

EcoStruxure IT

Guide d'installation et de configuration



1. ECOSTRUXURE IT	3
A. SE CONNECTER VIA LA PASSERELLE OU DCE ?	3
2. CONFIGURATION MINIMALE REQUISE.....	4
A. PREREQUIS PASSERELLE.....	4
ADAPTE AUX PETITES, MOYENNES ET GRANDES INSTALLATIONS	4
B. PARE-FEU	4
C. NAVIGATEURS PRIS EN CHARGE	4
D. SMARTPHONE	4
E. PERIPHERIQUES CONNECTES	4
F. CERTIFICAT DE SECURITE	5
3. CRÉER UN COMPTE ECOSTRUXURE IT ET TÉLÉCHARGER L'APPLICATION MOBILE	6
A. CRÉER UN COMPTE	6
B. TÉLÉCHARGEZ L'APPLICATION MOBILE ECOSTRUXURE IT	7
C. SCANNEZ LE QR CODE.....	7
4. CONNEXION D'ECOSTRUXURE IT VIA DCE.....	10
5. CONNEXION D'ECOSTRUXURE IT VIA UNE PASSERELLE.....	11
A. TÉLÉCHARGER ET INSTALLER LA PASSERELLE	11
B. CONFIGURER UN SERVEUR PROXY (OPTIONNEL).....	12
C. DÉTECTER LES PÉRIPHÉRIQUES	12
D. CONFIGURER LES PARAMETRES DE TRANSFERT DE FICHIERS DU PERIPHERIQUE.....	14
E. ENREGISTRER ET CONNECTER UNE PASSERELLE	15
6. ACTIVATION D'ECOSTRUXURE IT EXPERT – 90 JOURS GRATUITS	16
7. ACTIVATION D'ECOSTRUXURE ASSET ADVISOR – 90 JOURS GRATUITS.....	16

1. EcoStruxure IT

Pour démarrer, vous aurez besoin des éléments suivants :

- Une **passerelle (Gateway) ou StruxureWare Data Center Expert (DCE)** pour gérer les communications avec vos périphériques surveillés, collecter et envoyer des données des périphériques pour émettre des notifications d'alarme intelligentes.
- **L'interface web EcoStruxure IT** pour effectuer les configurations nécessaires à la bonne surveillance de vos équipements, accéder à l'inventaire de vos assets, aux descriptifs des alarmes, aux données capteurs et obtenir des recommandations grâce aux fonctionnalités Assessments et Benchmark.
- **L'application mobile EcoStruxure IT** pour Android ou iPhone, qui permet de recevoir des alertes et de connaître l'état des périphériques surveillés à tout moment et où que vous soyez (instructions d'installation en page 11)

a. Se connecter via la Passerelle ou DCE ?

Si vous utilisez déjà DCE v7.4.x ou plus, vous pouvez enregistrer votre DCE sur EcoStruxure IT afin d'accéder à l'inventaire de vos assets depuis le Cloud et de recevoir des notifications d'alarme intelligentes grâce au Service Asset Advisor. [Pour en savoir plus](#) (ou aller en page 10).

PS : Un enregistrement d'un DCE sur EcoStruxure IT ne permet pas d'activer l'offre EcoStruxure IT Expert. L'installation d'une passerelle est obligatoire. Vous pouvez cependant enregistrer votre DCE pour bénéficier du service de supervision à distance 24h/24 Asset Advisor.

Si vous ne disposez pas de DCE et que vous souhaitez utiliser EcoStruxure IT Expert et/ou Asset Advisor, vous devez créer un compte en vous rendant sur www.ecostruxureit.com / sign up / Customer.

Enfin suivez les instructions à l'écran pour télécharger la passerelle.

2. Configuration minimale requise

a. Prérequis Passerelle

- Un serveur ou un PC allumé en permanence et fonctionnant sur un système d'exploitation Microsoft® Windows® 7 64 bits, Windows 2008 R2 SP1 64 bits ou une version ultérieure,
- Red Hat Enterprise Linux 7 or CentOS 7 ou version ultérieure.
- Un processeur comprenant au moins 2 cœurs et 4 Go de RAM, 2 Go d'espace disque libre.

La passerelle EcoStruxure IT a été testée sur Microsoft Windows Server 2008 R2 SP1, Server 2012 SP1 et Server 2016. L'application nécessite 225 Mo d'espace disque et le serveur conserve au maximum 8 jours de données, soit environ 128 Mo par jour.

Adapté aux petites, moyennes et grandes installations

Taille	Nombre de périphériques	Nombre de capteurs	Mémoire RAM	Processeur(s)	Taille sur le disque
Petites	250	34 000	4 Go	2	128 Mo par jour
Moyennes	2 000	270 000	8 Go	8	512 Mo par jour
Grandes	5 000	540 000	16 Go	24	1,1 Go par jour

b. Pare-feu

- Port TCP 443 sortant,
- Pour vous connecter à l'aide d'adresses IP statiques, ajoutez les adresses IP 40.84.62.190 et 23.99.90.28.

c. Navigateurs pris en charge

- Microsoft Edge
- Mozilla® Firefox®
- Google Chrome™
- Safari

Définissez la résolution de l'écran sur une résolution d'au moins 1024 x 768.

d. Smartphone

- iPhone 4S et versions plus récentes, iOS 8.0 et versions plus récentes.
- Android 4.4 et versions plus récentes.

e. Périphériques connectés

- Carte de gestion réseau intelligente, Modbus TCP ou SNMP V1 et V3 activés

Veillez à ce que vos cartes NMC soient correctement configurées afin d'assurer la bonne découverte de vos équipements dans EcoStruxure IT.

- Connecté à un réseau TCP/IP auquel la passerelle a accès.

f. Certificat de sécurité

Lors de l'ouverture de la passerelle, le navigateur peut vous afficher un message d'erreur indiquant que la connexion n'est pas sécurisée. Comme l'application est installée sur une machine locale, le certificat de sécurité est auto-signé. L'ajout d'une exception à votre navigateur pour <https://localhost> est sécurisée.

3. Créer un compte EcoStruxure IT et télécharger l'application mobile

L'application EcoStruxure IT est disponible uniquement en anglais pour les systèmes d'exploitation iOS et Android dans [ces pays](#).

Le système d'authentification informatique EcoStruxure IT a été mis à jour afin de prendre en charge les dernières normes de sécurité.

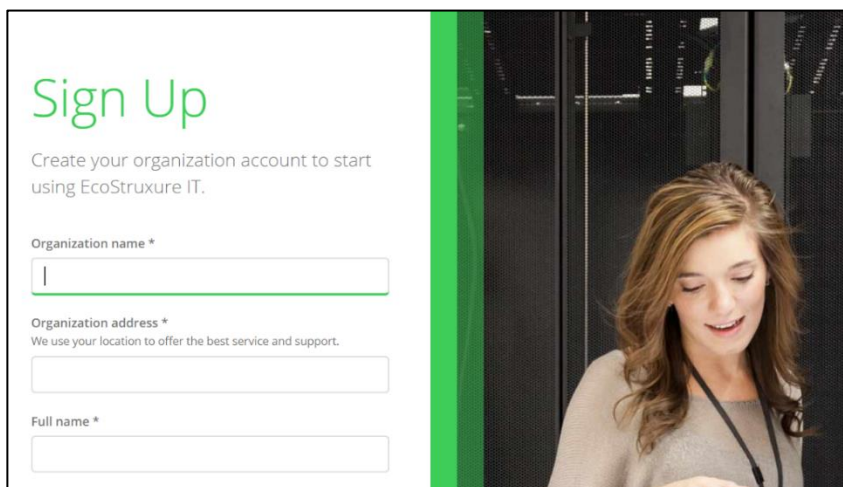
Le SMS n'est plus recommandé au titre de dispositif d'authentification le plus sécurisé. La nouvelle méthode recommandée utilise l'authentification à 2 facteurs. Ce dispositif améliore la sécurité et améliore l'expérience dans les domaines où les codes SMS ne sont pas fiables en raison d'une mauvaise réception cellulaire.

Vous devez maintenant choisir une méthode d'authentification à 2 facteurs : **l'application EcoStruxure IT, le SMS ou l'application Google Authenticator.**

L'authentification recommandée utilise votre application EcoStruxure IT.

a. Créer un compte

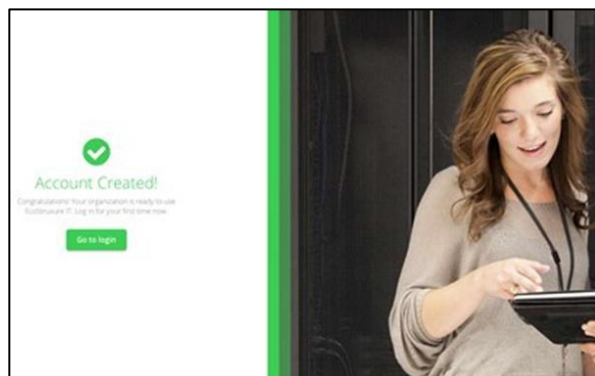
Lors de votre 1^{ère} création de compte, accédez à la page <https://app.ecostruxureit.com/manage/register> à **partir d'un ordinateur, et non depuis un périphérique mobile**. La page de signup s'affiche.



Entrez vos informations de signup et enregistrez-vous.

Vous verrez un message de confirmation indiquant que votre compte a été créé.

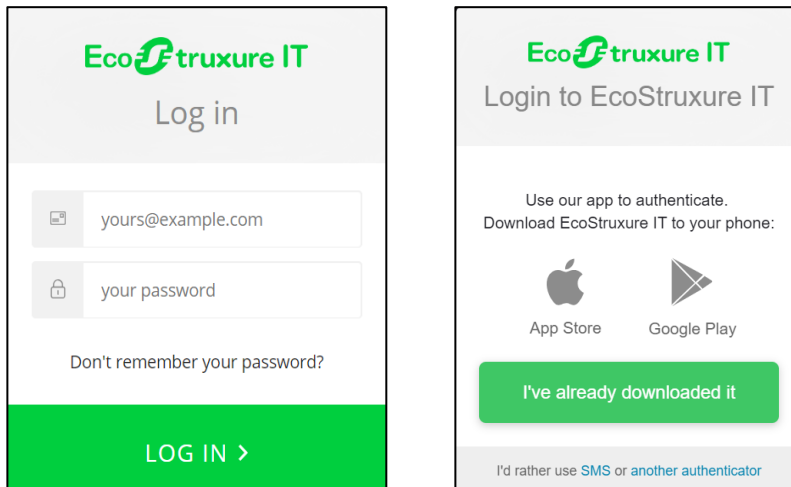
Cliquez sur **Go to Login**.



b. Téléchargez l'application mobile EcoStruxure IT

Entrez vos informations de login sur l'ordinateur (email et mot de passe) et cliquez sur login.

La fenêtre ci-dessous apparait et vous propose de télécharger l'application mobile EcoStruxure IT via Google Play Store (Android) ou l'App Store (Iphone). Une fois l'application téléchargée, cliquez sur « **I've already downloaded it** » pour utiliser l'application EcoStruxure IT comme méthode d'authentification.

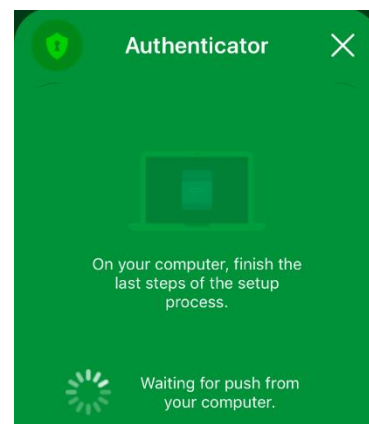
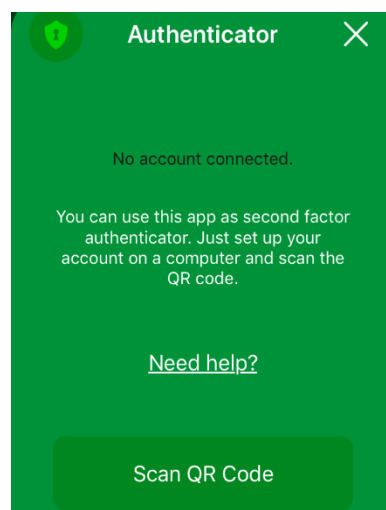
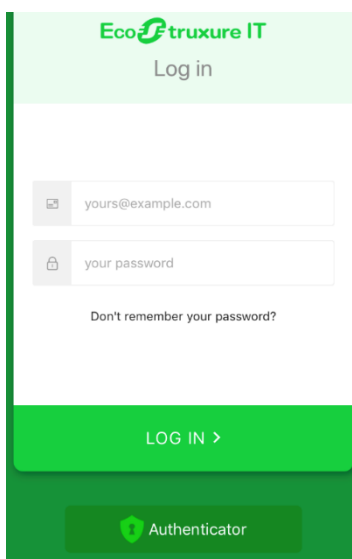
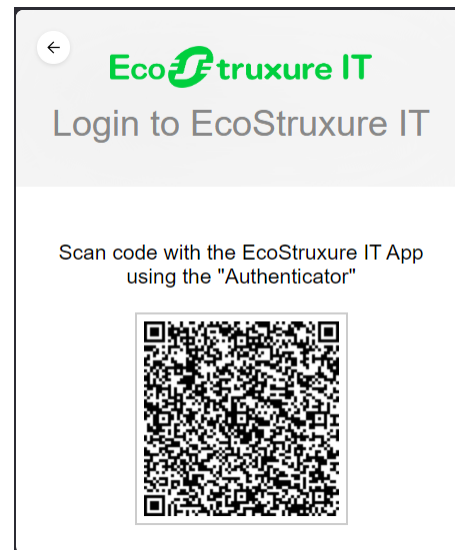


c. Scannez le QR code

L'authentification multi facteur est une procédure à ne réaliser qu'une fois. L'application se souviendra de votre méthode préférée lors de votre prochaine connexion.

La prochaine étape est de scanner le QR code qui apparait sur votre écran d'ordinateur avec l'application mobile.

Sur votre téléphone, veuillez cliquer sur le bouton « **Authenticator** » (n'entrez pas vos identifiants), puis scannez le QR code sur votre ordinateur.



Une fois le code scanné, vous recevrez sur votre ordinateur un code de récupération.

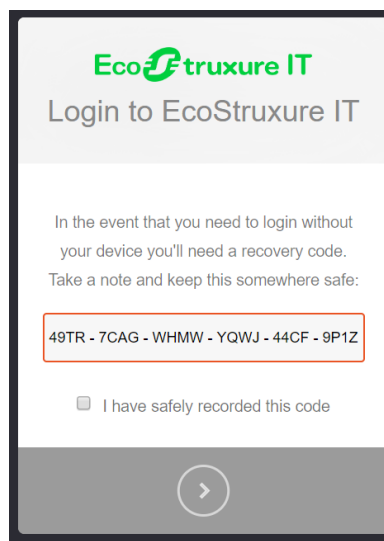
Copiez et enregistrez le code de récupération.

Vous pouvez utiliser ce code pour vous connecter à <https://app.ecostruxureit.com/manage/app-login> lorsque vous n'avez pas votre périphérique mobile sur vous.

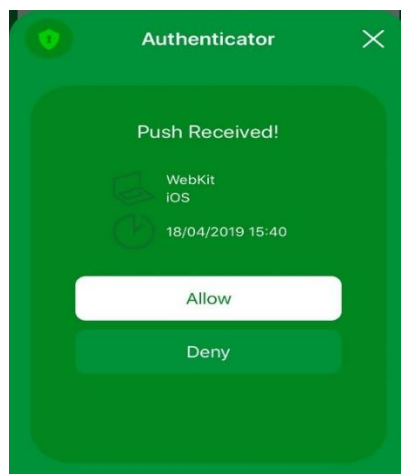
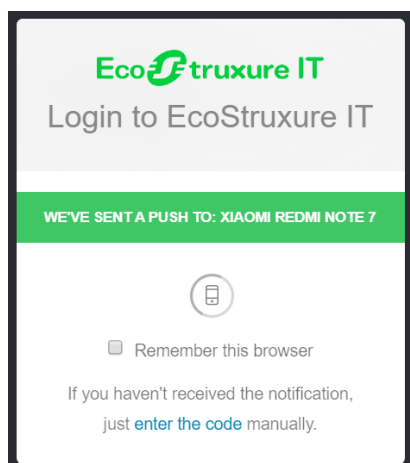
Pour continuer, cochez la case pour confirmer que vous avez enregistré votre code de récupération.

Il vous incombe de le conserver en sécurité.

Cliquez sur la flèche pour continuer.

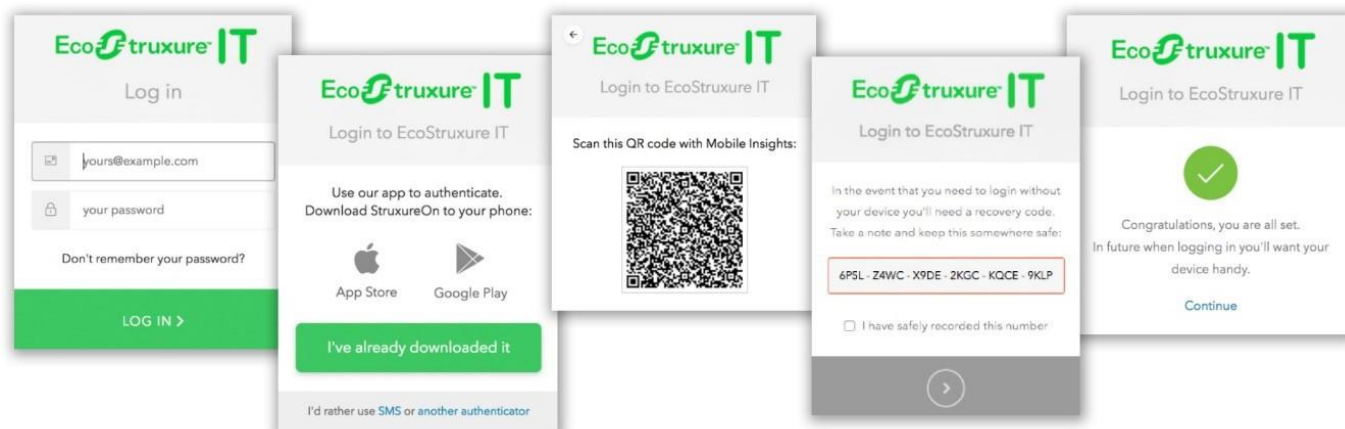


Vous recevez à présent une notification sur votre ordinateur vous informant qu'une autorisation push vous a été envoyée sur votre smartphone. Cliquez sur « Allow ».

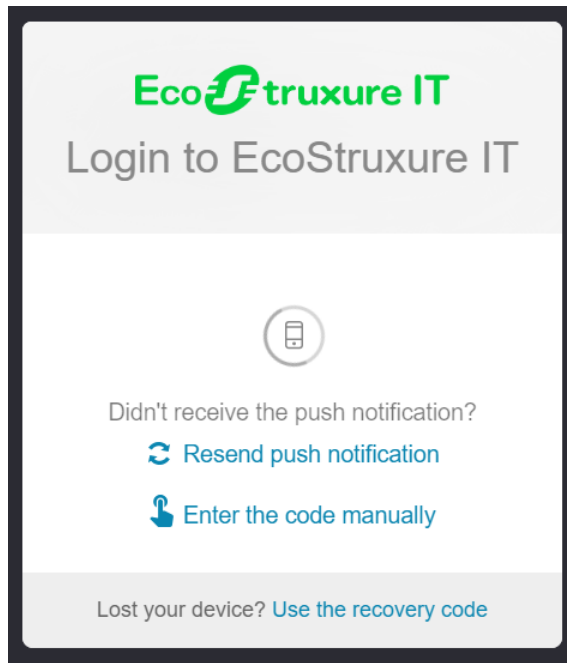


C'est terminé, vous pouvez ensuite commencer à utiliser l'application !

Les prochaines fois que vous vous connecterez, vous recevrez une notification push via votre application EcoStruxure IT pour vous authentifier.



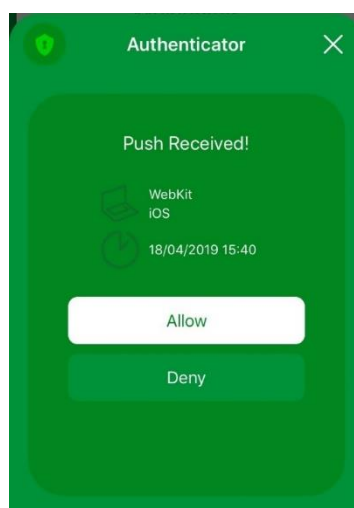
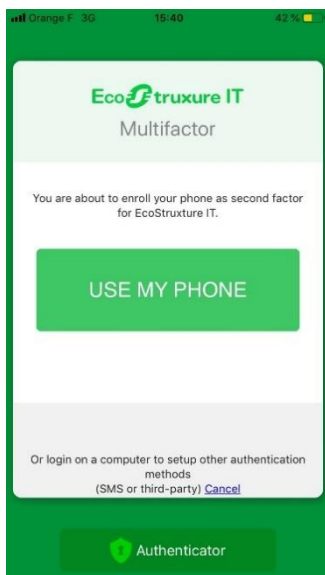
PS : Si vous ne voyez pas l'option de scanner un QR code depuis votre téléphone, il est probable que vous ayez entré vos identifiants directement depuis votre smartphone, le QR code n'a pas été scanné dans le temps imparti et on vous demande de vous authentifier à nouveau en sélectionnant l'option « Resend » ou « Enter code manually ».



Choisissez votre option favorite et connectez-vous.

2FA Reset depuis votre smartphone

Lors d'un reset de votre authentification multi-facteur, entrez vos identifiants sur votre téléphone puis cliquez sur « **Use my phone** » pour sélectionner l'application EcoStruxure II comme méthode préférée d'authentification. Cliquez sur « Allow » pour autoriser.



4. Connexion d'EcoStruxure IT via DCE

Cette procédure est destinée aux utilisateurs de StruxureWare Data Center Expert souhaitant connecter des périphériques à EcoStruxure IT.

Vous aurez besoin des éléments suivants :

- La dernière version des périphériques de surveillance de serveur
- StruxureWare Data Center Expert et l'application EcoStruxure IT pour Android ou iPhone.

Si vous utilisez le service RMS (Service de surveillance à distance) sur votre serveur DCE, vous devez le désactiver avant de vous connecter à EcoStruxure IT.

Instructions

1. Effectuez une mise à niveau vers la dernière version de Data Center Expert.

Contactez le **0810102424** et demandez une mise à jour de votre DCE pour vous connecter au service EcoStruxure Asset Advisor.

Afin d'effectuer cette mise à jour, vérifiez que vous disposez d'un contrat de support logiciel valide vous permettant de recevoir le fichier de mise à jour StruxureWare Data Center Expert.

Une adhésion à un contrat de support du logiciel est nécessaire pour activer EcoStruxure Asset Advisor sur votre Data Center Expert

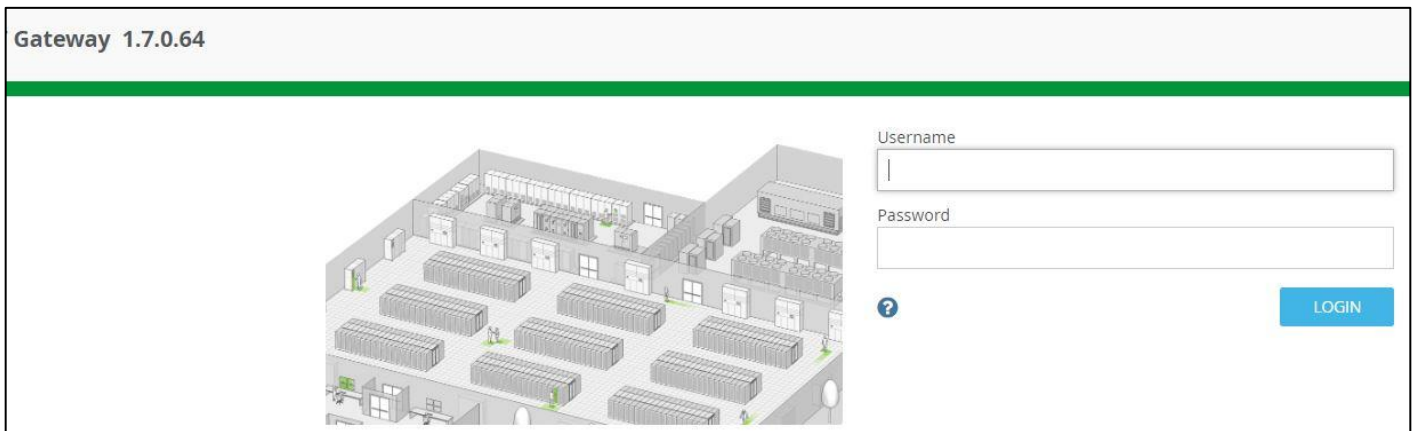
2. Effectuez l'enregistrement Data Center Expert

Pour plus d'information et pour vous accompagner dans la démarche d'enregistrement, veuillez contacter le support par téléphone.


5. Connexion d'EcoStruxure IT via une passerelle

a. Télécharger et installer la passerelle

- Téléchargez et installez la passerelle [ici](#) afin d'ajouter vos équipements sur site au cloud d'EcoStruxure IT (voir prérequis passerelle p.4).
- Connectez-vous à la passerelle. Accédez à la page <https://localhost/gateway> sur n'importe quel ordinateur ayant un accès réseau au serveur. Le nom d'utilisateur et le mot de passe par défaut sont **admin/admin**. Vous pourrez modifier votre mot de passe par la suite.



La page « **Votre connexion n'est pas privée** » peut apparaître avant d'arriver sur la page de connexion.



Votre connexion n'est pas privée

Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site **localhost** (mots de passe, messages ou numéros de carte de crédit, par exemple).
[En savoir plus](#)

NET::ERR_CERT_AUTHORITY_INVALID

Contribuez à améliorer la sécurité de Chrome en envoyant à Google les [URL de certaines pages que vous consultez, ainsi que des informations système limitées et une partie du contenu de certaines pages.](#) [Règles de confidentialité](#)

[Masquer les paramètres avancés](#) [Revenir en lieu sûr](#)

Impossible de vérifier sur le serveur qu'il s'agit bien du domaine **localhost**, car son certificat de sécurité n'est pas considéré comme fiable par le système d'exploitation de votre ordinateur. Cela peut être dû à une mauvaise configuration ou bien à l'interception de votre connexion par un pirate informatique.

[Continuer vers le site localhost \(dangereux\)](#)

L'accès à une page HTTPS nécessite un certificat. Ce certificat n'est pas connu sur cette page localhost, il vous suffit d'aller dans les **paramètres avancés** et de cliquer sur **Continuer vers le site localhost**.

b. Configurer un serveur proxy (optionnel)

Le serveur de la passerelle doit utiliser Internet pour communiquer avec EcoStruxure IT. Si vous utilisez un serveur proxy, spécifiez les paramètres.

- ✓ Dans la passerelle, cliquez sur l'onglet « EcoStruxure IT »
- ✓ Cliquez sur **Paramètres du proxy**.
- ✓ Vous pouvez choisir de détecter automatiquement les paramètres du proxy ou de configurer ces paramètres manuellement. Indiquez l'adresse du serveur proxy, le port HTTP et le port HTTPS utilisés pour communiquer avec le serveur proxy, ainsi que le nom d'utilisateur et le mot de passe pour y accéder.
- ✓ Cliquez sur **OK** pour confirmer que le serveur de passerelle est en mesure d'accéder au serveur proxy en utilisant ces paramètres.

PROXY SERVER SETTINGS
Specify proxy settings and test the connection to your proxy server.

No proxy
 Automatically detect proxy settings
 Configure manually

Proxy server address
[Empty text box]

HTTP port
80

HTTPS port
443

Username
[Empty text box]

Password
[Empty text box]

Confirm password
[Empty text box]

OK CANCEL

c. Détecter les périphériques

Après avoir installé la passerelle EcoStruxure IT, vous devez configurer les périphériques à surveiller par le système pour lui permettre de récupérer des données et d'émettre des notifications d'alarme, etc.

Vous pouvez détecter des périphériques SNMPv1, SNMPv3 et NetBotz avec le mode de détection standard, des périphériques Modbus avec le mode de détection Modbus, et des périphériques SNMP spécifiques avec le mode de détection SNMP ciblé.

1. Connectez-vous à la passerelle, puis dans l'onglet « Devices » cliquez sur le bouton « Discover »
2. Créez et exécutez les détections de périphérique pour les modes Standard (périphériques SNMPv1, SNMPv3 et NetBotz) ou Avancé en spécifiant un nom pour chacun de ceux-ci.

Pour détecter les périphériques standard, spécifiez une plage d'adresses IP.

Utilisez un astérisque pour rechercher sur la totalité d'un sous-réseau : 192.168.1. *

Utilisez un tiret pour rechercher sur une plage d'adresses IP : 192.168.1.100-254. Vous pouvez spécifier plusieurs adresses IP ou des plages d'adresses IP, puis sélectionner le protocole SNMP ou NetBotz, ou les deux protocoles.

SNMP : Spécifiez s'il s'agit du protocole SNMPv1 ou SNMPv3.

- Pour le protocole SNMPv1, spécifiez le nom de communauté en lecture (option définie par défaut sur « public »), le nom de communauté en écriture (privé par défaut) et le port (161 par défaut).

- Pour SNMPv3, spécifiez le nom d'utilisateur, le type d'authentification (MD5 ou SHA), le mot de passe d'authentification, le type de cryptage (DES, DES3, AES128, AES192, AES256), le mot de passe de cryptage et le port (161 par défaut).

NetBotz : Spécifiez le nom d'utilisateur, le mot de passe et le port (défini par défaut sur 80, ou 443 avec SSL activé).

1. La détection avancée est uniquement nécessaire pour les périphériques spécifiques répertoriés dans cette option. Pour détecter les périphériques avancés, spécifiez le type de périphérique, le fournisseur du périphérique, la famille de périphériques et l'adresse IP, et spécifiez le protocole utilisé : SNMPv1 ou SNMPv3.

- Pour le protocole SNMPv1, spécifiez le nom de communauté en lecture (option définie par défaut sur « public »), le nom de communauté en écriture (privé par défaut) et le port (161 par défaut).

- Pour SNMPv3, spécifiez le nom d'utilisateur, le type d'authentification (MD5 ou SHA), le mot de passe d'authentification, le type de cryptage (DES, DES3, AES128, AES192, AES256), le mot de passe de cryptage et le port (161 par défaut).

2. Pour détecter les périphériques Modbus, spécifiez le type de périphérique, l'adresse IP, le port (502 est la valeur définie par défaut) et l'ID esclave, ainsi que d'autres informations nécessaires pour le protocole TCP ou série.

Remarque : Si vous vous apercevez qu'un ou plusieurs de vos périphériques ne sont pas encore pris en charge suite au message d'erreur « This device is not supported », vous pouvez [demander la création ou modification d'un fichier DDF](#) (Device Definition File).

DEVICE DISCOVERY

Name

A name is required.

Standard
 Advanced
 Modbus

IP OR IP ADDRESS RANGE

Use an asterisk to search an entire subnet: 192.168.1.*
 Use a dash to search a range of IP addresses: 192.168.1.100-254

IP address

Enter a valid IP address.

[+ Add another](#)

PROTOCOLS

SNMP
 NetBotz
 Redfish

SNMP

SNMPv1
 SNMPv3

Read community

Write community

Port

d. Configurer les paramètres de transfert de fichiers du périphérique

La méthode de transfert de fichier se fait uniquement via FTP. Le transfert de fichiers est activé par défaut, vous devez cependant spécifier le nom d'utilisateur et le mot de passe dans la passerelle.

La configuration des paramètres du périphérique par défaut est appliquée à tous les périphériques SNMP, sauf lorsqu'un périphérique est spécifié dans une autre configuration.

Il est nécessaire d'activer FTP afin d'utiliser les fonctionnalités de configuration en masse et de mise à jour du Firmware des équipements depuis EcoStruxure IT.

Remarque : Vous pouvez désactiver le transfert de fichiers FTP dans la configuration des paramètres du périphérique par défaut et créer une autre configuration pour activer le transfert de fichiers FTP.

1. Dans la passerelle, accédez à l'onglet **Device File Transfer Settings**.
2. Spécifiez un nom d'utilisateur, un mot de passe et un port.
3. Cliquez sur « **Apply** »

Remarque : La passerelle rassemble quotidiennement les entrées du journal event.txt pour la plupart des périphériques APC/Schneider Electric à l'aide des informations d'identification FTP de la passerelle, apc/apc par défaut.

Assurez-vous que les identifiants de la passerelle correspondent à ceux des périphériques. Autrement, un e-mail d'avertissement sera envoyé chaque jour et ce, pour chaque périphérique concerné.

Details

DEFAULT DEVICE SETTINGS

Enable Default File Transfer Settings

Username

Password

Confirm Password

FTP Port

*Settings are applied to all devices unless the device is specified in another configuration.

e. Enregistrer et connecter une passerelle

Dans la passerelle, accédez à l'onglet **EcoStruxure IT** pour démarrer l'enregistrement de votre organisation et connecter votre passerelle.

Cliquez sur **Register** et spécifiez l'adresse du site de votre organisation. Le système lie le code d'enregistrement à votre organisation lorsque vous sélectionnez **Se connecter à la passerelle**.

Une fois l'enregistrement terminé, vos équipements apparaîtront dans l'interface web et sur l'application mobile.

 **EcoStruxure IT Digital Service**
Connectivity with the service not yet established 

Registration in progress
You are almost there, go to ecostruxureit.com using the link below and register your organization.

6YFSP6
[Register](#)

6. Activation d'EcoStruxure IT Expert – 90 jours gratuits

Afin de bénéficier de toutes les fonctionnalités de supervision d'EcoStruxure IT, vous devez souscrire à EcoStruxure IT Expert. Nous vous invitons dès à présent à activer votre période d'essai gratuite d'EcoStruxure IT Expert pendant 90 jours.

Pour activer la période d'essai, merci de suivre ces instructions :

- Connectez-vous à votre application web EcoStruxure IT : <https://app.ecostruxureit.com/manage/>
- Allez dans l'onglet **Administration/Souscription**
- Cliquez sur **Activer ma période d'essai**

Passé ce délai de 90 jours, vos équipements seront toujours disponibles dans la plateforme, cependant vous ne bénéficierez plus des fonctionnalités dédiées IT Expert.

Nous vous invitons à contacter notre [Customer Success Manager](#) pour vous procurer une souscription annuelle.

7. Activation d'EcoStruxure Asset Advisor – 90 jours gratuits

Une fois vos équipements ajoutés dans la plateforme EcoStruxure IT, **contactez le 0810102424** afin d'activer gratuitement vos équipements pendant 3 mois.