



FAQ EasyBuilderPro

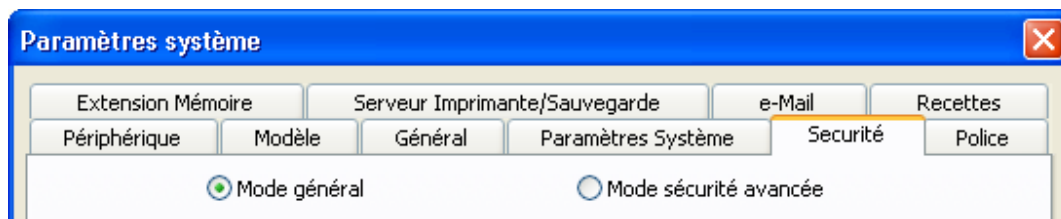
Utiliser le mode de sécurité avancée

KEPFrance SAS
Z.A. Belle Aire
3 rue Vasco de Gama
17440 AYTRE
Tél : 05 46 07 44 40
Fax : 05 46 07 44 44
Site internet : www.kepfrance.fr
E-mail commercial : commercial@kepfrance.fr
E-mail technique : technique@kepfrance.fr

1. Introduction	3
2. Activer la fonction mode sécurité avancée.	4
3. Configurer les différents utilisateurs, mot de passe et niveau d'accès.....	5
4. Liste des commandes possibles	10
5. Note sur le mode de sécurité avancée	11

1. Introduction

Il existe deux modes de sécurité dans le logiciel EasyBuilderPro : le mode général et le mode sécurité avancée.



Le mode général est identique au système de sécurité du logiciel EasyBuilder8000, merci de se référer au fichier « **FAQ-Comment-Mettre-En-Place-Des-Droits-D-Acces.pdf** » pour plus d'informations.

Récapitulatif des fonctions possibles selon le mode sélectionnée :

	Général	Sécurité avancée
Nombre maximal d'utilisateurs	12	127
Nombre de niveaux d'accès	6 (niveaux A à F)	12 (niveaux A à L)
Création dynamique de comptes	Non	Oui
Suppression dynamique de comptes	Non	Oui
Modification dynamique du mot de passe	Oui	Oui
Modification dynamique des droits d'accès	Non	Oui
Utilisation d'une clé de sécurité externe	Non	Oui
Création de compte utilisateur secret	Non	Oui
Format du mot de passe	Numérique	Alpha numérique
Format du nom utilisateur	Numérique	Alpha numérique

Le mode de sécurité avancée est à utiliser dans les cas où l'on souhaite implémenter une gestion d'utilisateur dynamique. C'est-à-dire de pouvoir ajouter, modifier et supprimer un compte directement depuis le pupitre ou l'automate sans avoir à utiliser le logiciel de programmation EBPro ni de recharger le projet présent dans le pupitre.

Ce mode permet également d'utiliser une clé de sécurité externe, c'est-à-dire que les éléments de connexion (nom utilisateur, mot de passe, droits d'accès) sont physiquement stockés dans un fichier crypté sur un support externe (clé USB / carte SD). La connexion via ce compte est impossible si le support physique n'est pas connecté au pupitre. Il est ainsi impossible d'accéder aux pages protégées sans ce support.

Ce document explique comment mettre en place ce mode de sécurité avancée.

Pour rappel, chaque objet nécessitant un appui de la part de l'opérateur peut être protégé par un niveau de sécurité requis. Ces objets peuvent être un interrupteur, une saisie de valeur, un menu déroulant, un bouton d'ouverture de page etc ... Un opérateur ne peut cliquer que sur les objets dont il a accès. Les niveaux d'accès sont identifiés par des lettres, de A à E en mode standard, de A à L en mode avancé. Un niveau d'accès élevé n'autorise pas l'accès aux niveaux inférieur.

Par exemple il est possible de définir le cas suivant :

Utilisateur	Accès Niveau A	Accès Niveau B	Accès Niveau C
Opérateur	Oui	Non	Non
Maintenance	Oui	Oui	Non
Fabriquant	Non	Non	Oui

L'utilisateur opérateur a accès uniquement au niveau A.

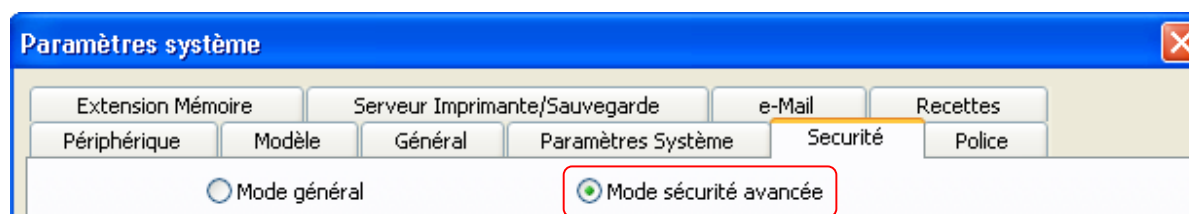
L'utilisateur maintenance a accès aux niveaux A et B.

L'utilisateur fabricant a accès uniquement au niveau C.

2. Activer la fonction mode sécurité avancée.

Aller dans Edition > Paramètres Système, puis dans l'onglet Sécurité

Cocher la case Mode sécurité avancée



3. Configurer les différents utilisateurs, mot de passe et niveau d'accès.

Ces comptes utilisateurs seront intégrés dans le pupitre à chaque chargement du projet. Les comptes ayant été créés de manière dynamique seront écrasés. Pour ne pas écraser ces comptes, cocher la case utiliser compte utilisateur MMI.

Pour se connecter, un utilisateur a trois choix :

- Saisie du **nom d'utilisateur** ainsi que du **mot de passe** via un **clavier**
- Saisie du **nom d'utilisation** via un **menu déroulant** et **saisie du mot de passe** via un **clavier**
- Connexion via un **support externe** de sécurité (clé USB ou carte SD)

Ce chapitre détaille les différents éléments de l'onglet *sécurité*.

a. déclaration des utilisateurs, mots de passe et droits d'accès

Paramètres système

Extension Mémoire Serveur Imprimante/Sauvegarde e-Mail Recettes

Périphérique Modèle Général Paramètres Système **Sécurité** Police

☐ Mode général ☒ Mode sécurité avancée

Sélectionner les classes autorisées pour chaque utilisateurs

☐ Utiliser compte utilisateur MMI

No.	Actif	Utilisateur secret	Nom utilisateur	Mot de passe	Level A	Level B	Level C	Level D
1	☒	☐	Chef de ligne	abc123	☒	☐	☐	☐
2	☒	☐	Maintenance	def456	☒	☒	☐	☐
3	☒	☒	Constucteur	ghi798	☐	☐	☒	☐
4	☐	☐	user4	4	☐	☐	☐	☐
5	☐	☐	user5	5	☐	☐	☐	☐
6	☐	☐	user6	6	☐	☐	☐	☐
7	☐	☐	user7	7	☐	☐	☐	☐

Elément	Description
No.	Liste le numéro d'utilisateur. Il est possible de créer jusqu'à 11 utilisateurs à partir du logiciel EBPro. Il est possible d'atteindre un maximum de 127 utilisateurs de manière dynamique via le pupitre.
Actif	Permet de rendre actif ou non l'utilisateur. Si cette case n'est pas cochée, la ligne est ignorée et est considérée comme vide.
Utilisateur secret	Cette option permet de rendre l'utilisateur secret pour les objets menu déroulant. En effet l'objet menu déroulant propose l'option de lister l'ensemble des utilisateurs disponibles, sauf les utilisateurs définis comme secret. Dans ce cas la connexion d'un utilisateur secret se fait uniquement via une saisie manuelle du nom ou via une clé de sécurité externe.
Nom utilisateur	Identifiant de l'utilisateur, ce champ est requis lors d'une connexion.
Mot de passe	Mot de passe, ce champ est requis lors d'une connexion.
Level A ~Level L	Chaque objet nécessitant un appui de la part de l'opérateur peut être protégé par un niveau de sécurité requis. Un opérateur ne peut cliquer que sur les objets dont il a accès. Cocher les différents niveaux accessibles pour chaque utilisateur.

b. Commentaires sur les différents niveaux.

Level	Description	
Level A	Accès pages historiques alarmes et événements	
Level B	Accès gestion dynamique comptes utilisateurs	
Level C	Accès pages de recettes machines	
Level D		

Ce tableau est à titre indicatif, il n'est pas nécessaire de le remplir, il informe juste des différences entre les divers niveaux.

c. Administrateur

Administrateur

☐ Utilisateur secret

Nom d'utilisateur : Mot de passe :

Il existe un compte utilisateur par défaut ayant accès à tous les niveaux et ne pouvant pas être supprimé. Configurez ici son mot de passe ainsi que l'option utilisateur secret (voir point a. pour plus d'informations).

d. Adresse de contrôle.

Adresse contrôle

Nom API :

Adresse :

Configurez le bloc d'adresse de contrôle permettant les différentes actions (création d'un compte utilisateur, suppression, connexion via saisie manuelle, connexion via menu déroulant ...). Le bloc d'adresses de contrôle a une longueur de 20 registres consécutifs (20 mots de 16 bits).

Le détail de chaque registre et de chaque utilisation est détaillé dans le point f.

e. Connexion/Déconnexion auto de l'utilisateur lors de l'insertion d'une clé de sécurité.

Déconnexion auto de l'utilisateur lors d'une insertion d'une clé USB

☒ Activer * La simulation ne supporte pas cette fonction

Adresse de statut

Nom API :

Adresse :

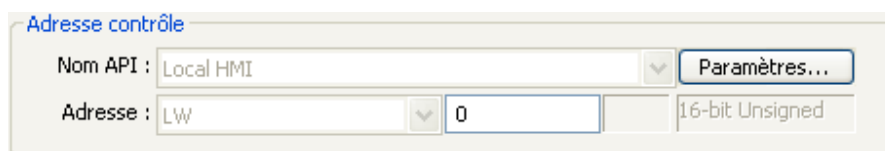
Cette fonction permet une connexion et une déconnexion automatique lors d'un branchement d'un support externe de sécurité (clé USB ou carte SD). Le mot de statut permet de connaître l'état de cette connexion.

Valeur contenu dans le registre de statut	Description
1	Connexion automatique réussie
4	Connexion automatique échouée
8	Déconnexion automatique réussie
10	Déconnexion automatique échouée

f. Adresse de contrôle, détails et utilisation

Comme précisé en point d., la fonction de sécurité avancée nécessite un bloc de 20 mots consécutifs du registre interne au pupitre LW.

Lorsque cette option est utilisée, la librairie de tags est automatiquement mise à jour avec l'ensemble des divers éléments de contrôle.



Voici le détail de chaque élément de ce bloc de mot. N correspond à l'adresse configurée, dans l'exemple ci-dessus N= LW 0

Adresse	Exemple	Elément
N	LW 0	Mot de commande
N+1	LW 1	Résultat de la commande
N+2	LW 2	Index compte utilisateur
N+3	LW 3	Droits d'accès
N+4 à N+ 11	LW 4 à LW 11	Nom utilisateur
N+12 à N+20	LW 12 à LW 20	Mot de passe

Description de chaque élément :

Mot de commande :

Ce mot permet d'exécuter les diverses commande : connexion, création/modification/suppression d'un compte ... Chaque commande étant spécifique, il est nécessaire de paramétrer les autres éléments avant d'exécuter la commande. La liste et le détail des éléments pré-requis se trouvent en point 4.

Résultat de la commande :

Ce mot permet de savoir si la commande exécutée s'est correctement déroulé. Par exemple, si la commande de suppression d'un compte utilisateur a réussi ou non.

Liste des différentes valeurs possibles :

Valeur	Signification
1	La commande s'est correctement déroulée
2	Commande invalide
4	Echec : le compte utilisateur existe déjà
8	Echec : le compte utilisateur n'existe pas
16	Echec : erreur de mot de passe
32	Echec : commande rejetée
64	Echec : nom utilisateur invalide
128	Echec : le mot de passe contient des caractères invalides
256	Echec importation de données via support externe : le fichier de données est invalide
512	Echec connexion via support externe : la date de validité du compte est dépassée.

Index compte utilisateur

Ce registre correspond à l'index du compte utilisateur lors d'une sélection du compte via un objet menu déroulant. En effet, pour faciliter la connexion d'un utilisateur, le développeur peut utiliser un menu déroulant configuré en temps que « compte utilisateur ». De cette manière, le pupitre affiche automatiquement dans un menu déroulant la liste de tous les comptes utilisateurs disponibles sur le pupitre.

Nouveau Menu déroulant Objet

Menu déroulant Mapping Sécurité Forme Label

Description :

Attribut

Mode : List box Fond :

Sélection :

Source de donnée element : Compte utilisateur

Trier

☐ Montant ☒ Descendant

Affichage

☐ Privileges ☐ Utilisateur secret

Adresse de moniteur

Nom API : Local HMI Paramètres...

Adresse : LW 2 16-bit Unsigned

☐ Ecrire lorsque le bouton est relâché

L'adresse du moniteur doit être celle correspondante à l'élément index compte utilisateur (dans notre exemple $N+2 = LW\ 2$).

Les droits d'accès de chaque utilisateur peuvent également être affichés dans le menu déroulant en cochant la case privilèges.

La case utilisateurs secrets permet de masquer/afficher les utilisateurs définis comme secret.

Droits d'accès :

Ce registre permet de définir ou visualiser (selon la commande exécutée) les droits d'accès d'un compte utilisateur. Les niveaux d'accès correspondent aux bits de ce mot.

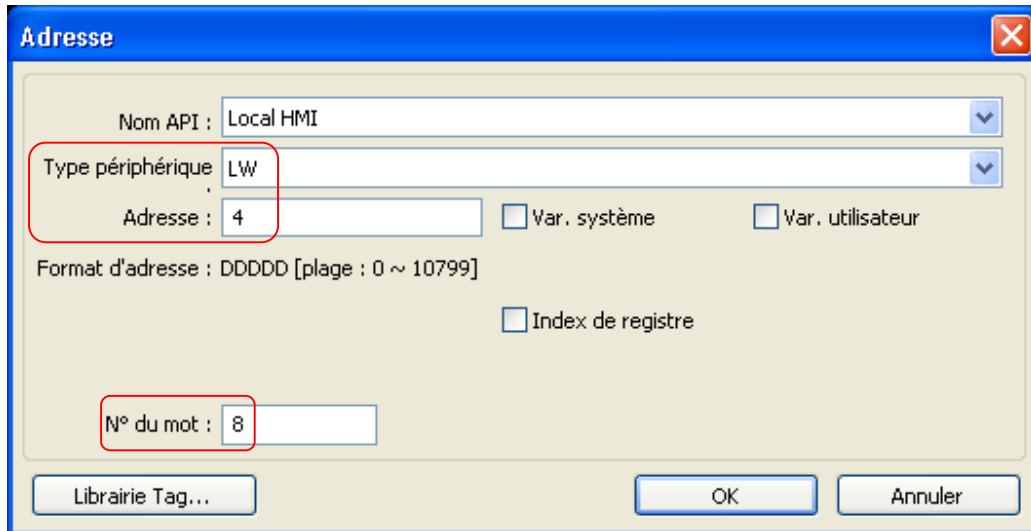
Numéro du bit	Niveau correspondant	Exemple
00	A	LW_Bit 3.00
01	B	LW_Bit 3.01
02	C	LW_Bit 3.02
03	D	LW_Bit 3.03
04	E	LW_Bit 3.04
05	F	LW_Bit 3.05
06	G	LW_Bit 3.06
07	H	LW_Bit 3.07
08	I	LW_Bit 3.08
09	J	LW_Bit 3.09
10	K	LW_Bit 3.10
11	L	LW_Bit 3.11

Note d'informations : fin de vie et remplacement d'un produit

Nom utilisateur

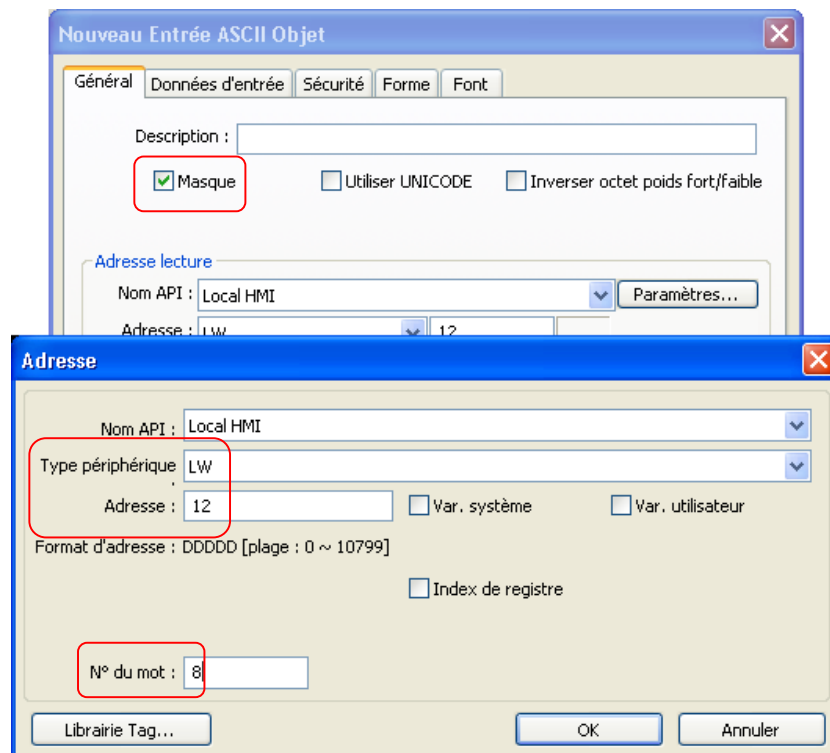
Cet élément est un bloc de 8 mots consécutifs (chaîne de 16 caractères) et permet de renseigner le nom du compte utilisateur manuellement via un clavier pour les commandes de connexion / suppression / modification ...

Il faut utiliser l'objet entrée ASCII configuré de cette manière



Mot de passe

Cet élément est un bloc de 8 mots consécutifs (chaîne de 16 caractères) et permet de renseigner le mot de passe manuellement via un clavier pour les commandes de connexion / création de compte / modification de mot de passe ...



La case à cocher masque permet de remplacer les caractères saisis à l'affichage par des étoiles.

4. Liste des commandes possibles

La table ci-dessous liste l'ensemble des commandes possibles. Pour exécuter une commande, il est nécessaire de renseigner les éléments requis et de forcer la valeur correspondante dans le mot de commande (ici N= LW 0)
Le résultat de chaque commande est automatiquement mis à jour dans le mode statut (N+1= LW 1).

Commande	Eléments requis	Valeur
Connexion via saisie manuelle du nom	Nom d'utilisateur Mot de passe	1
Connexion via saisie par un menu déroulant	Index compte utilisateur Mot de passe	2
Déconnexion	-	3
Modifier mot de passe de l'utilisateur courant*	Nom d'utilisateur Mot de passe	4
Ajouter un compte utilisateur	Nom d'utilisateur Mot de passe Droits d'accès	5
Ajouter un compte utilisateur temporaire**	Nom d'utilisateur Mot de passe Droits d'accès Index compte utilisateur	6
Supprimer un compte utilisateur via saisie manuelle du nom	Nom d'utilisateur	7
Supprimer un compte utilisateur via saisie par un menu déroulant	Index compte utilisateur	8
Modifier droits d'accès d'un utilisateur via saisie manuelle du nom	Nom d'utilisateur Droits d'accès	9
Modifier droits d'accès d'un utilisateur via saisie par un menu déroulant	Index compte utilisateur Droits d'accès	10
Modifier le mot de passe d'un utilisateur via saisie manuelle du nom	Nom d'utilisateur Mot de passe	11
Modifier le mot de passe d'un utilisateur via saisie par un menu déroulant	Nom d'utilisateur Index compte utilisateur	12
Visualiser les droits d'accès d'un utilisateur via saisie manuelle du nom***	Nom d'utilisateur	13
Visualiser les droits d'accès d'un utilisateur via saisie par un menu déroulant***	Nom d'utilisateur	14

*pour cette commande, l'élément *nom d'utilisateur* doit contenir le mot de passe actuel de l'utilisateur connecté, l'élément *mot de passe* doit contenir le nouveau mot de passe.

** pour cette commande, l'élément *index compte utilisateur* doit le délai (en minutes) de validation du compte temporaire. Si le délai est égal à 0, le compte temporaire sera valide jusqu'au prochain redémarrage du pupitre.

*** lorsque cette commande réussie, l'élément *droits d'accès* est mise à jour avec les droits actuel de l'utilisateur demandé

5. Note sur le mode de sécurité avancée

Comptes temporaires :

Les comptes temporaires ne sont pas stockés dans le système du pupitre, ces comptes seront automatiquement supprimés lorsque le délai de validation est dépassé ou lors d'un redémarrage du pupitre.

Suppression de comptes :

Il est impossible de supprimer le compte utilisateur courant, il est nécessaire de se déconnecter afin de pouvoir supprimer ce compte. L'utilisateur courant est l'utilisateur actuellement connecté.

Compte admin :

Ce compte ne peut pas être supprimé, il dispose de tous les droits d'accès.

Mot système :

Le bloc de mots systèmes LW 10754 (longueur 8 mots) contient le nom de l'utilisateur courant.

Journal d'événements :

Il est possible de facilement lister l'ensemble des événements de gestion de connexion / ajout de compte / modification / suppression en utilisant le gestionnaire d'alarme et le mot de statut N+1. Il faut déclarer un événement pour chaque résultat de commande possible.

Alarme (gestionnaire d'évènements)						
Catégorie :		Tout [11]				
No.	Catégorie	Texte	Mode	Condition	Adresse lecture	Notification adress
1	0	Commande réussie	WORD	== 1.00	Local HMI : LW-1	Désactive
2	0	Commande invalide	WORD	== 2.00	Local HMI : LW-1	Désactive
3	0	Le compte existe déjà !	WORD	== 4.00	Local HMI : LW-1	Désactive
4	0	Le compte n'existe pas !	WORD	== 8.00	Local HMI : LW-1	Désactive
5	0	Erreur de mot de passe	WORD	== 16.00	Local HMI : LW-1	Désactive
6	0	Commande incorrecte	WORD	== 32.00	Local HMI : LW-1	Désactive
7	0	Nom utilisateur invalide	WORD	== 64.00	Local HMI : LW-1	Désactive
8	0	Le mot de passe contient des caractères invalides	WORD	== 128.00	Local HMI : LW-1	Désactive
9	0	Echec d'importation données support externe	WORD	== 256.00	Local HMI : LW-1	Désactive
10	0	Délai données support externe dépassé	WORD	== 512.00	Local HMI : LW-1	Désactive