1. Identifiant de connexion

Session Windows :

Identifiant :

- Prenom.nom

Mot de passe :

- Wxcvbn123@

Changement de mot de

passe

- Dès la première connexion, il est nécessaire de modifier le mot de passe.
- Assurez-vous que votre mot de passe comporte au moins 12 caractères, incluant des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux.
- Il est interdit de partager le mot de passe avec d'autres personnes.
- Évitez d'écrire le mot de passe sur un post-it ou de le sauvegarder dans des fichiers accessibles à d'autres personnes. **En cas d'oubli de mot de passe**
- Contactez le service informatique afin de le réinitialiser.

Équipes Support
DSI
14 rue Victor Hugo
34 000 Montpellier
01 34 40 28 39
www.assurmer.fr

2 . MISE A DISPOSITION DE MATERIEL

Nous avons le plaisir de vous informer que vous avez reçu le matériel professionnel appartenant à Assurmer pour faciliter vos activités au sein de notre entreprise. Il s'agit d'un ordinateur portable identifié par les caractéristiques suivantes :

- Numéro de série : [numéro de série]
- État : [état du matériel]
- Complet avec son chargeur et son câble.

Nous tenons à souligner que l'usage de ce matériel est strictement professionnel. En l'utilisant, vous vous engagez à respecter les conditions suivantes :

- Prendre soin de l'équipement afin d'éviter tout dommage, perte ou vol, en ne le laissant pas dans un véhicule non sécurisé.
- Restituer l'appareil dans un état adéquat au bon fonctionnement, en cas de départ de l'entreprise.
- Ne pas installer d'applications ou de logiciels non validés par Assurmer.

La direction d'Assurmer compte sur votre respect de ces consignes. Toute négligence pourrait entraîner des sanctions.

Cette communication est émise à [lieu] le [date]. Nous vous prions de bien vouloir lire et approuver ces termes.

Lu et approuvé,

[Nom et Prénom du collaborateur] [Signature du collaborateur]	Cachet et signature du service informatique

2. Procédure de Retour du Matériel

Nous espérons que le matériel professionnel que vous avez utilisé pour faciliter vos activités au sein d'Assurmer a été bénéfique.

Il est désormais temps de procéder au retour de l'équipement conformément aux normes de l'entreprise. Veuillez cocher les étapes suivantes pour confirmer que chacune a été effectuée :

- J'ai rendez-vous au service informatique avec l'ensemble du matériel fourni :
  - Ordinateur portable identifié par le numéro de série : [numéro de série]
  - Chargeur et câble associés
- J'ai vérifié que le matériel est en bon état d'entretien et de fonctionnement. Tout dommage ou dysfonctionnement a été signalé au service informatique.
- J'ai désinstallé toutes les applications ou logiciels ajoutés qui n'étaient pas initialement validés par Assurmer.
- J'ai remis le matériel ainsi que tous ses accessoires au service informatique.

Il est impératif de respecter ces étapes afin de garantir un retour en bonne et due forme dumatériel.

Nous vous remercions par avance pour votre coopération dans cette démarche. En cas dequestions ou de besoin d'assistance, n'hésitez pas à contacter le service informatique.

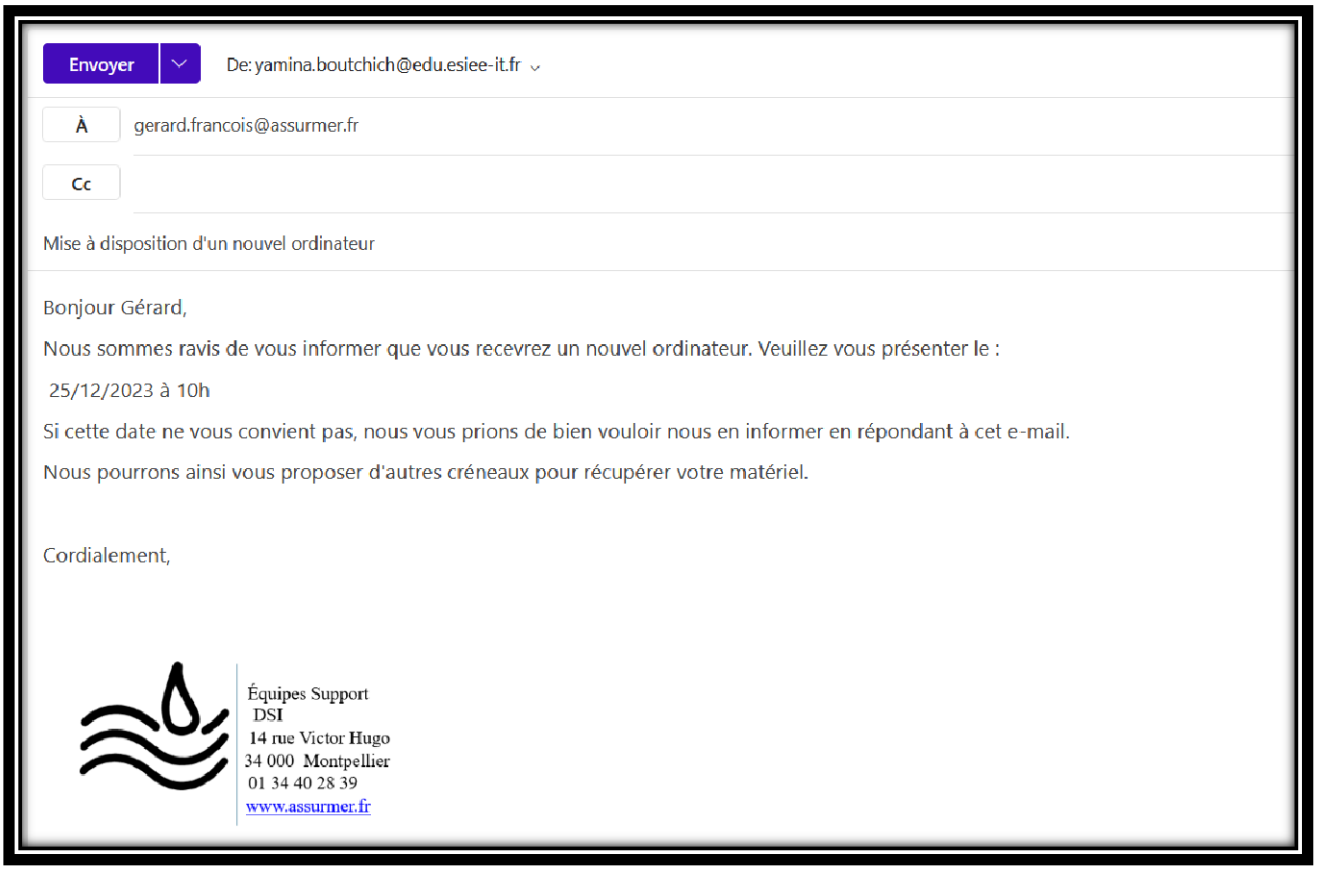
Fait à : Date :

[Nom et Prénom du collaborateur] [Signature du collaborateur]	Cachet et signature du service informatique

3. Mail d'information

Nous avons informé nos collaborateurs de la remise en main propre des équipements informatiques en leur envoyant un mail indiquant la date et l'heure à laquelle ils devaient venir les récupérer.

Voici un exemple de mail :



Envoyer | De: yamina.boutchich@edu.esiee-it.fr

À gerard.francois@assurmer.fr

Cc

Mise à disposition d'un nouvel ordinateur

Bonjour Gérard,

Nous sommes ravis de vous informer que vous recevrez un nouvel ordinateur. Veuillez vous présenter le :

25/12/2023 à 10h

Si cette date ne vous convient pas, nous vous prions de bien vouloir nous en informer en répondant à cet e-mail.

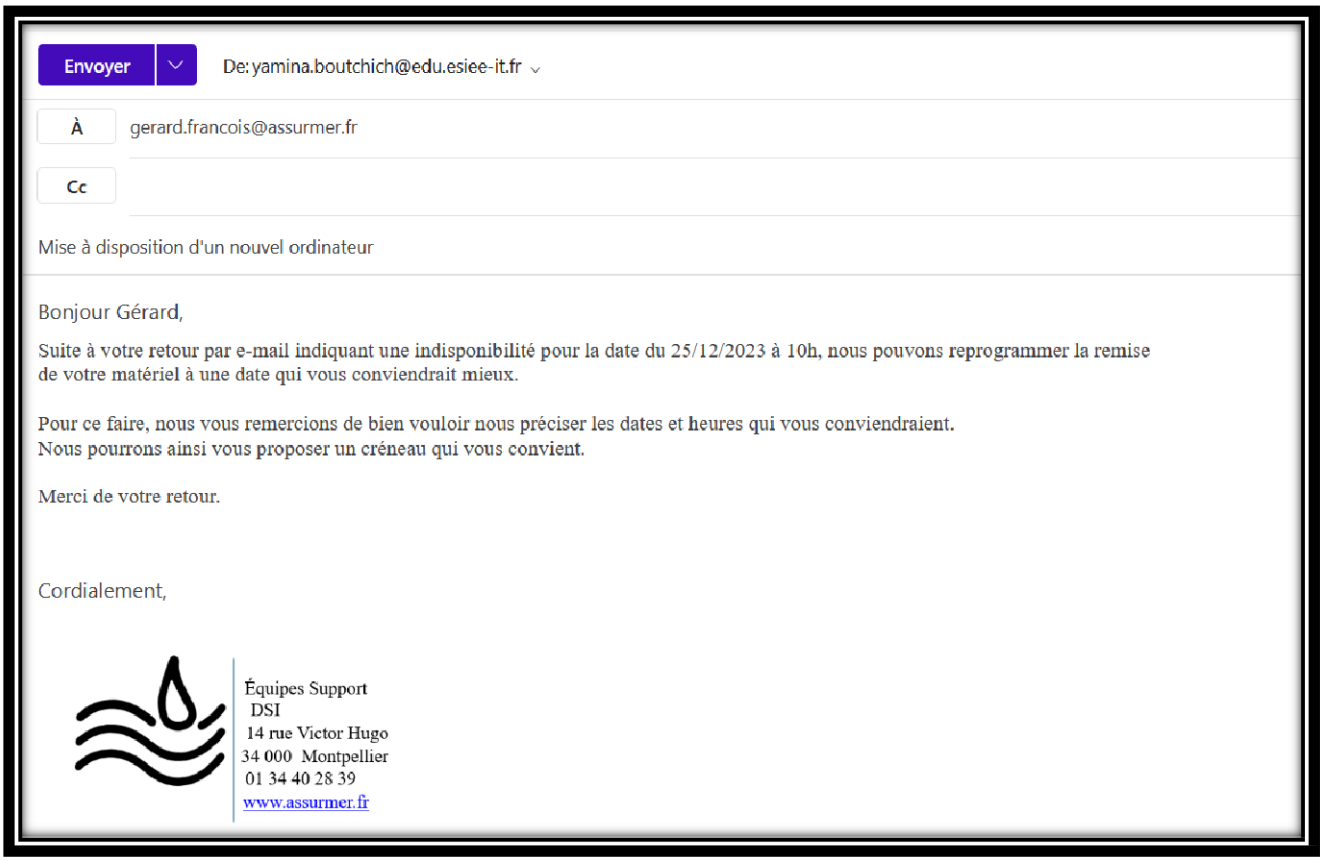
Nous pourrons ainsi vous proposer d'autres créneaux pour récupérer votre matériel.

Cordialement,

Équipes Support
DSI
14 rue Victor Hugo
34 000 Montpellier
01 34 40 28 39
www.assurmer.fr

Nous avons également proposé une solution alternative pour les personnes qui ne pourraient pas être présentes le jour J.

Voici un exemple de mail :



Envoyer | De: yamina.boutchich@edu.esiee-it.fr

À gerard.francois@assurmer.fr

Cc

Mise à disposition d'un nouvel ordinateur

Bonjour Gérard,

Suite à votre retour par e-mail indiquant une indisponibilité pour la date du 25/12/2023 à 10h, nous pouvons reprogrammer la remise de votre matériel à une date qui vous conviendrait mieux.

Pour ce faire, nous vous remercions de bien vouloir nous préciser les dates et heures qui vous conviendraient.
Nous pourrons ainsi vous proposer un créneau qui vous convient.

Merci de votre retour.

Cordialement,

Équipes Support
DSI
14 rue Victor Hugo
34 000 Montpellier
01 34 40 28 39
www.assurmer.fr

Charte Informatique d'Assurmer, Montpellier

Préambule :

Assurmer met à disposition de ses utilisateurs un système d'information (SI) et des moyens informatiques nécessaires à l'exécution de ses missions et activités. Cela inclut notamment un réseau informatique, un réseau téléphonique, ainsi que d'autres actifs précisés dans la charte. Dans un souci de transparence, cette charte établit les règles d'utilisation de ces ressource

Article 1 : Utilisateurs concernés :

- La présente charte s'applique à tous les utilisateurs du système d'information :
  - Dirigeants, salariés, intérimaires, stagiaires, employés de sociétés prestataires et partenaires externes, notamment ceux de compagnies partenaires d'assurance.
- Les salariés de l'organisation sont responsables de faire accepter cette charte à toute personne à laquelle ils permettraient l'accès au SI.

Article 2 : Périmètre du système d'information :

Le système d'information comprend, entre autres :

- **Ordinateurs :**
  - Postes de travail, ordinateurs portables et tout autre matériel informatique utilisé dans le cadre des activités professionnelles au sein d'Assurmer.
- **Téléphones :**
  - Téléphones fixes et mobiles attribués aux employés pour les communications professionnelles.
- **Réseau informatique :**
  - Serveurs, routeurs, connectique et tout équipement associé permettant la transmission et le traitement des données au sein de l'entreprise.
- **Photocopieurs :**
  - Dispositifs de copie et de numérisation utilisés dans le cadre des activités administratives.
- **Logiciels :**
  - Applications, programmes et systèmes logiciels utilisés pour les opérations métier et administratives.
- **Données informatisées :**
  - Informations stockées et traitées électroniquement au sein du SI, comprenant les données clients, les bases de données internes, etc.
- **Messagerie :**
  - Systèmes de communication électronique utilisés pour les échanges professionnels, y compris les courriels et autres outils de messagerie.

Tous les matériels connectés au SI de l'entreprise, qu'ils soient mentionnés ci-dessus ou non, sont régis par cette charte.

Article 3 : Règles générales d'utilisation :

- **Utilisation à des fins professionnelles :**

  - Le Système d'Information (SI) mis à disposition doit être utilisé exclusivement à des fins professionnelles alignées sur les objectifs et les missions d'Assurmer. Cela comprend l'exécution des tâches liées aux assurances, à la gestion des dossiers clients, aux communications internes, et autres activités directement reliées aux fonctions de l'entreprise.

- **Exceptions prévues par la loi ou la charte :**

  - Toute exception à cette règle doit être conforme à la loi ou explicitement autorisée par des dispositions spécifiques de la charte informatique d'Assurmer. Ces exceptions doivent être justifiées et ne doivent en aucun cas compromettre les intérêts, la réputation ou la sécurité de l'entreprise.

- **Interdiction d'usage concurrent ou préjudiciable :**

  - Il est strictement interdit d'utiliser le SI d'Assurmer à des fins concurrentes ou pour des activités préjudiciables à l'entreprise. Cela inclut l'utilisation abusive des ressources, la divulgation d'informations confidentielles, l'accès non autorisé à des données sensibles, ou toute autre action portant atteinte aux intérêts de l'entreprise.

Article 4 : Sécurité Informatique :

4.1 Principe général de responsabilité et obligation de prudence :

L'utilisateur est responsable des ressources informatiques qui lui sont confiées. Il doit agir avec prudence et utiliser les ressources de manière raisonnable, en adéquation avec ses missions.

4.2 Obligation générale de confidentialité :

L'utilisateur s'engage à préserver la confidentialité des informations, notamment des données personnelles, traitées sur le SI de l'organisation. Il doit prendre toutes les précautions pour éviter toute divulgation non autorisée de ces informations confidentielles.

4.3 Mot de passe :

- Le mot de passe doit être :

  - Composé de plus de 12 caractères.
  - Une combinaison complexe de caractères alphanumériques incluant des chiffres, des lettres (majuscules et minuscules) et des caractères spéciaux.
  - Il ne doit en aucun cas contenir des informations personnelles telles que des prénoms, noms, dates de naissance, ou toute autre donnée facilement identifiable.

- Éviter l'utilisation de séquences logiques, de mots du dictionnaire, ou toute information facilement déductible.
- Il est recommandé de changer régulièrement son mot de passe et de ne pas le réutiliser pour différents comptes ou systèmes.

4.4 Verrouillage de sa session :

L'utilisateur doit impérativement verrouiller sa session dès qu'il quitte son poste de travail, que ce soit pour une courte absence ou à la fin de sa journée de travail. Cette pratique est essentielle pour protéger l'accès non autorisé à son espace de travail et éviter toute utilisation non souhaitée de ses informations professionnelles.

4.5 Installation de logiciels :

Afin de prévenir les risques liés aux virus informatiques et de maintenir l'intégrité des systèmes informatiques d'Assurmer, il est strictement interdit à l'utilisateur d'installer, de copier, de modifier ou de supprimer des logiciels sur son poste informatique sans l'accord préalable du service informatique de l'entreprise. Ceci vise à assurer la sécurité des données et la stabilité des systèmes en évitant l'introduction de logiciels non autorisés ou potentiellement dangereux.

4.6 Copie de données informatiques :

Pour toute opération de copie de données sur des supports amovibles tels que des clés USB ou tout autre support de stockage externe, l'utilisateur doit suivre les procédures définies par l'entreprise. Cela inclut l'obtention préalable de l'accord de son supérieur hiérarchique et le respect strict des règles de sécurité établies pour éviter toute perte de données ou fuite d'informations confidentielles. Cette mesure vise à assurer la protection des données et à prévenir tout incident de sécurité potentiel lors du transfert ou du stockage sur des supports amovibles.

Article 5 : Modalités d'utilisation des ressources informatiques :

Postes de travail :

Les postes de travail attribués aux employés d'Assurmer doivent être utilisés de manière exclusive pour l'exécution des tâches professionnelles. Les utilisateurs sont responsables de l'intégrité et de la sécurité de leur poste de travail, y compris de la protection physique des équipements.

Applications et logiciels :

Les applications informatiques mises à disposition des employés d'Assurmer doivent être utilisées conformément aux objectifs et aux missions de l'entreprise. Tout accès ou utilisation non autorisé des logiciels ou des applications est strictement interdit.

Téléphonie mobile :

Les dispositifs de téléphonie mobile attribués aux employés pour les communications professionnelles doivent être utilisés de manière responsable et conforme aux directives de l'entreprise. Ils doivent être protégés par des mots de passe sécurisés et ne doivent pas être utilisés pour des activités non liées au travail.

Accès aux données et à la messagerie :

L'accès aux données et à la messagerie d'Assurmer doit être utilisé dans le cadre des activités professionnelles. Les informations confidentielles ou sensibles ne doivent en aucun cas être divulguées à des tiers non autorisés.

Utilisation des ressources partagées :

Toute utilisation des ressources partagées, telles que les dossiers partagés sur le réseau, doit se faire dans le respect des règles de partage établies par l'entreprise. Il est important de respecter l'intégrité des données et de ne pas altérer, supprimer ou copier des informations sans autorisation préalable.

Article 6 : Accès à Internet :

L'accès à Internet est autorisé via le Système d'Information (SI) d'Assurmer. Cependant, des restrictions d'accès à certains sites peuvent être appliquées pour des raisons de sécurité. Ces restrictions visent à protéger les systèmes informatiques de l'entreprise contre les menaces potentielles telles que les logiciels malveillants, les sites non sécurisés ou les contenus inappropriés. Les employés doivent utiliser Internet de manière responsable et s'abstenir de contourner ces restrictions de sécurité pour accéder à des contenus non autorisés.

Article 7 : Messagerie :

Chaque employé se voit attribuer une adresse e-mail dédiée à ses missions professionnelles au sein d'Assurmer. Tous les messages envoyés ou reçus par le biais de cette messagerie sont présumés être professionnels et liés aux activités de l'entreprise. L'utilisation à des fins personnelles est tolérée dans les limites légales, mais ces messages doivent être clairement identifiés comme "personnels" dans l'objet du message et être classés dans un répertoire distinct dédié aux messages personnels. Il est crucial de respecter la confidentialité des communications professionnelles et de ne pas compromettre la sécurité des données ou la réputation de l'entreprise par le biais de la messagerie électronique.

Article 8 : Sanctions :

Tout manquement aux règles énoncées dans cette charte peut entraîner des sanctions, lesquelles peuvent varier en fonction de la gravité de l'infraction. Ces sanctions peuvent comprendre des avertissements formels, des limitations d'usage du Système d'Information (SI), des mesures disciplinaires telles que des suspensions temporaires d'accès au SI ou d'autres ressources informatiques, voire des sanctions disciplinaires conformément aux politiques de l'entreprise. La nature et l'étendue des sanctions seront déterminées au cas par cas, en tenant compte de la gravité de l'infraction et des circonstances entourant celle-ci.

Article 9 : Information et entrée en vigueur :

Cette charte fait partie intégrante du règlement intérieur d'Assurmer et sera communiquée individuellement à chaque employé. Chaque employé devra prendre connaissance de son contenu et s'engager formellement à respecter les directives énoncées dans la charte. Elle entrera en vigueur à partir de sa date d'approbation, fixée au [indiquer la date d'approbation par la direction ou les autorités compétentes]. Tous les nouveaux employés seront informés de cette charte dès leur intégration, tandis que les employés actuels devront prendre connaissance de son contenu dans les plus brefs délais après son approbation.

Mise à disposition de la charte informatique :

La présente charte informatique sera rendue accessible à tous les employés d'Assurmer. Elle sera disponible sur l'intranet de l'entreprise, affichée dans les locaux désignés et distribuée électroniquement à tous les employés concernés.

Validation :

La présente charte informatique a été approuvée par le Comité d'Entreprise (CE), le département des Ressources Humaines (RH) et le Service Informatique, en date du 10/01/2024.

Fait à : Signature :

Équipes Support
DSI
14 rue Victor Hugo
34 000 Montpellier
01 34 40 28 39
www.assurmer.fr

1. **Mots clés :**

MDT : **Microsoft Deployment Toolkit** est un outil d'automatisation de la fabrication et d'installation des systèmes Windows. Il permet de créer des images de systèmes d'exploitation personnalisées et de les déployer sur des ordinateurs clients à distance.

WDS : **Windows Deployment Services** est un rôle facultatif de Windows Server et correspond au service de déploiement Windows. Il permet de déployer des images desystèmes d'exploitation Windows sur des ordinateurs clients à distance.

PXE : **Preboot eXecution Environment** est un protocole réseau qui permet à un ordinateur client de démarrer depuis le réseau en récupérant un programme d'amorçage (boot loader) surun serveur. Ce boot loader permet ensuite de charger une image de système d'exploitation.

AD DS : **Active Directory Domain Services** est un service de gestion des identités et des accès de Microsoft. Il permet de centraliser la gestion des utilisateurs, des groupes et des ordinateurs dans un domaine.

DNS : **Domain Name System** traduit les noms de domaine en adresses IP pour permettre aux appareils de se connecter entre eux sur Internet.

DHCP : **Dynamic Host Configuration Protocol** est un protocole réseau qui permet de configurer automatiquement les paramètres IP d'une station ou d'une machine. Il permet notamment d'attribuer automatiquement une adresse IP, un masque de sous-réseau, une passerelle par défaut et des serveurs DNS à une station ou une machine.

ISO : **International Organization for Standardization** est une organisation internationale qui élabore des normes techniques. Une image ISO est un fichier image qui contient les données d'un disque optique, tel qu'un CD ou un DVD.

TFTP (Trivial File Transfer Protocol) est un protocole de transfert de fichiers simple utilisé principalement pour le transfert de fichiers sur un réseau, souvent dans des environnements de démarrage ou de configuration.

GPO (Group Policy Object) fait référence à un ensemble de règles et de paramètres de configuration appliqués à des utilisateurs et des ordinateurs dans un réseau Windows, permettant de gérer et de contrôler les politiques de sécurité, les accès aux ressources et d'autres paramètres système.

ADK : un ensemble d'outils de Microsoft pour personnaliser et déployer des systèmes d'exploitation Windows.

2. Les références :

MDT/WDS :https://openclassrooms.com/fr/courses/2356306-prenez-en-main-windows- server/5836371-implementez-un-service-de-deploiement

Fog project : https://fogproject.org/

Procédure d'installation AD :https://www.vemotech.fr/tutorials/configurer-un-controlleur-de-domaine- avec-windows-server-2022-668999

Installation DHCP et DNS : https://mathisthuault.wordpress.com/2019/05/01/configuration-dun-serveur-dhcp-et-dns-ad-ds-ipv4-securise-sur-windows-server-2016/

Installation MDT/WDS : https://www.it-connect.fr/installer-mdt-sur-windows-server-2022-pour-deployer-windows-11-22h2/