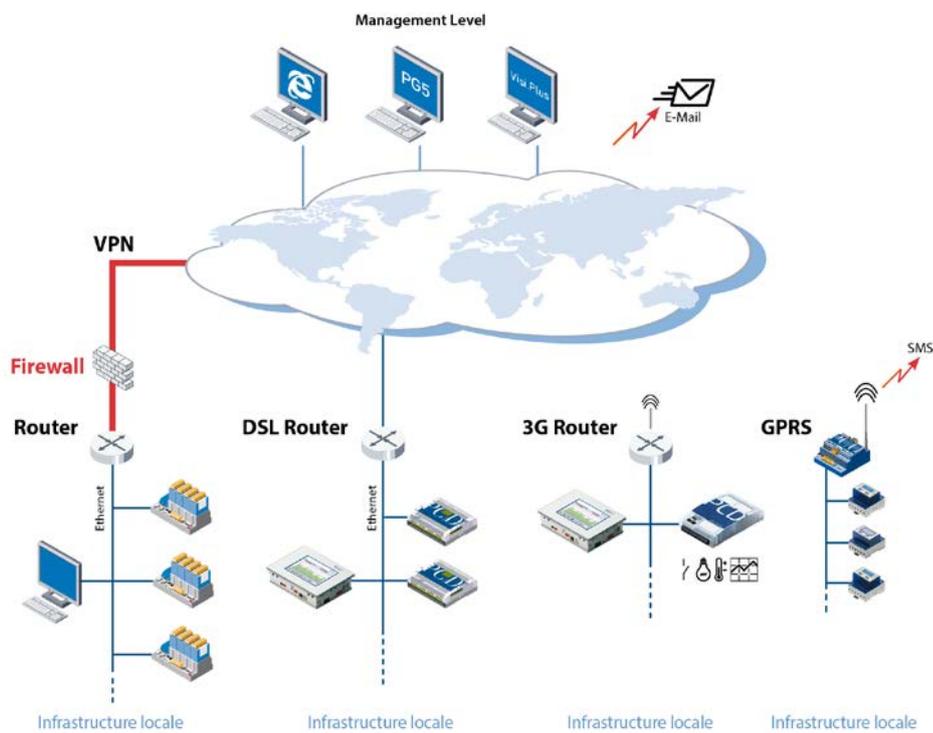


# Recommandations pour le raccordement d'automates Saia PCD à l'Internet



## Historique du document

| Version | Élaboration | Publication | Remarques    |
|---------|-------------|-------------|--------------|
| FR01    | 06.05.2013  | 06.05.2013  |              |
| FR04    | 14-02-2014  | 14-02-2014  | Nouveau logo |

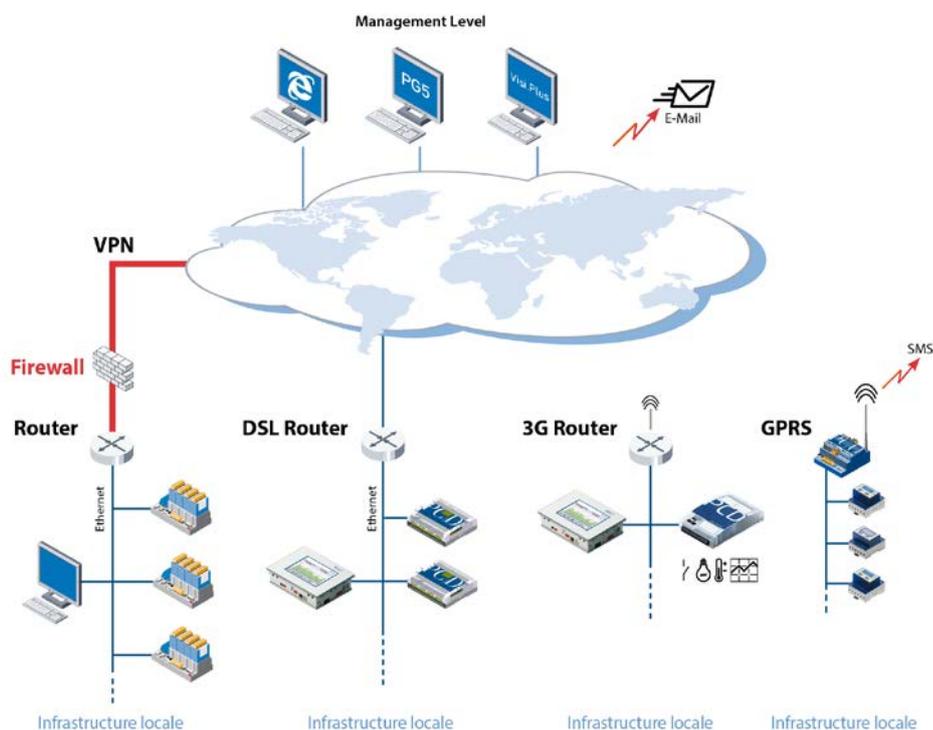
## Contenu

|  |    |
|--|----|
| 1. Introduction.....   | 3  |
| 2. Réalisation d'un réseau privé virtuel (VPN) .....                                     | 5  |
| 3. Protection du serveur Web du PCD.....   | 6  |
| Fonction du mécanisme de mot de passe.....   | 6  |
| 3.1 Paramétrages dans le Device Configurator de PG5 .....                                | 6  |
| Activation du mot de passe du serveur Web du PCD.....                                    | 6  |
| 3.2 Entrée du mot de passe dans le Client Web .....                                      | 9  |
| 3.2.1 Pupitre Web MB (Micro-Browser).....  | 9  |
| 3.2.2 Pupitres Web CE et eXP.....  | 11 |
| 3.2.3 Application Micro-Browser pour iOS.....  | 11 |
| 3.2.4 Navigateur PC avec applet Java.....  | 11 |
| 3.2.5 SBC.Net Web Connect / WebFTP .....   | 12 |
| 3.3 Compatibilité des versions PG5 et Firmware COSinus .....                             | 14 |
| Activation du mot de passe du serveur Web du PCD avec le Device Configurator .....       | 15 |
| Activation du mot de passe du serveur Web du PCD avec le Web Server Project (.wsp) ..... | 16 |
| 4. Protection du serveur FTP .....   | 17 |
| 5. Protection de l'Ethernet S-Bus .....  | 19 |

## 1. Introduction

Il existe différentes manières de raccorder les automates Saia PCD à l'Internet.

La représentation ci-dessous vous montre les possibilités les plus souvent utilisées.



Pour de simples installations distantes, le raccordement d'un automate Saia PCD est réalisé dans la plupart des cas, avec un routeur DSL ou 3G. Un PCD3.WAC se raccorde directement avec son modem GPRS intégré. Les automates Saia PCD exploités sur un réseau local d'entreprise protégé, ne sont accessibles de l'extérieur qu'à travers un pare-feu sécurisé ou un réseau privé virtuel (VPN). Dans ce cas, la protection d'accès est assurée par ces composants.

Lorsque l'automate est accessible au travers d'un routeur DSL ou 3G sans protection particulière, des mesures supplémentaires doivent absolument être entreprises. Dans ces cas, soit l'automate reçoit une adresse IP publique ou les services IP sont acheminés via redirection de Port sur l'automate local.

Sur un PCD les services suivants sont à disposition :

Port 80/81 : Protocole http pour l'accès au serveur Web

Port 21 : Protocole FTP pour l'accès au serveur FTP

Port 5050 : Protocole Ether-S-Bus pour l'accès avec l'outil de programmation PG5 ou un système SCADA avec S-Bus ou respectivement au travers d'un serveur OPC avec S-Bus

Les automates reliés à l'Internet sont simplement vulnérables.

Deux différentes fonctions sont à disposition dans les automates PCD pour la protection de l'application Web :

- Le mécanisme de mot de passe dans l'éditeur Web
- La protection par mot de passe du serveur Web

#### **Le mécanisme de mot de passe dans l'éditeur Web**

Le mécanisme de mot de passe à disposition dans l'éditeur Web permet, par l'entremise de l'applet Java, l'identification de l'utilisateur pour le guider spécifiquement au sein de l'application. Il s'agit d'avantage d'un mécanisme d'identification que de sécurité. La vérification de mot de passe s'effectue dans le navigateur et des personnes avec des connaissances IT spécifiques peuvent contourner cette protection. Ce mécanisme est utile pour la réalisation d'une application IHM pour guider l'utilisateur et offre une protection contre des manipulations involontaires, respectivement des interventions non désirées.

#### **La protection par mot de passe du serveur Web**

Pour une protection accrue (contre les attaques malveillantes), l'accès au serveur Web du PCD peut également être protégé par mot de passe. Malgré cette fonction de protection supplémentaire, nos automates demeurent vulnérables. À ce stade, des connaissances IT spécialisées et un accès direct au réseau IT sont nécessaires. Qui plus est, une telle attaque est une action criminelle.

#### **Solution sécurisée avec un réseau privé virtuel**

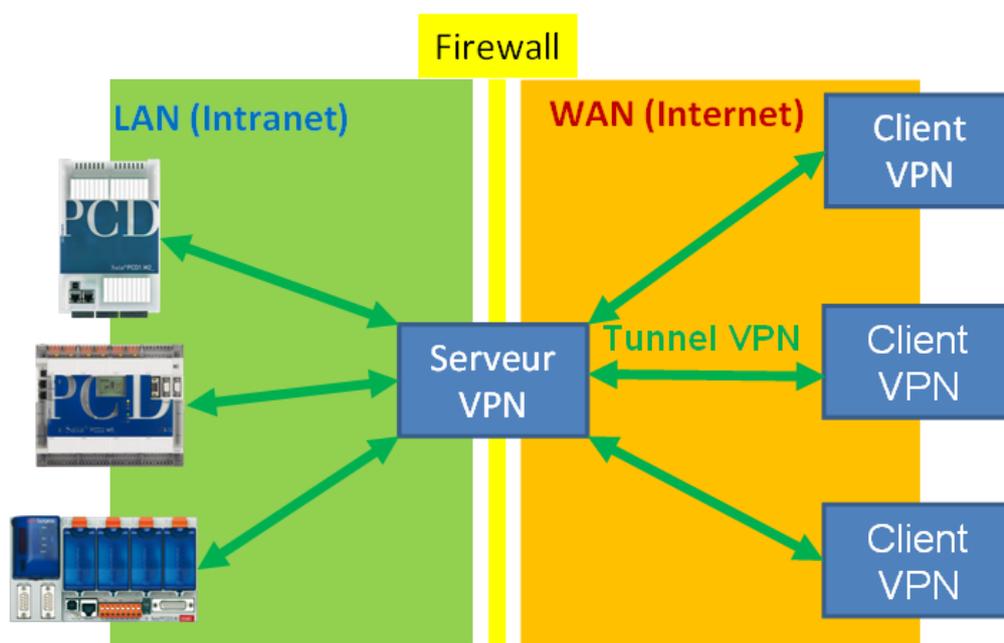
Concernant les installations critiques au niveau sécurité, nous préconisons formellement de les protéger en utilisant un pare-feu (Firewall) et/ou un réseau privé virtuel (VPN).

## 2. Réalisation d'un réseau privé virtuel (VPN)

Une connexion VPN offre un accès sécurisé aux systèmes d'un réseau privé en transitant par le réseau Internet (WAN) au travers d'un «tunnel» virtuel.

Fondamentalement, une telle structure se compose d'un serveur VPN et d'un client VPN. Nous recommandons l'utilisation d'un routeur avec fonctionnalité de serveur VPN. Le client VPN est généralement installé en tant que logiciel sur le dispositif client (PC, tablette, Smartphone, etc.).

Le client VPN ou respectivement le client logiciel VPN se connecte via Internet avec le serveur VPN. Une fois l'inscription réussie, le dispositif sur lequel le client VPN a été démarré se trouve dans l'intranet du serveur VPN via un tunnel sécurisé. À partir de ce moment, il peut atteindre tous les dispositifs et utiliser tous les services dans la plage d'adressage allouée du serveur VPN.



Selon l'application, différents critères définiront le choix du router.

Évidemment, le routeur doit disposer d'un serveur VPN. Pour la réalisation de liaisons VPN, le routeur utilise différents protocoles. Le protocole de communication doit être supporté aussi bien par le routeur que par les dispositifs Client VPN (PC, tablettes, Smartphone). Cela signifie qu'il faut s'assurer que le logiciel client VPN est disponible pour le dispositif client correspondant. IPSec est sans doute la technologie la plus largement utilisée et est supportée directement par de nombreux appareils. IPSec est cependant assez complexe à configurer et à utiliser.

La variante OpenVPN disponible en « opensource » est plus facile à configurer. Celle-ci utilise (également) le protocole de cryptage SSL et ne pose pas de problème avec les pare-feux pour cette

raison. Différents logiciels Client OpenVPN sont disponibles pour de nombreux dispositifs et systèmes d'exploitation.

Actuellement, nous évaluons un routeur avec les fonctions de sécurité appropriées et seront à même de vous le recommander, respectivement de vous l'offrir sous peu.

### 3. Protection du serveur Web du PCD

L'accès au serveur Web du PCD peut être protégé avec un mécanisme de mot de passe.

#### Fonction du mécanisme de mot de passe

Ce mécanisme permet de bloquer l'accès général aux fichiers ainsi qu'à tous les médias du PCD (registres, Flags, DBs/textes, etc.). Lors d'un accès au serveur Web du PCD avec un navigateur (pour PC, d'un pupitre Web, d'un iPad, ...), le serveur vérifie si le mot de passe stocké dans l'automate a été entré correctement. Si aucun mot de passe n'est transmis ou que le mot de passe n'est pas valide, une boîte de dialogue apparaît dans le navigateur pour entrer le mot de passe. La comparaison des mots de passe a lieu dans le serveur Web de l'automate PCD. Cela garantit que pour l'établissement de la connexion les mots de passe de références ne soient pas transmis pour la vérification. Par contre, le mot de passe entré par l'utilisateur est transmis de manière non codée à l'automate.

#### 3.1 Paramétrages dans le Device Configurator de PG5

##### Activation du mot de passe du serveur Web du PCD

Le paramétrage de la configuration de l'automate Saia PCD s'effectue dans le Device Configurator de l'outil de programmation PG5. La configuration du mécanisme de mot de passe se trouve dans l'onglet „Web Server“ sous „Advanced Parameters“.

Pour l'activation de la protection, le paramètre „Access Checks Enabled“ doit être mis sur „Yes“ !



#### Access Check Enabled:

Active le mécanisme de mot de passe serveur Web du PCD

Paramétrage standard : „Yes“

Paramétrage recommandé : „**Yes**“

### Access Timeout

Lors d'une interruption de la communication d'une liaison http S-Bus, la demande de mot de passe est réactivée après le temps paramétré. Ce paramètre est utilisé seulement pour une application http S-Bus.

Paramétrage standard : „60s“

Paramétrage recommandé : „ne pas modifier le paramétrage standard“

### Access Controls Form Page

Ce paramètre définit la page à appeler pour l'entrée d'un mot de passe lors d'un accès au serveur Web sans mot de passe valide.

Paramétrage standard : „pwdform.htm“

Paramétrage recommandé : „ne pas modifier le paramétrage standard“

Remarque : ce formulaire est enregistré dans le serveur Web du système.

Selon besoin, le programmeur peut également créer sa propre page de connexion.

### Paramétrage des mots de passe pour la protection d'accès

Le serveur Web du PCD dispose d'une protection d'accès à 4 niveaux :

„File Access“ → Niveau 1

„Read CGI Access“ → Niveau 2

„Read/Write CGI Access“ → Niveau 3

„Global Access“ → Niveau 4

Dans la plupart des cas, il est suffisant de protéger l'accès de manière générale sur le serveur Web du PCD. Pour cela, **le mot de passe de niveau 1 (File Access)** doit être défini. Nous vous recommandons absolument de définir ce mot de passe ! Tous les autres mots de passe n'ont pas besoin d'être définis ! Après une connexion réussie, les niveaux 1 à 4 sont automatiquement libérés.

S'il devait encore être nécessaire de différencier les droits de lecture et d'écriture à travers le mot de passe, les règles suivantes s'appliquent :

- si aucun mot de passe n'est défini dans aucun niveau, aucune protection n'est activée et l'utilisateur a un accès complet à toutes les fonctions sans entrer de mot de passe
- un mot de passe défini active la protection d'accès à partir de son niveau. Par exemple, s'il y a uniquement un mot de passe défini pour le niveau 1 → Le serveur Web est protégé contre tous accès et l'entrée d'un mot de passe est requise. Après l'entrée du mot de passe, tous les niveaux supérieurs sont également libérés pour autant qu'ils n'aient pas de protection par mot de passe.
- un mot de passe défini donne l'accès à son niveau, ainsi qu'aux niveaux supérieurs respectivement jusqu'au prochain niveau pour lequel un mot de passe est également défini. Par exemple, si des mots de passe sont définis pour les niveaux 1 et 3 → L'entrée du mot de passe niveau 1 libère également le niveau 2. L'entrée du mot de passe niveau 3 libère les niveaux 1 à 4.

### **File Access Password:**

Avec ce mot de passe, l'accès en lecture pour les fichiers et tous les niveaux supérieurs peut être protégé respectivement libéré.

Paramétrage standard : „“

Paramétrage recommandé : „**mot de passe à définir**“

→ À définir absolument, ainsi le serveur Web est totalement protégé.

Attention : la boîte de dialogue est affichée d'une manière générale (pour tous les niveaux) seulement lorsque qu'un mot de passe a été défini pour ce niveau.

### **Read CGI Access Password:**

Avec ce mot de passe, l'accès en lecture sur l'interface CGI ainsi que tous les accès de niveaux supérieurs sont protégés respectivement libérés. L'interface CGI est protégée pour la lecture des médias du PCD (registres, DBs, Flags, textes, ...).

Paramétrage standard : „“

Paramétrage recommandé : „“

Pour un utilisateur ayant besoin d'un accès en lecture avec mot de passe pour par exemple lire des fichiers ou afficher les états de l'installation, il suffit de définir un mot de passe de niveau 1 (**File Access**) et 3 (**Read/Write CGI Access**).

### **Read/Write CGI Access Password:**

Avec ce mot de passe, l'accès en écriture sur l'interface CGI ainsi que tous les accès de niveaux supérieurs sont protégés respectivement libérés. L'interface CGI est protégée pour l'écriture dans les médias PCD (registres, DBs, Flags, textes, ...).

Paramétrage standard : „“

Paramétrage recommandé : „possibilité de définir un mot de passe pour la protection en écriture“

C'est ici que doit être défini un mot de passe pour un utilisateur en ayant besoin seulement pour l'écriture.

### **Global Access Password:**

Ce mot de passe est présent pour des raisons historiques et ne doit pas être défini.

Paramétrage standard : „“

Paramétrage recommandé : „pas nécessaire“

### **Règles pour le choix d'un mot de passe :**

Le mot de passe peut être composé de 31 caractères au maximum et ne doit pas contenir de caractère spécial, de tréma ou d'espace. Il n'y a pas de différenciation entre les majuscules et minuscules.

Pour bénéficier d'une bonne protection, l'emploi au minimum de 10 caractères est recommandé (plus le mot est long plus la sécurité est élevée). Il ne faut pas utiliser de terme facile à deviner tel que le nom de l'installation.

## 3.2 Entrée du mot de passe dans le Client Web

### 3.2.1 Pupitre Web MB (Micro-Browser)

La protection par mot de passe du serveur Web est supportée à partir de la version 1.20.3x des pupitres Web MB.

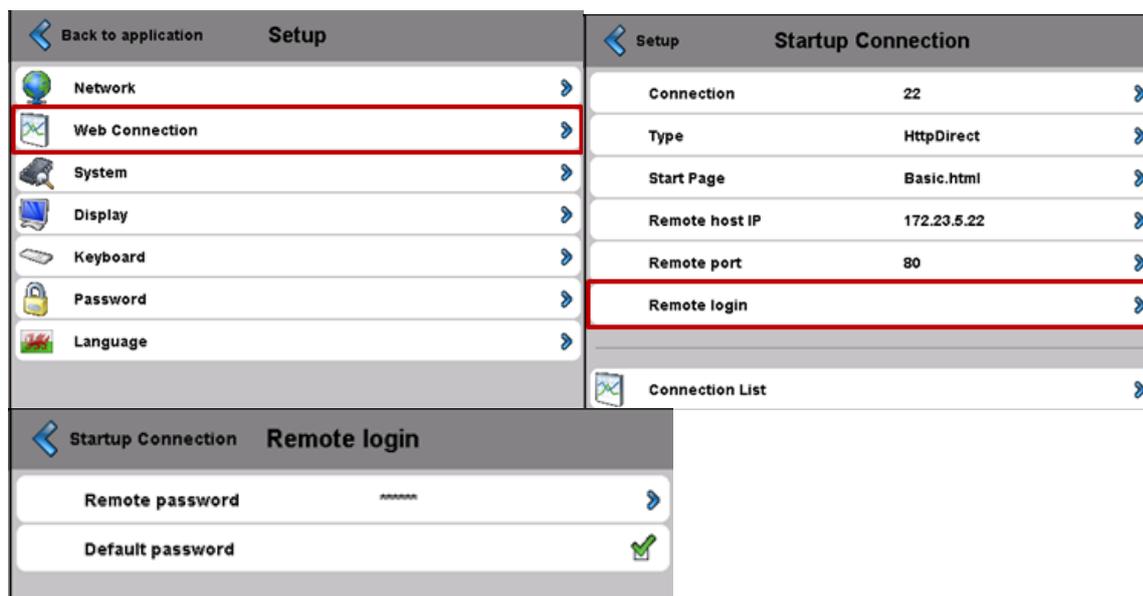
À partir de cette version, il est possible de stocker les mots de passe dans le menu de configuration du pupitre Web MB. Les instructions pour la configuration du mot de passe se trouvent ci-après. Si aucun mot de passe n'est spécifié, le message „PCD Password required!“ apparaîtra sur l'écran. Pour une connexion réussie, le mot de passe doit obligatoirement être enregistré dans le menu de configuration du pupitre Web MB.

Étape 1) Ouvrir le menu de configuration (Setup) du pupitre Web MB

Ce menu peut être ouvert au démarrage de l'appareil ou à un autre moment par une longue pression (d'environ 10 secondes) dans une surface vide de l'application.

Étape 2) Définir la connexion Web

- ➔ Setup ➔ Web Connection ➔ Remote login
- ➔ Remote Password
  - Le mot de passe pour l'accès au serveur Web doit être entré ici.
  - Il est possible de le définir comme mot de passe par défaut. Dans ce cas, il sera toujours utilisé lors d'une connexion lorsqu'un mot de passe est demandé par le serveur Web. Si un mot de passe est défini dans une station de la liste de connexion (Connection List), il sera utilisé en premier. S'il n'est pas possible d'établir une connexion avec le serveur Web à partir d'un mot de passe enregistré dans la liste de connexion, un deuxième essai est fait à partir du mot de passe par défaut.



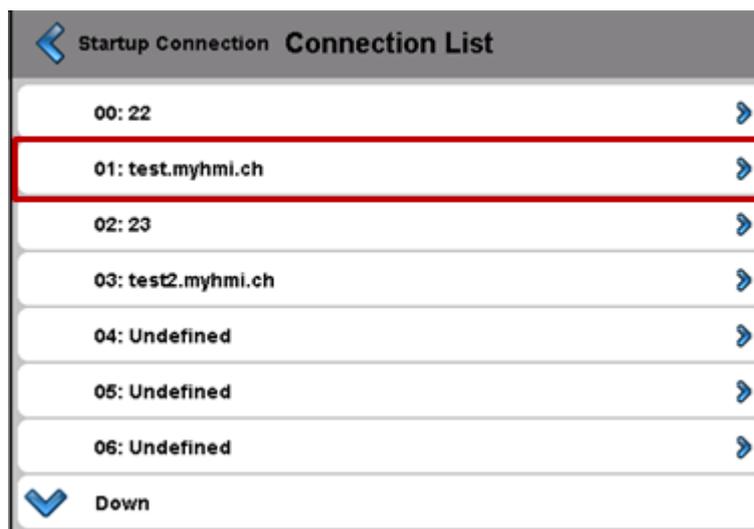
### Étape 3) Traiter la liste de connexion (Connection List)

Si l'on souhaite accéder avec le même pupitre Web MB sur plusieurs automates avec différents mots de passe, il faut définir une connexion spécifique pour chaque automate (Connection List) avec le mot de passe correspondant.



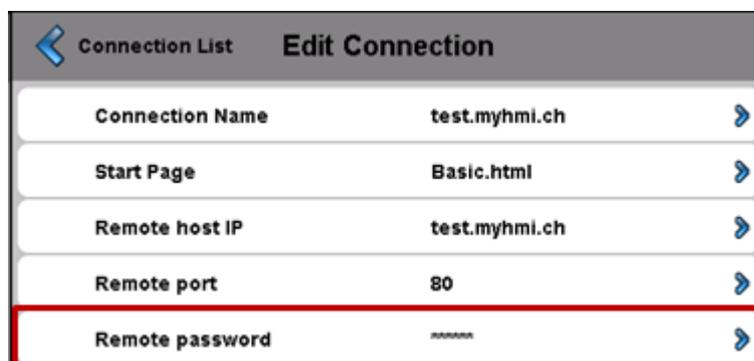
**Setup Startup Connection**

|   |             |   |
|---|-------------|---|
| Connection  | 22          | > |
| Type  | HttpDirect  | > |
| Start Page  | Basic.html  | > |
| Remote host IP  | 172.23.5.22 | > |
| Remote port   | 80          | > |
| Remote login  |             | > |
|  Connection List |             | > |



**Startup Connection Connection List**

|  |   |
|--|---|
| 00: 22   | > |
| 01: test.myhmi.ch  | > |
| 02: 23   | > |
| 03: test2.myhmi.ch   | > |
| 04: Undefined  | > |
| 05: Undefined  | > |
| 06: Undefined  | > |
|  Down |   |



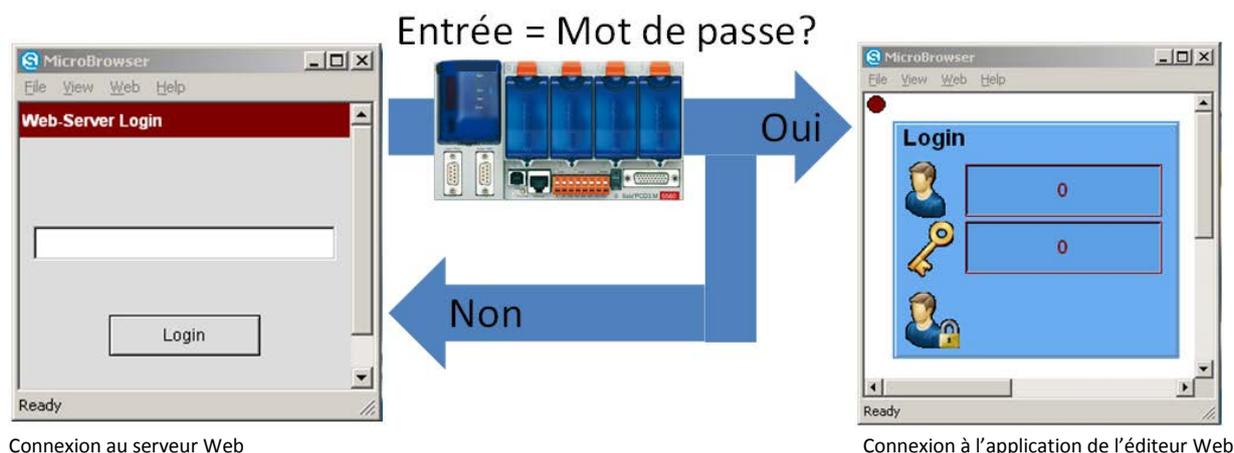
**Connection List Edit Connection**

|                 |               |   |
|-----------------|---------------|---|
| Connection Name | test.myhmi.ch | > |
| Start Page      | Basic.html    | > |
| Remote host IP  | test.myhmi.ch | > |
| Remote port     | 80            | > |
| Remote password | *****         | > |

### 3.2.2 Pupitres Web CE et eXP

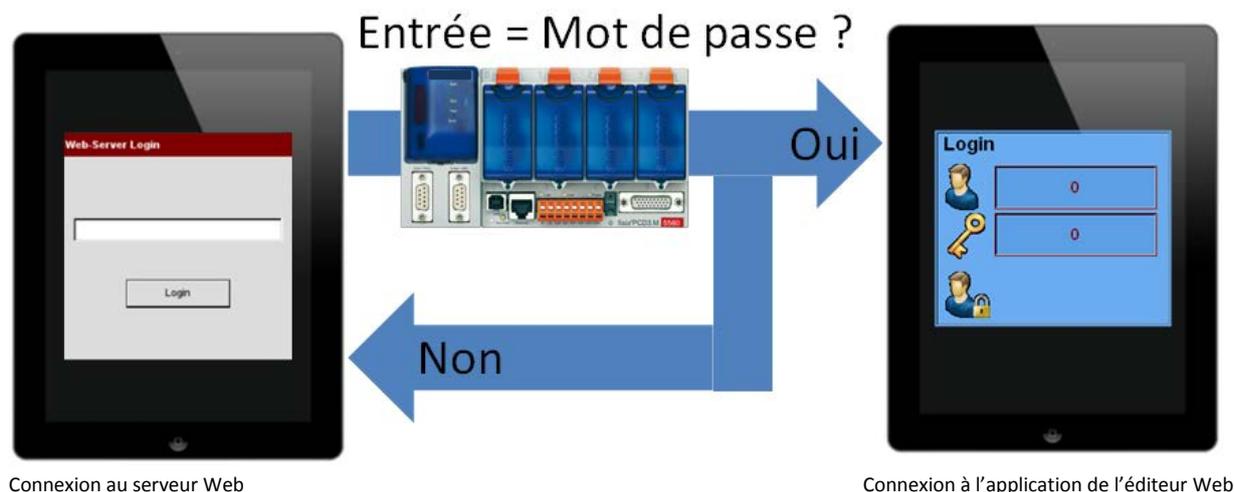
Le navigateur des pupitres Web avec Windows embarqué supporte la connexion au serveur Web à partir de la version 1.5.15.130.

Dans un automate PCD avec un serveur Web protégé par mot de passe, l'utilisateur doit tout d'abord s'annoncer pour accéder au serveur Web et ensuite s'identifier pour le guidage de l'utilisateur dans l'application de l'éditeur Web.



### 3.2.3 Application Micro-Browser pour iOS

L'application Micro-Browser pour les appareils Apple supporte la connexion au serveur Web à partir de la version 1.5.15.130



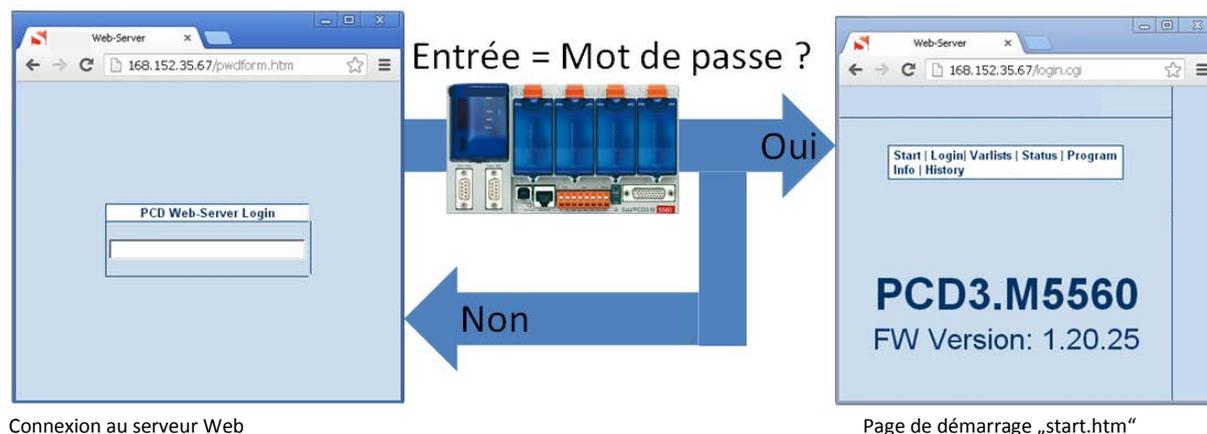
### 3.2.4 Navigateur PC avec applet Java

L'Applet Java pour les navigateurs PC supporte le mécanisme de mot de passe du serveur Web du PCD. Lors de l'accès au serveur Web d'un PCD protégé par mot de passe, le formulaire „pwdform.htm“ défini dans le Device Configurator est affiché automatiquement. Cela permet

d'envoyer le mot de passe au serveur Web du PCD. Si l'entrée est correcte, le fichier „start.htm“ défini dans le Device Configurator est chargé et la visualisation est démarrée.

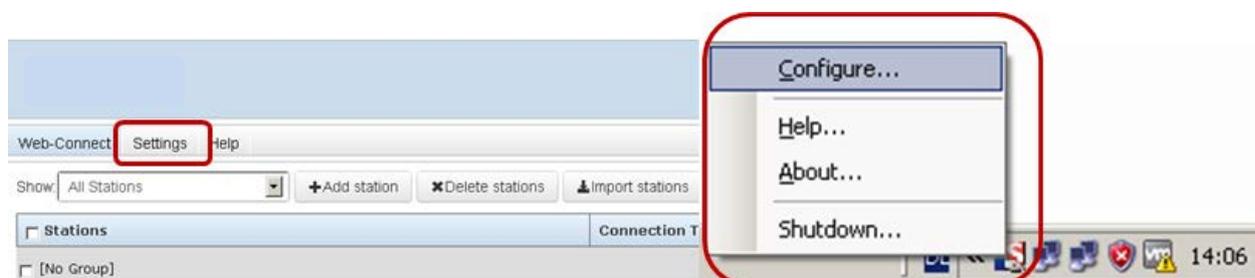
Remarque : après l'entrée du mot de passe, il est possible de charger directement la page HTML du projet Web définissant celle-ci comme page de démarrage dans le Device Configurator.

Note : la page d'état du serveur Web du PCD peut être affichée en tout temps dans le navigateur du PC en entrant „Status.htm“.



### 3.2.5 SBC.Net Web Connect / WebFTP

SBC.Net dispose déjà de sa propre gestion de compte intégrée pouvant être administrée via l'interface utilisateur.

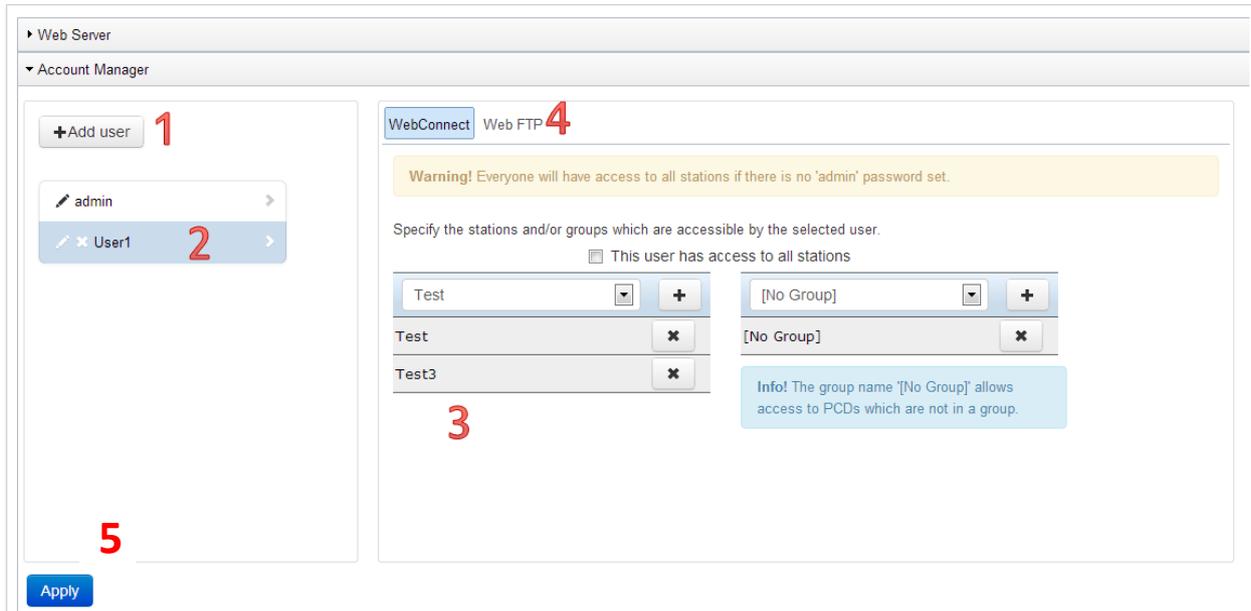


La gestion de compte se trouve dans les paramètres de SBC.Net. Les utilisateurs et les mots de passe peuvent y être définis ainsi que les droits d'accès de l'utilisateur sélectionné.

Un mot de passe pour l'utilisateur „admin“ doit être défini afin que l'accès à toutes les stations soit possible.

- 1) Ajouter un nouvel utilisateur. Chaque utilisateur a besoin d'un nom d'utilisateur et d'un mot de passe correspondant.
- 2) Liste des utilisateurs existants.  
Il est possible d'effacer un utilisateur ou d'en modifier le nom ainsi que le mot de passe correspondant.
- 3) Droits de l'utilisateur sélectionné.  
Les droits sont modifiés selon les fonctions activées de SBC.Net
- 4) Sélection des fonctions Web Connect ou Web FTP

5) Apply, prise en compte, respectivement sauvegarde des modifications.

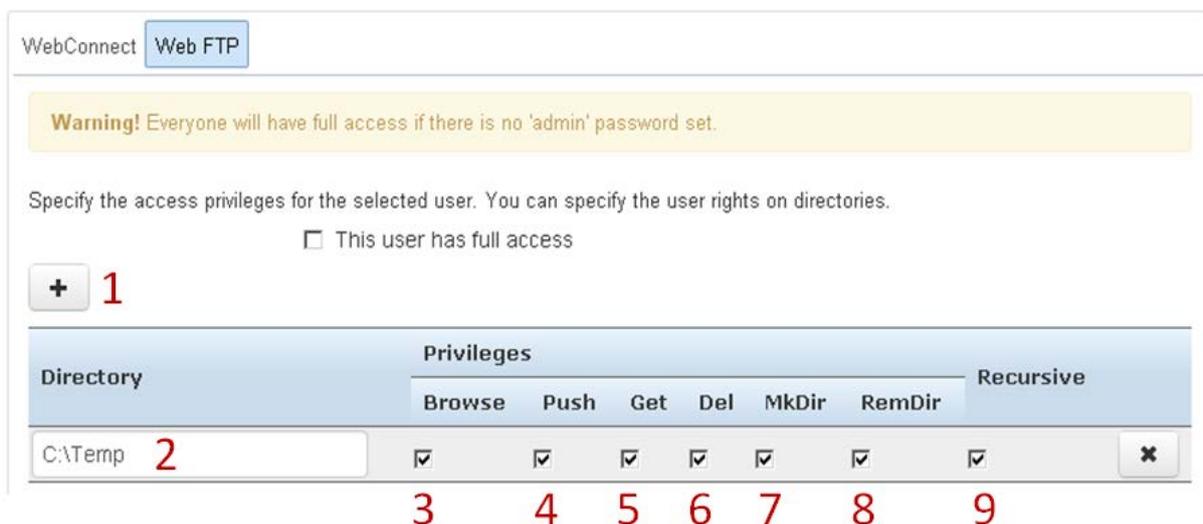


L'onglet WebFTP permet de définir les droits de l'utilisateur du serveur local WebFTP de SBC.Net

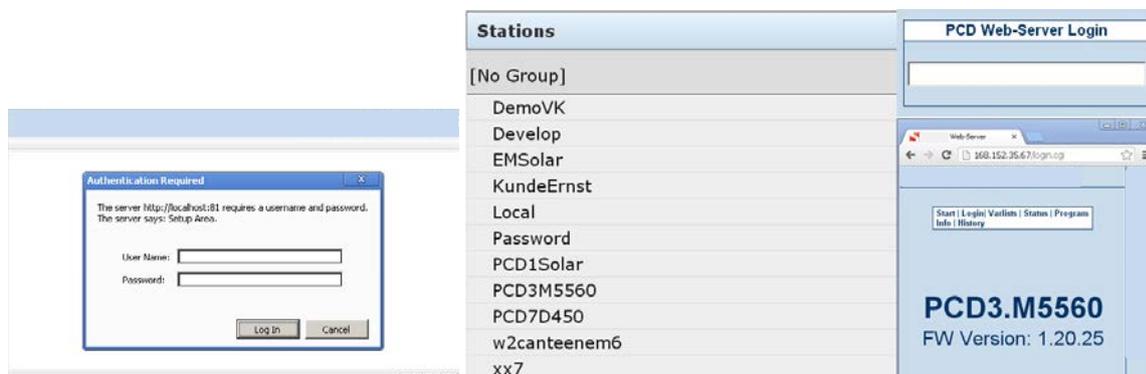
- 1) Ajouter un nouveau répertoire pour l'utilisateur actuellement sélectionné
- 2) Emplacement du répertoire local devant être libéré via WebFTP.

Les droits de l'utilisateur sont les suivants :

- 3) Browse: Consulter le contenu du répertoire courant
- 4) Push: Écrire des fichiers dans le répertoire
- 5) Get: Lire des fichiers dans le répertoire
- 6) Del: Effacer des fichiers dans le répertoire
- 7) Mkdir: Création de sous-répertoires
- 8) RemDir: Renommer les répertoires existants
- 9) Recursive: Inclure tous les sous-répertoires dans la chaîne de droits définie.



Lors de l'ouverture de SBC.Net WebConnect une invite s'affiche pour l'entrée du nom d'utilisateur et du mot de passe. Après inscription vous bénéficiez des droits correspondants à l'utilisateur. Il peut être accédé au serveur Web du PCD en cliquant sur une des stations mises à disposition de l'utilisateur.



### 3.3 Compatibilité des versions PG5 et Firmware COSinus

Les fonctions de protection décrites sont supportées depuis longtemps par les automates PCD. Pour une application correcte, les fonctions doivent également être supportées par les appareils de navigation et le Device Configurator de PG5.

Pour les appareils de navigation Web, les versions suivantes supportent le mécanisme de mot de passe du serveur Web :

| Produit                        | Type de produit | À partir de la version de Firmware | Remarques                            |
|--------------------------------|-----------------|------------------------------------|--------------------------------------|
| Pupitres Web MB<br>VGA et SVGA | PCD7.D4xxWTPF   | 1.20.36                            |                                      |
|                                | PCD7.D457VTCF   | 1.20.36                            |                                      |
|                                | PCD7.D410VTCF   | 1.20.36                            |                                      |
|                                | PCD7.D412VTPF   | 1.20.36                            |                                      |
|                                | PCD7.D4xxVT5F   | 1.20.25                            |                                      |
| Produit                        | Type de produit | Version de Firmware                | Remarques                            |
| Pupitres Web MB<br>QVGA        | PCD7.D457BTCF   | Pas supportée                      |                                      |
|                                | PCD7.D457STCF   | Pas supportée                      |                                      |
|                                | PCD7.D457SMCF   | Pas supportée                      |                                      |
| Produit                        | Type de produit | À partir de la version de Firmware | Remarques                            |
| Pupitres Web eWinCE            | PCD7.D51xxTX010 | 1.5.15.130                         |                                      |
|                                | PCD7.D51xxTL010 | 1.5.15.130                         |                                      |
|                                | PCD7.D51xxTA010 | 1.5.15.130                         |                                      |
| Pupitres Web eWinXP            | PCD7.D61xxTL010 | 1.5.15.130                         |                                      |
|                                | PCD7.D61xxTA010 | 1.5.15.130                         |                                      |
| Produit                        | Type de produit | Version de Firmware                | Remarques                            |
| Application MB iOS             |                 | 1.5.15.130                         |                                      |
| Application MB iOS<br>LITE     |                 | 1.5.15.130                         |                                      |
| Application MB Android         |                 | Pas supportée                      | Nouvelle version disponible sous peu |

Le tableau suivant montre les dépendances concernant la configuration du Web serveur dans le PG5 et les versions FW des automates PCD.

|                        | Web Server Project (.wsp) | Device Configurator |
|------------------------|---------------------------|---------------------|
| FW < 1.14.xx           | Oui*                      | Non                 |
| FW ≥ 1.14.xx < 1.20.xx | Oui *                     | Oui                 |
| FW ≥ 1.20.xx           | Non                       | Oui                 |

\*Avec PG52.x une version de Firmware < 1.14.xx doit être paramétrée dans le Device Configurator

**Aucune** mise à jour de l’outil de programmation PG5 n’est requise pour l’activation du mot de passe du serveur Web.

Pour des versions de Firmware plus petites que 1.14.xx les paramétrages du mot de passe et du serveur Web doivent être définis avec le Web Server Project (.wsp).

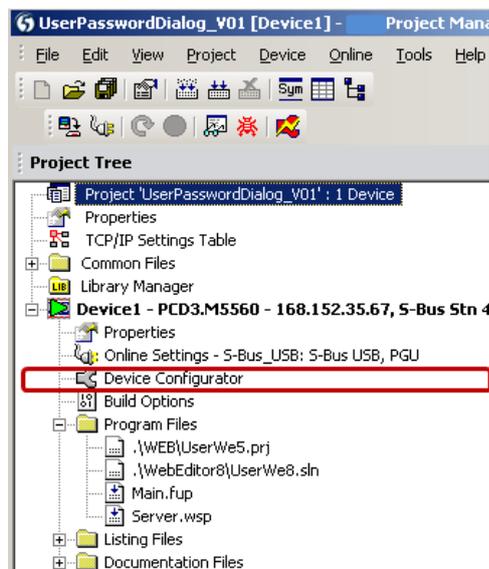
Les versions de Firmware dans la plage de 1.14.xx à 1.16.xx supportent aussi bien la configuration via le Web Server Project que le Device Configurator.

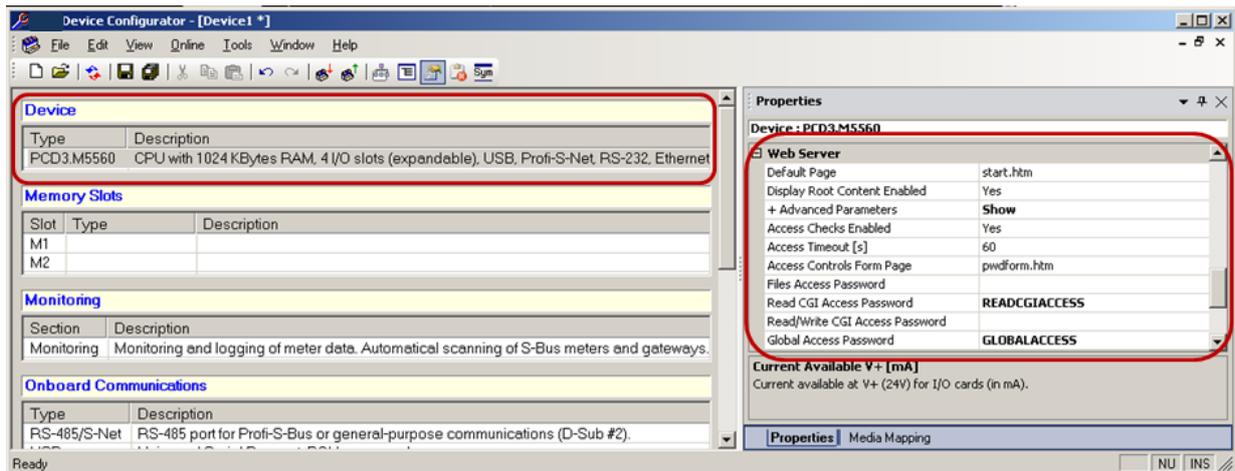
À partir de la version de Firmware 1.20.xx les paramétrages sont modifiables uniquement via le Device Configurator.

### Activation du mot de passe du serveur Web du PCD avec le Device Configurator

La configuration du serveur Web est définie dans le Device Configurator.

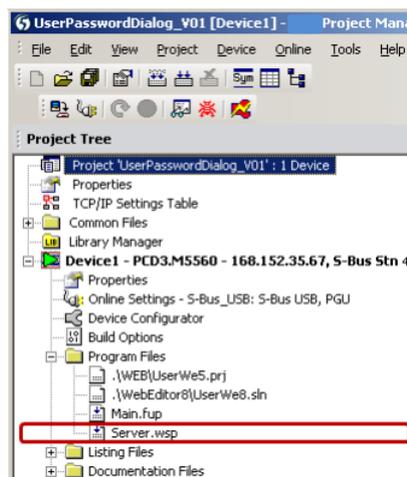
Le paramétrage se trouve dans l’onglet du CPU





### Activation du mot de passe du serveur Web du PCD avec le Web Server Project (.wsp)

La configuration du serveur Web est définie dans le Web Server Project. Cela fait partie des fichiers du programme et est chargé dans l'automate lors d'un download du programme dans l'automate.



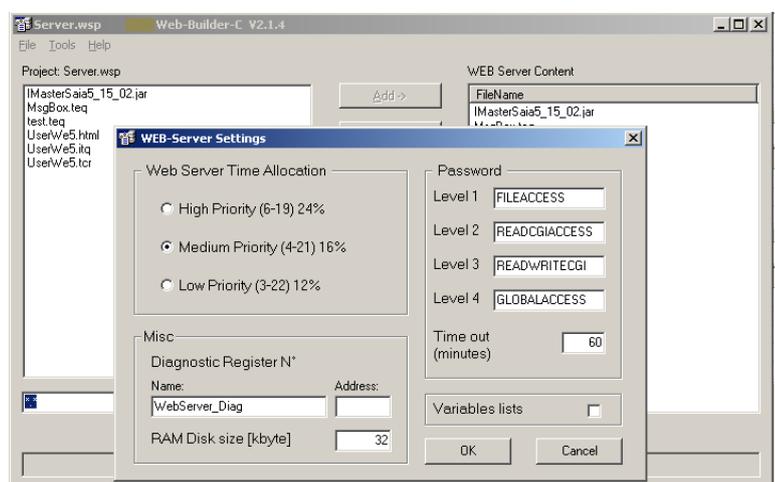
Dans le Web-Server Project (.wsp), l'onglet « Setting » permet d'appeler la fenêtre contenant la configuration de mots de passe.

Niveau 1: File Access Password:

Niveau 2: Read CGI Access Password:

Niveau 3: Read/Write CGI Access Password:

Niveau 4: Global Access Password:

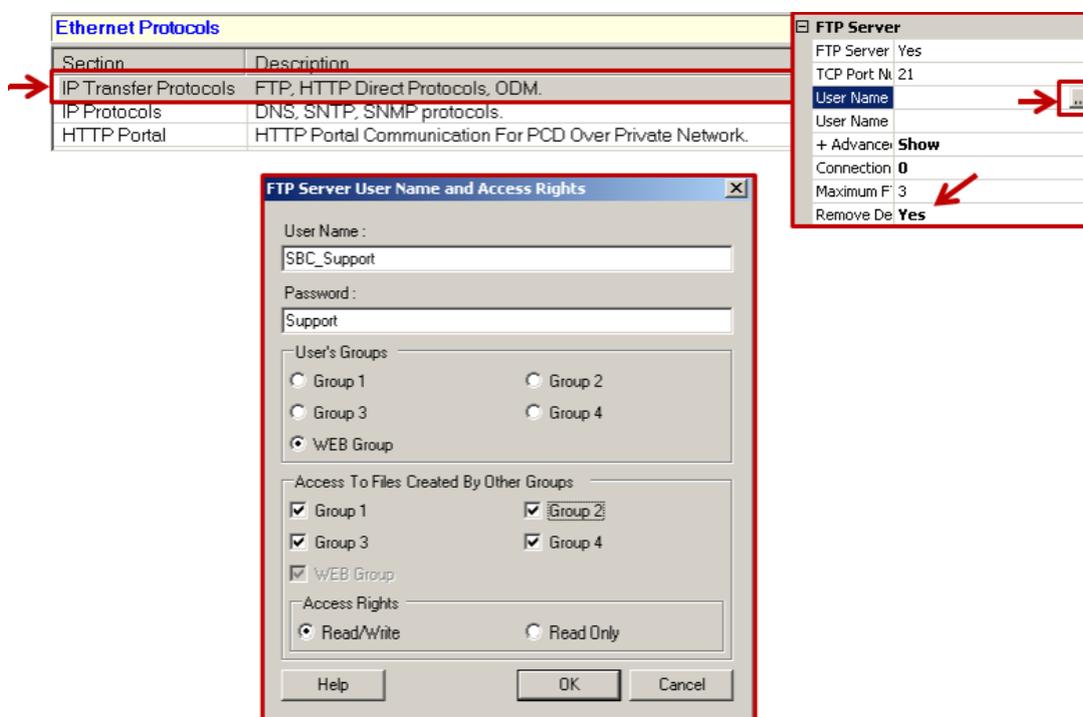


## 4. Protection du serveur FTP

Actuellement tous les automates Saia PCD sont livrés avec un utilisateur standard „root“ et son mot de passe correspondant „rootpasswd“. Cet utilisateur standard doit être désactivé et remplacé par un nouveau dans le Device Configurator.

Le nom d'utilisateur ainsi que le mot de passe correspondant peuvent être définis avec une longueur maximale jusqu'à 20 caractères.

Les paramètres du serveur FTP se trouvent sous l'onglet Ethernet Protocols.



### FTP Server ( Yes/No )

Activation ou désactivation du serveur FTP

Réglage par défaut : „Yes“

Réglage recommandé : „No“ pour les installations critiques

Dans les cas où le serveur FTP Server n'est pas nécessaire, il est recommandé de le désactiver. Un accès avec un logiciel FTP-Client n'est alors plus possible.

### Remove Default User

L'utilisateur par défaut doit être désactivé pour bloquer un accès non-autorisé avec des mots de passe connus ou communiqués publiquement. Après cela, il faut créer au minimum 1 utilisateur.

## Saia-Burgess Controls AG

Rue de la gare 18 | CH-3280 Morat | Suisse  
T +41 26 672 72 72 | F +41 26 672 74 99 | [www.saia-pcd.com](http://www.saia-pcd.com)

Réglage par défaut : „No“

Réglage recommandé : „Yes“

### User Name

Permet de définir jusqu'à 10 utilisateurs individuels avec possibilité d'appartenance à un groupe ainsi qu'une autorisation d'accès en lecture ou écriture. Il peut également être défini des droits d'accès à un autre groupe. Il est possible de définir un compte „Administrateur“ ou « Root » donnant accès en lecture et écriture à tous les groupes.

### TCP Port Number

Le Port 21 est défini par défaut pour une communication FTP.

Ce paramètre permet de modifier le numéro du port du serveur FTP.

Réglage par défaut : „21“

Réglage recommandé : „à modifier seulement si besoin“

### Connection Timeout (s)

Si une connexion existante avec le serveur FTP n'échange pas de données, elle sera fermée après le temps paramétré. Afin que la connexion du serveur soit fermée même si le Client ne le fait pas correctement, une valeur standard de 2 heures (7200 secondes) est recommandée.

Réglage par défaut : „0“

Réglage recommandé : „7200“

### Maximum FTP Connections

Définit le nombre maximal de connexions parallèles au serveur FTP.

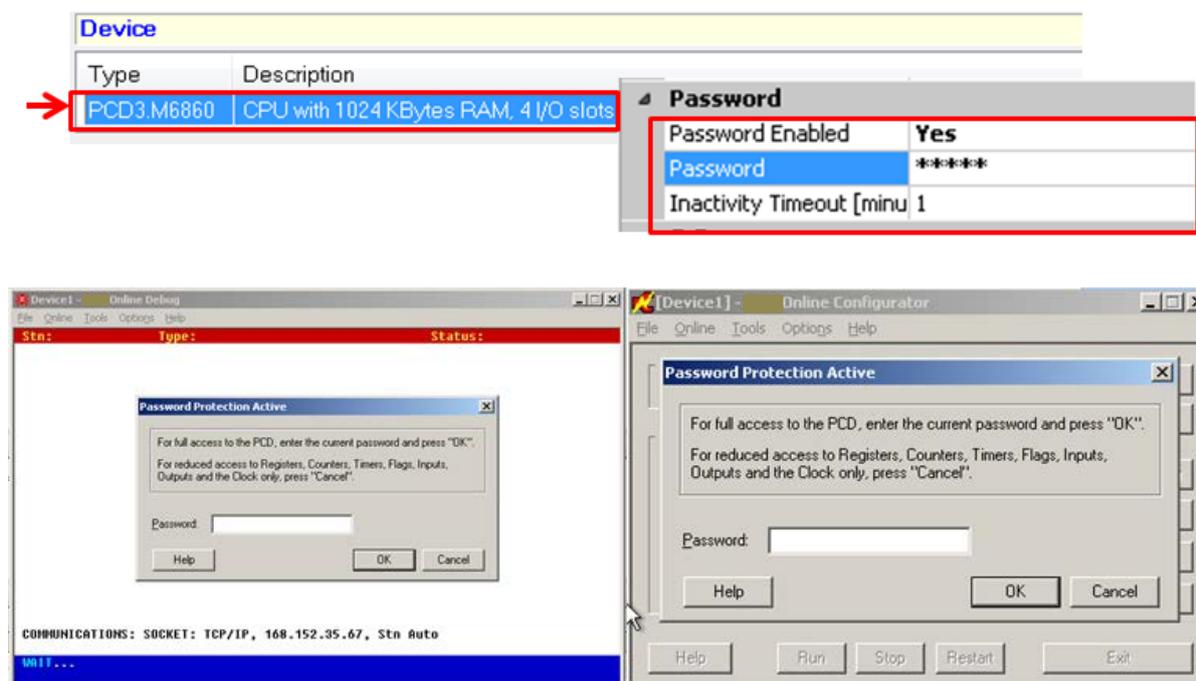
Réglage par défaut : „3“

Réglage recommandé : „à modifier seulement si besoin“

## 5. Protection de l’Ethernet S-Bus

Ether-S-Bus supporte tous les services et toutes les fonctions pour l’échange de données, la programmation, la mise en service et la maintenance des automates Saia PCD. L’accès par Ether-S-Bus est utilisé par l’outil de programmation PG5 ou un système SCADA ou encore un serveur OPC (seulement pour l’échange de données).

Les droits d’accès pour l’Ether-S-Bus peuvent être paramétrés dans le Device Configurator de PG5.



Il faut tenir compte des règles suivantes :

Si le mot de passe est désactivé, tous les services de toutes les interfaces PGU (Ethernet, USB, série) sont supportés sans restriction.

Si un mot de passe est défini, il devra être entré avec l’outil de programmation PG5 lors de la connexion avec toutes les interfaces PGU (Ethernet, USB, série).

Le mot de passe peut être d’une longueur maximale de 25 caractères et doit être composé de majuscules (A, B, C) et de chiffres (0-9).

Pour une bonne protection, nous recommandons un minimum de 10 caractères composé de lettres et de chiffres (plus le mot est long plus la sécurité est élevée). Il ne faut pas utiliser de mot facile à deviner comme le nom de l’installation par exemple.

La communication Ether-S-Bus peut aussi être complètement désactivée dans des installations critiques **avec un Firmware à partir de la version 1.20.xx et PG5 2.1.**

Dans ce cas, il faut prendre en considération que la communication S-Bus ne peut plus être utilisée,

ni avec l'outil de programmation PG5, ni avec les autres systèmes (SCADA, serveur OPC).

Attention : lors de la perte du mot de passe, l'automate doit être réinitialisé avec la fonction Reset.

| Onboard Communications |   |
|------------------------|---|
| Type                   | Description   |
| RS-485/S-Net           | RS-485 port for Profi-S-Bus or general-purpose communications (D-Sub #2). |
| USB                    | Universal Serial Bus port, PGU or general-purpose.                        |
| RS-232/PGU             | RS-232, PGU or general-purpose serial port (D-Sub #1).                    |
| RS-485                 | RS-485 port for general-purpose communications (Terminal block).          |
| <b>Ethernet</b>        | <b>Ethernet port. IP Settings, DHCP.</b>                                  |

| Ether-S-Bus         |           |
|---------------------|-----------|
| Channel Number      | 9         |
| Ether-S-Bus Enabled | <b>No</b> |
| IP Node             | <b>41</b> |
| PGU Port            | Yes       |
| Slave               | Yes       |
| Network Groups      | (Default) |

PG5 2.1 et version de Firmware > 1.20.xx indispensables.