait l'objet d'une journalisation dans votre système. Les entrées de journalisation dans les fichiers « prolog » sont signées et il est donc impossible de les manipuler de manière anonyme.

Dois-je ouvrir mon pare-feu pour les connexions entrantes ?
Non. Vous n'avez pas besoin de connexion entrante.

Dans le détail
La caractéristique de UNITED GRINDING Digital Solutions™ est l'activation et la désactivation structurées de connexions TCP sécurisées par TLS. Les connexions entre le Site Control et notre serveur sont toujours établies à l'initiative du Site Control. Pour le pare-feu, il s'agit donc de connexions sortantes. Il n'est donc pas nécessaire de disposer de ports entrants ouverts. La connexion TLS (auparavant SSL) sortante communique via un seul port (par défaut 443) et peut aussi être pilotée via un serveur proxy Web. La communication entre notre Service Cockpit et le Site Control de votre côté est établie à la suite d'une demande d'intervention via une connexion tunnelisée.

La gestion restrictive des ports constitue un avantage essentiel offert par la technologie de sécurité de UNITED GRINDING Digital Solutions™ par rapport aux solutions VPN classiques. En effets, tous les ports restent ouverts pendant toute la durée de connexion avec les solutions VPN alors que UNITED GRINDING Digital Solutions™ procède à une activation des ports en fonction des besoins : Si des tunnels d'application de bout en bout sont lancés, par exemple des programmes d'accès à distance ou des outils de programmation d'automates programmables, seuls les ports pertinents pour ces tunnels seront activés pendant toute la durée d'utilisation de l'application concernée. L'accès que vous autorisez est donc strictement limité aux besoins de l'intervention. La technologie de sécurité UNITED GRINDING Digital Solutions™ s'applique également aux fonctions étendues du UNITED GRINDING Digital Solutions™ Conference Center : Pour sécuriser la communication avec le technicien, les moyens sont disponibles sont la vidéotéléphonie, le dialogue en ligne (« chat »), le tableau blanc avec fonctionnalité photo et une conférence VNC.

Quelles données me concernant sont-elles reçues par UNITED GRINDING et ces données sont-elles chiffrées ?
Dans le cas de télémaintenance / Remote Service, les données transmises par défaut à UNITED GRINDING sont uniquement vos données de connexion. La communication entre notre serveur et le Site Control est chiffrée et sécurisée.

Dans le détail
La connexion en retour passe par un tunnel, lequel a été mis en place uniquement par votre demande d'intervention. En d'autres termes : Lorsqu'une machine est équipée d'un Customer Cockpit de UNITED GRINDING Digital Solutions™, toute la communication est sécurisée à l'aide d'un chiffrement basé sur un certificat. Les données qui sont enregistrées auprès de UNITED GRINDING concernent uniquement les connexions proprement dites, c'est-à-dire les données comme l'heure d'accès et la durée de connexion l'adresse IP de la personne demandant l'accès, etc.

Ces données sont enregistrées dans les fichiers-journaux et transportées jusqu'à notre serveur. Il est impossible que des données sensibles concernant votre machine quittent votre entreprise sans votre autorisation.

En bref

L'installation de UNITED GRINDING Digital Solutions™ dans votre réseau est donc simple et sûre.
UNITED GRINDING Digital Solutions™ a pour base le langage de programmation Java et comprend des composants logiciels intégrés dans une architecture exigeant peu de ressources.
Votre machine est équipée d'une UNITED GRINDING Digital Solutions™ Site Control Box.

Dans le détail
Cette Site Control Box est un équipement qui sert de de serveur pour le Customer Cockpit. Le Customer Cockpit constitue l'interface utilisateur permettant l'accès à votre machine et, même sans connexion à notre serveur, ce cockpit offre déjà de nombreuses fonctions utiles pouvant être exploitées directement sur votre machine.

La solution matérielle UNITED GRINDING Digital Solutions™ Site Control Box est préconfigurée avec un logiciel pré-installé. Elle est installée dans l'armoire électrique de votre machine et est ensuite connectée au réseau de la machine.

La solution UNITED GRINDING Digital Solutions™ Site Control Box Industrial est un PC industriel intégrable à une armoire électrique qui dispose d'une distribution sécurisée CentOSLinux.

UNITED GRINDING

Vous avez des questions ? N'hésitez pas à nous contacter.

Réservez dès maintenant l'offre qui vous convient.
N'hésitez pas à nous appeler, nous vous conseillerons avec plaisir.

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

Blohm Jung GmbH
Hambourg, Allemagne
Tél. +49 40 7250 02
customercare-hh@blohmjung.com

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

Fritz Studer AG
Thoune, Suisse
Tél. +41 33 439 11 11
info@studer.com

Schaudt Mikrosa GmbH
Leipzig, Allemagne
Tél. +49 341 49 71 123
customercare@schaudtmikrosa.com

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

Ewag AG
Etziken, Suisse
Tél. +41 32 613 31 31
customercare@ewag.com

United Grinding North America, Inc.
Miamisburg (Ohio), États-Unis
Tél. +1 937 847 1234
customercare@grinding.com

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

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