dormakaba

Community

Guide d'installation

PK3695 2.6 - 08/2026
Document original

FR

dormakaba Canada, Inc.
105 Marcel-Laurin Blvd
Montréal, Québec, H4N 2M3
Téléphone : +1 866-dormakaba (1-866-367-6252)

www.dormakaba.com

Copyright © dormakaba 2026
Tous droits réservés.

Aucune partie de ce document ne peut être reproduite ou utilisée sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de dormakaba Canada.

Tous les noms et logos des produits et services de tiers sont la propriété de leurs détenteurs respectifs. MIFARE, MIFARE Classic, MIFARE Plus EV2, MIFARE Ultralight et MIFARE DESFire sont des marques déposées de NXP B.V.

Sous réserve de modifications techniques.

Table des matières

1 À propos de ce document 6
1.1 Validité 6
1.2 Public cible 6
1.3 But et objectif 6
1.4 Documents supplémentaires 6
2 Bienvenue 7
2 Vue d'ensemble de la sécurité 7
2.1 Mode de sécurité renforcée 7
2.2 Sécurité physique 8
2.2.1 Sélection du matériel 8
2.2.2 Installation / mises à niveau 8
2.3 Sécurité du réseau 8
2.3.1 Installation 8
2.3.2 Configuration 9
2.4 Sécurité de l'application 9
2.4.1 Normes en matière de données 9
2.4.2 Fonctions de sécurité 9
2.4.3 Décisions de conception exclusive 10
2.5 Sécurité de l'utilisateur 11
3 Exigences 12
3.1 Exigences du système 12
3.2 Exigences du réseau 13
3.2.1 Déploiement sur une machine virtuelle 13
3.2.2 Ports de communication 13
3.3 Exigences du périphérique 13
3.3.1 Clés RFID 13
3.3.2 Encodeurs 14
3.3.3 Programmateurs M-Unit 14
3.3.4 Serrures 15
3.3.5 Contrôleurs d'ascenseur 16
3.3.6 Passerelles Zigbee 17
3.4 Exigences en matière d'interface 17
3.5 Interfaces et périphériques de communication en ligne 17
3.6 Support de serrure pour la communication en ligne 18

3.7 Exigences No Touring 18
3.8 Composants prérequis tiers 19
4 Liste de contrôle avant l'installation 20
4.1 Exigences 20
4.2 Recommandations 20
5 Préparer l'utilisation d'une instance existante de SQL Server 21
5.1 Configuration d'un pare-feu Windows pour l'accès au moteur de base de données 23
6 Installation du serveur Community 30
6.1 Page Choisir la langue d'installation 30
6.2 Page de bienvenue 31
6.3 Page du contrat de licence 32
6.4 Page Choisissez l'emplacement de destination 33
6.5 Page de sélection de l'adresse IP/du nom du serveur 34
6.6 Page Type d'installation 35
6.7 Page SQL Database Server 36
6.8 Page État de l'installation 38
6.9 Page Type de configuration 39
6.9.1 Choisissez le certificat SSL 39
6.9.2 Page Mot de passe 40
6.10 Page Installation terminée 41
7 Installation du client Community 42
7.1 Page de bienvenue 43
7.2 Page du contrat de licence 44
7.3 Page Choisissez l'emplacement de destination 45
7.4 Page État de l'installation 46
7.5 Page Installation terminée 47
8 Liste de contrôle après l'installation 48
9 Mises à niveau Community 49
9.1 Liste de contrôle avant la mise à niveau 49
9.2 Processus de mise à niveau 49
9.3 Liste de contrôle après la mise à niveau 50
9.4 Mises à jour de SQL Server 50
10 Démarrer avec Community 51
10.1 Activation du produit 51
10.2 Flux de travail pour la configuration du site 52
10.3 N'oubliez pas ... 52

A Annexe A : Gestionnaire de services 53
A.1 Installation / renouvellement du certificat SSL après l'installation 53
A.1.1 Serveur 53
A.1.2 Client 54
A.2 Modification de l'adresse IP du serveur 54
A.2.1 Serveur 54
A.2.2 Client 54
A.3 Restaurer la base de données en ligne 55
A.4 Désactiver/activer la fonction Watchdog 55
B Annexe B: Database restore 56
B.1 Required preparatory steps 56
B.1.1 Install the Community server on a reserve machine 56
B.1.2 Identify database backups 56
B.1.3 Copy backup files to the new server 56
B.1.4 Obtain and configure the dormakaba restore tool 57
B.2 Restore the SQL Server database 57
B.3 Restore the MongoDB database 60
B.4 Static IP address only. Update IP address 65
B.5 Update Community workstations 65
B.6 Community only. Update API server 65

1 À propos de ce document

1.1 Validité

Ce document décrit le produit :

Désignation du produit :	Community
Version :	2.6

1.2 Public cible

Ce document est destiné aux spécialistes informatiques responsables de toutes les tâches liées à l'installation du Serveur Community et du Client Community.

1.3 But et objectif

Ce document fournit des informations et des instructions pour toutes les tâches liées à l'installation de Community. Le document énumère les exigences et comprend des listes de contrôle avant et après l'installation pour les nouvelles installations et les mises à niveau.

1.4 Documents supplémentaires

Community Guide d'utilisation 2.6 (PK3706-EN)

Community Notes de mise à jour 2.6 (PK3696)

Community Sécurité renforcée des clés 2.6 (PK3776)

2 Bienvenue

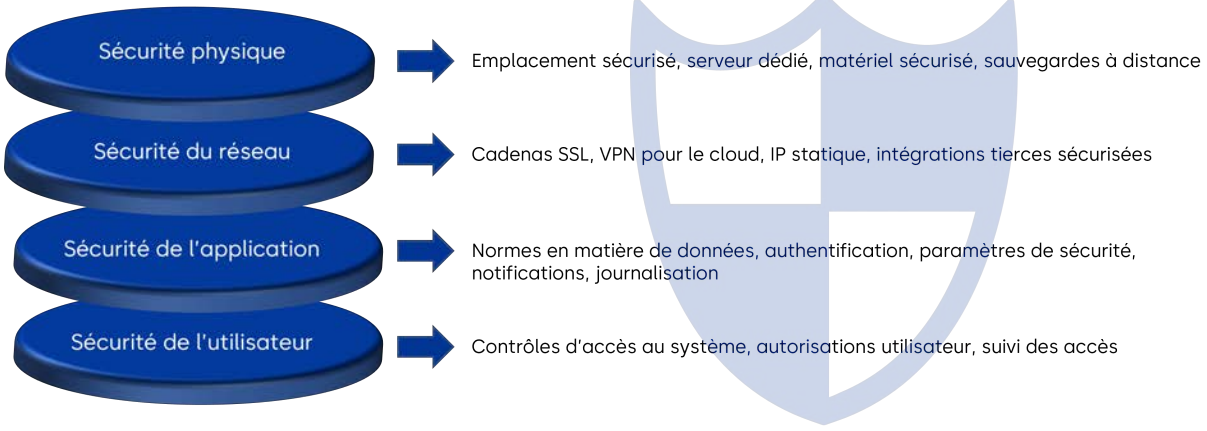
Community® est un logiciel de gestion flexible et facile à utiliser dédié aux logements collectifs. Développée pour la sécurité et conçue pour les utilisateurs, cette application simplifie la gestion du contrôle d'accès et fournit un moyen efficace et convivial pour configurer et faire fonctionner les immeubles d'appartements, les résidences pour étudiants, les établissements pour personnes âgées et autres propriétés multi-locataires. Les options de configuration et d'intégration flexibles offrent un ensemble de fonctionnalités robustes, y compris un accès aux clés mobiles et la gestion des visiteurs par les résidents. Les flux de travail guidés simplifient la configuration de l'établissement, la gestion du personnel et des prestataires, la remise des clés et la gestion des résidents. Les autorisations configurables des utilisateurs permettent de sécuriser l'accès au système. La collecte de données sur les serrures et le système permet d'effectuer des audits et des rapports détaillés sur les points d'accès. La gestion des serrures à distance permet un contrôle immédiat et pratique des points d'accès. Une intégration harmonieuse avec un contrôle d'accès Keyscan Aurora permet d'étendre la gestion aux portes du périmètre connectées et évite d'avoir à synchroniser les données des résidents et du personnel entre différents systèmes.

2 Vue d'ensemble de la sécurité

En tant que leader du marché du contrôle d'accès, dormakaba est consciente de la nature évolutive des technologies de sécurité. Nous nous efforçons d'apporter des améliorations continues à nos produits et invitons nos clients à améliorer leurs protocoles d'authentification et de cryptage. De plus, dormakaba recommande de configurer les options de sécurité disponibles dans Community et d'adopter les meilleures pratiques standard.

Ce chapitre présente les options de sécurité et les meilleures pratiques selon la couche de sécurité concernée. Le mode de sécurité renforcée est considéré comme la recommandation principale et la plus forte pour garantir la sécurité de bout en bout.

Mode de sécurité renforcée Ambiance



2.1 Mode de sécurité renforcée

L'activation du mode de sécurité renforcée constitue une couche de sécurité supplémentaire pour la protection des données sur les clés RFID. Cette évolution technologique renforce l'intégrité de l'ensemble du système de gestion des accès. Grâce au mode de sécurité renforcée des clés :

- La sécurité de toutes les clés est renforcée.
- Les données encodées sur les clés sont protégées par des normes de cryptage mondiales.
- Les encodeurs prennent en charge des normes de cryptage avancées.
- La programmation des serrures est protégée par un cryptage et une authentification renforcés.
- Les serrures sont programmées pour n'accepter que les clés de haute sécurité.

La sécurité renforcée des clés nécessite des périphériques conformes aux normes de cryptage et aux protocoles d'authentification avancés. Les serrures, les encodeurs, les programmateurs M-Unit, les clés RFID et les contrôleurs d'ascenseur doivent répondre aux exigences minimales. Pour en savoir plus, consultez les sections correspondantes dans Exigences du périphérique.

La mise en œuvre d'une sécurité des clés implique de définir les exigences du périphérique et d'activer le mode de sécurité renforcée dans Paramètres du système. Reportez-vous au document *Community Sécurité renforcée des clés* disponible à la racine du dossier de téléchargement du logiciel. Ce document décrit les options et fournit des instructions détaillées pour l'activation du mode de sécurité renforcée. Ce document contient également des informations importantes pour les sites qui effectuent une mise à niveau sans sécurité renforcée des clés.

2.2 Sécurité physique

La sécurité physique est la base sur laquelle reposent toutes les couches de sécurité supplémentaires.

2.2.1 Sélection du matériel

Lors de la planification d'un déploiement initial ou d'une mise à niveau, utilisez du matériel qui offre une sécurité renforcée :

- Serveur – Un serveur dédié est et/ou recommandé pour Community.
- Serrures – Tous les profils de serrure dans Community offrent une sécurité renforcée, à l'exception de RT et Confidant.
- M-Units – (Programmateurs M-Unit) Utilisez uniquement le type M-Unit Saflok HH6 NFC. Requis pour le mode de sécurité renforcée.
- Encodeurs – Utilisez uniquement le type dormakaba RFID Encodeur II, référence 75720. Requis pour le mode de sécurité renforcée.
- Clés RFID – Veuillez noter que de nombreuses cartes d'accès utilisées dans les systèmes RFID sont susceptibles d'être clonées et de faire l'objet d'attaques au fil des ans. Certaines technologies de cartes anciennes ont notamment fait l'objet de rapports de vulnérabilité publiés. dormakaba recommande l'utilisation d'identifiants utilisant MIFARE DESFire EV2/EV3 afin de fournir une couche supplémentaire de sécurité pour la version installée de Community
  - Pour les identifiants des résidents, choisissez les identifiants plus sûrs MIFARE DESFire EV2/EV3 dont les fonctions de sécurité offrent une protection supplémentaire contre le clonage.
  - Pour les identifiants du personnel/prestataire, nous recommandons également d'utiliser MIFARE DESFire EV2/EV3. Cela offrira une couche de sécurité supplémentaire pour le logiciel de gestion des accès actuellement installé sur votre site. Nous avons intégré l'identifiant MIFARE Plus afin d'assurer la compatibilité avec les solutions existantes, en particulier MIFARE Classic. Par conséquent, pour cette application spécifique, MIFARE Plus n'offrira pas le même niveau de sécurité qu'Ultralight C.

2.2.2 Installation / mises à niveau

- Installez le serveur Community dans un emplacement physique sécurisé.
- dormakaba recommande vivement de programmer des sauvegardes automatiques sur un serveur distant et de conserver les copies de sauvegarde et les données archivées dans un endroit sûr hors site. Les exigences s'appliquent à la sauvegarde sur un serveur distant. Pour les mises à niveau, faites une sauvegarde de la base de données avant d'effectuer la mise à niveau. Pour les systèmes en ligne, faites des sauvegardes des bases de données SQL Server et MongoDB Community. Voir Paramètres du système > Sauvegarde de la base de données.

2.3 Sécurité du réseau

Avant le déploiement, un technicien dormakaba travaille avec l'équipe informatique du site pour discuter des exigences du réseau. Consultez les meilleures pratiques et les options de sécurité suivantes.

2.3.1 Installation

- Avant de commencer l'installation, vérifiez que toutes les mises à jour de Windows sont installées.
- Configurez le serveur Community avec une adresse IP statique.

- dormakaba recommande vivement d'installer un certificat SSL pour activer le protocole HTTPS. Le certificat SSL permettant d'activer le mode HTTPS doit être fourni par une autorité de certification reconnue et fiable. Si vous choisissez d'installer un certificat SSL après l'installation, utilisez le Gestionnaire de services pour une transition simplifiée.
- En cas de déploiement de Community sur une VM (machine virtuelle) dans le cloud, un VPN (réseau privé virtuel) est requis pour sécuriser la communication entre le site et la machine virtuelle dans le cloud.
- Les contrôles de version exigent que les postes de travail Community utilisent la même version que le serveur Community pour programmer les serrures et encoder/lire les clés.

2.3.2 Configuration

- Ports de communication – Les ports sécurisés par défaut sont énumérés dans les notes de mise à jour du produit. Si nécessaire, consultez un technicien dormakaba pour personnaliser les ports. Voir Ports de communication.
- Certificat du navigateur HTTPS — Lorsque Community est déployé avec un certificat SSL, indiquez le nombre de jours avant l'expiration du certificat pour commencer à recevoir un avertissement quotidien. Voir Paramètres du système > Sécurité > Certificat du navigateur HTTPS.
- Notifications sécurisées par e-mail – Lorsque SSL est activé et que les certificats de sécurité sont valides, toutes les données des e-mails envoyés à partir du serveur de messagerie électronique vers les clients de messagerie électronique sont privées et sécurisées. Voir Paramètres du système > Configuration e-mail.
- Intégrations – Intégrer uniquement avec des applications tierces qui prennent en charge la communication sécurisée. Voir Ports de communication et obtenir la documentation sur l'intégration auprès du service client de dormakaba.

2.4 Sécurité de l'application

Community prend en charge les normes de données de l'industrie et recommande de tirer parti des options de sécurité. Voir également Décisions de conception exclusive.

2.4.1 Normes en matière de données

- PCI-DSS – Choisissez d'activer ou non la norme PCI-DSS (Payment Card Industry Data Security Standard), une norme de sécurité de l'information pour les organisations gérant des cartes de crédit. Valeur recommandée : OUI. Lorsque vous activez la norme PCI-DSS, l'option Activer les questions de sécurité dans Réinitialisation du mot de passe est réglée sur OUI et ne peut être désactivée.
- RGPD – La déclaration de protection des données de dormakaba est disponible sur le serveur à l'emplacement suivant : \Community Server\GDPR. Les clients sont invités à imprimer une copie de la déclaration et à la conserver dans leurs locaux pour s'y référer.

2.4.2 Fonctions de sécurité

- Mode de sécurité renforcée – Ce paramètre permet d'activer le cryptage amélioré pour l'encodage des données sur les clés. Valeur par défaut : NON. Voir Paramètres du système > Sécurité > Mode de sécurité renforcée.
- Authentification unique (SSO) : cette option sous licence est désactivée par défaut. Le SSO centralise l'authentification, ce qui permet aux organisations de mettre en œuvre des contrôles de sécurité plus stricts.
- Types de clés RFID – dormakaba recommande d'activer le mode de sécurité renforcée qui prend en charge MIFARE DESFire EV2/EV3 (recommandé), MIFARE Plus et MIFARE Ultralight C. Lorsque le mode de sécurité renforcée n'est pas activé, dormakaba recommande MIFARE DESFire EV2/EV3 (sécurité standard). Voir Paramètres du système > Avancés > Types de clés RFID.
- Sécurité des périphériques – Ce paramètre est activé par défaut pour les nouvelles installations. Les certificats SSL côté service et côté client sécurisent la communication pour les encodeurs, les périphériques de la passerelle II et les périphériques MFC. Pour les mises à niveau, les certificats doivent être activés manuellement.
- Authentification de M-Unit – Choisissez de demander ou non une authentification de M-Unit. Lorsque l'authentification est activée, les identifiants de M-Unit sont requis pour programmer et auditer des serrures. Si l'authentification est activée, des identifiants du programmateur M-Unit doivent être configurés dans Gestion du personnel/prestataire pour au moins un opérateur. Requis pour le mode de sécurité renforcée. Voir Paramètres du système > Sécurité > Programmateur M-Unit.

- Code de sécurité M-Unit – Si le mode de sécurité renforcée est activé, un code de sécurité est nécessaire pour programmer les serrures avec M-Unit. Voir Paramètres du système > Sécurité > Mode de sécurité renforcée.
- PMS API – Indiquez si une authentification doit être demandée pour les requêtes API. Si l'authentification est activée, des identifiants API doivent être configurés dans Gestion du personnel/prestataire pour au moins un opérateur. Voir Paramètres du système > Sécurité > API.
- Accès aux serrures – Vérifiez les paramètres de Sortie/retour, de Reverrouillage rapide et de Mode désactivation pour affiner l'accès aux serrures une fois la porte ouverte. Voir Paramètres du système > Sécurité > Accès aux serrures.
- Sécurité des données – dormakaba recommande vivement de programmer des sauvegardes automatiques sur un serveur distant et de conserver les copies de sauvegarde et les données archivées dans un endroit sûr hors site. Les exigences s'appliquent à la sauvegarde sur un serveur distant. Voir Paramètres du système > Sauvegarde de la base de données.
- Confidentialité des données – Conformément au RGPD (Règlement général sur la protection des données), dormakaba crypte toutes les PII (informations personnelles identifiables) avec une clé symétrique spécifique au site.
- PPK/SPK – Les clés de programmation primaire et secondaire peuvent être créées à l'avance dans Clés Système afin de préparer la reprise après sinistre. La PPK est essentielle pour récupérer une base de données corrompue ou totalement perdue.
- Clés à sécurité intégrée – Les clés à sécurité intégrée sont des sauvegardes des clés individuelles des qui sont créées à l'avance et conservées en jeux complets à remettre en cas de panne du système ou de courant. Voir Paramètres du système > Clés à sécurité intégrée.
- Clés du personnel/clés système – Indiquez toujours un porteur de clé lors de la création de clés du personnel et de clés système. Même si cela n'est pas obligatoire, l'identification du porteur de clé est utile pour le suivi et la responsabilité. Voir Clés du personnel et Clés Système.
- Invalidez l'accès le cas échéant :
  - Utilisez les fonctions Bloquer et Désactiver dans Gestion du personnel/prestataire pour restreindre l'accès de l'opérateur, si nécessaire. Voir Gestion du personnel/prestataire.
  - Utilisez les clés système sur les serrures pour invalider l'accès du personnel et des résidents. Voir Clés Système.
  - Utilisez la fonction Effacer la clé (dans la boîte de dialogue Lire la clé) pour invalider les clés. Voir la barre d'outils Community.
  - Utilisez la fonction Désactiver le résident le cas échéant. Voir Gestion des résidents.
- Suivi des accès – Les rapports de suivi de l'accès du personnel/prestataire et des résidents peuvent être générés dans la boîte de dialogue Lire la clé.
- Notifications – Configurez des groupes de notification, puis affectez des souscriptions aux membres du personnel dans Gestion du personnel/prestataire. Voir Notifications et Gestion du personnel/prestataire.
- Journalisation – Des journaux complets sont générés pour faciliter le dépannage.
- Mises à niveau du firmware – Définissez un horaire pour mettre à niveau les périphériques avec la dernière version de firmware prise en charge.
- Rapports – Définissez un horaire pour exécuter et examiner les rapports Community. Voir Rapports.

2.4.3 Décisions de conception exclusive

Une approche de la configuration du site axée sur la sécurité implique une planification détaillée.

- Configurateur de site – Planifiez, créez et maintenez des points d'accès de manière réfléchie. Établissez des normes pour la création de types de points d'accès privés et d'accès aux portes de foyer, ainsi que pour la sélection de l'option d'accès limité aux espaces communs pour le personnel et les résidents. Voir Configurateur de site.
- Gestion des accès – Planifiez, créez et maintenez de manière réfléchie les contrôles de gestion des accès à l'aide d'horaires, d'identifiants et d'accès aux espaces communs. Voir Gestion des accès.
  - Identifiants – Configurez soigneusement tous les identifiants.
  - Clés d'urgence – Si nécessaire, obtenez une licence pour les clés d'urgence. Seules les clés d'urgence forcent *toujours* l'ouverture du pêne dormant projeté ou du verrou d'intimité actif.

2.5 Sécurité de l'utilisateur

Les contrôles d'accès au système comprennent les options et les meilleures pratiques suivantes :

- Paramètres de mot de passe, de connexion et de compte – Personnalisez les paramètres globaux pour empêcher l'accès non autorisé de l'opérateur. Voir Paramètres du système > Sécurité.
- Authentification unique (SSO) : cette option sous licence est désactivée par défaut. Le SSO simplifie l'accès pour les utilisateurs et réduit au minimum la gestion des identifiants.
- Gestion des rôles – Les rôles de l'opérateur déterminent le niveau d'accès aux caractéristiques et fonctions Community. Planifiez et attribuez les rôles de l'opérateur de manière réfléchie. Si nécessaire, créez des rôles personnalisés. Voir Gestion des rôles.
- Gestion du personnel/prestataire – Les profils des membres du personnel/prestataires sont conçus pour stocker des informations sur tous les membres du personnel/prestataires. Précisez tous les détails disponibles dans l'onglet Informations sur les membres du personnel/le prestataire. Pour les opérateurs, créez des identifiants de connexion à l'API dans l'onglet Informations sur l'opérateur. Les identifiants sont validés lorsque l'authentification de M-Unit et de l'API est activée. Voir Gestion du personnel/prestataire.
- Compte admin par défaut – Après l'installation, connectez-vous au compte Admin01 par défaut pour modifier le mot de passe par défaut. Créez des mots de passe forts en utilisant au moins huit caractères comprenant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.

3 Exigences

Cette section énumère les exigences minimales du système, du réseau, du périphérique et de l'interface pour l'installation et l'utilisation de Community. Des ressources supplémentaires peuvent être requises en fonction de la configuration et de l'utilisation du site.

3.1 Exigences du système

Les exigences minimales pour le serveur Community dépendent du nombre de points d'accès. Des remarques supplémentaires figurent à la fin du tableau. [1]

Un serveur dédié est recommandé mais pas obligatoire.

	Serveur			Poste de travail
	Petit < 500 points d'accès	Moyen 500 à 2 000 points d'accès	Grand > 2 000 points d'accès	sans objet
Processeur [2]	2 GHz/Intel x64 bits/4 core	2 GHz/Intel x64 bits/8 core	2 GHz/Intel x64 bits/16 core	2 GHz/Intel x64 bits/dual core
RAM	16 Go ou plus	16 Go ou plus	32 Go ou plus	8 GO
Espace disponible sur le disque dur [3]	30 Go	60 Go	100 Go	50 MO
Contrôleur réseau	Gigabit Ethernet – 1 Go/seconde	Gigabit Ethernet – 1 Go/seconde	Gigabit Ethernet – 1 Go/seconde	Gigabit Ethernet – 1 Go/seconde
Port USB 2.0	Requis pour connecter l'encodeur	Requis pour connecter l'encodeur	Requis pour connecter l'encodeur	Requis pour connecter l'encodeur
Système d'exploitation [4]	▪ Microsoft Windows Server 2025/2022/2019 Standard ▪ Microsoft Windows 11 Pro/Enterprise [5]	▪ Microsoft Windows Server 2025/2022/2019 Standard	▪ Microsoft Windows Server 2025/2022/2019 Standard	▪ Microsoft Windows 11 Pro/Enterprise [5]
	Remarque : Microsoft Windows 11 Pro/Enterprise ne prend pas en charge la gestion des serrures à distance en raison des limites imposées par Microsoft sur le nombre de connexions réseau simultanées.			
Base de données [6]	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	▪ SQL Server Express 2022/2019/2017 ▪ SQL Server 2022/2019/2016	sans objet
Navigateur Internet [7]	▪ Google Chrome (dernière version) ▪ Microsoft Edge (dernière version)	▪ Google Chrome (dernière version) ▪ Microsoft Edge (dernière version)	▪ Google Chrome (dernière version) ▪ Microsoft Edge (dernière version)	▪ Google Chrome (dernière version) ▪ Microsoft Edge (dernière version)

[1] Le matériel supplémentaire recommandé pour le serveur comprend : sauvegarde UPS, carte graphique HD intégrée, clavier/souris.

[2] Processeurs pris en charge : Intel et AMD x64.

[3] Un espace disque libre supplémentaire peut être requis en fonction des paramètres de sauvegarde et archivage de base de données.

[4] Community est localisé pour tous les systèmes d'exploitation pris en charge. Langues : anglais, français. Notez que les paramètres de langue du navigateur peuvent affecter le texte à l'écran.

[5] TPM (Trusted Platform Module) 2.0 est requis pour exécuter Windows 11.

[6] a) SQL Server 2022 Express est regroupé avec Community et peut être sélectionné pour être installé pendant l'installation. b) IMPORTANT : Pour des raisons de sécurité, dormakaba recommande vivement d'utiliser SQL Server 2022 (Standard ou Express). c) IMPORTANT : en raison des limitations de SQL Server Express, dormakaba recommande SQL Server Standard pour les déploiements à moyenne et grande échelle. Pour en savoir plus, consultez la documentation Microsoft. d) Pour des déploiements à grande échelle, dormakaba recommande d'utiliser un serveur dédié pour la base de données Community. e) Microsoft signale des problèmes qui empêchent SQL Server de s'installer correctement sur un contrôleur de domaine. Évitez d'installer SQL Server sur un contrôleur de domaine. f) Le support de stockage sur lequel SQL Server sera installé ne peut pas dépasser une taille de secteur de 4 096 octets. Les lecteurs dont la taille des secteurs est plus importante ne sont pas pris en charge et entraîneront l'échec de l'installation.

[7] Résolution recommandée pour le navigateur Internet : 1366 x 768 ou plus.

3.2 Exigences du réseau

L'IT du site est responsable de l'établissement et de la maintenance d'un environnement réseau sécurisé (Ethernet ou Wi-Fi) sur lequel le serveur Community, les postes de travail et les interfaces intégrées sont déployés et utilisés.

3.2.1 Déploiement sur une machine virtuelle

En cas de déploiement de Community sur une VM (machine virtuelle) dans le cloud, un VPN (réseau privé virtuel) est requis pour sécuriser la communication entre le site et la machine virtuelle dans le cloud.

3.2.2 Ports de communication

Le tableau suivant énumère les paramètres de port par défaut du serveur Community. Si vous disposez d'un pare-feu, des modifications de configuration peuvent être nécessaires pour rendre les ports accessibles au serveur Community. Les ports entrants nécessitent une règle de pare-feu pour autoriser la communication avec le serveur.

> Les ports du service Windows Sync Share (80/443) sont en conflit avec l'interface utilisateur Web Community. dormakaba recommande de supprimer ou de désactiver cette fonctionnalité Windows.

10000-14999 et 30000-39000			Plages de ports disponibles pour la surveillance et l'analyse par des tiers
Port entrant	Port sortant	Protocole	Description
80/443		HTTP/S	Community Interface utilisateur Web
8083/443		HTTP/S	API SOAP Community
6120/6121		HTTP/S	API REST Community
28000/28001		TCP	Encodeur RFID I dormakaba (28000)/Encodeur RFID II dormakaba (28001, requis pour le mode de sécurité renforcée)
27700	27701	TCP	EN LIGNE – Passerelle I, Contrôle 4 (27701 est le port d'écoute sur le matériel)
28002		TCP	EN LIGNE – Passerelle II, RAC5-MFC/XT
	23211	TCP	EN LIGNE – INNCOM (23211 est le port d'écoute du serveur INNCOM)
123	123	UDP	Ouvrez un accès entrant et sortant sur le port UDP 123 afin que le trafic NTP (Network Time Protocol) soit autorisé et accessible en permanence à partir des serrures/passerelles.
40100		HTTP/S	Client Community et Programmateur M-Unit Aucune règle de pare-feu n'est requise. Ce port n'est pas exposé à un ordinateur externe ; il est réservé à l'hôte local.

Liste des URL autorisées

Établir une liste d'autorisation pour les URL suivantes :

- Licences : https://api.simat.dormakaba-tech.com
- Clés mobiles activées : https://api.legicconnect.com
- Authentification unique: https://*dormakaba-server*/WebAPI/Saml2 and https://*<dormakaba-server>*/WebAPI/Saml2/Acs

3.3 Exigences du périphérique

Cette section énumère les périphériques intégrés requis pour utiliser Community et les **dernières** versions de firmware.

> Les périphériques Community sont rétrocompatibles avec toutes les versions antérieures de firmware.

3.3.1 Clés RFID

Le tableau suivant présente les types de clés RFID prises en charge par Community.

Type de clé	Sécurité renforcée des clés	Sécurité des clés standard	Sécurité des clés héritées
MIFARE DESFire EV2/EV3	✓	✓	Non pris en charge
Cartes / porte-clés dormakaba RFID ComID (traité comme MIFARE DESFire, non répertorié dans l'interface utilisateur)	✓	✓	Non pris en charge
MIFARE Plus EV2	✓	Non pris en charge	✓
MIFARE Ultralight C	✓	✓	Non pris en charge

3.3.2 Encodeurs

Le tableau suivant répertorie les encodeurs pris en charge par Community et la **dernière** version de firmware.

Type d'encodeur	Dernier FW	Types de clés pris en charge
ENCODEUR RFID I dormakaba (référence 064-514822 ou 74750) (non pris en charge lorsque le mode de sécurité renforcée est activé)	1.015	MIFARE Plus EV2 MIFARE Ultralight C
ENCODEUR RFID II dormakaba (référence 75720) (requis lorsque le mode de sécurité renforcée est activé)	3.003 Version de l'applet : 1.003	MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C

Les encodeurs livrés avant septembre 2022 peuvent ne pas disposer de la version de l'applet requise pour une sécurité renforcée des clés. Pour plus d'informations, contactez le service de support dormakaba.

3.3.3 Programmateurs M-Unit

Le tableau suivant répertorie les programmateurs M-Unit pris en charge par Community et les **dernières** versions de firmware.

Type de programmeur	Dernière version de FW prise en charge	Version minimale de FW pour une sécurité renforcée
M-Unit SAFLOK HH6	1.53	Non pris en charge
M-Unit SAFLOK HH6 NFC (requis lorsque le mode de sécurité renforcée est activé)	2.46	2.40

3.3.4 Serrures

Le tableau suivant répertorie les serrures prises en charge et les **dernières** versions de firmware.

Le mode bascule n'est actuellement pas pris en charge pour RAC5 lorsque le mode de sécurité renforcée est activé.

Les dernières versions de firmware sont requises lors de la programmation des unités et des unités de suite en mode bascule pour les habitations multi-résidentielles.

Profil de la serrure	Boot & Main	Lecteurs pris en charge	Types de clés pris en charge	BLE	Zigbee AVR
Utilisation en mode de sécurité renforcée, standard et héritée					
Confidant NFC	03.09.26.4	Lecteur intégré	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	2.0.1.0	1.10x, 5.13x, 6.05x
MT4/Quantum (boot sécurisé)	02.19.26.4	Quantum (boot sécurisé) : 08.12.25.5	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
Quantum MT6 (boot sécurisé)	11.13.25.04	LEGIC	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	4.0.0.0	1.10x, 5.13x, 6.05x
Pixel +	11.13.25.04	LEGIC	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	4.0.0.0	1.10x, 5.13x, 6.05x
Pixel	02.19.26.4	Quantum (boot sécurisé) : 08.12.25.5	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
Nova	03.09.26.4	Lecteur intégré	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x/ 5.13x
RAC5 XT/Lite (matériel pour les espaces communs)	04.27.26.4 (principal uniquement)	Lecteur mural NFC : 04.27.26.3	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	2.0.1.0	N/A
RCU	02.19.26.4	Lecteur mural SR : 07.22.25.3	Apple Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
RT+	03.09.26.4	Lecteur intégré	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	2.0.1.0	1.10x, 5.13x, 6.05x
Saffire LX-D	03.09.26.4	Lecteur intégré	Apple Wallet, Google Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	2.0.1.0	5.13x/ 6.05x

Profil de la serrure	Boot & Main	Lecteurs pris en charge	Types de clés pris en charge	BLE	Zigbee AVR
SRK (Secure Reader Keyscan)	09.19.25.3	LEGIC	Apple Wallet, BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	2.0.1.0	1.10x, 5.13x, 6.05x
Utilisation en mode de sécurité standard et héritée					
Confidant	09.03.19.2	Lecteur intégré	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x/ 5.13x
MT4/Quantum	10.11.19.2	Quantum (boot sécurisé) : 09.17.16.1	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x
RT	06.14.18.2	Lecteur intégré	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x, 5.13x, 6.05x

Tous les profils de la serrure prennent en charge toutes les versions antérieures du firmware, à l'exception de RT ; la serrure RT prend en charge les versions du firmware depuis 2015.

Les modèles de serrure RT et hérités Confidant ne prennent pas en charge la fonction des espaces communs étendus.

-

3.3.5 Contrôleurs d'ascenseur

Le tableau suivant répertorie les contrôleurs d'ascenseur pris en charge et les **dernières** versions de firmware.

	Boot & Main	Lecteurs pris en charge	Types de clés pris en charge	BLE	Zigbee AVR
Sécurité renforcée, standard et héritée					
ECU/RCU4	02.19.26.4	Quantum (boot sécurisé) : 08.12.25.5	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x
RAC5-MFC	04.27.26.4	Lecteur mural NFC : 04.27.26.3	Apple Wallet, Google Wallet. BLE MIFARE DESFire EV2/EV3 MIFARE Plus EV2 MIFARE Ultralight C	2.0.1.0	N/A
Sécurité standard et héritée					
ECU/RCU4	10.11.19.2	Quantum (boot sécurisé) :09.17.16.1	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	1.10x
Anciens MFC	0.017 (principal uniquement)	Lecteur intégré	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	N/A
EMCC	20090929 (principal uniquement)	Lecteur intégré	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	N/A

	Boot & Main	Lecteurs pris en charge	Types de clés pris en charge	BLE	Zigbee AVR
MCC 8/12	0.031398 (principal uniquement)	Lecteur intégré	BLE MIFARE Plus EV2 MIFARE Ultralight C	1.3.1.0	N/A

3.3.6 Passerelles Zigbee

Le tableau suivant présente les passerelles Zigbee prises en charge par Community et les **dernières** versions de firmware.

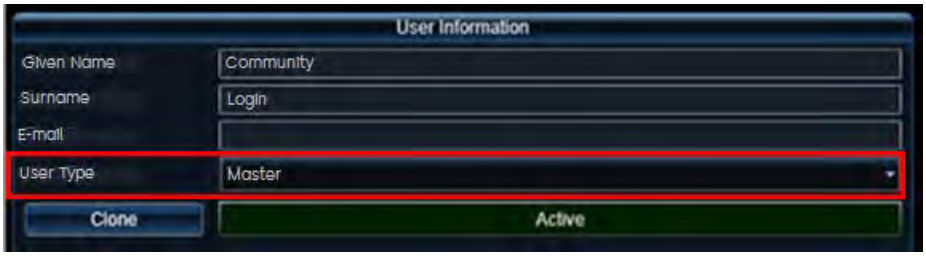
	Boot	BLE	Zigbee
Passerelle I	0.221	N/A	1.10x/5.13x
Passerelle II	0.022	N/A	6.05x

3.4 Exigences en matière d'interface

Community prend en charge ce qui suit :

- Aurora sous licence pour SDK — v1.0.19 à v1.0.25

Pour les sites avec des intégrations Aurora, vérifiez que le Type d'utilisateur est défini sur « Maître » pour l'utilisateur du système Community créé dans Aurora, conformément au manuel d'intégration Aurora. Les autres Types d'utilisateurs ne fonctionneront plus avec Community 2.6.0.



Pour les intégrations Aurora, les exigences suivantes s'appliquent lorsque la licence Community inclut la Gestion des visiteurs :

- Activer le code PIN étendu (7 chiffres), (Application)
- Activer la génération automatique de codes PIN
- Activer les identifiants Keyscan pour le format de carte étendu
- Activer le Mode intégré KABA
- Activer le mode Expiration automatique
- Activer le comptage des cartes sur les ACU
- Selon l'ACU, sélectionnez le mode de lecteur S - Intégration KABA

Pour en savoir plus, reportez-vous au *CommunityManuel de déploiement et de support de l'intégration Aurora* (PK3769).

3.5 Interfaces et périphériques de communication en ligne

Le tableau suivant présente les combinaisons de passerelles en ligne prises en charge par Community. Par exemple, le périphérique Passerelle I est compatible avec d'autres périphériques Passerelle I, les contrôleurs d'ascenseur RAC5 et MFC, et une interface tierce.

	Périphérique Passerelle I compatible avec	Périphérique Passerelle II compatible avec	Rx-Link compatible avec	RAC5-MFC/XT compatible avec
Périphérique Passerelle I	✓	Non pris en charge	Non pris en charge	✓
Périphérique Passerelle II	Non pris en charge	✓	✓	✓
Rx-Link	Non pris en charge	✓	✓	✓
RAC5-MFC	✓	✓	✓	✓
RAC5 XT	✓	✓	✓	✓
Anciens MFC	✓	Non pris en charge	Non pris en charge	Non pris en charge
Interfaces tierces (mutuellement exclusives)				
INNCOM	✓	✓	✓	✓
INTEREL	✓	Non pris en charge	Non pris en charge	Non pris en charge
Telkonet	Non pris en charge	Non pris en charge	✓	Non pris en charge
Control4	✓	Non pris en charge	Non pris en charge	Non pris en charge

3.6 Support de serrure pour la communication en ligne

Le tableau suivant présente les serrures compatibles avec la gestion des serrures à distance (communication en ligne).

	Passerelle I / Anciennes interfaces tierces Interfaces (Zigbee Gen I)	Passerelle II / Rx-Link	
		Zigbee Gen II Phase 1	Zigbee Gen II Phase 2
Pixel	✓	✓	✓
Pixel+	✓	✓	✓
MT4	✓	✓	✓
MT6	✓	✓	✓
RCU4	✓	✓	✓
RT	✓	✓	Non pris en charge
RT+	✓	✓	✓
Saffire LX	✓	✓	✓
Nova	✓	✓	✓
Confidant	✓	✓	Non pris en charge
Confidant NFC	✓	✓	✓

3.7 Exigences No Touring

La fonction No Touring annule l'accès aux espaces communs lorsqu'une clé de résident est annulée avant la date d'expiration. Pour utiliser cette fonction, les conditions suivantes doivent être remplies :

- Les serrures doivent être mises à jour avec la dernière version du firmware.
- Le programmateur M-Unit (HH6) doit être mis à jour avec le dernier firmware.



Pour plus d'informations sur le programmateur M-Unit, consultez le *Guide d'utilisation de Saflok HH6*.

3.8 Composants prérequis tiers

The following table lists components installed with Community and validated for this release.

Third-Party Software	Version
Microsoft .NET Framework	4.8.1 Full
Microsoft .NET Windows Server Hosting	8.0.30.26373
Microsoft ODBC Driver 17 for SQL Server	17.10.6.1
Microsoft Command Line Utilities 15 for SQL Server	15.0.4298.1
Microsoft OLE Database Driver 19 for SQL Server	19.4.2.0
Microsoft OLE Database Driver 18 for SQL Server	18.7.5.0
RabbitErlang	4.3.4
Erlang	OTP 27.3.4.15 (ERTS 15.2.7.11)
Redis on Windows	3.2.100
Redis Desktop Manager	0.8.3.3850
MongoDB	8.2.12 2008R2Plus SSL x64
Mongosh	2.9.2
Microsoft SQL Server Express (if selected)	2022 16.0.4265.3
Microsoft SQL Server update	KB5093420
IIS URL Rewrite Module 2	7.2.1952
Microsoft Visual C++ Redistributable	12.0.30501.0 x64
Microsoft Visual C++ Redistributable	2015-2022 14.44.35112.1 x64
Microsoft Visual C++ Redistributable	2015-2022 14.44.35112.1 x86

4 Liste de contrôle avant l'installation

Les éléments suivants s'appliquent uniquement aux installations initiales.

4.1 Exigences

1	☐	Serveur/Client. Vérifiez que toutes les exigences applicables sont satisfaites.
2	☐	Serveur. Vérifiez que les paramètres Date/heure et Fuseau horaire sont corrects. (Le serveur Community et les serrures installées aux points d'accès doivent être configurés pour le même fuseau horaire.)
3	☐	**IMPORTANT !** Serveur/Client. Vérifiez que toutes les mises à jour Windows sont installées.
4	☐	Serveur. Vérifiez que Windows PowerShell 4.0 est installé.
5	☐	Serveur. Vérifiez que les programmes suivants ne sont **PAS** installés :
6	☐ SQL Server (uniquement si vous ne vous connectez pas à une instance SQL existante)	
7	☐ Redis	
8	☐ RabbitMQ	
9	☐ Serveur web IIS	
10	☐	Serveur. Vérifiez que vous disposez d'une clé d'activation pour Community .
11	☐	Désactivez les paramètres d'économie d'énergie USB de Windows (pour que les encodeurs connectés via USB fonctionnent correctement).
12	☐	Supprimez ou désactivez le service Windows Sync Share. La fonction utilise des ports en conflit avec Community.
13	☐	Serveur/Client. Vérifiez que le système d'exploitation est opérationnel et activé.
14	☐	Serveur/Client. Effectuez l'installation en tant qu'**Administrateur local**.
15	☐	Le cas échéant, préparez-vous à vous connecter à une instance existante de SQL Server.
16	☐	Serveur. Assurez-vous que le logiciel antivirus est désactivé avant de procéder à l'installation du serveur.
17	☐	Serveur. Si la langue utilisée pour l'interface utilisateur est différente de la langue du système d'exploitation du serveur, il est nécessaire d'installer le pack de langues Microsoft Windows correspondant à la langue de l'interface utilisateur pour les rapports Community afin d'afficher les informations appropriées.
18	☐	Vérifiez que le support de stockage sur lequel SQL Server sera installé ne dépasse pas une taille de secteur de 4 096 octets. Les lecteurs dont la taille des secteurs est plus importante ne sont pas pris en charge et entraîneront l'échec de l'installation.

4.2 Recommandations

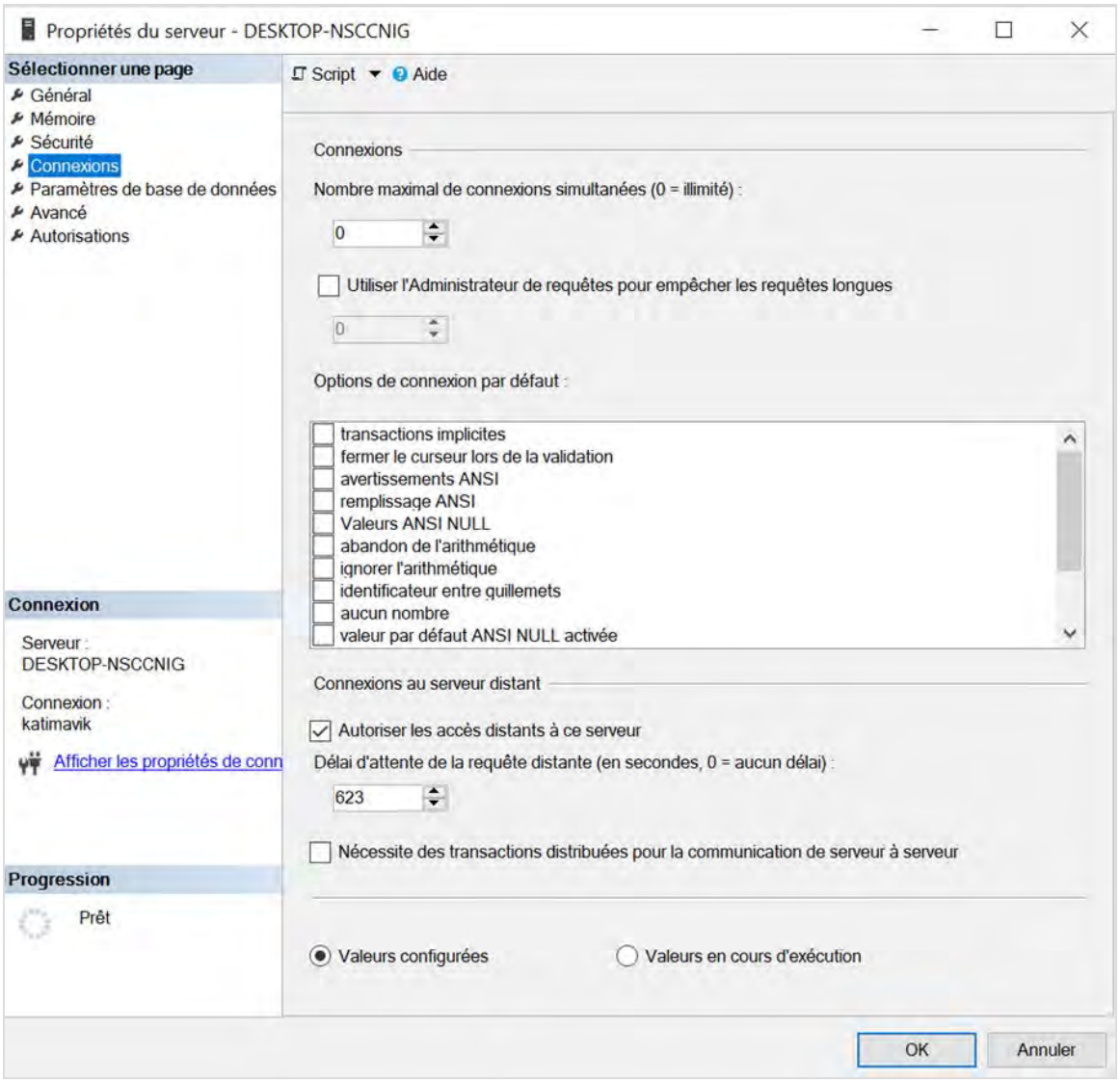
1	☐	**IMPORTANT !** Installez le serveur Community dans un emplacement physique sécurisé.
2	☐	**IMPORTANT !** Vérifiez bien que l'édition de SQL Server répond aux exigences de l'organisation.
3	☐	Serveur. En cas de déploiement sur une machine virtuelle dans le cloud, configurez un VPN pour sécuriser la communication entre le site et la machine virtuelle dans le cloud.
4	☐	Serveur. Vérifiez si le serveur sur lequel SQL Server est installé n'est pas un contrôleur de domaine.
5	☐	Serveur. Si possible, désactivez Windows Defender pendant la durée de l'installation.
6	☐	Serveur. Configurez le serveur Community avec une adresse IP statique.
7	☐	Assurez-vous que le programme d'installation de votre système d'exploitation Windows est disponible.

5 Préparer l'utilisation d'une instance existante de SQL Server

Si vous souhaitez vous connecter à une base de données existante de SQL Server (locale ou distante), vous devez vous préparer avant de commencer l'installation.

1. Dans le pack d'installation Community, accédez au dossier COMMUNITY_PREREQUIS et copiez le fichier de base de données maître (Community.mdf) sur l'ordinateur distant où est installé Microsoft SQL Server. Chemin recommandé :
   C:\Program Files\Microsoft SQL Server\MSSQL*version.instanceName*\MSSQL\DATA\.
2. Cliquez avec le bouton droit de la souris sur le fichier de base de données et sélectionnez **Propriétés**. Désélectionnez l'attribut Lecture seule, puis cliquez sur **Appliquer** > **OK**.
3. Attachez la base de données :
   a. Ouvrez SQL Server Management Studio.
   b. Connectez-vous à une instance du moteur de base de données SQL Server.
   c. Dans l'Explorateur d'objets, développez la vue de l'instance.
   d. Cliquez avec le bouton droit de la souris sur **Bases de données** puis sélectionnez **Attacher**.
   e. Dans la boîte de dialogue Attacher des bases de données, cliquez sur **Ajouter**.
   f. Dans la boîte de dialogue Localiser les fichiers de base de données, naviguez jusqu'au fichier .mdf (précédemment collé à l'étape 1) et sélectionnez-le.
   g. Cliquez sur **OK**.

4. Cliquez avec le bouton droit de la souris sur le serveur et sélectionnez **Propriétés**.



5. Pour les **Connexions**, sélectionnez **Autoriser les connexions à distance à ce serveur**, puis cliquez sur **OK.**
6. Ouvrez le gestionnaire de configuration SQL Server.
7. Naviguez vers SQL Server Network Configuration > Protocols for instanceName (COMMUNITY).
8. Cliquez avec le bouton droit de la souris sur **TCP/IP** et sélectionnez **Propriétés**.
9. Dans la boîte de dialogue Propriétés TCP/IP, sélectionnez l'onglet **Adresses IP** et faites défiler jusqu'à **IPAll**.
10. Définissez les **Ports dynamiques TCP** sur vide et **Port TCP** sur **1433**. (Le port 1433 est l'instance par défaut utilisée par SQL Server).
11. Cliquez sur **Appliquer** > **OK**.

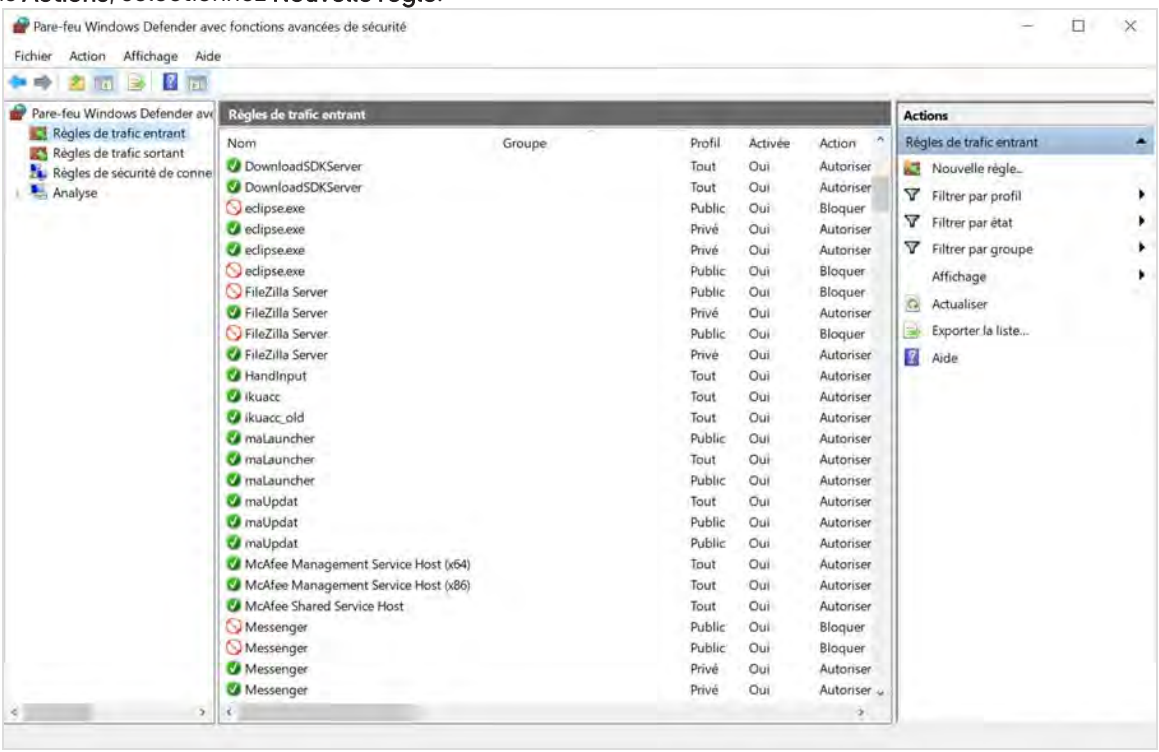
Si vous utilisez un pare-feu, passez à la section suivante pour ouvrir l'accès au moteur de base de données.

5.1 Configuration d'un pare-feu Windows pour l'accès au moteur de base de données

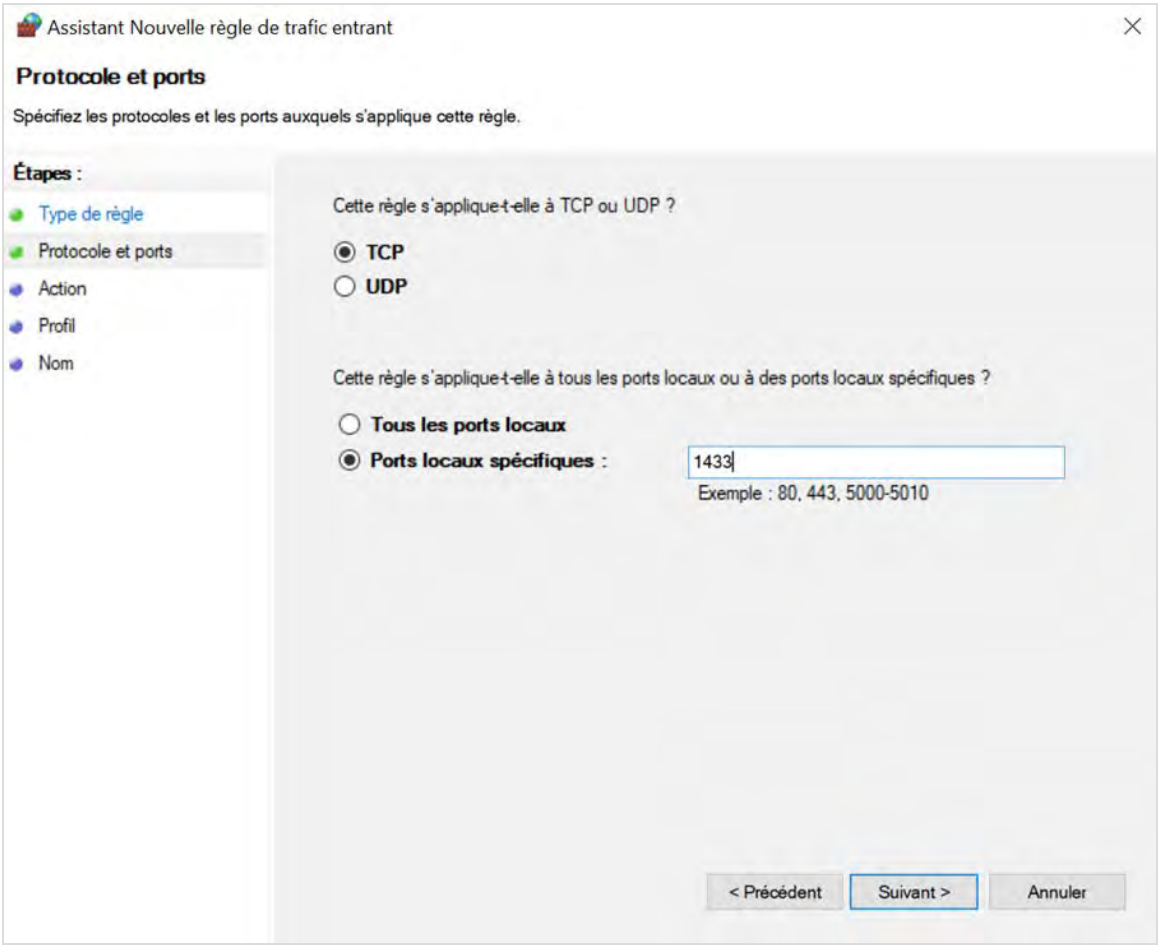
Si le pare-feu est activé, vous devez ajouter une exception pour le port 1433 afin d'autoriser le trafic TCP/IP sur le port 1433 et le trafic UDP sur le port 1434.

1. Dans la barre de recherche Windows, recherchez et ouvrez Outils d'administration.
2. Ouvrez le pare-feu Windows Defender avec Advanced Security.
3. Sélectionnez **Règles entrantes**.

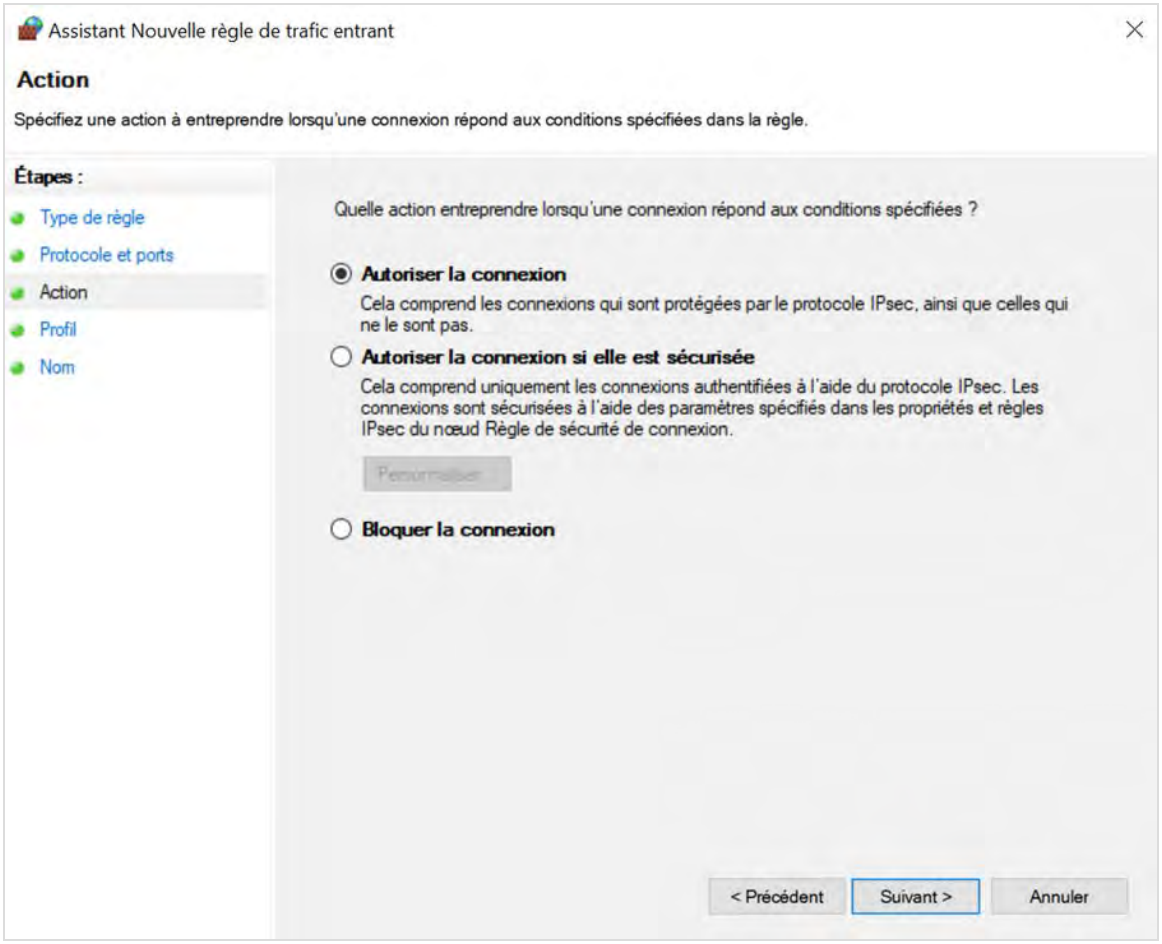
4. Sous **Actions**, sélectionnez **Nouvelle règle**.



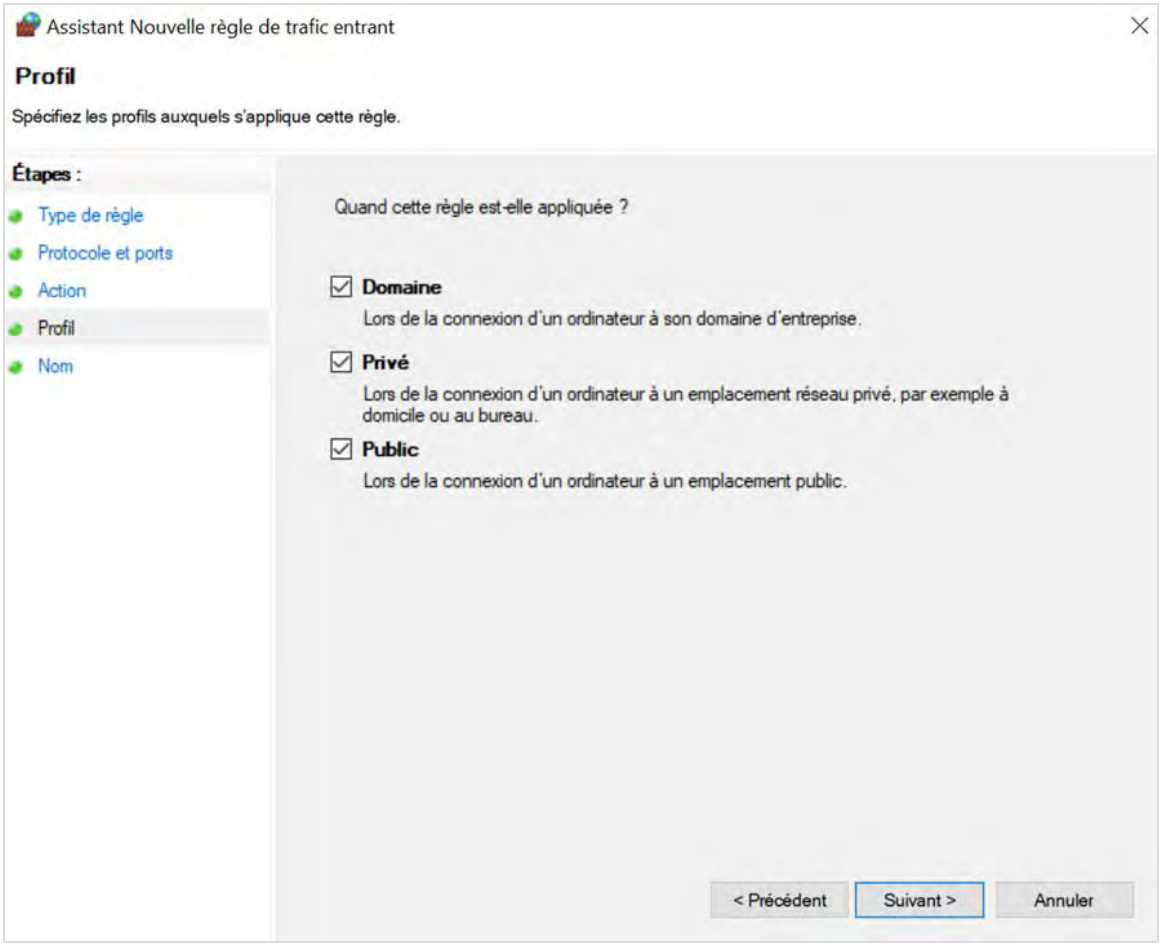
5. Pour le type de règle, sélectionnez **Port**, puis cliquez sur **Suivant**.
6. Pour les protocoles et les ports, sélectionnez **TCP** et spécifiez **1433** pour les **Ports locaux spécifiques**, puis cliquez sur **Suivant**.



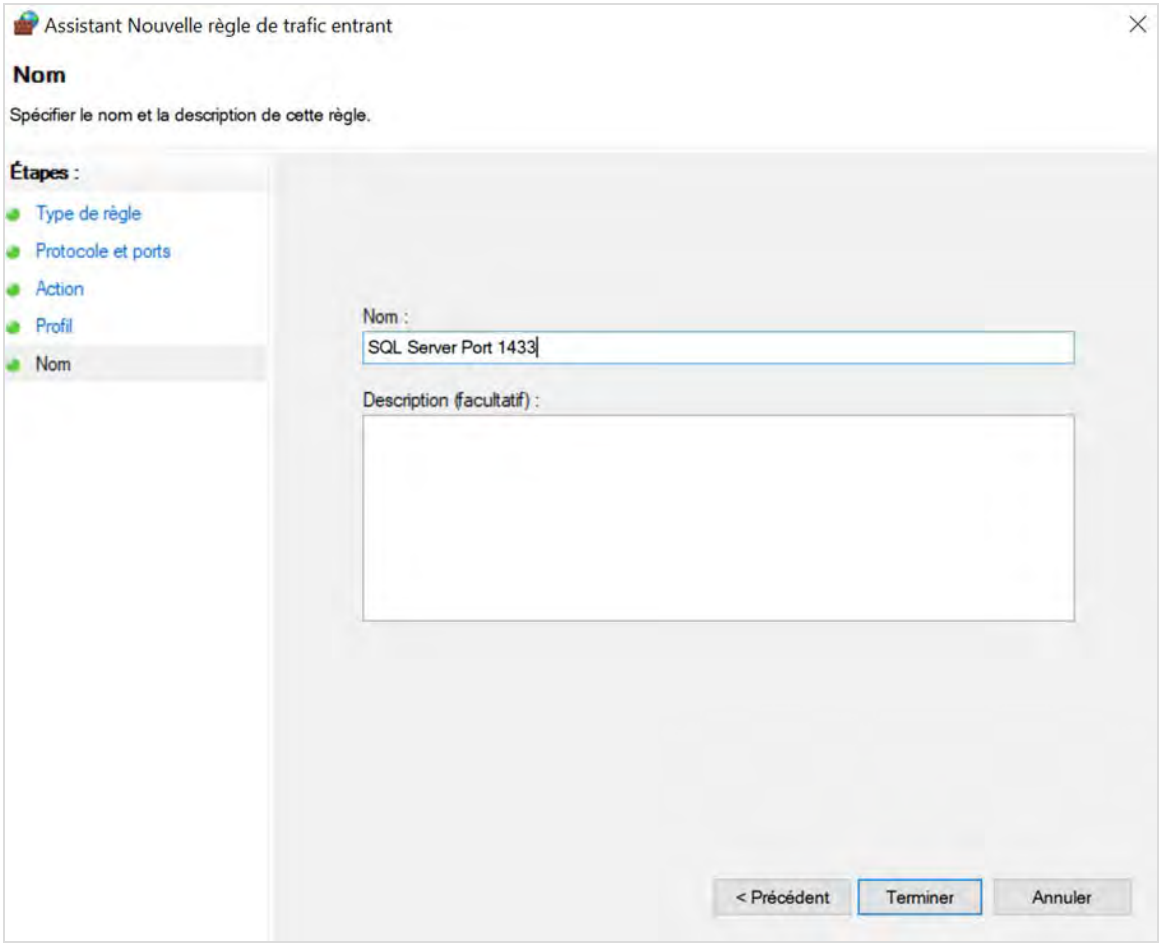
7. Pour l'action, sélectionnez **Autoriser la connexion** (pour spécifier l'action à entreprendre lorsqu'une connexion correspond aux conditions spécifiées dans la règle).



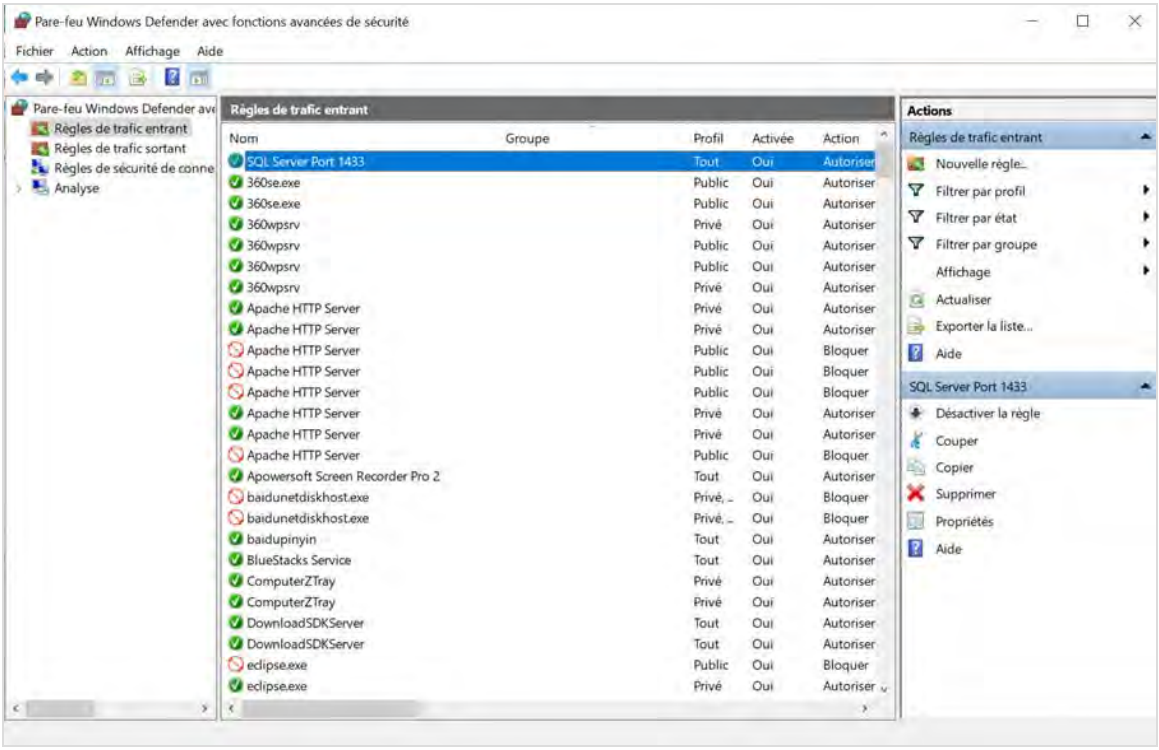
8. Pour les profils, sélectionnez les profils auxquels la règle s'applique, puis cliquez sur **Suivant**.



9. Pour le nom, indiquez le nom de la nouvelle règle, puis cliquez sur **Terminer**.



Vous pouvez maintenant voir la règle créée dans la liste des règles entrantes.



10. Répétez les mêmes étapes pour ajouter le port UDP 1434.

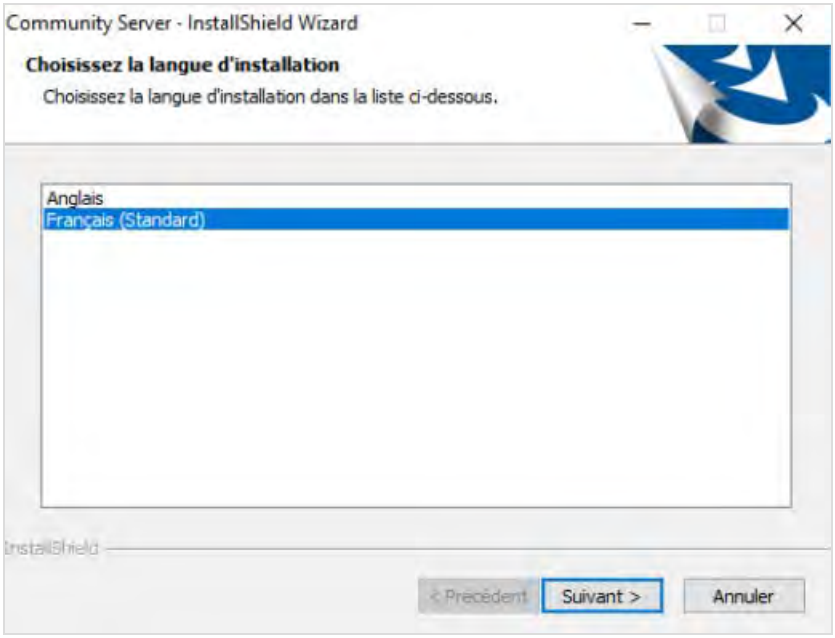
6 Installation du serveur Community

Ce chapitre porte sur les premières installations. Si l'installation est une mise à niveau, reportez-vous à *Mises à niveau Community*.

Pour installer le serveur Community :

1. Dans le dossier dormakaba/Community, ouvrez le dossier SERVER (SERVEUR).
2. Double-cliquez sur **CommunityServer.exe**. L'assistant d'installation s'ouvre et prépare l'installation. En fonction du serveur, vous pouvez être invité à installer des composants prérequis tiers.
3. Suivez les instructions pour chacune des pages suivantes de l'assistant. Lorsqu'un redémarrage est requis, confirmez pour procéder à l'installation.

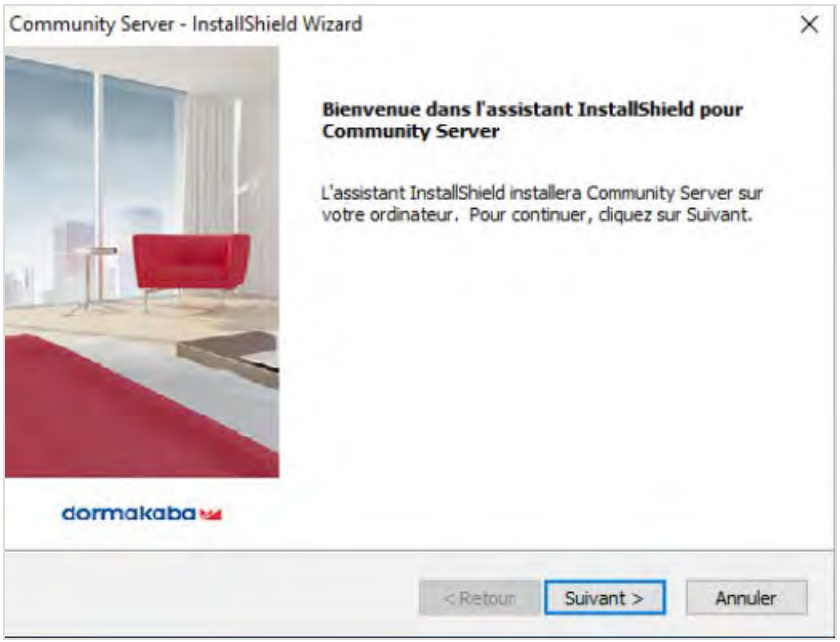
6.1 Page Choisir la langue d'installation



Sur la page Choisir la langue d'installation :

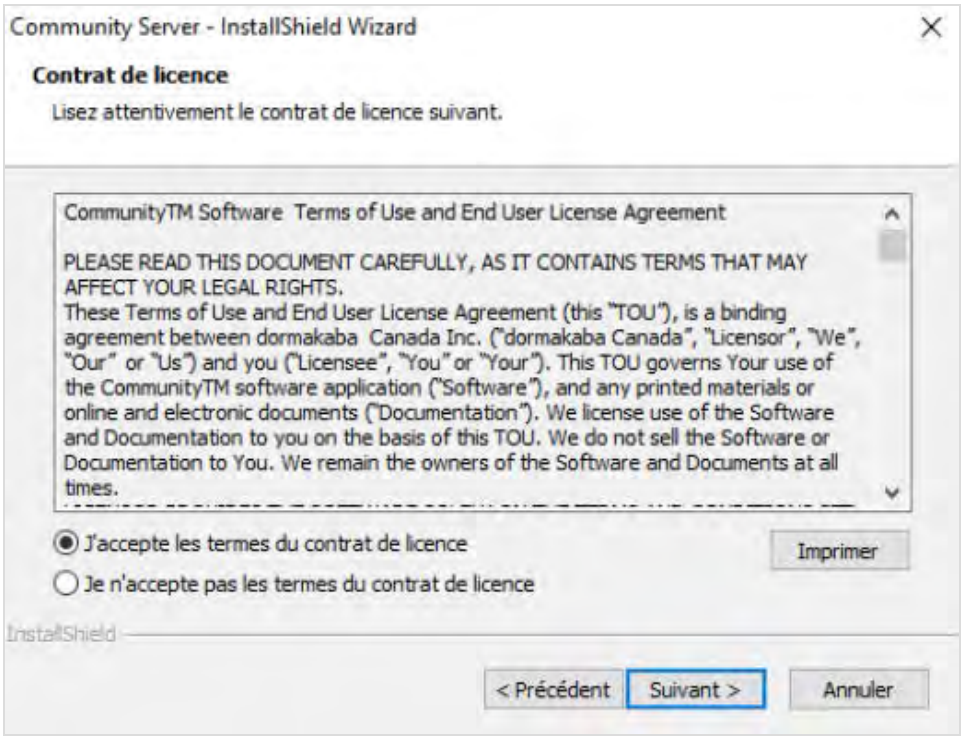
1. Sélectionnez **Français (Standard)**.
2. Cliquez sur **Suivant**.

6.2 Page de bienvenue



Sur la page de bienvenue, cliquez sur **Suivant**.

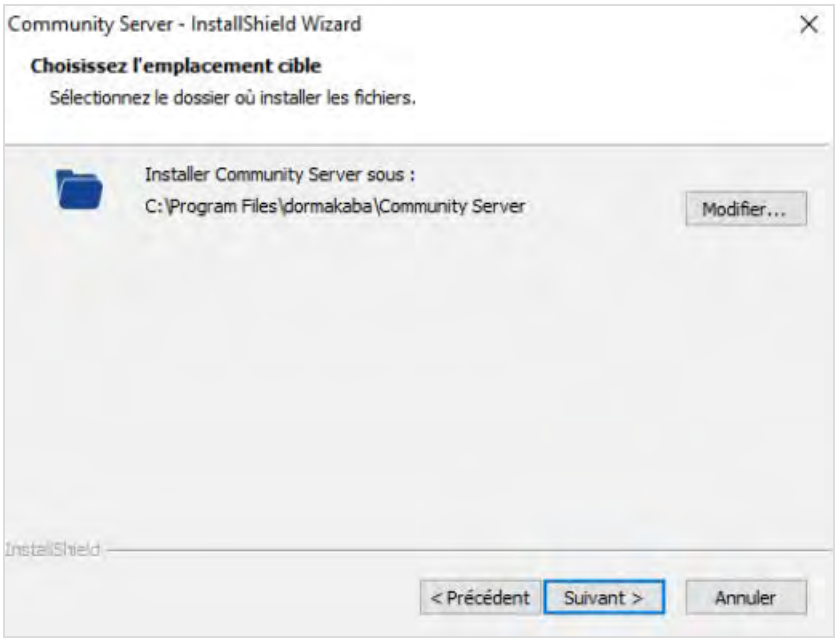
6.3 Page du contrat de licence



Sur la page du contrat de licence :

1. Acceptez les conditions du contrat de licence.
   Vous pouvez éventuellement imprimer le contrat.
2. Cliquez sur **Suivant**.

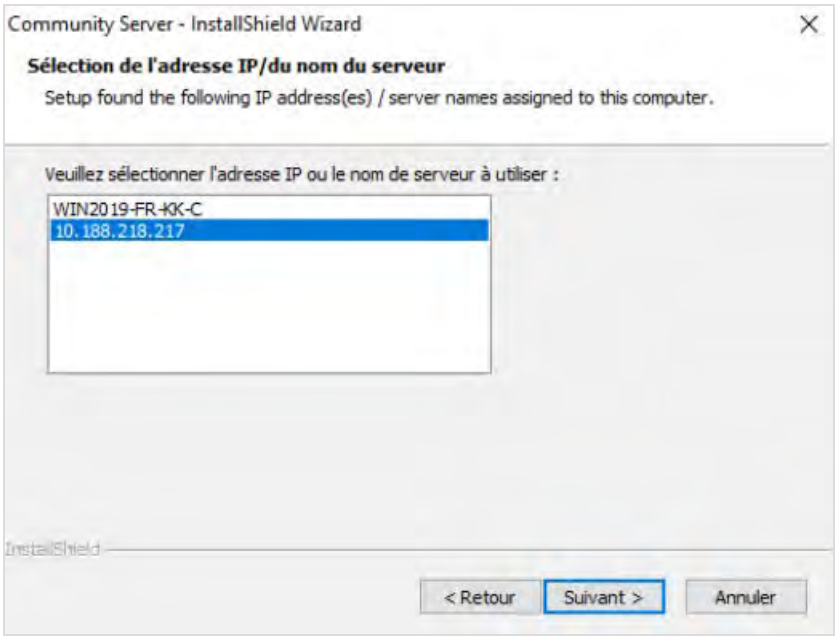
6.4 Page Choisissez l'emplacement de destination



Sur la page Choisissez l'emplacement de destination :

1. Choisissez l'emplacement d'installation des fichiers du serveur Community :
   - Acceptez l'emplacement par défaut (recommandé).
   - Cliquez sur **Modifier** puis accédez à un emplacement sur le serveur.
2. Cliquez sur **Suivant**.

6.5 Page de sélection de l'adresse IP/du nom du serveur



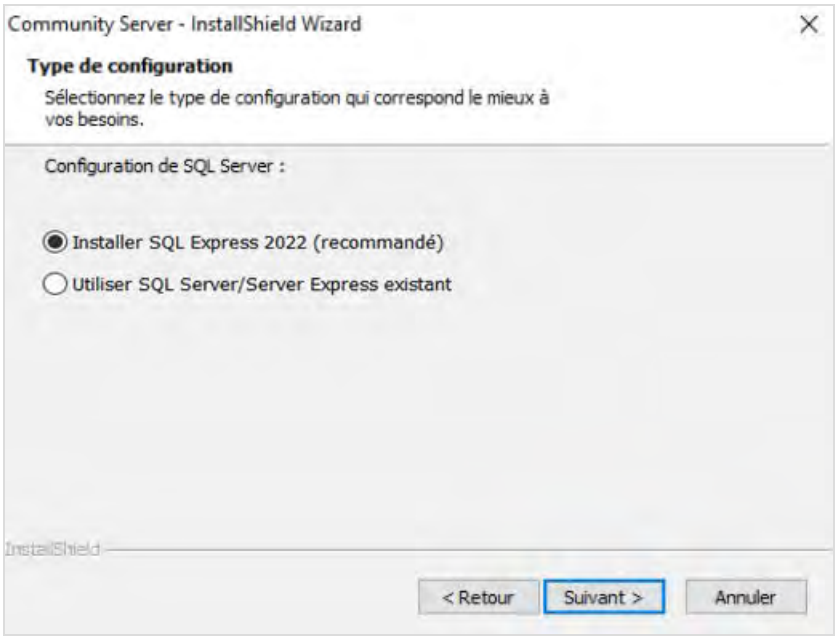
Sur la page de sélection de l'adresse IP/du nom du serveur :

1. Sélectionnez l'adresse IP ou le nom d'hôte à utiliser pour l'installation.
2. Cliquez sur **Suivant**.

Community doit être installé à l'aide d'une adresse IP statique (et non d'un nom d'hôte) pour que l'authentification unique fonctionne correctement.

6.6 Page Type d'installation

Cette page ne s'affiche que si le programme d'installation détecte une instance existante de SQL Server.

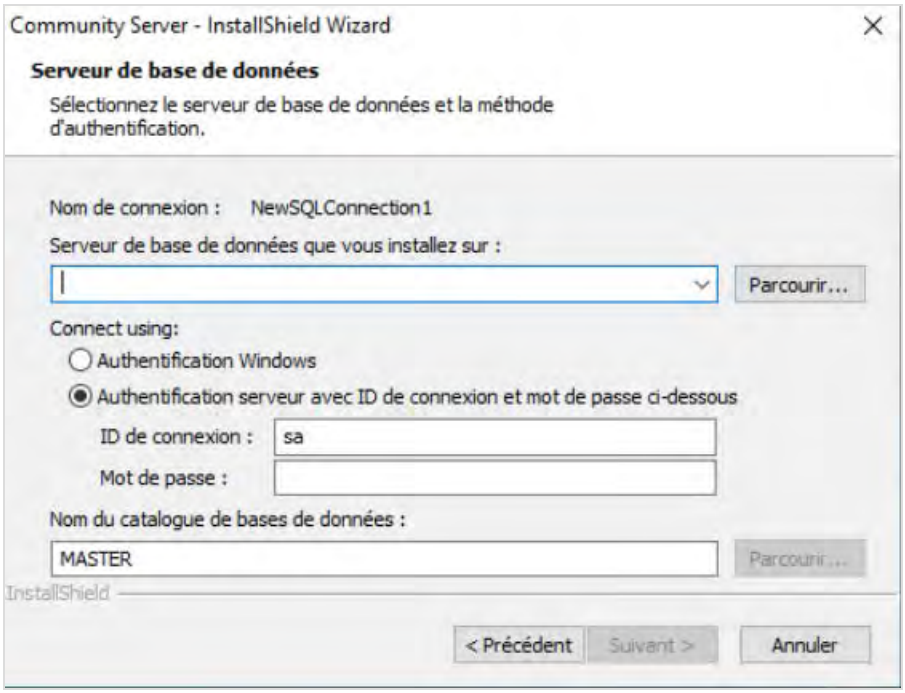


Sur la page Type d'installation :

Choisissez si vous souhaitez installer une nouvelle instance de SQL Server ou vous connecter à une instance de base de données SQL Server/Server Express locale ou distante. Si vous installez une nouvelle instance, SQL Server Express 2022 est installé. Toute instance à laquelle vous vous connectez doit être une version prise en charge (voir *Exigences*).

- Si vous installez une nouvelle instance, cliquez sur **Suivant** et passez à la *Page État de l'installation*.
- Si vous vous connectez à une instance existante, cliquez sur **Suivant** puis passez à la *Page SQL Database Server*.

6.7 Page SQL Database Server



Sur la page SQL Database Server :

1. Cliquez sur Parcourir, naviguez pour sélectionner la bonne instance SQL.
2. Saisissez des identifiants SQL Server valides
3. Cliquez sur **Suivant**.

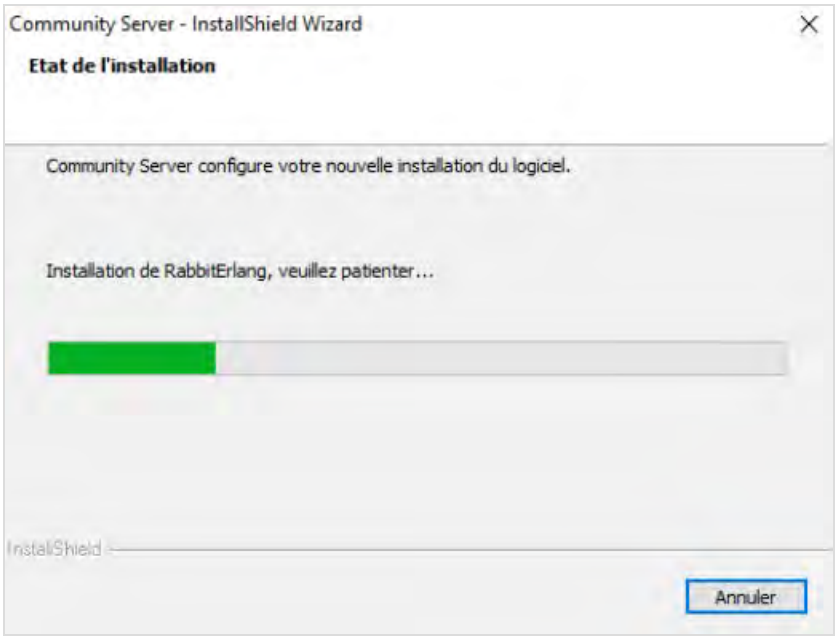
Si aucune base de données n'est attachée à l'instance sélectionnée, un message vous informe de vous préparer à utiliser une instance existante de SQL Server. Pour les instructions, voir le chapitre précédent.

Reportez-vous aux emplacements par défaut suivants.

Protection des	Emplacement de stockage	Option de sauvegarde	Fréquence	Conservation
SQL Server	Répertoire spécifié (local ou distant) Valeur par défaut : C:\Program Files\Microsoft SQL Server\MSSQL16.COMMUNITY\MSSQL\Backup	À la demande	À la demande	Sauvegarde actuelle
	Valeur par défaut pour les mises à niveau : les paramètres existants sont conservés	Par horaire	Par horaire	Par réglage
Clé symétrique RGPD	ProgramData\DormaKaba\Community\backup (local uniquement)	Selon la politique du site		

Protection des	Emplacement de stockage	Option de sauvegarde	Fréquence	Conservation
MongoDB	Dossier MongoDB dans le répertoire spécifié (local uniquement) Valeur par défaut pour les nouvelles installations et les mises à niveau avec SQL Server distant : aucune Valeur par défaut pour les mises à niveau avec SQL Server local : les paramètres existants sont conservés	Par horaire	Par horaire	Dernière sauvegarde
Archive	Répertoire spécifié (local autorisé mais disque dur externe, lecteur réseau ou serveur distant recommandé) Valeur par défaut : C:\Program Files\dormakaba\Community Server\Archive Valeur par défaut pour les mises à niveau : les paramètres existants sont conservés	Par horaire	Par horaire	Indéfini

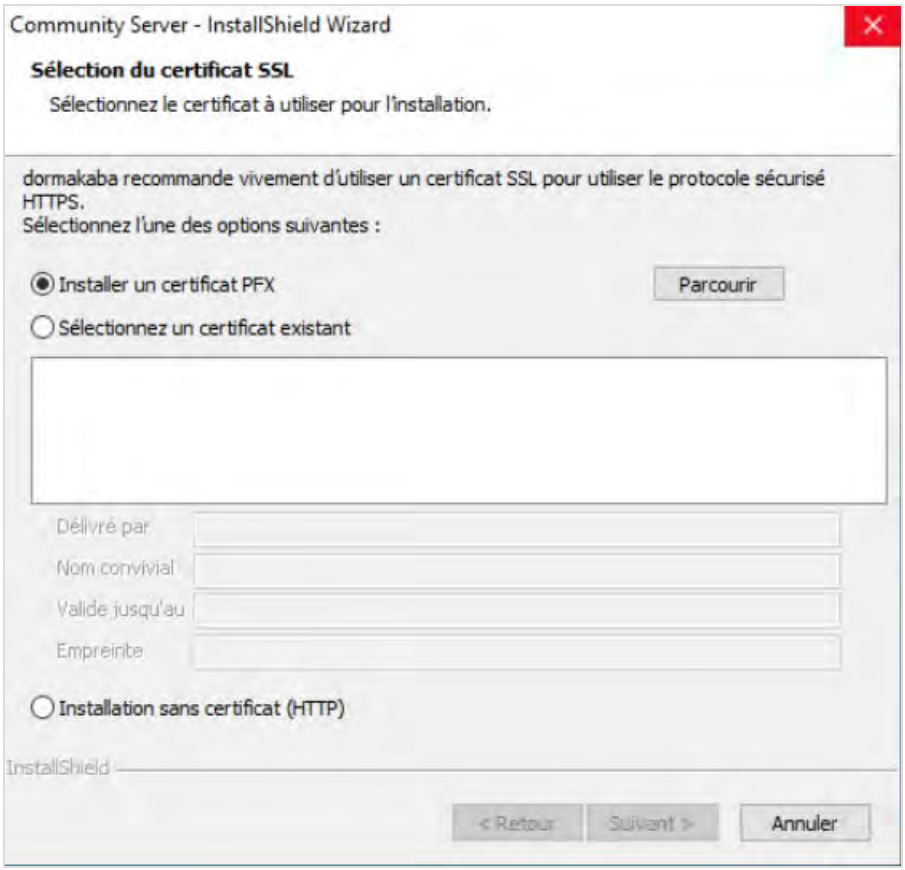
6.8 Page État de l'installation



La page État de l'installation affiche l'état de l'installation. Lorsque vous y êtes invité, cliquez sur **Suivant**.

6.9 Page Type de configuration

La sécurité dépend de vous. dormakaba recommande vivement d'installer un certificat SSL pour activer le protocole HTTPS. Le certificat SSL permettant d'activer le mode HTTPS doit être fourni par une autorité de certification reconnue et fiable.



Sur la page Type d'installation :

1. Choisissez d'installer ou non un certificat SSL.
2. Cliquez sur **Suivant**. Si vous continuez sans installer de certificat, un avertissement s'affiche.

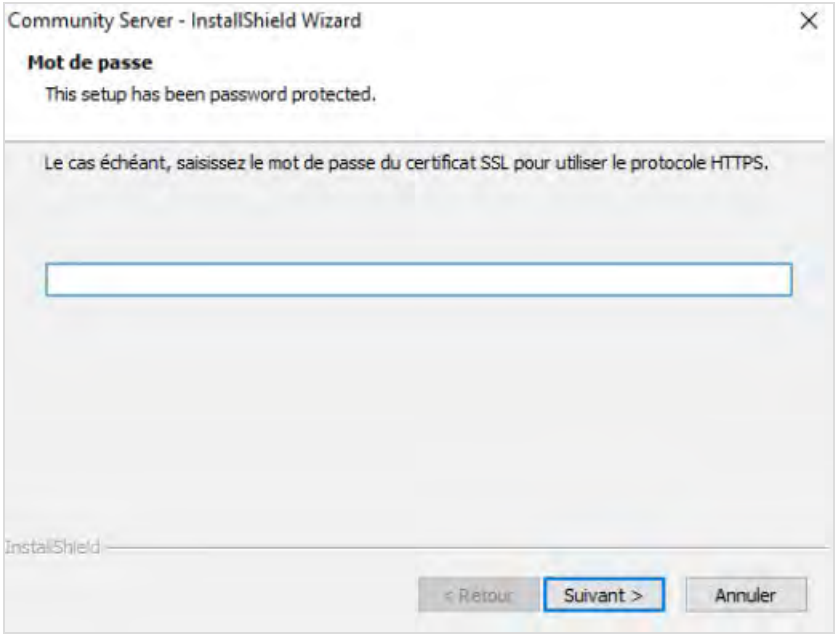
Pour installer un certificat SSL après l'installation, utilisez le Gestionnaire de services (sur le serveur) ; utilisez le Gestionnaire de services (sur les postes de travail) pour passer de l'IP/du nom du serveur à https://.

6.9.1 Choisissez le certificat SSL

Dans l'explorateur de fichiers :

1. Naviguez et sélectionnez le certificat SSL à installer.
2. Cliquez sur **Ouvrir**.

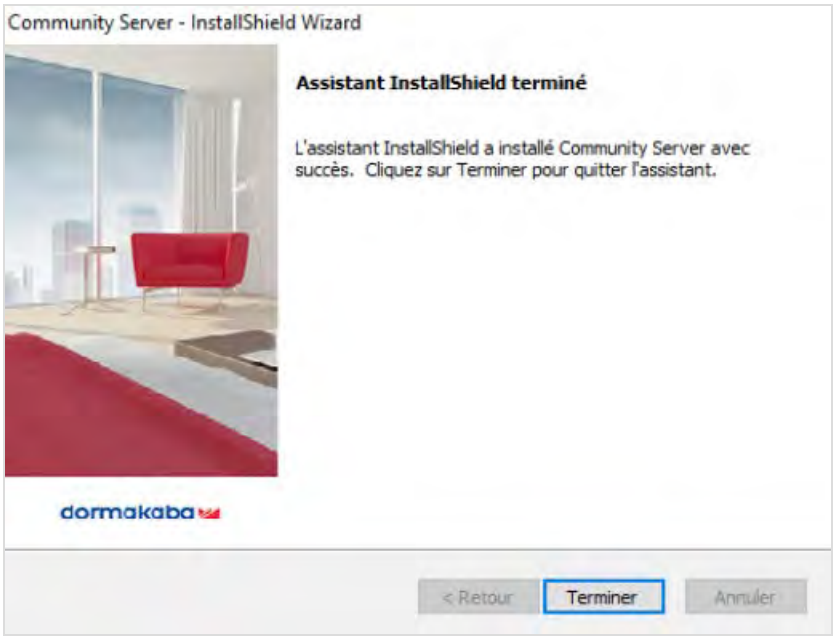
6.9.2 Page Mot de passe



Sur la page Mot de passe :

1. Saisissez le mot de passe du certificat SSL que vous avez sélectionné.
2. Cliquez sur **Suivant**.

6.10 Page Installation terminée



Lorsque vous êtes informé que l'installation est terminée, cliquez sur **Terminer**.

Une fois le serveur Community installé, mis à niveau ou redémarré, attendez deux à trois minutes avant d'utiliser Community.

7 Installation du client Community

Ce chapitre vous guide tout au long de l'installation du Client Community. Vous devez installer le Client sur chaque poste de travail où un encodeur USB et/ou un programmateur M-Unit est requis.

Pour installer le Client Community :

1. Dans un navigateur pris en charge, accédez à l'adresse IP du serveur Community.
2. Connectez-vous.
3. Accédez à Gestion des périphériques.

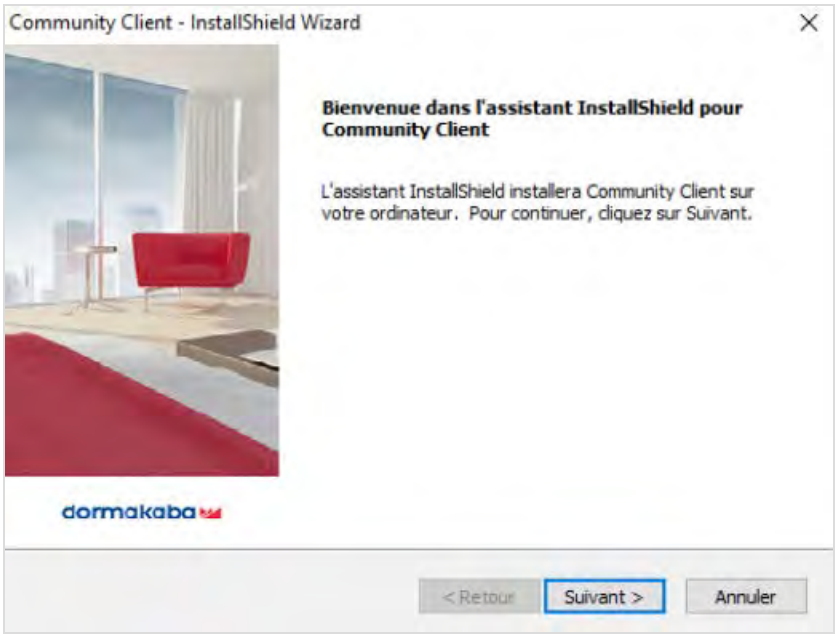


4. Dans la barre d'outils, cliquez sur installer le client Community.



5. Cliquez sur Télécharger. Trois fichiers sont nécessaires Community_Client.exe, serverURL.config et token.txt.
6. Ouvrez **Community.exe**. L'assistant d'installation s'ouvre et prépare l'installation. Selon l'ordinateur, l'étape suivante peut avoir lieu pendant l'installation :
   - L'assistant recherche Microsoft .NET 8.0 et l'installe s'il est introuvable.
7. Suivez les instructions pour chacune des pages suivantes de l'assistant.

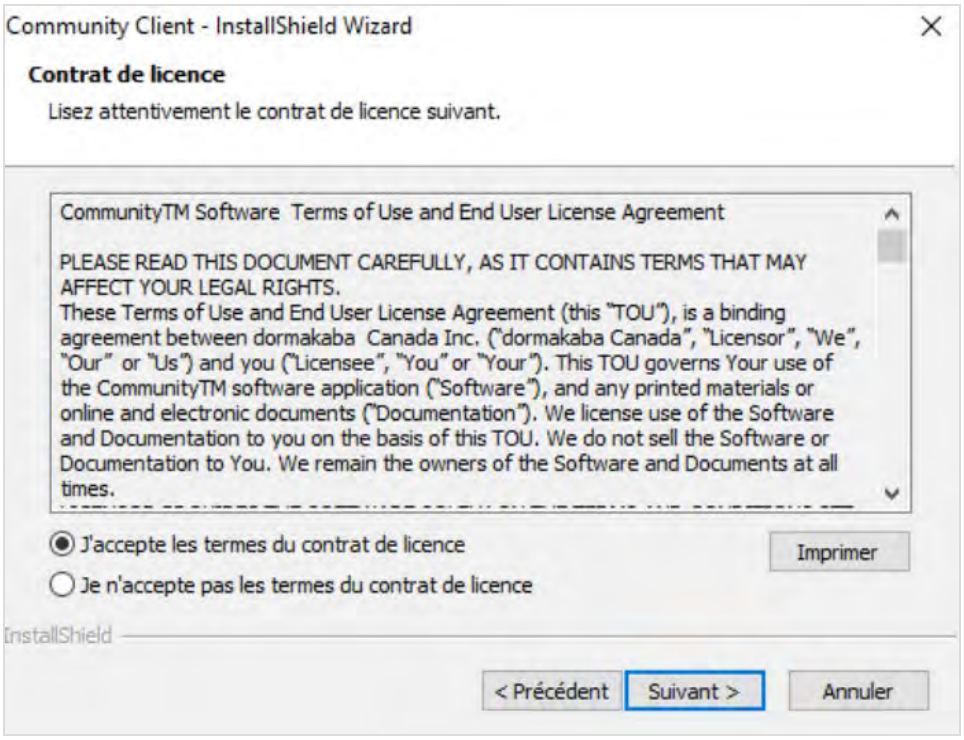
7.1 Page de bienvenue



Sur la page de bienvenue :

- Cliquez sur **Suivant**.

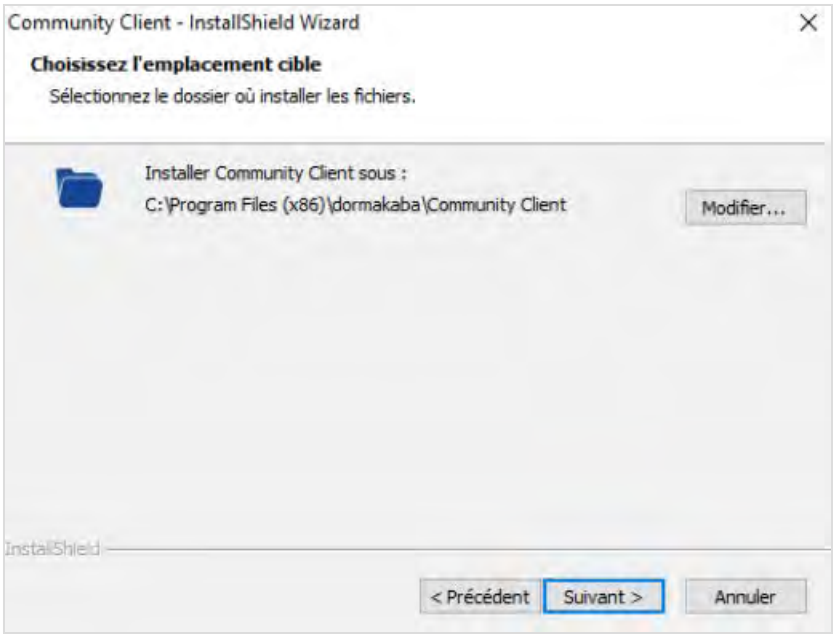
7.2 Page du contrat de licence



Sur la page du contrat de licence :

1. Acceptez les conditions du contrat de licence.
   Vous pouvez éventuellement imprimer le contrat.
2. Cliquez sur **Suivant**.

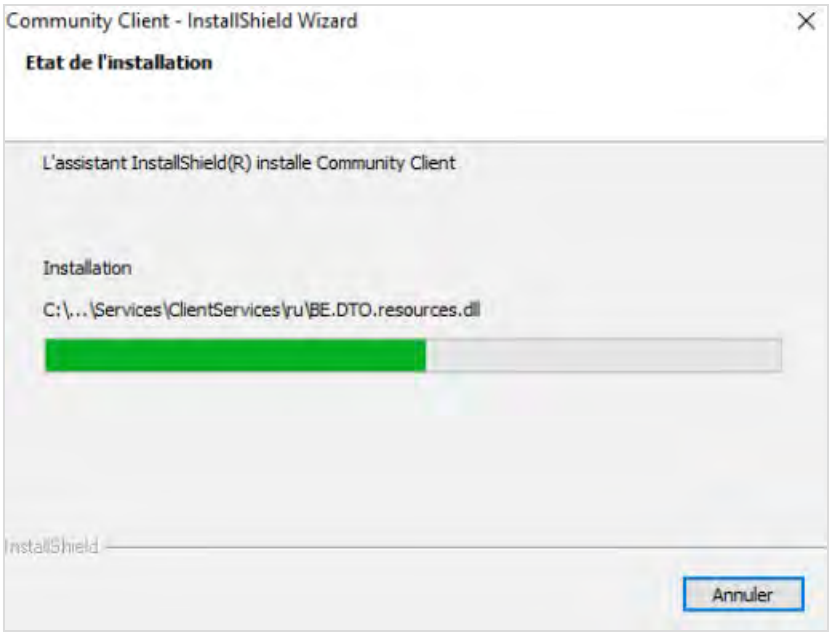
7.3 Page Choisissez l'emplacement de destination



Sur la page Choisissez l'emplacement de destination :

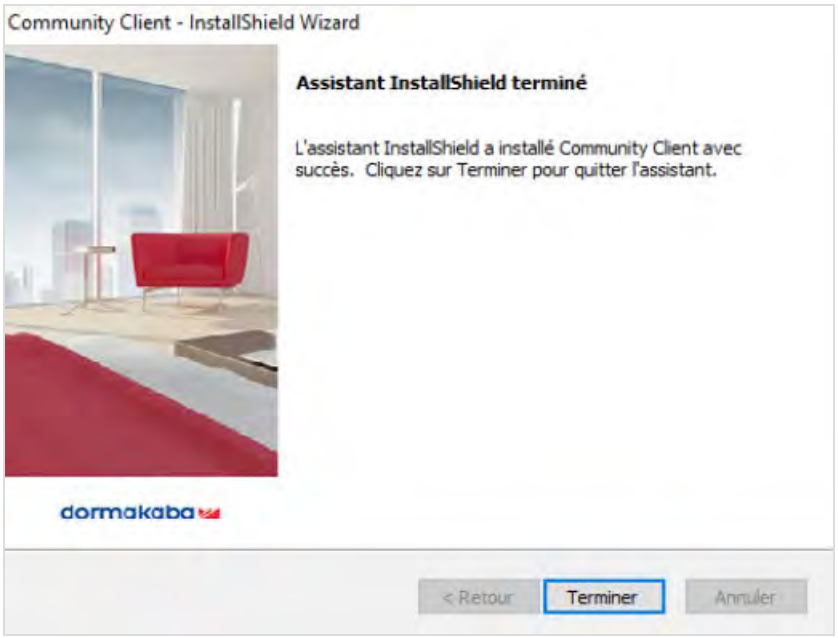
1. Choisissez l'emplacement d'installation des fichiers Client Community :
   - Acceptez l'emplacement par défaut (recommandé).
   - Cliquez sur **Modifier** puis accédez à un emplacement sur le serveur.
2. Cliquez sur **Suivant**.

7.4 Page État de l'installation



La page État de l'installation affiche l'état de l'installation. Lorsque vous y êtes invité, cliquez sur **Suivant**.

7.5 Page Installation terminée



Lorsque vous êtes informé que l'installation est réussie, cliquez sur Terminer.

8 Liste de contrôle après l'installation

Les éléments suivants s'appliquent uniquement aux installations initiales.

1	☐	Serveur. Réactivez le logiciel antivirus.
2	☐	Serveur. Si nécessaire, réactivez Windows Defender.
3	☐	Serveur. Activez le produit. Ouvrez Community dans un navigateur pris en charge et saisissez une clé d'activation valide pour Community 2.6.0.
4	☐	Serveur ou Client. Modifiez le mot de passe par défaut.
5	☐	Serveur (Installations en ligne uniquement). Assurez-vous que les versions du firmware de la passerelle et du point d'accès sont mises à jour, conformément à la section « Exigences des périphériques ».
6	☐	Microsoft Edge. Un problème avec Windows empêche le navigateur Edge de détecter/se connecter à un programmateur M-Unit. Les points d'accès ne peuvent donc pas être programmés ou audités sans intervention. Ouvrez l'Invite de commande et envoyez la commande suivante : `C:\windows\system32\CheckNetIsolation.exe LoopbackExempt -a -n=Microsoft.MicrosoftEdge_8wekyb3d8bbwe`
7	☐	Microsoft Edge. Ajoutez l'adresse IP du serveur Community comme site de confiance. Accédez au *Panneau de configuration > Réseau et Internet > Options Internet > Sécurité > Sites de confiance*. Cliquez sur Sites puis ajoutez l'adresse IP du serveur Community.
8	☐	Microsoft Edge. La sécurité par défaut du navigateur Microsoft Edge de Windows 10 bloque l'accès à l'hôte local, empêchant ainsi la communication du programmateur M-Unit pour procéder à la programmation des points d'accès et à des opérations d'audit. Utilisez Chrome ou exécutez la commande suivante à partir de la console Windows : ▪ Windows 10 Build 10158 ou supérieure : CheckNetIsolationLoopbackExempt-a-n=Microsoft.MicrosoftEdge_8wekyb3d8bbwen ▪ Pour les versions antérieures : CheckNetIsolationLoopbackExempt-a-n=Microsoft.Windows.Spartan_cw5n1h2txyewy
9	☐	Serveur. Accédez à ProgramData\DormaKaba\Community\backup, faites une copie du fichier de clé symétrique GDPR et stockez la clé dans un endroit sûr.

9 Mises à niveau Community

Ce chapitre fournit des informations et des instructions pour la mise à niveau des versions de Community et de SQL Server.

Conformément au Règlement général sur la protection des données (RGPD), lors d'une mise à niveau avec des données cryptées avec une clé symétrique générique, toutes les IPI (informations personnelles identifiables) sont recryptées avec une clé symétrique spécifique au site.

Les chemins de mise à niveau suivants sont pris en charge :

- 1.6 et supérieur à 2.6.0.

Community 2.3 a introduit le mode de sécurité renforcée pour fournir une couche supplémentaire de sécurité des clés. Même si la fonction est désactivée par défaut, dormakaba recommande vivement d'activer le mode de sécurité renforcée.

Avant de procéder à la mise à niveau, consultez le document *Community Sécurité renforcée des clés* pour connaître les conditions requises pour le mode de sécurité renforcée et obtenir des informations importantes sur la mise à niveau sans activer le mode de sécurité renforcée. Le document est disponible à la racine du dossier de téléchargement du logiciel.

9.1 Liste de contrôle avant la mise à niveau

1	☐	IMPORTANT ! Serveur/Client. Vérifiez que toutes les mises à jour Windows sont installées.
2	☐	IMPORTANT ! Serveur. Pour les sites en ligne, sauvegardez la base de données MongoDB. **Cette étape est nécessaire pour conserver les données de transaction.**
3	☐	Serveur. Faites une sauvegarde de la base de données de SQL Server.
4	☐	Serveur. Veillez à enregistrer une sauvegarde de la clé symétrique RGPD dans un emplacement sécurisé distinct. L' emplacement par défaut est : ProgramData\DormaKaba\Community\backup.
5	☐	Serveur/Client. Effectuez l'installation en tant qu'**Administrateur local**.
6	☐	Serveur. Assurez-vous que le logiciel antivirus est désactivé avant de procéder à l'installation du serveur.
7	☐	Serveur. Si possible, désactivez Windows Defender pendant la durée de l'installation.

9.2 Processus de mise à niveau

La mise à niveau est installée avec les mêmes options que celles sélectionnées lors de l'installation initiale.

1. Dans le dossier dormakaba/Community, ouvrez le dossier SERVER (SERVEUR).
2. Double-cliquez sur **CommunityServer.exe**. L'assistant d'installation s'ouvre et prépare l'installation.
3. Sur la page de bienvenue, cliquez sur **Suivant**.
4. Sur la page Contrat de licence, acceptez les conditions du contrat de licence puis cliquez sur **Suivant**. Vous pouvez éventuellement imprimer le contrat. Le processus de mise à niveau démarre.
5. Lorsque vous y êtes invité, indiquez si vous souhaitez redémarrer le serveur. Le redémarrage est nécessaire pour terminer la mise à niveau.

Le processus de mise à niveau comprend la mise à niveau de la base de données Community.

9.3 Liste de contrôle après la mise à niveau

1	☐	Redémarrez le Serveur Community.
2	☐	Serveur. Réactivez le logiciel antivirus.
3	☐	Serveur. Si nécessaire, réactivez Windows Defender.
4	☐	Serveur. Pour les propriétés en ligne qui passent de la version 2.4.2 et antérieure à la version 2.5 et ultérieure, et si votre SQL Server est distant, configurez l'emplacement de sauvegarde pour MongoDB dans *Paramètres du système > Sauvegarde de la base de données > Paramètres de sauvegarde de la base de données MongoDB*. Si votre SQL Server est local, la sauvegarde MongoDB reste enregistrée dans le dossier MongoBackup où sont stockées les sauvegardes de SQL Server, mais vous avez désormais la possibilité de configurer un autre emplacement.
5	☐	IMPORTANT ! Serveur. Restaurer la base de données MongoDB.

9.4 Mises à jour de SQL Server

dormakaba recommande vivement d'utiliser SQL Server 2022 (ou SQL Server Express 2022).
Pour effectuer une mise à niveau vers SQL Server 2022 :

1. Sauvegardez la base de données Community.
2. Dans le gestionnaire de services, arrêtez tous les services Community.
3. Exécutez la commande suivante :

   SQLEXPR_x64_ENU.exe /QS /ACTION=UPGRADE /INSTANCENAME= COMMUNITY /ISSVCAccount="NT Authority\Network Service" /IACCEPTSQLSERVERLICENSETERMS
4. Restaurez la base de données sauvegardée.
5. Redémarrez tous les services Community.

SQL Server 2022 (16.x) prend en charge la mise à niveau à partir des versions suivantes de SQL Server :

- SQL Server 2012 (11.x) SP4 ou version supérieure
- SQL Server 2014 (12.x) SP3 ou version supérieure
- SQL Server 2016 (13.x) SP3 ou version supérieure
- SQL Server 2017 (14.x)
- SQL Server 2019 (15.x)

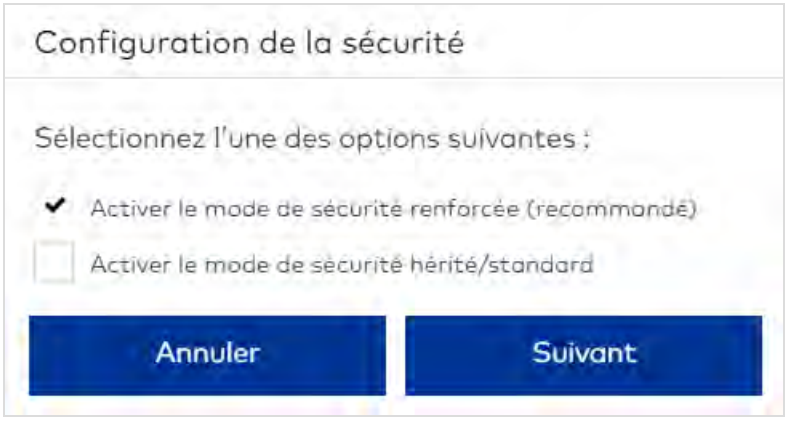
10 Démarrer avec Community

Ce chapitre fournit des informations de base pour démarrer avec Community.

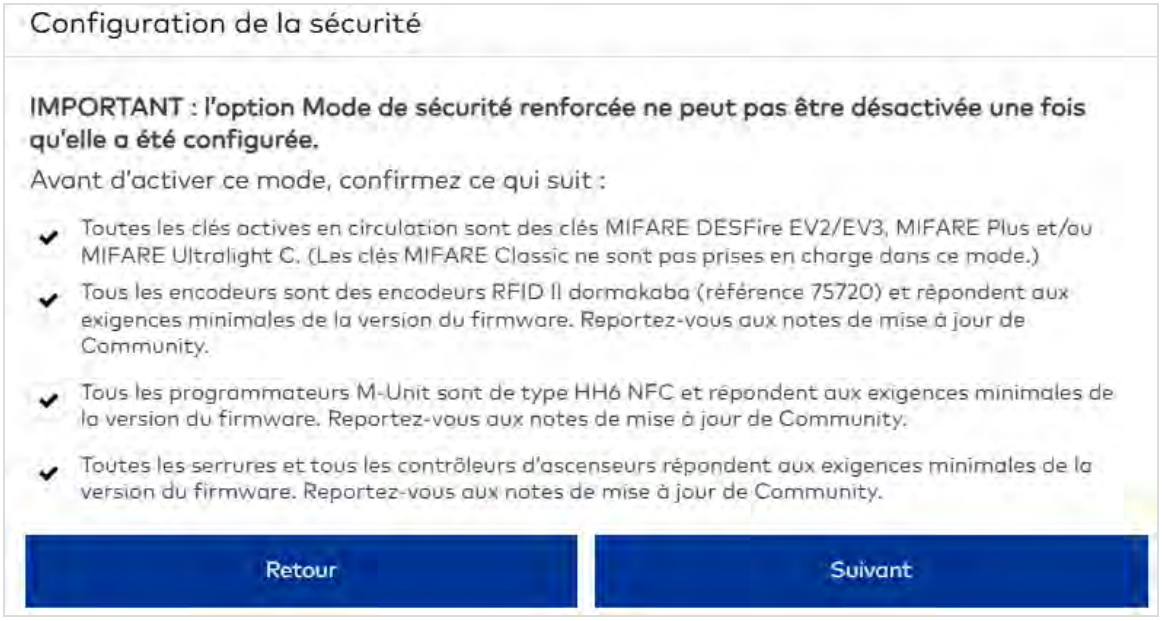
10.1 Activation du produit

Community doit être activé pour accéder au produit, le configurer et l'utiliser.

1. Accédez à l'adresse IP du serveur Community dans la barre d'adresse d'un navigateur pris en charge.
2. Indiquez une clé d'activation valide. dormakaba fournit la clé d'activation lors de l'achat du produit ou sur demande lorsqu'une nouvelle clé d'activation est requise.
3. Connectez-vous en utilisant le compte Admin01. Le mot de passe par défaut est fourni lors de l'achat du produit. Les invites Community demandent de changer le mot de passe du compte Admin01.
   - Pour les connexions initiales d'une nouvelle installation, passez à l'étape suivante.
   - Pour toutes les autres connexions, la page d'accueil s'affiche. Procédez à la configuration du produit.
4. Choisissez d'activer ou non le mode de sécurité renforcée, puis cliquez sur Suivant.



   - Si l'option Activer le mode de sécurité renforcée a été sélectionnée, passez à l'étape suivante.
   - Si l'option Activer le mode de sécurité héritée/standard a été sélectionnée, la page d'accueil s'affiche. Procédez à la configuration du produit.
5. Confirmez que les conditions requises pour activer le mode de sécurité renforcée sont remplies, puis cliquez sur Suivant.



La page d'accueil s'affiche. Procédez à la configuration du produit.

10.2 Flux de travail pour la configuration du site

Le flux de travail Community est une excellente ressource pour guider votre déploiement. Le document donne un aperçu du flux des demandes et des premières mesures à prendre dans chaque module pour configurer Community.

Le *Guide d'utilisation Community* est une nouvelle ressource fournissant des informations et instructions à tous les opérateurs de Community.

- La section « Configuration du site » fournit un flux de travail facile à suivre et des instructions pas à pas pour paramétrer Community.
- La section « Utiliser Community » fournit des instructions sur l'utilisation au quotidien après la Mise en service et comprend les sujets *Dépannage* et *Utiliser ...* qui traitent certaines des situations les plus complexes.

Recherchez le guide dans le dossier de téléchargement du logiciel.

10.3 N'oubliez pas ...

- Accéder à **Paramètres du système** > **Sauvegarde de la base de données** pour configurer les sauvegardes régulièrement programmées et la conservation des données pour la base de données SQL Server Community et, pour les systèmes en ligne, la base de données MongoDB. Il est recommandé de stocker les sauvegardes dans un emplacement externe sécurisé.
- Accédez à ProgramData\DormaKaba\Community\backup, faites une copie du fichier de clé symétrique GDPR et stockez la clé dans un endroit sûr.
- Une fois la configuration du site terminée, accédez à **Paramètres du système** > **Clés à sécurité intégrée** pour créer des clés de sauvegarde.
- Si la licence ne comprend pas le stockage des PPK/SPK, accédez à Clés Système et créez des clés de programmation primaire et secondaire.

A Annexe A : Gestionnaire de services

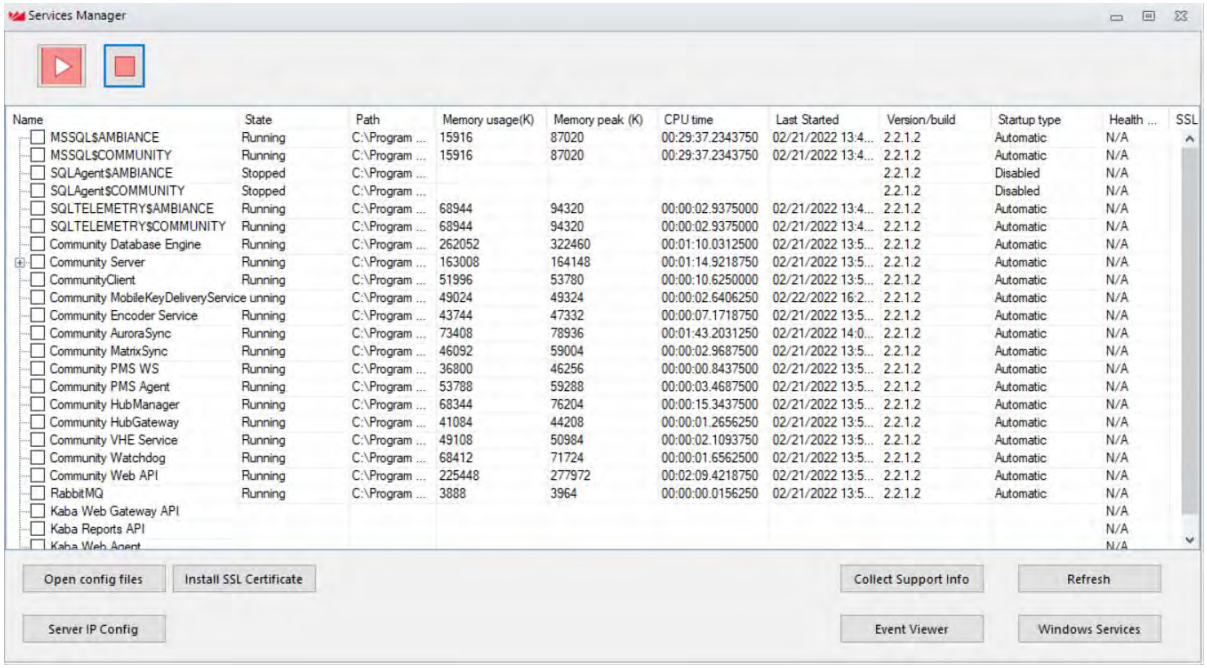
Le Gestionnaire de services offre un accès pratique aux options de configuration post-installation. Accédez au Gestionnaire de services aux emplacements suivants :

- Sur le serveur Community :

C:\Program Files\dormakaba\Community Server\Services\Service Manager\ServiceManager.exe

- Sur le client Community :

C:\Program Files (x86)\dormakaba\Community Client\Services\Service Manager\ServiceManager.exe



A.1 Installation / renouvellement du certificat SSL après l'installation

Utilisez le Gestionnaire de services pour installer ou renouveler un certificat SSL sur le serveur Community après l'installation. Chaque poste de travail Community doit être mis à jour pour utiliser le protocole HTTPS.

Cette fonction s'applique au certificat pour le navigateur.

A.1.1 Serveur

1. Sur le serveur Community, ouvrez le Gestionnaire de services.
2. Cliquez sur Installer le certificat SSL.
3. Ignorez le message d'avertissement et cliquez sur Oui pour continuer.



4. Le cas échéant, indiquez le mot de passe du certificat.
5. Cliquez sur Sélectionner le fichier.
6. Naviguez et sélectionnez le certificat (.pfx).
7. Lorsque vous êtes informé que le certificat a été installé, cliquez sur OK.

A.1.2 Client

Les étapes suivantes doivent être suivies sur chaque poste de travail Community.

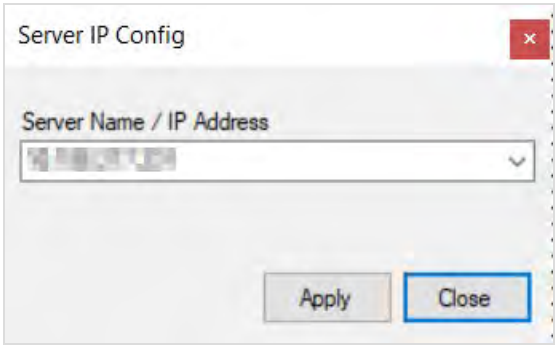
1. Ouvrez le Gestionnaire de services.
2. Sélectionnez le service Client Community et cliquez sur  pour arrêter le service.
3. Cliquez sur Ouvrir les fichiers de configuration.
4. Modifiez les valeurs « WebAPIUrl » et « signalrURL » pour rediriger vers **https** :
   - De :
     <add key="WebAPIUrl" value="http://<Community Server IP>/WebAPI/" />
     <add key="signalrURL" value="http://< Community Server IP>/
     WebAPI/signalr/" />
   - À :
     <add key="WebAPIUrl" value="https://< Community Server IP>/WebAPI/" />
     <add key="signalrURL" value="https://< Community Server IP>/
     WebAPI/signalr/"/>
5. Sauvegardez et fermez le fichier de configuration.
6. Cliquez sur  pour redémarrer le service Client Community.

A.2 Modification de l'adresse IP du serveur

Utilisez le Gestionnaire de services pour modifier l'adresse IP du serveur Community après l'installation. La modification de l'adresse IP nécessite que le client Community soit désinstallé et réinstallé sur chaque poste de travail.

A.2.1 Serveur

1. Sur le serveur Community, ouvrez le Gestionnaire de services.
2. Cliquez sur Configuration de l'IP serveur.
3. Ignorez le message d'avertissement et cliquez sur Oui pour continuer.
4. Indiquez la nouvelle adresse IP, puis cliquez sur Appliquer.



5. Redémarrez le Serveur Community.

A.2.2 Client

Les étapes suivantes doivent être suivies sur chaque poste de travail Community.

1. Ouvrez le Gestionnaire de services.
2. Sélectionnez le service Client Community et cliquez sur  pour arrêter le service.
3. Cliquez sur Ouvrir les fichiers de configuration.
4. Modifiez les valeurs « WebAPIUrl » et « signalrURL » pour rediriger vers la nouvelle adresse IP.
   - De :
     <add key="WebAPIUrl" value="https://<Community Server IP>/WebAPI/" />
     <add key="signalrURL" value="https://< Community Server IP>/
     WebAPI/signalr/" />
   - À :
     <add key="WebAPIUrl" value="https://< Community NewServer IP>/WebAPI/" />
     <add key="signalrURL" value="https://< Community NewServer IP>/
     WebAPI/signalr/"/>
5. Sauvegardez et fermez le fichier de configuration.
6. Cliquez sur  pour redémarrer le service Client Community.

A.3 Restaurer la base de données en ligne

Utilisez le Gestionnaire de services pour restaurer la base de données MongoDB lorsque la communication en ligne est activée.

1. Sur le serveur Community, ouvrez le Gestionnaire de services.
2. Cliquez sur Restaurer MongoDB.
3. Cliquez sur Sélectionner un dossier de sauvegarde, puis naviguez jusqu'au dossier de la collection de sauvegardes MongoDB Community(qui contient les fichiers .json) et sélectionnez-le.

4. Cliquez sur Restaurer la base de données. Un message indique si la restauration a bien été effectuée.

5. Redémarrez le Serveur Community.

A.4 Désactiver/activer la fonction Watchdog

Le Gestionnaire de services comprend une fonction Watchdog qui effectue des contrôles réguliers de l'état du serveur. La fonction Watchdog est activée par défaut. Pour désactiver/activer la fonction Watchdog, ouvrez le Gestionnaire de services et cliquez sur le bouton approprié.

B Annexe B: Database restore

This document contains instructions for restoring the Community SQL Server and MongoDB databases. The encryption key (added in Community 2.4.x) requires an additional restore step using an internal tool accessible only by dormakaba Support. All customers using Community 2.4.x+ must contact Support to restore the SQL Server database and when online communication is enabled, the MongoDB database.

The restore process includes the following steps:

1. Perform required preparatory steps:
   - Install the Community server on a reserve machine.
   - Identify database backups. When conditions allow, take an on-demand backup. Go to System Settings/Database Backup, scroll to the bottom of the page, then click Back Up Database.
   - Copy the SQL Server backup and secure key files to the new server.
   - Obtain and configure the dormakaba restore tool RestoreSiteSpecGDPRKeyRelease.
   - Delete the empty Ambiance database on the reserve machine.
   - If MongoDB data already exists, copy all MongoDB collections to the reserve machine.
2. Restore the SQL Server database.
3. When Online Communication is enabled, restore the MongoDB database. When there is no back up for the MongoDB database, all gateways must be reconfigured after restoring the SQL Server database.
4. When the Ambiance server uses a static IP address, update IP addresses at System Settings > Online Communication and Device Management > Registered Gateways and Paired Access Points.
5. Update the server IP address on workstations. Alternatively, uninstall and re-install the client on each workstation to ensure all references to the Community server are updated.
6. Update the API server with the current IP address.
7. Start all Community Windows services.
8. Restart the Community server.

This following sections list the minimum steps to restore the SQL Server database after a total system failure.

B.1 Required preparatory steps

Perform all of the following steps in preparation to restore the SQL Server database, and when online communication is enabled, the MongoDB database.

B.1.1 Install the Community server on a reserve machine

Re-install the Community server on a new or reformatted machine. For instructions, refer to *Community Installation Guide*. Wait until after the restore to activate Community.

B.1.2 Identify database backups

If database backups are stored off-site, retrieve the backup files; or, if conditions permit, take an on-demand backup.

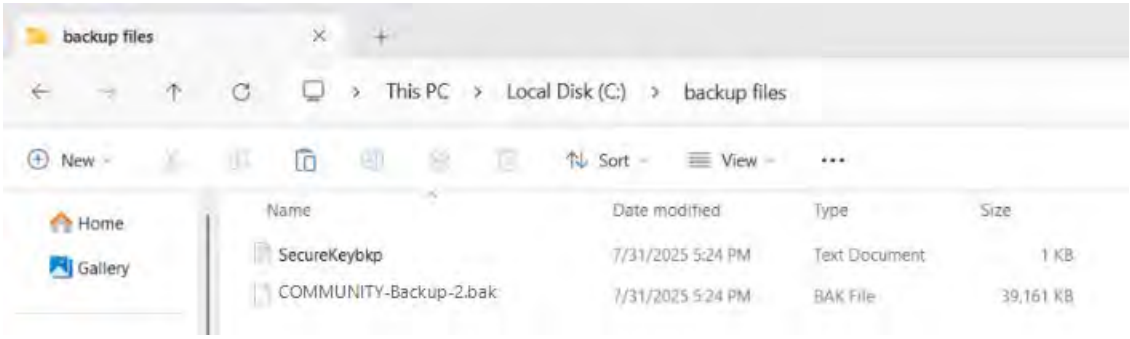
- Go to System Settings > Database Backup, scroll to the bottom and click Back Up Database.

> If Online Communication is enabled and there is no backup of the MongoDB database, be prepared to reconfigure the entire online environment.

B.1.3 Copy backup files to the new server

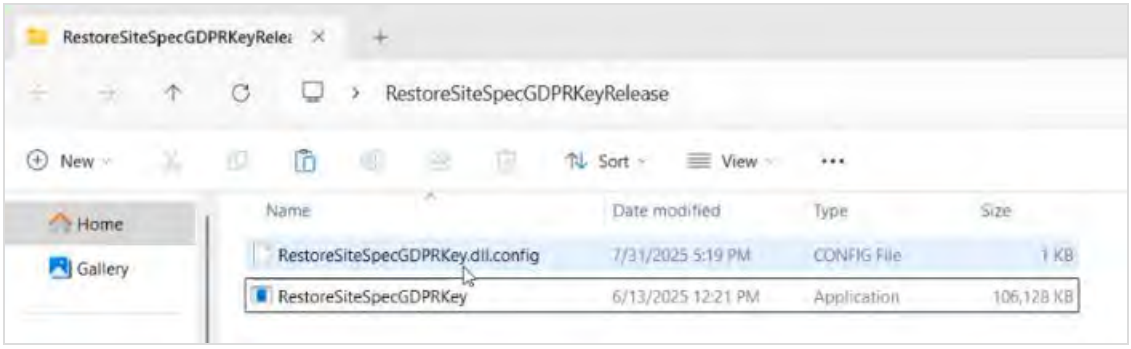
Copy the following backup files to the new server:

- COMMUNITY-backup.bck
- SecureKeybkp

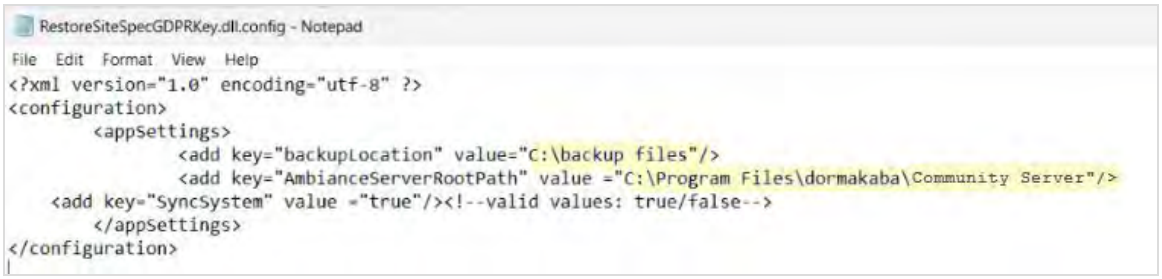


B.1.4 Obtain and configure the dormakaba restore tool

1. Obtain the tool RestoreSiteSpecGDPRKeyRelease.



2. Open the RestoreSiteSpecGDPRKey.dll.config file, then configure and backupLocation and CommunityServerRootPath.



B.2 Restore the SQL Server database

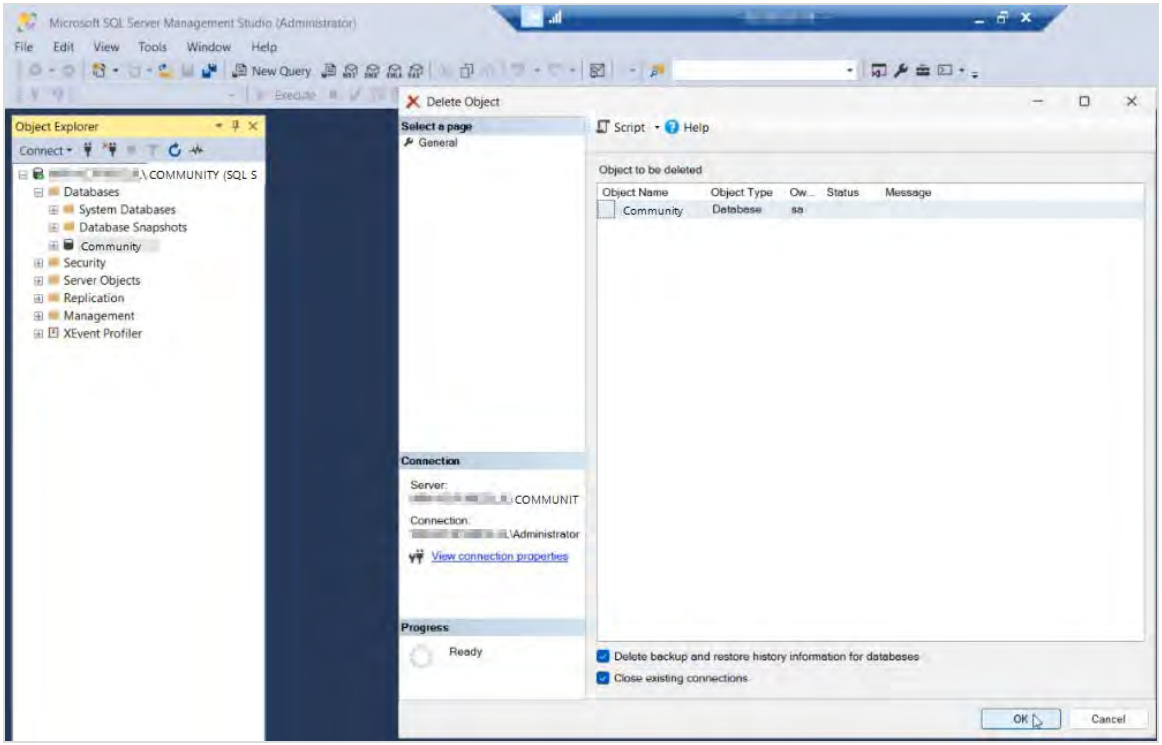
All sites must restore the Community SQL Server database.

Perform the following steps when the Community database has been corrupt or when transferring the database to a different machine:

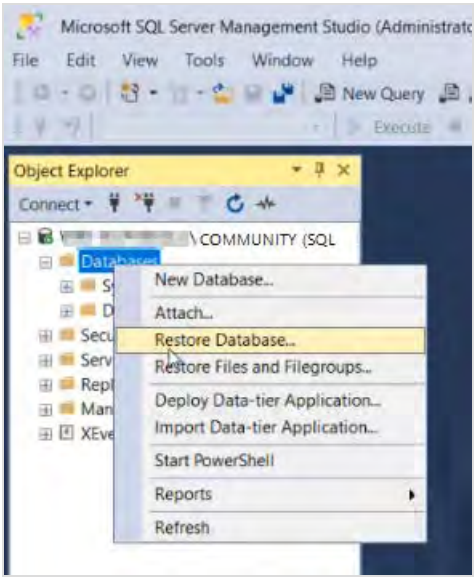
1. Install SQL Server Management Studio. Go to the installation folder \SERVER\Community_PREREQUIS\ and run SSMS-Setup-ENU.exe.
2. Open SQL Server Management Studio.
3. Connect to the server using Windows Authentication and Encryption Optional.



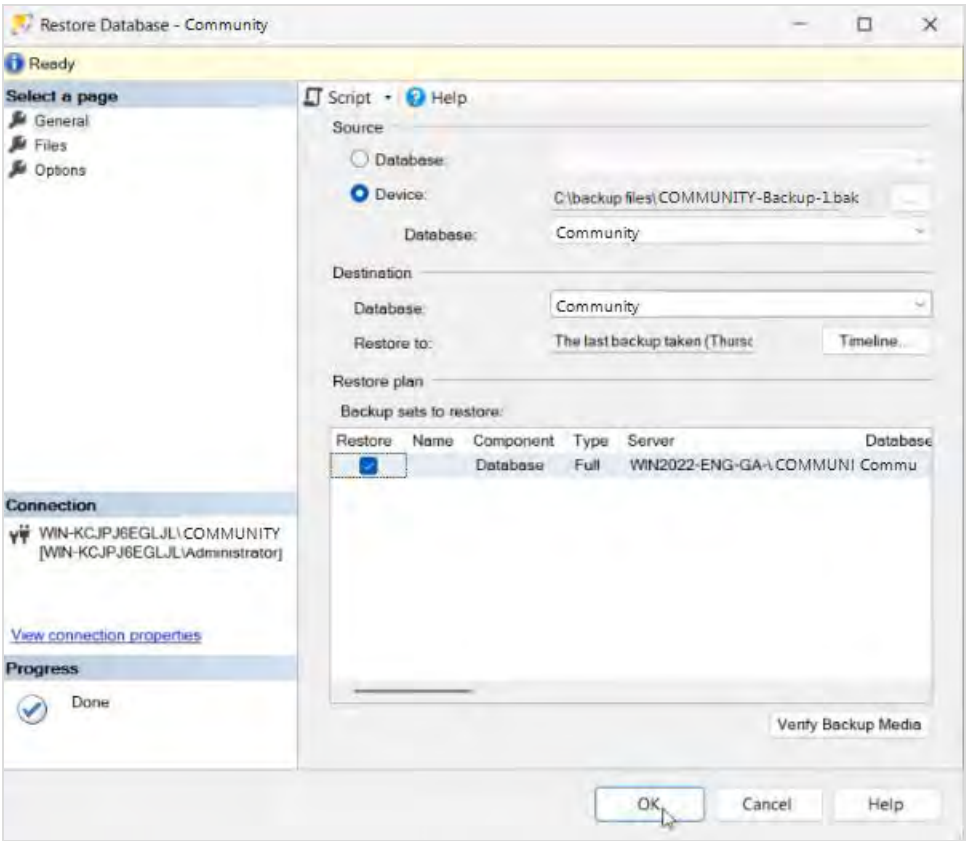
4. Delete the empty Community database. Expand the Databases folder, right-click the COMMUNITY database, then select Delete. On the Delete Object screen, click OK.



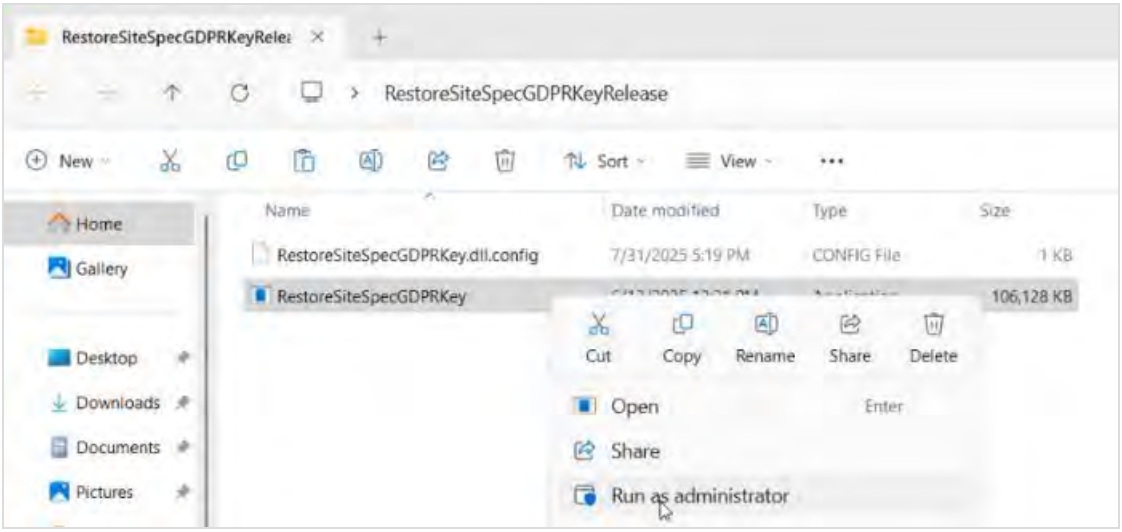
5. After the empty database is deleted, right-click the Databases folder again and select Restore Database.



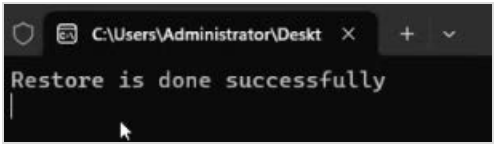
6. On the Restore Database screen, select Device. For Database, click ... to navigate to and select the SQL Server backup file. Click OK.



7. When the database is successfully restored, click OK.
8. Navigate to the RestoreSiteSpecGDPRKeyRelease tool.



9. Right-click RestoreSiteSpecGDPRKey and select Run as administrator. The program runs and notifies when the restore is successful. Press any key to close the tool.



10. Restart the Community server.
11. Go the login page to find the SQL Server database is restored. No activation is required.



B.3 Restore the MongoDB database

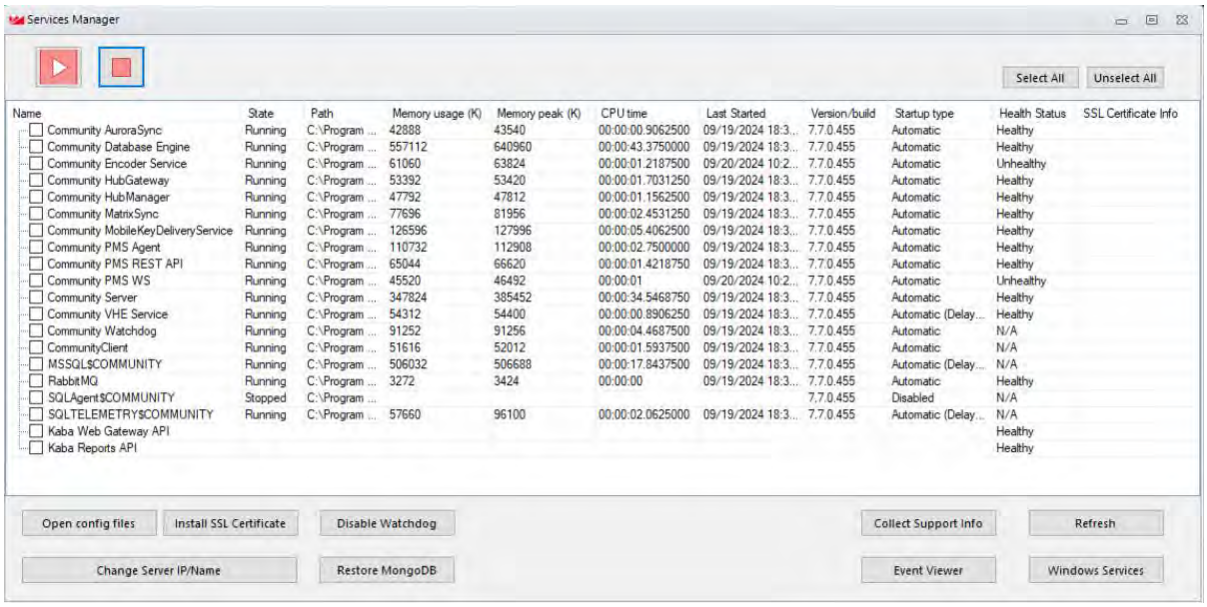
Sites where Online Communication is enabled must restore the MongoDB database.

> For sites where Online Communication is enabled and no backup of the MongoDB exists, all gateways must be reconfigured. After restoring the SQL Server database, go to Device Management and refer to Context Help or "Remote Lock Management" in the the *Community User Guide* for instructions how to set up gateways and pair access points.

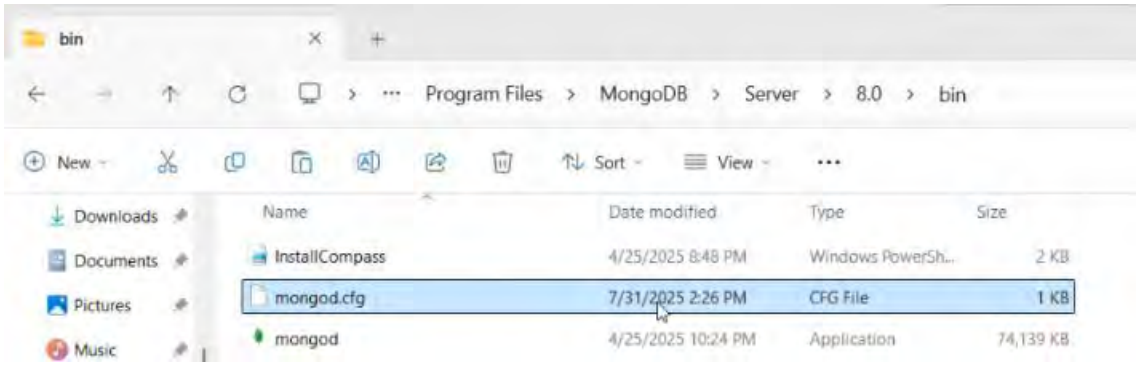
Use the Service Manager to restore the MongoDB database.

- On the Community server:

C:\Program Files\dormakaba\Community Server\Services\Service Manager\ServiceManager.exe



1. On the Community server, navigate to the MongoDB configuration file mongod.cfg.



2. Open the configuration file and change the security authorization to disabled.

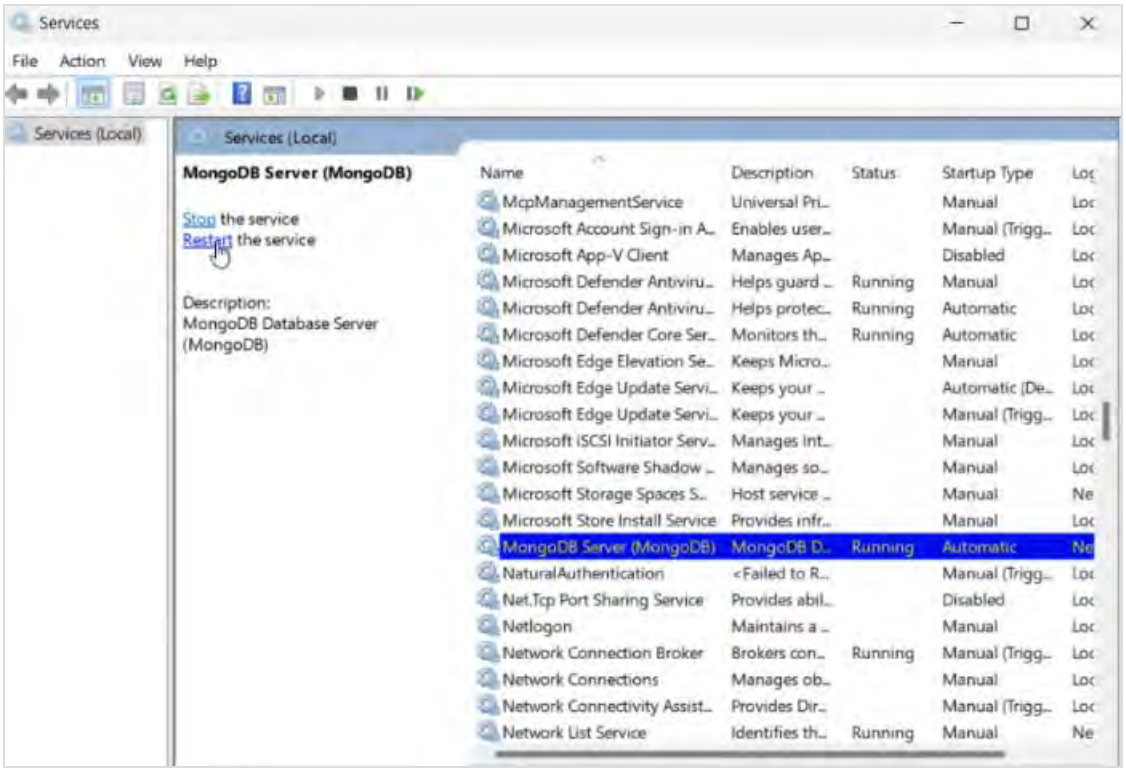
*mongod.cfg - Notepad

File Edit Format View Help

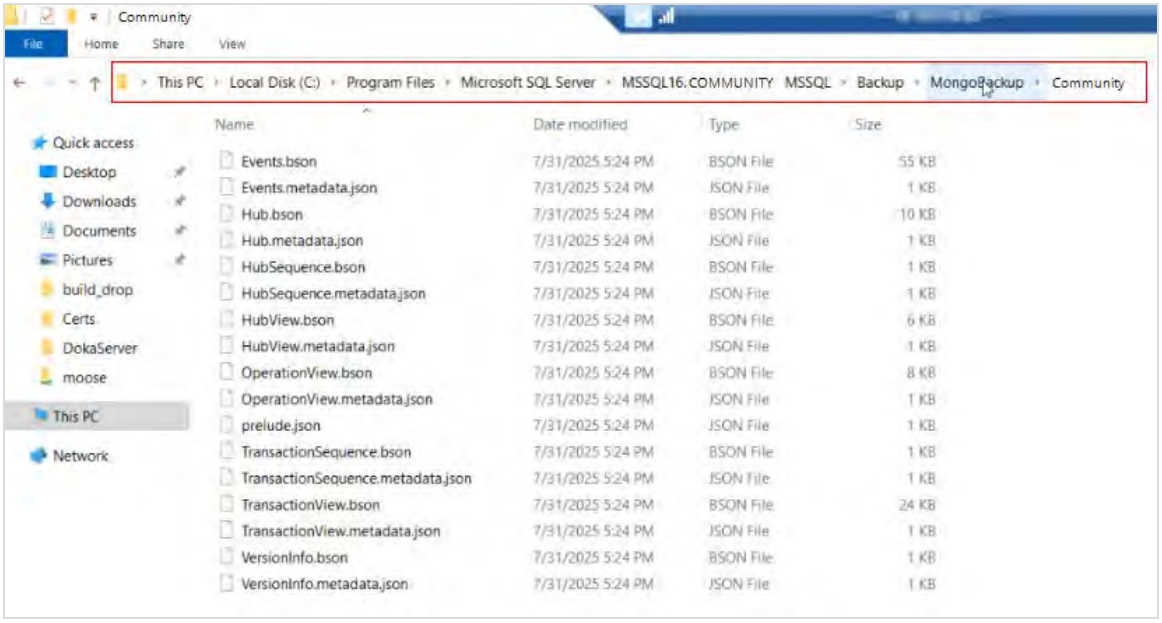
```
# mongod.conf
# for documentation of all options, see:
#   http://docs.mongodb.org/manual/reference/configuration-options/
# Where and how to store data.
storage:
  dbPath: C:\Program Files\MongoDB\Server\8.0\data
# where to write logging data.
systemLog:
  destination: file
  logAppend: true
  path:  C:\Program Files\MongoDB\Server\8.0\log\mongod.log
# network interfaces
net:
  port: 27017
  bindIp: 127.0.0.1

#processManagement:
security:
    authorization: "disabled"
#operationProfiling:
#replication:
#sharding:
## Enterprise-Only Options:
#auditLog:
```

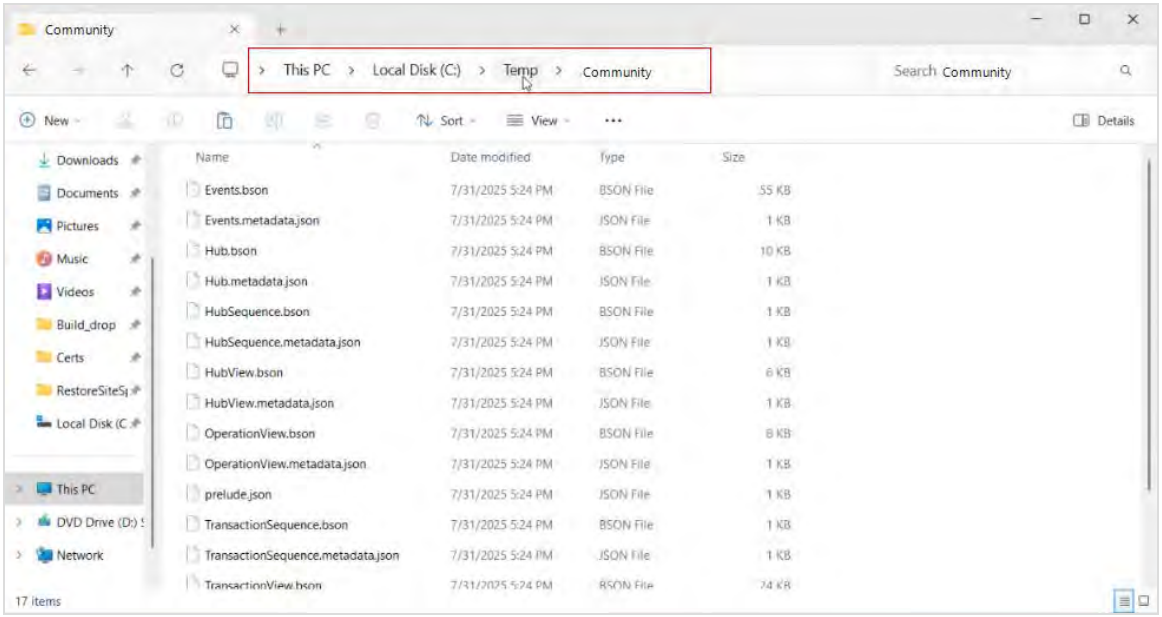
3. Restart the MongoDB Server service.



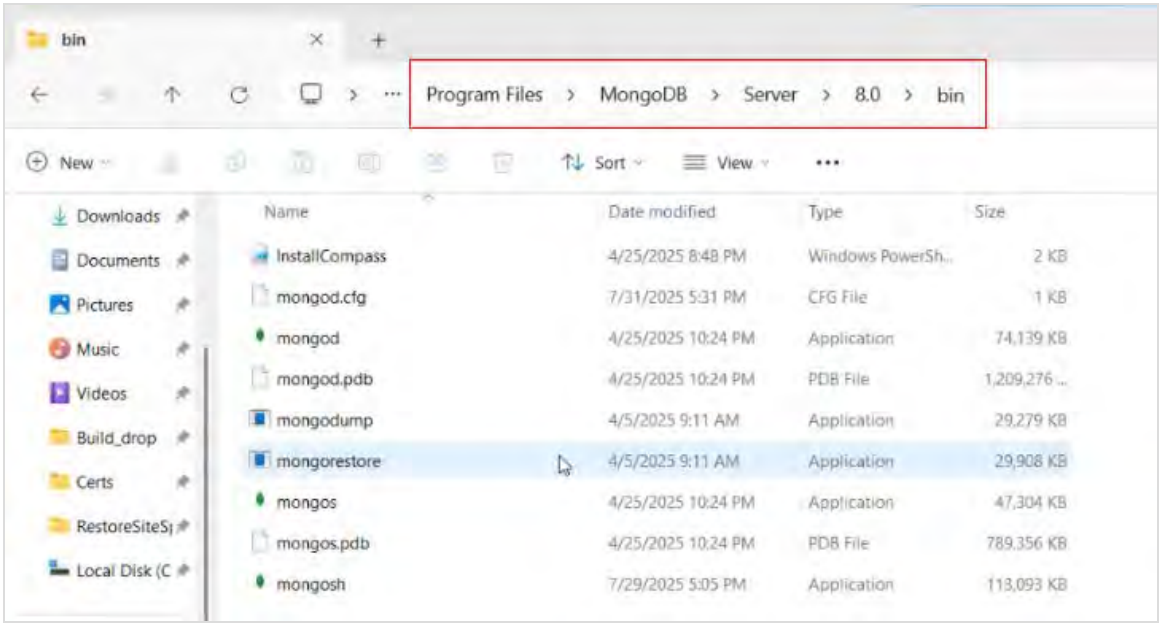
4. Retrieve the Mongo backup files. Select the Community folder that contains all of .json files (events).



5. Copy files to the new server.



6. Go to the same directory where the configuration file is located.



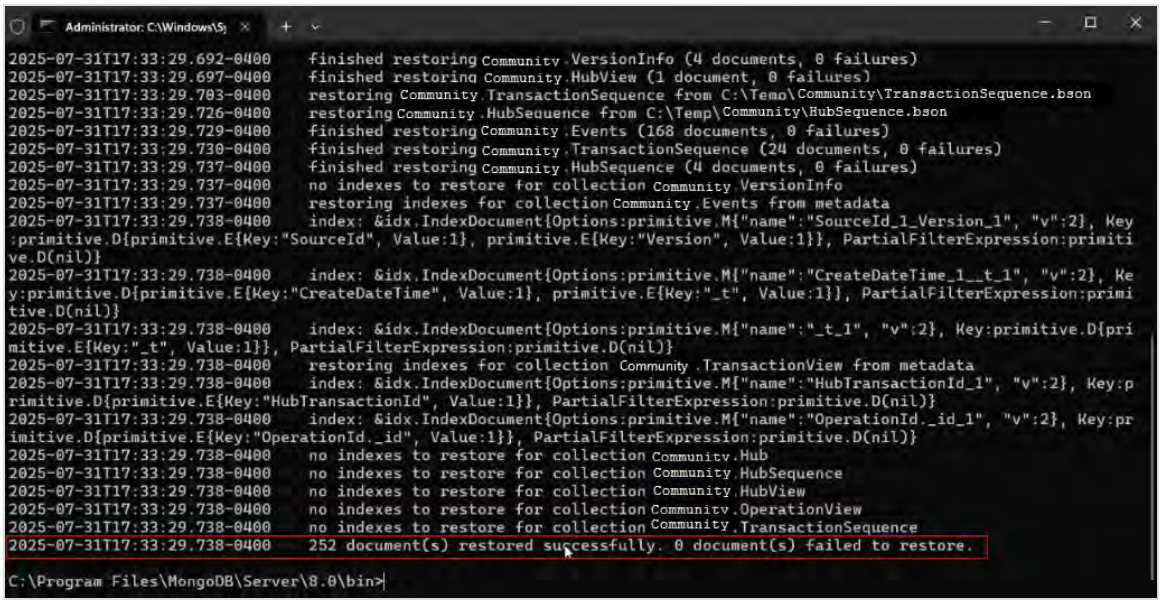
7. In Command Prompt, run the command mongorestore as shown in the following figure. ("C:\Temp\Community" is where the MongoDB backup files were placed on the new server.)



It may be necessary to specify the username and password:

```
c:>Program Files\MongoDB\Server\8.0\bin>mongorestore --username value --password value --db Community C:\Temp\Community
```

8. When the command completes, the message indicates all files were restored successfully.



Verify that all online operations and events display in the Monitoring module.

B.4 Static IP address only. Update IP address

The following steps are required if Community is configured using a static IP address.

1. In Community, go to System Settings > Online Communication, update the Server IP address, then click Save.
2. Go to Device Management > Registered Gateways and Paired Access Points, select all gateways and issue the Set Communication Settings command. The new IP address is updated on all gateways.

B.5 Update Community workstations

On each workstation, use the Service Manager to change/update the current Community server IP address. The Service Manager is located at:

C:\Program Files\dormakaba\Community Server\Services\Service Manager\ServiceManager.exe

Alternatively, uninstall and re-install the client on each workstation to ensure all references to the Community server are updated.

B.6 Community only. Update API server

The API vendor must update the API Server with the current Community server IP address.

PK3695-FR 2.6 - 08/2026
Copyright © dormakaba 2026

www.dormakaba.com

dormakaba Canada
105 Marcel-Laurin Blvd
Montreal, Quebec H4N 2M3
Canada
T: +1 877 468-3555

www.dormakaba.com