

# SIEMENS



## CFG3.F200

### Guide d'installation rapide

### Guide de démarrage rapide

## Note de publication

Sous réserve de modification des spécifications techniques et de la disponibilité sans préavis.

Ce document ne peut pas être reproduit, diffusé à des tiers ou traité et son contenu ne peut pas être utilisé ou diffusé sans autorisation écrite préalable. Le non-respect de ces dispositions provoquera une action en compensation de préjudice. Tous les droits, y compris ceux résultant d'une demande de brevet acceptée et de l'enregistrement d'un modèle d'utilité ou d'un brevet de conception, sont réservés.

Version : 29/12/2022

ID document : A6V12893144\_fr--\_c

© Siemens 2019-2022



---

## Copyright

Ce document ne peut être reproduit et distribué qu'avec l'accord de Siemens, et, le cas échéant, uniquement à des personnes physiques ou morales habilitées disposant des connaissances techniques appropriées.

# Sommaire

<b>1</b>	<b>Présentation du document</b> .....	<b>6</b>
1.1	Domaine d'application.....	6
1.2	Public visé.....	6
1.3	Résumé du processus d'installation.....	6
<b>2</b>	<b>Configurer le F200</b> .....	<b>7</b>
<b>3</b>	<b>Choisir un réseau et activer le F200</b> .....	<b>10</b>
<b>4</b>	<b>Configurer le pare-feu du F200</b> .....	<b>13</b>
<b>5</b>	<b>Activer l'accès web à distance dans l'interface du F200</b> .....	<b>14</b>
<b>6</b>	<b>Ajouter des équipements</b> .....	<b>15</b>
<b>7</b>	<b>Vérifier l'état de l'enregistrement et les mises à jour de logiciels</b> .....	<b>21</b>
<b>8</b>	<b>Gérer les licences du F200</b> .....	<b>22</b>
<b>9</b>	<b>Annexe A – Configurer le masque de sous réseau</b> .....	<b>24</b>
<b>10</b>	<b>Annexe B - Mettre les serveurs de l'application Équipements dans une liste blanche</b> .....	<b>25</b>



## Exclusion de responsabilité en matière de cybersécurité

Siemens fournit une gamme de produits, solutions, systèmes et services qui contiennent des fonctions de sécurité pour permettre un exploitation sécurisée des installations, systèmes, machines et réseaux. Dans le domaine des technologies du bâtiment, cela s'applique aux systèmes d'automatisation et de gestion des bâtiments, de protection incendie, de gestion de la sûreté ainsi qu'aux systèmes de sûreté physique.

Afin de protéger les installations, les systèmes, les machines et les réseaux contre les cybermenaces, il est nécessaire de mettre en œuvre, et de maintenir en permanence, une stratégie de sécurité holistique et moderne. Le portfolio de Siemens ne constitue qu'un aspect d'une telle stratégie.

Vous devez empêcher tout accès non autorisé à vos installations, systèmes, machines et réseaux qui ne doivent être connectés à un réseau d'entreprise ou à Internet que si et dans la mesure où une telle connexion est nécessaire et uniquement lorsque des mesures de sécurité appropriées (par ex. pare-feu et/ou segmentation du réseau) sont en place. De plus, les directives de Siemens sur les mesures appropriées doivent être prises en compte. Pour toute information complémentaire, contactez votre représentant Siemens ou rendez-vous sur <https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html>.

Siemens développe continuellement son offre pour la rendre plus sûre et recommande vivement d'appliquer les mises à jour dès qu'elles sont disponibles et d'utiliser les versions les plus récentes. Si vous utilisez de versions qui ne sont plus prises en charge et n'appliquez pas les dernières mises à jour, vous risquez d'accroître votre exposition aux cybermenaces. Il est fortement conseillé de se conformer aux avis de sécurité sur les dernières menaces et d'implémenter les correctifs et autres mesures connexes, publiés, entre autres, sous <https://www.siemens.com/cert/en/cert-security-advisories.htm>.

# 1 Présentation du document

## 1.1 Domaine d'application

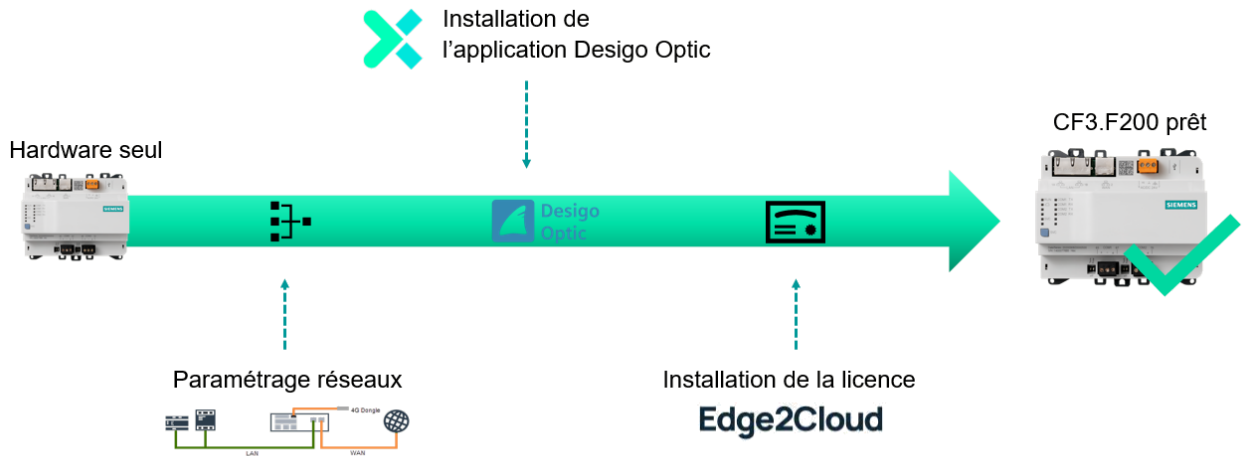
Ce guide fournit une vue d'ensemble du F200 et des instructions pour le configurer afin de commander votre système de gestion technique.

## 1.2 Public visé

Ce document s'adresse à des personnes qui ont des connaissances en réseau et peuvent répondre aux questions suivantes :

- Votre réseau dessert-il un seul site ou est-il distribué ?
- Des adresses IP statiques sont-elles nécessaires pour votre système? Si oui, quelles sont-elles ?
- Quel est le masque de sous-réseau?
- Quelle est la passerelle?
- Quel est le serveur DNS ?

## 1.3 Résumé du processus d'installation



## 2 Configurer le F200

Cette section traite de l'installation, du choix de réseau et des identifiants de connexion pour le F200.

Il y a deux manières d'accéder à l'interface de configuration :

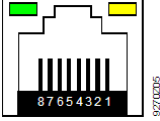



1. Connectez le switch Ethernet 2 ports (4a) à un serveur DHCP et ouvrez une nouvelle fenêtre du navigateur. Une adresse IP est automatiquement affectée au serveur DHCP.
2. Connectez le switch Ethernet 2 ports (4a) à votre ordinateur. Appuyez sur le bouton SVC (3) jusqu'à que la LED SVC s'allume en rouge. Dans la barre d'adresse du navigateur, entrez l'adresse IP suivante : **169.254.169.254**.
  - ⇒ La configuration de sécurité du réseau doit ressembler à ceci :
    - **Mode réseau unique (combiné)**: WAN sur switch Ethernet 2 ports (4a).



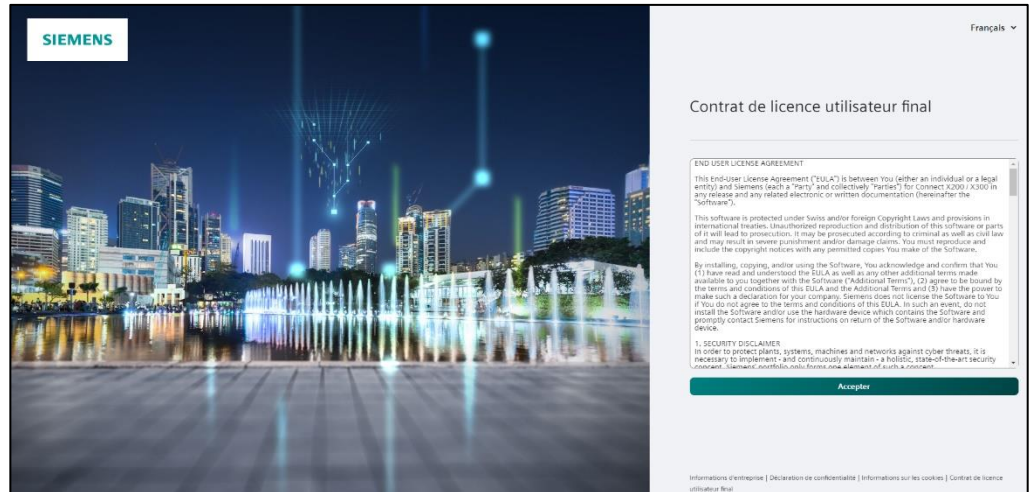
Seul le switch Ethernet 2 ports (4a) prend en charge une connexion locale vers le F200. Si le LAN et le WAN sont des réseaux différents, ils doivent avoir des sous-réseaux distincts.

	1	Boîtier plastique
	2	LED de communication et d'état
	3	Touche de service
	4a	Switch Ethernet 2 ports avec 2 LED par port
	4b	Interface Ethernet 1 port avec 2 LED pour le WAN (accès internet)
	5	Bornier amovible à vis Alimentation
	6	Interface USB pour dongles 4G
	7	Inutilisé (pour une version future)
	8	Inutilisé (pour une version future)
	9	Coulisseau pour montage sur rails standard
	10	Œillets pour serre-câble
	11	Orifices pour montage mural
12	Date / Série et N° de série	

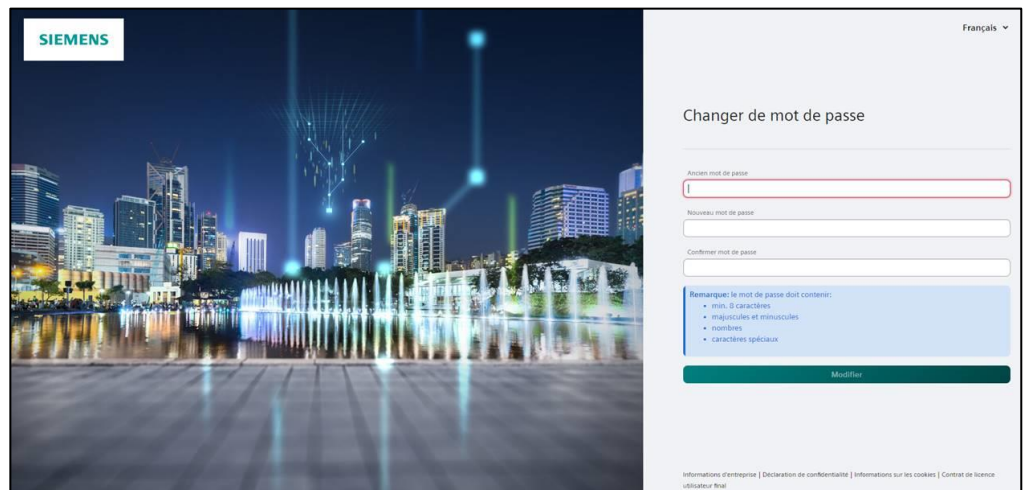
Il existe plusieurs signalisations par LED sur le F200. Le tableau ci-dessous indique la fonction de ces signalisations :

Élément	LED / interface	Couleur	Activité	Fonction
	Ethernet 1...3	Vert	Allumée	Liaison active
			Éteinte	Pas de connexion
			Clignote	Activité sur le réseau
		Jaune	Allumée	Liaison 100 Mbit/s
Éteinte	Liaison 10 Mbit/s			
	RUN	Vert	Allumée	Appareil opérationnel
			Éteinte	Appareil non opérationnel
			Clignote	Démarrage ou programme arrêté
		Rouge	Allumée	OK
			Éteinte	Défaut matériel ou logiciel – Éteignez et rallumez le F200
			Clignote rapidement	Firmware ou application manquant/endommagé
		Bleu	Allumée	Connexion au cloud OK
			Clignote	Pas de connexion au cloud Intégration dans le cloud incomplète ou certificats d'équipement pas mis à jour
	SVC	Rouge	Éteinte	Adresse IP non affectée au port LAN
			Allumée	Adresse IP affectée au port LAN
 SVC	Touche de service		Commencez par éteindre l'appareil. Maintenez ensuite le bouton appuyé pendant environ 20 secondes.	Retour au réglage usine Toutes les données de configuration et apps installées sont supprimées Si la LED RUN reste allumée en vert, le retour aux réglages usine a réussi
			Pression brève	L'adresse IP 169.254.169.254 est affectée au port LAN pendant 15 minutes.

1. Dans la page d'accueil de Desigo Optic, cliquez sur **Accepter** pour confirmer votre accord avec le contrat de licence utilisateur final.



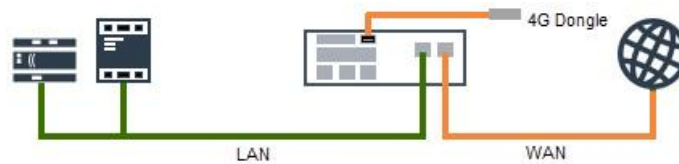
2. Entrez ensuite les identifiants suivants dans les champs correspondants:
  - **Mot de passe** : admin (en minuscules)
3. Vous êtes ensuite invité à changer le mot de passe par défaut. Ce mot de passe est spécifique à l'équipement auquel vous êtes connecté. Sélectionnez un mot de passe en respectant les consignes suivantes :
  - Au moins 8 caractères
  - Majuscules et minuscules
  - Chiffres
  - Caractères spéciaux
4. Sélectionnez **Modifier** lorsque vous avez terminé.



5. Vous êtes alors redirigé. Enregistrez le nouveau mot de passe pour les connexions ultérieures.

## 3 Choisir un réseau et activer le F200

### Mode séparé



Un réseau configuré en mode séparé permet à deux sous-réseaux d'accéder à la passerelle via deux ports distincts et d'utiliser le pare-feu natif. Dans cette configuration, un réseau local d'équipements est isolé du réseau WAN connecté à internet.

### Mode unique



Un réseau configuré en mode unique achemine tout le trafic de la passerelle sur un même réseau via un routeur partagé. Dans cette configuration, les équipements vulnérables seront exposés aux attaques provenant du trafic internet externe. Pour cette raison, il est recommandé d'instaurer des mesures de sécurité périmétriques supplémentaires comme des pare-feux pour sécuriser les sous-réseaux.



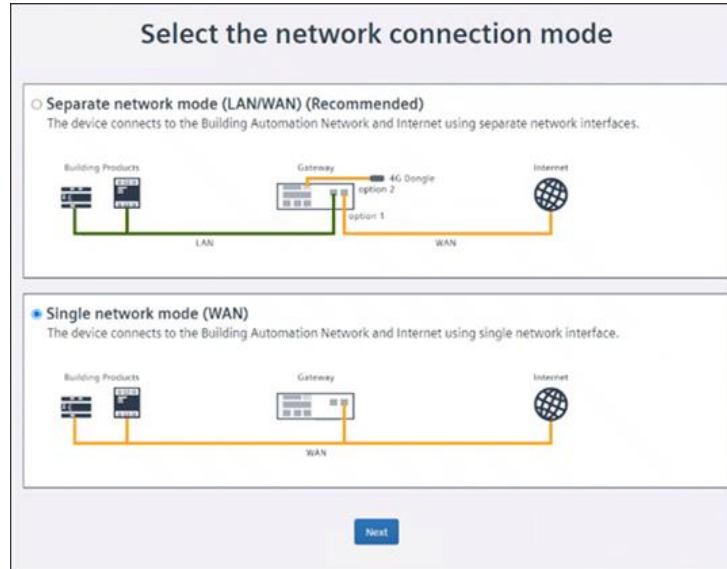
---

Siemens recommande d'utiliser le mode réseau séparé pour les raisons suivantes :

1. Sécurité renforcée avec le pare-feu natif.
  2. Conformité avec le niveau de sécurité 2 (SL2).
- 

Après vous être enregistré sur l'équipement F200, procédez comme suit :

1. Sélectionnez un mode de connexion réseau.
  - Si vous prévoyez d'utiliser des fonctions d'architecture distribuée qui s'appliquent à plusieurs sous-réseaux, vous devez sélectionner le **mode réseau séparé**.
  - Si vous n'envisagez pas d'utiliser des fonctions d'architecture distribuée et que votre réseau de gestion du bâtiment est isolé de l'accès internet et protégé par un pare-feu, sélectionnez **mode réseau unique**.



**⚠ ATTENTION**



Cette sélection est irréversible. Vérifiez le mode de connexion réseau de votre bâtiment avant de faire votre choix. Si vous changez d'avis, il faudra réinitialiser la configuration, ce qui entraînera la perte de la configuration réseau actuelle et des données du projet.

**⚠ ATTENTION**

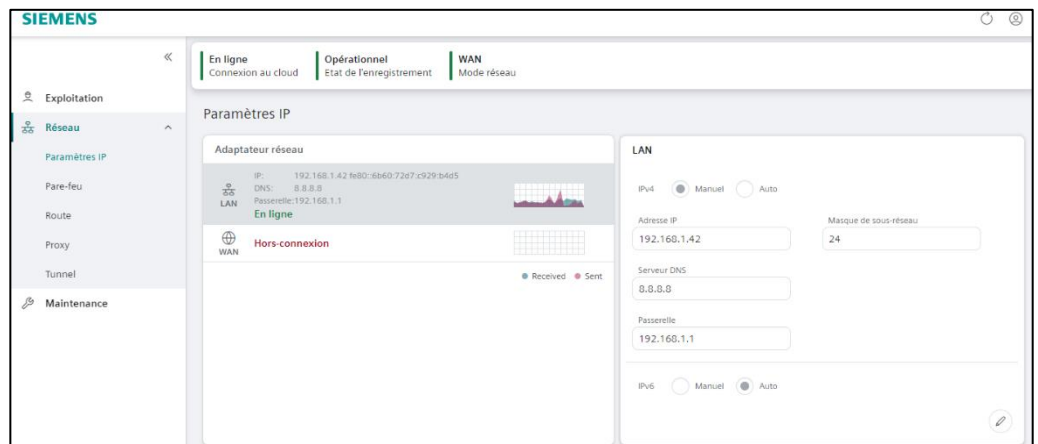


**Mode réseau unique et cybersécurité**

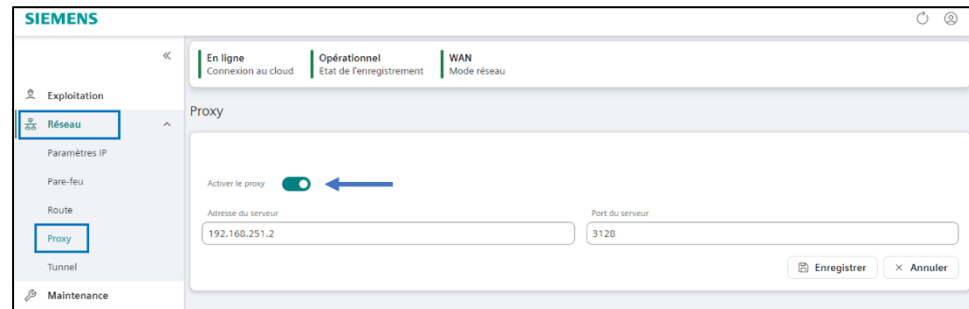
Si vous sélectionnez **Mode réseau unique**, il vous incombe de sécuriser le réseau avec des mécanismes appropriés.

2. Pour configurer l'adresse IP de substitution et les paramètres du proxy, cliquez sur l'onglet **Paramètres IP** sous l'onglet **Réseau**.

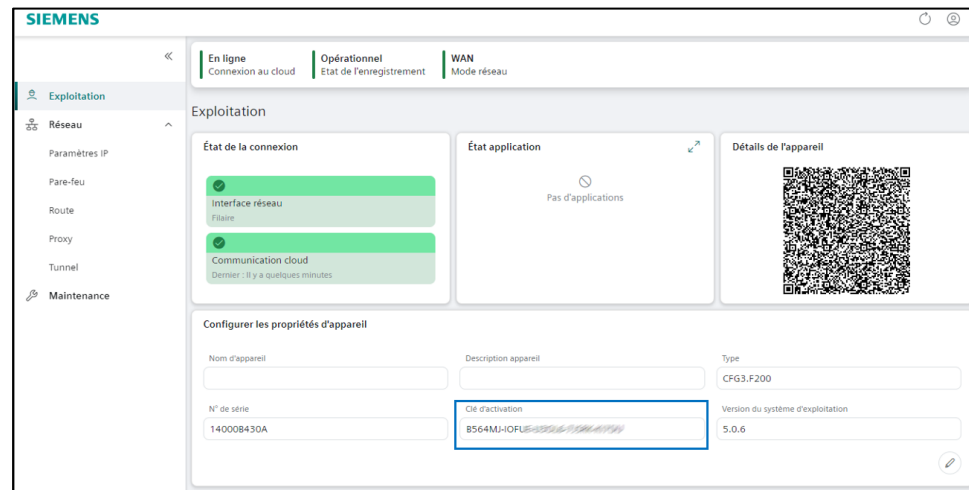
**NOTA:** Pour configurer le **Masque de sous-réseau**, définissez le nombre de bits masqués. Voir Annexe A [→ 23] pour plus d'informations.



3. (Facultatif) Si vous devez régler un proxy pour une adresse IP WAN de substitution, cliquez sur l'onglet **Réseau**, puis sur **Proxy**.
4. (Facultatif) Enclenchez le bouton d'activation du proxy. Entrez les valeurs adéquates dans les zones prévues.



5. Dans l'onglet **Exploitation**, copiez la clé d'activation. Passez à l'application **Équipements** pour terminer l'activation de la passerelle.



Il se peut que l'équipement soit signalé comme déconnecté du cloud.

## Résolution des problèmes

Si votre équipement F200 ne s'enregistre pas correctement ou que l'état de connexion au cloud s'affiche comme désactivé, procédez comme suit :

1. Éteignez la passerelle.
  2. Allumez la passerelle.
  3. Appuyez sur le bouton SVC.
  4. Connectez directement votre PC au port LAN via 169.254.169.254.
- ⇒ L'équipement F200 est alors correctement enregistré, et l'état de connexion au cloud affiche En ligne.

## 4 Configurer le pare-feu du F200

Par défaut, aucun trafic entrant n'est autorisé sur l'équipement. Vous devez ouvrir les ports qui permettent au F200 de communiquer avec le réseau de gestion du bâtiment.

Pour configurer manuellement le F200 :

1. Sélectionnez l'onglet **Réseau**. Sélectionnez ensuite **Pare-feu**.
2. Créez les règles de trafic **entrant** suivantes pour:

### Réseaux

Description	Protocole	Port source
Équipements BACnet IP	udp	47808
Client web Desigo Optic	tcp	8090 (HTTPS) 8085 (HTTP)
Défaut	Tous refusés	

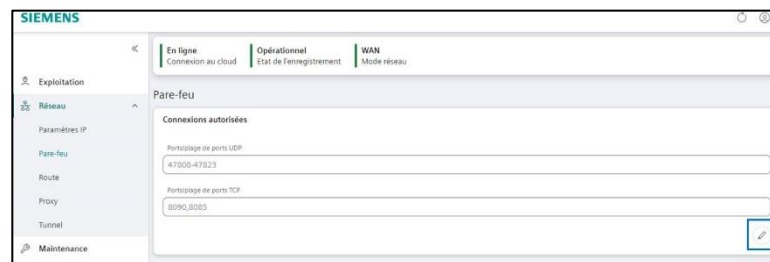
### Cloud

Description	Protocole	Port source
HTTPS	tcp	443
MQTTS	tcp	443
NTP	udp	123



En fonction de la configuration du réseau de gestion du bâtiment sur site, les ports source peuvent être différents.

◆ Cliquez sur **Éditer**  pour modifier le port.



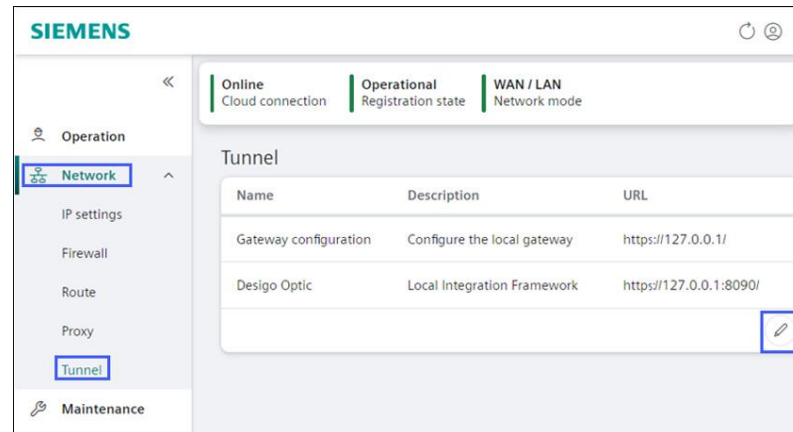
## 5 Activer l'accès web à distance dans l'interface du F200

Pour utiliser l'accès web à distance, vous devez configurer les points terminaux dans le F200. Pour ce faire, procédez comme suit.

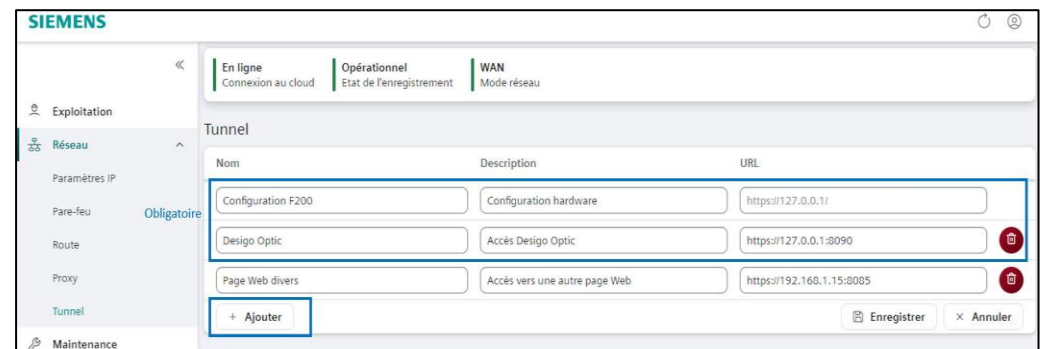
NOTA : Si vous configurez une adresse IP statique, vous devez entrer une adresse de passerelle pour l'interface connectée à internet.

▷ Dans l'interface de configuration :

1. Sélectionnez **Réseau...** > **Tunnel** > **Éditer** 

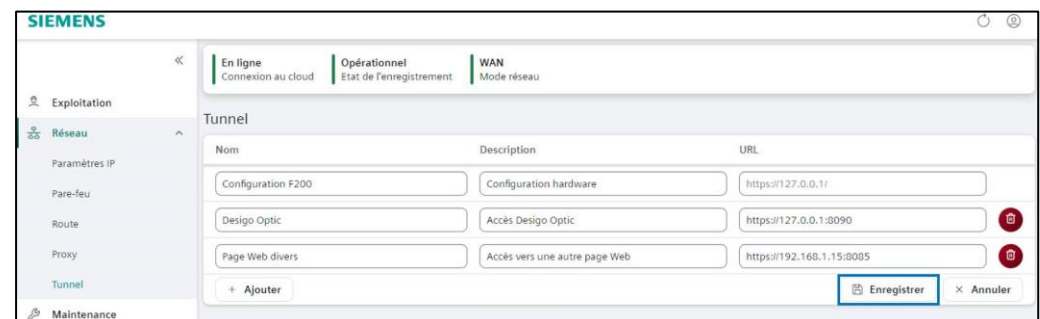


2. Cliquez sur **Ajouter**.



3. Entrez le Nom, la Description et l'URL.

4. Cliquez sur **Enregistrer**.



## 6 Ajouter des équipements

Avant d'utiliser Desigo Optic, vous devez créer un site, ajouter et activer votre équipement, et mettre à jour votre équipement dans l'application Équipements.

1. Utilisez le lien suivant pour accéder à l'application Équipements :  
<https://assets.bpcloudapps.siemens.com/#/login>
2. Connectez-vous avec vos identifiants.

### REMARQUE



Si le lien précédent ne vous donne pas accès à l'application Équipements, il faut vous assurer que vous possédez une licence active FIN-CLOUD-OPTIC.

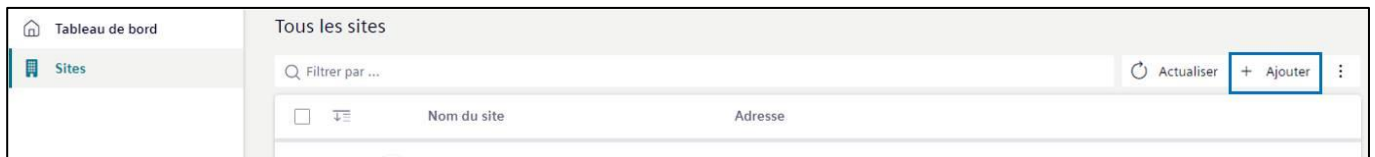
### Créer un site

▷ Dans **Équipements**:

1. Créez un nouveau site avec l'une des options ci-dessous :
  - Allez à **Tableau de bord > Nouveau site**.



- Allez à **Sites > Ajouter**.



2. Remplissez les champs du formulaire **Ajouter site**.

**Ajouter site** [X]

Bâtiment  Campus

Nom \*  
Siemens Exemple 15/256

Adresse \*  
Av. Morane Saulnier, Vélizy-Villacoublay, France

Pays \*  
France [v]

Fuseau horaire \*  
Europe/Paris [v]

Optionnel [v]

3. Cliquez sur **Ajouter**.



Le champ **Adresse** propose automatiquement des adresses. Si vous en choisissez une, la zone **Fuseau horaire** est automatiquement remplie. Si l'API Google n'est pas disponible, vous devez entrer une adresse et un fuseau horaire manuellement.

### Ajouter et activer un équipement

▷ Après avoir ajouté un site, dans **Équipements**:

1. Allez à **Sites**.
2. Sélectionnez le site auquel vous souhaitez ajouter un équipement.
3. Cliquez sur **Ajouter**.

Tableau de bord

Sites

Siemens Exemple  
Av. Morane Saulnier, Vélizy-Villacoublay, France

Tous les appareils

Q Filtrer par ... Actualiser + Ajouter [X]

4. Entrez la clé d'activation de l'équipement et cliquez sur **Valider**.

**Ajouter un appareil** [X]

Entrez la clé d'activation de l'appareil

B564MJ-IOFL [X]



Pour les équipements F200, la clé d'activation se trouve dans l'onglet **Exploitation** de l'interface de configuration.

5. Vérifiez les informations de l'équipement.
6. Cliquez sur **Ajouter**.

Ajouter un appareil

Entrez la clé d'activation de l'appareil

B564MJ-IO... X Valider

Nom personnalisé Description personnalisée

CFG3.F200 Exemple CFG3 #G

Identifiant externe

Type d'appareil Numéro de série

CFG3.F200 14000B430A

Annuler Ajouter



Lorsque vous définissez ou modifiez le nom personnalisé de l'équipement, ceci n'affecte que le nom affiché dans le cloud. Les champs Nom personnalisé et Description personnalisée peuvent rester vides.

## Affecter des distributions



Vous n'aurez à affecter une distribution qu'une seule fois. La fenêtre pop-up d'affectation de la distribution n'apparaît qu'une fois qu'un équipement a été ajouté à un site. Si vous n'affectez pas de distribution, la fenêtre continuera d'apparaître tant qu'une distribution n'est pas affectée à l'équipement.

Après avoir ajouté et activé l'équipement, vous devez lui attribuer une distribution Desigo Optic. Pour affecter une distribution à l'équipement, procédez comme suit.

▷ Dans **Équipements**:

1. Allez à **Sites**.
2. Sélectionnez le site hébergeant l'équipement F200.
3. Sélectionnez l'équipement.
4. Allez à **Applications**.
5. Dans la fenêtre pop-up, utilisez les menus déroulants pour **Sélectionner la distribution** et **Sélectionner la version de distribution**.  
**NOTA:** Vérifiez que la **version de distribution** la plus récente est sélectionnée.
6. Cliquez sur **Sauvegarder**.

**Affecter la distribution** ×

Sélectionnez la distribution Sélectionnez la version de distribution

Desigo Optic (Chicago Edge ... 2.8.23

Dernière modification le : 01/12/2022 20:17:56

Description : Building Integration Platform

## Mettre à jour des distributions

Pour mettre à jour une distribution sur un équipement, procédez comme suit.

▷ Dans **Équipements**:

1. Dans l'onglet **Sites**, sélectionnez le site hébergeant l'équipement F200.
2. Sélectionnez l'équipement.
3. Allez à **Applications**.
4. Pour mettre à jour la distribution, cliquez sur **Modifier**

×

Informations   Mises à jour   Applications   Accès à distance   Services

---

**Détails de distribution**

Nom : Desigo Optic

Version installée : 2.8.24

Version la plus récente : 2.8.30

---

**Applications**

**Desigo Optic**

Manage BACnet, Modbus and Alarm data for Desigo Optic

Version : 2.8.23

Licences OSS [📄](#)

Désinstaller

5. Confirmez avec **Mise à jour**.
6. Dans certains cas, Desigo Optic n'est pas installé par défaut. Pour installer Desigo Optic, cliquez sur **Installer** > **Synchroniser**. Pour suivre l'avancement, allez sur l'onglet **Services**

×

Informations   Mises à jour   Applications   Accès à distance   >

---

**Détails de distribution**

Nom : Desigo Optic

Version installée : 2.8.23

---

**Applications**

**Desigo Optic**

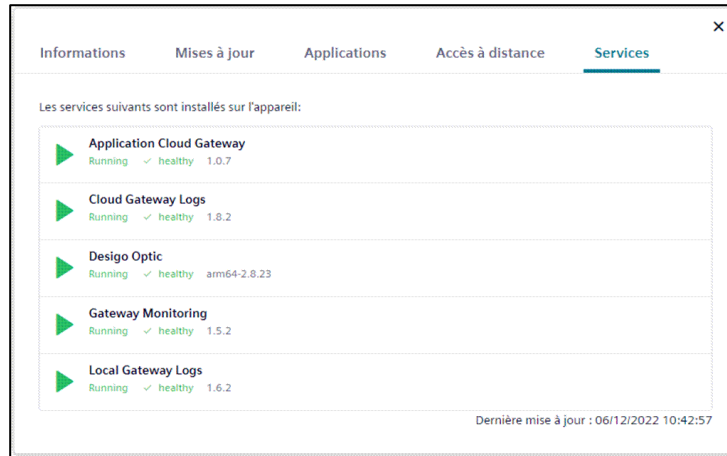
Manage BACnet, Modbus and Alarm data for Desigo Optic

Version : 2.8.23

Licences de logiciel libre [📄](#)

Installer

7. Cliquez sur l'onglet **Services** et recherchez l'état de votre application. Le contrôleur est prêt à être utilisé lorsque les attributs **Running** et **Healthy** s'affichent pour les 5 applications. Si après 15 minutes, les 5 applications n'ont pas les attributs Running et Healthy, contacter le support.

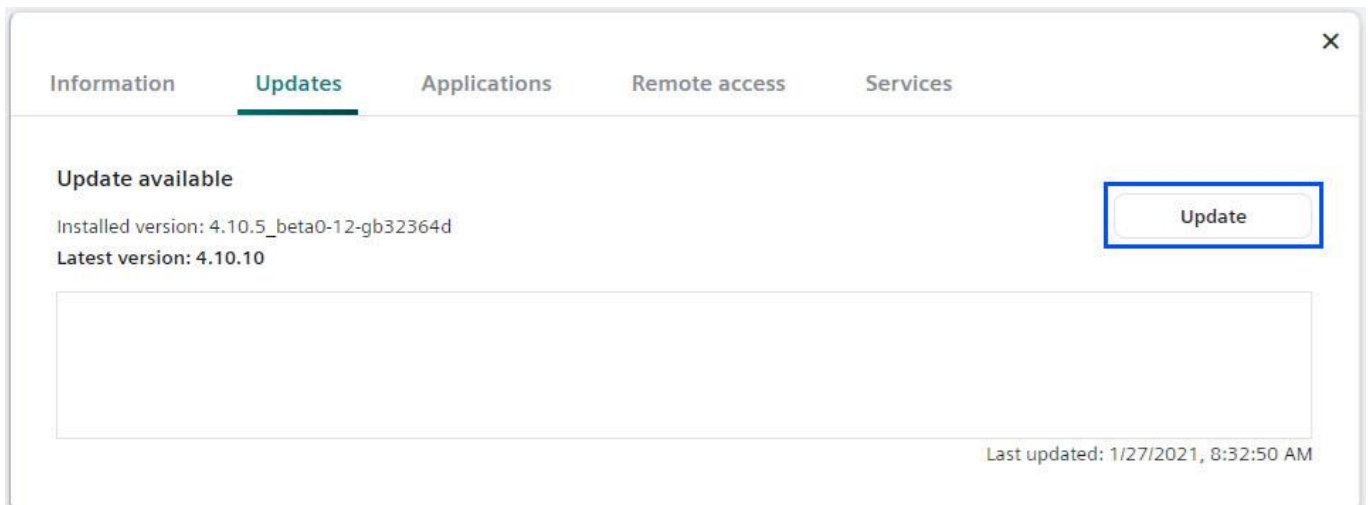


### Mettre à jour le système d'exploitation

Pour mettre à jour le système d'exploitation de l'équipement Connect, procédez comme suit.

▷ Dans **Équipements**:

1. Allez à **Sites**.
2. Sélectionnez le site hébergeant l'équipement F200.
3. Sélectionnez l'équipement > **Mises à jour**.
4. Cliquez sur **Mise à jour**



5. Confirmez avec **Mise à jour**.



La mise à jour du système d'exploitation peut prendre jusqu'à 20 minutes environ selon la bande passante du réseau. Assurez-vous d'avoir une vitesse de téléchargement d'au moins 8Mbit/seconde, sinon le délai de téléchargement risque d'expirer. Attendez avant de passer à l'étape suivante.

Si vous mettez à jour le système d'exploitation, vous serez déconnecté de l'interface de l'équipement F200.


---

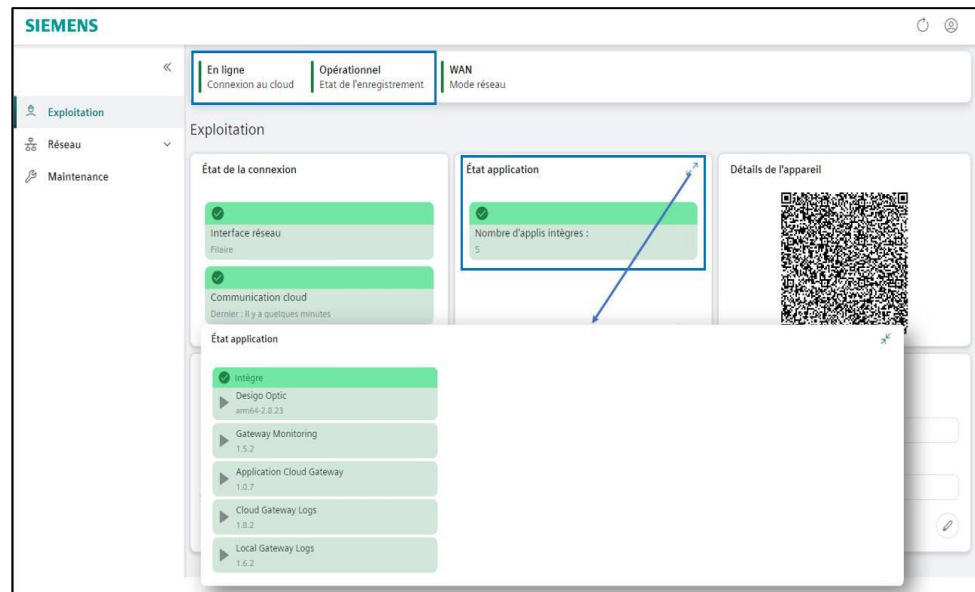
▷ (Facultatif) dans l'équipement F200 :

- ◆ Allez à l'onglet **Maintenance** dans Desigo Optic pour suivre la mise à jour du logiciel en temps réel.

## 7 Vérifier l'état de l'enregistrement et les mises à jour de logiciels

▷ (Facultatif) dans Desigo Optic:

1. Pour vérifier l'état de toutes les applications dans l'équipement F200, sélectionnez l'onglet **Exploitation** dans la barre de navigation latérale.
2. Cliquez sur  pour développer le menu **Applications**. Assurez vous que toutes les applications sont intègres (healthy). Vous remarquerez aussi que la **Connexion au cloud** et l'**Etat de l'enregistrement** sont respectivement “En ligne” et “Opérationnel”.

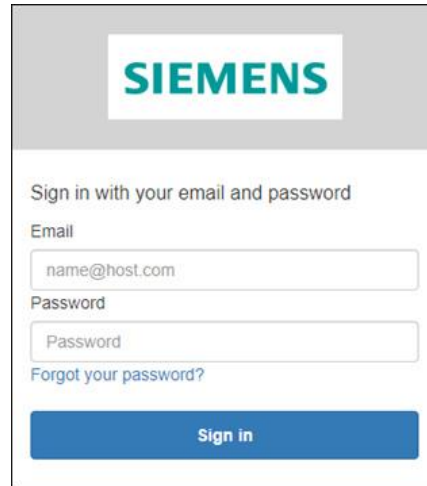


Si vous mettez à jour le système d'exploitation de Desigo Optic, vous serez déconnecté de l'interface du F200.

## 8 Gérer les licences du F200

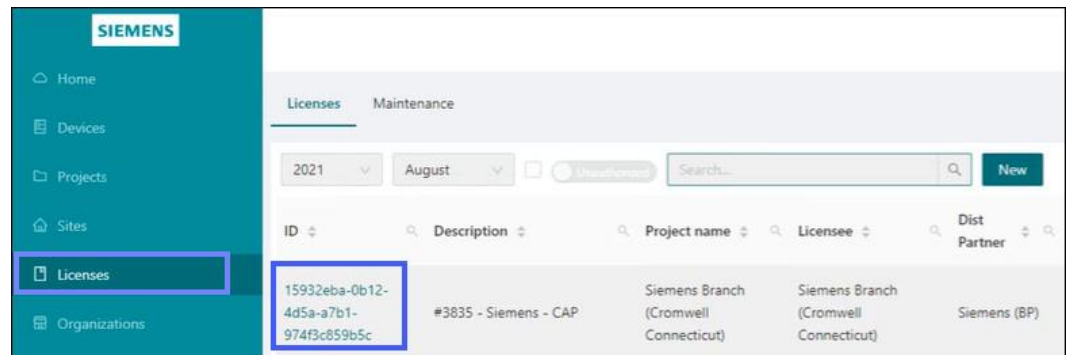
Suivez cette procédure pour ajouter une licence au F200 via Edge2Cloud.

1. Utilisez le lien suivant pour accéder à Edge2Cloud : <https://portal.e2cloud.io/>
2. Entrez vos informations d'identification pour vous connecter.



The image shows the Siemens login page. At the top is the Siemens logo. Below it, the text reads "Sign in with your email and password". There are two input fields: "Email" with the placeholder "name@host.com" and "Password" with the placeholder "Password". Below the password field is a link that says "Forgot your password?". At the bottom is a blue button labeled "Sign in".

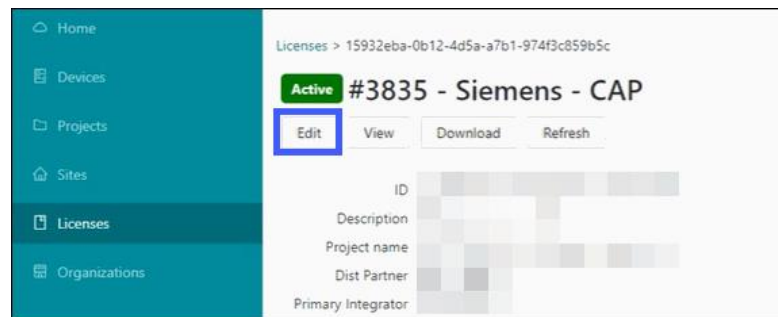
3. Cliquez sur **Licences**.
4. Recherchez votre licence dans la liste > après vous être assuré d'avoir trouvé la licence que vous avez achetée, cliquez sur l'**ID**.



The image shows the Siemens Licenses page. On the left is a navigation menu with "Licences" highlighted. The main content area shows a table of licenses. The table has columns for ID, Description, Project name, Licensee, and Dist Partner. One license is highlighted with a blue box around its ID.

ID	Description	Project name	Licensee	Dist Partner
15932eba-0b12-4d5a-a7b1-974f3c859b5c	#3835 - Siemens - CAP	Siemens Branch (Cromwell Connecticut)	Siemens Branch (Cromwell Connecticut)	Siemens (BP)

5. Une page s'ouvre avec vos informations de licence. Cliquez sur **Edit**.



The image shows the Siemens License details page. The page title is "Licenses > 15932eba-0b12-4d5a-a7b1-974f3c859b5c". The license is labeled "Active #3835 - Siemens - CAP". There are four buttons: "Edit", "View", "Download", and "Refresh". The "Edit" button is highlighted with a blue box. Below the buttons is a table with the following fields: ID, Description, Project name, Dist Partner, and Primary Integrator. The content of these fields is blurred.

6. Renseignez l'**Host ID** de votre équipement.

7. Cliquez sur **Save**.



L'Host ID de l'équipement se trouve dans l'interface d'administration de Desigo Optic, dans la rubrique licence et en cliquant sur Host Info

8. Cliquez sur Download.

9. Dans l'interface d'administration de Desigo Optic, cliquez sur Install et sélectionner le fichier de licence. (fichier .props)

10. Redémarrez le contrôleur à partir de l'onglet **Gateway Maintenance**.

⇒ Le contrôleur est à présent sous licence

## 9 Annexe A – Configurer le masque de sous réseau

Aidez-vous du tableau suivant pour déterminer le nombre de bits dans un **masque de sous-réseau**.

Masque de sous-réseau	Nombre de bits
255.255.255.252	30
255.255.255.248	29
255.255.255.240	28
255.255.255.224	27
255.255.255.192	26
255.255.255.128	25
255.255.255.0	24
255.255.254.0	23
255.255.252.0	22
255.255.248.0	21
255.255.240.0	20
255.255.224.0	19
255.255.192.0	18
255.255.128.0	17
255.255.0.0	16

## 10 Annexe B - Mettre les serveurs de l'application Équipements dans une liste blanche

Pour faciliter l'accès des services Cloud dans un environnement de PROD, les URL de serveur suivantes doivent être joignables via les ports du pare-feu correspondants. Vous trouverez des informations complémentaires dans la **Directive de durcissement à paraître prochainement**.

Service	Point terminal Cloud	Port	Remarques
Bootstrap	<i>Anciennement</i> <a href="https://bootstrap.siemens.com">https://bootstrap.siemens.com</a> <i>Actuellement</i> <a href="https://bootstrap.connectivity.siemens.com">https://bootstrap.connectivity.siemens.com</a>	443	L'ancienne entrée sera autorisée jusqu'à nouvel ordre.
Broker MQTT	<i>Anciennement</i> mqttps://vernemq-device-prod.horizoncloud.io <i>Actuellement</i> mqttps://mqtt.device.horizoncloud.io	443	
Mise à jour du logiciel de l'app	<i>Anciennement</i> <a href="https://registry.horizoncloud.io">https://registry.horizoncloud.io</a> <i>Actuellement</i> <a href="https://ota-update.connectivity.siemens.com">https://ota-update.connectivity.siemens.com</a>	443	
Mises à jour de l'OS	<a href="https://proxy-hawkbite.horizoncloud.io">https://proxy-hawkbite.horizoncloud.io</a> <a href="https://hawkbite.horizoncloud.io">https://hawkbite.horizoncloud.io</a>	443	
Proxy d'autorisation	<i>Anciennement</i> <a href="https://sb-auth-proxy-v2.horizoncloud.io">https://sb-auth-proxy-v2.horizoncloud.io</a> <i>Actuellement</i> <a href="https://proxy.connectivity.siemens.com">https://proxy.connectivity.siemens.com</a>	443	
Synchronisation horaire	0.siemens.pool.ntp.org (serveur principal) 1.siemens.pool.ntp.org (serveur de secours) 2.siemens.pool.ntp.org (serveur de secours) 3.siemens.pool.ntp.org (serveur de secours)	123 UDP	
DNS de secours	8.8.8.8	443	

<i>Référentiel de conteneurs actuel d'AWS</i>	*.dkr.ecr.eu-west-1.amazonaws.com <i>Et</i> <a href="https://registry.horizoncloud.io">https://registry.horizoncloud.io</a> <i>Actuellement</i> <a href="https://registry.connectivity.siemens.com">https://registry.connectivity.siemens.com</a>	443	Nous procédons actuellement à la mise à niveau d'openshift sur AWS, donc les deux URL sont obligatoires.
<i>DNS prévu</i>	*.connectivity.siemens.com		Dans une version future, nous migrerons vers le nouveaux DNS dans lequel tous les points terminaux de connectivité utiliseront cet URL.

Publié par  
Siemens Industry, Inc.  
Smart Infrastructure  
1000 Deerfield Pkwy  
Buffalo Grove IL 60089  
+1 847-215-1000

© Siemens 2019-2022

Sous réserve de modification des spécifications techniques et de la disponibilité sans préavis.

A6V12893144\_fr--\_c