CYBERSECURITE PROTECTA - SMARTLINE S24

Manuel d'utilisation

NC$A 24LA2251606

La protection électrique en toute sérénité

MICROENER

SOMMAIRE

Gestion des modifications

Version	Date	Modification	Rédigé/Validé par
A	23/08/24	Diffusion	LA
Z1	23/08.24	Corrections mineures	LA
Z	02/03/23	Création	AA

INTRODUCTION

Ce document décrit le processus de gestion de la cybersécurité lors de la communication avec avec le relais de la Gamme PROTECTA. Il peut être utilisé comme guide technique pendant la phase d'ingénierie, d'installation et de mise en service, ainsi que pendant le fonctionnement normal.
Il fournit également des conseils techniques pour utiliser l'appareil localement à l'aide de l'écran LCD et à distance à l'aide d'un navigateur web.

Les fonctions de sécurité renforcées suivantes sont disponibles :

- Mise à jour sécurisée des logiciels avec signatures numériques - protection des fichiers firmware ;
- Protocole de communication crypté disponible, tel que HTTPS, afin d'accroître la sécurité du transfert de données ;
- Modes d'accès à l'interface web intégrée sélectionnables par l'utilisateur : activés, désactivés, en lecture seule ;
- L'accès à distance peut être autorisé uniquement pour les clients dédiés (liste blanche) ;
- Tous les événements relatifs à la sécurité sont consignés dans un journal de sécurité non effaçable et ces événements peuvent, en option, être signalés par le biais du protocole syslog à un serveur de journalisation distant ;
- Indication de l'alarme de sécurité ;
- Les accès à la gestion des appareils et au SCADA peuvent être contrôlés individuellement ;
- Restriction des ports TCP/UDP ouverts : tous les services ports peuvent être gérés via l'interface web ;
- Le contrôle d'accès basé sur les rôles (RBAC) fournit un modèle d'autorisation qui permet d'accéder aux opérations et aux configurations de l'appareil en fonction des rôles spécifiques et des comptes d'utilisateurs individuels configurés;
- Les mots de passe utilisés sont stockés sous forme cryptée et gérés dans le cadre de ce processus conforme au livre blanc du BDEW et aux recommandations du NERC CIP ;
- Exigences relatives au mot de passe de l'utilisateur conformément à IEEE 1686 ;
- Communication sécurisée entre le logiciel de configuration EuroCAP et le relais de protection (gestion de la configuration de l'appareil via un canal sécurisé (HTTPS)) ;
- Configuration sécurisée via un fichier de configuration signé numériquement (epcs) ;
- Le logiciel complet du relais de protection est protégé par des signatures numériques afin de détecter les modifications malveillantes. Seuls ces composants logiciels officiellement signés peuvent être chargés et exécutés dans l'appareil ( ) ;
- En option CyberProtect fonctionnalité :
    - Protocole LDAP (Lightweight Directory Access Protocol) disponible pour prendre en charge les fonctions d'authentification et d'autorisation du serveur AAA (Authentication Authorization Accounting)
    - Gestion avancée des utilisateurs avec la possibilité de créer des rôles définis par l'utilisateur pour gérer les interactions de l'utilisateur avec l'appareil par le biais de comptes d'utilisateurs.
- Sécurisation des communications IEC 61850 par IEC 61850 TLS

Ces caractéristiques de cybersécurité améliorées ont été développées conformément aux normes et recommandations NERC-CIP, IEEE 1686, BDEW Whitepaper et IEC 62351-8.

REMARQUE : le micrologiciel minimum requis pour couvrir toutes les fonctions de cybersécurité décrites dans le présent document est 2.10 .1 . 3000.

CONFIGURATION SÉCURISÉE DU RÉSEAU

Protection contre les logiciels malveillants EuroProt

Les relais des gammes PROTECTA et SMARTLINE S24 (IED) sont basés sur un réseau d'exploitation Linux intégré. Jusqu'à présent, les IED basés sur Linux sont considérés comme plus sûrs et moins exposés aux cybermenaces que leurs homologues sous Windows. En outre, ces relais sont équipés d'un pare-feu interne pour se protéger contre les attaques du réseau. Ce pare-feu est activé par défaut afin d'accroître la protection standard.
Néanmoins, l'appareil peut contenir des vulnérabilités inconnues. Les mises à jour du micrologiciel sont publiées aussi souvent que nécessaire en fonction des vulnérabilités exposées . La dernière mise à jour du micrologiciel doit être appliquée dès que possible pour minimiser le risque d'une éventuelle cyberattaque .

Sécurité de l'outil logiciel de configuration EuroCAP

L'outil logiciel de configuration EuroCAP est basé sur les systèmes d'exploitation Windows. Par conséquent, afin de se protéger contre les infections par des logiciels malveillants, il est recommandé d'installer un outil antivirus avec des schémas antivirus mis à jour en permanence.

HTTPS avec connexion d'authentification/autorisation est utilisé pour accéder aux appareils de ces Gammes depuis EuroCAP via le port TCP 443 standard avec une communication sécurisée via le fichier de configuration epcs signé numériquement. Le protocole HTTP, moins sécurisé, peut également être utilisé avec le port standard 80.

Ports et services de communication

L'appareil prend en charge plusieurs ports de communication pour le fonctionnement de plusieurs applications réseau.
Pour configurer le pare-feu d'un réseau, le tableau suivant résume tous les numéros de port utilisés par les appareils de ces deux Gammes. Tous les protocoles peuvent être désactivés individuellement dans "**System settings"** ou dans le menu "**Security settings"**.

Les ports dédiés qui sont ouverts par défaut peuvent être utilisés pour la configuration des relais de protection

Ports de la couche transport disponibles

PORT	DIRECTION	PROTOCOLE	DÉFAUT ÉTAT	SERVICE	COMMENTAIRE
22	IN	TCP	ouvert	SSH/ SFTP	Protocole de transfert de fichiers sécurisé
102	IN	TCP	fermé	IEC 61850	IEC 61850 communication MMS/rapports
3782	IN	TCP	fermé	IEC 61850 TLS	Communication sécurisée IEC 61850
80	IN	TCP	ouvert	HTTP	Configuration / Paramétrage (redirige vers HTTPS si le niveau de sécurité correspondant est sélectionné)
443	IN	TCP	fermé	HTTPS	Configuration / Paramétrage (recommandé)
123	OUT	UDP	fermé	SNTP	Synchronisation temporelle (SNTP)
389	OUT	TCP UDP	fermé	LDAP	Protocole d'accès à l'annuaire (LDAP)
636	OUT	TCP UDP	fermé	LDAPS	LDAP sur SSL
514	OUT	UDP	fermé	syslog	Protocole Syslog
4712 4713	IN/OUT	TCP UDP	fermé	SNTP	Synchrophase
2402	IN	TCP	fermé		IEC 60870-5-104

PORT	DIRECTION	PROTOCOLE	DÉFAUT ÉTAT	SERVICE	COMMENTAIRE
502	IN	TCP	fermé	MODBUS	MODBUS TCP
20000	IN	TCP	fermé	DNP	DNP3 TCP
2405	IN/OUT	UDP	fermé		Protocole propriétaire pour le contrôle du rétroéclairage des groupes d'appareils (allumage)
2406	IN/OUT	UDP	ouvert		Réseau ProtectionHood : protocole propriétaire pour la localisation des appareils

Les paramètres suivants, sous l'onglet **Ethernet comm.**, sont les paramètres liés à l'activation des différents protocoles utilisés pour la communication avec les postes électriques. Certains de ces ports mis en évidence ci-dessus peuvent être ouverts/fermés en modifiant ces paramètres.

Ethernet comm." Onglet des protocoles de communication Ethernet des postes

TITRE	EXPLICATION
Compatible avec la norme IEC 61850	La norme IEC 61850 peut être activée
IEC 104 activée	La norme IEC 104 peut être activée
Modbus TCP activé	Modbus TCP peut être activé
DNP3 TCP activé	DNP3 TCP peut être activé

Dans le menu **System Settings**, sous l'onglet **Time synchronisation**, le port de synchronisation temporal peut être activé.

Synchronisation temporelle NTP

TITRE	EXPLICATION
Timesync via NTP	Activation de la synchronisation temporelle NTP

Les paramètres relatifs au Lightweight Directory Access Protocol (LDAP) se trouvent dans le menu **Security** > **User manager**, onglet **LDAP authentication, authorization.**

Les ports HTTP/HTTPS et SSH peuvent être ouverts/fermés à partir du menu **Security > System services.**

Paramètres de sécurité (Security settings)

Secure handling

Ces paramètres sont cruciaux pour la cybersécurité et rendent l'utilisation de l'appareil plus sûre ou plus pratique . Dans le menu **Security > Security settings** sous l'onglet **Secure handling**, les trois paramètres suivants peuvent être activés/désactivés en fonction des besoins opérationnels.

Paramètres de traitement sécurisé

TITRE	EXPLICATION
Safe settings	Lorsque cette option est activée, un dialogue de confirmation s'affiche sur l'écran LCD physique lorsque des paramètres cruciaux du relais sont modifiés.
Remote front panel control	Lorsque cette option est activée, le panneau avant, c'est-à-dire l'écran LCD et les boutons de l'IHM (à l'exception des boutons I et O) peuvent être contrôlés depuis la page Web.
LCD monitoring	Lorsqu'elle est activée, la copie exacte en direct de l'écran LCD peut être visualisée à partir de la page web.

System services

Dans le menu **Security > Security settings** sous l'onglet **System services**, on trouve les paramètres de communication liés à la sécurité qui peuvent être désactivés/activés selon les besoins de l'opération.

Paramètres relatifs aux ports Ethernet "Services réseau".

TITRE	EXPLICATION
HTTP mode	Sélection du mode d'accès à l'interface web intégrée: *désactivé, lecture seule, accès complet* L'accès au Web est désactivé en mode *lecture seule.*
HTTPS security level	Sélection du niveau de sécurité : *HTTP*, *HTTPS* ou *HTTPS uniquement*
Network protection hood	Activation de la protection de la protection globale
SFTP/SSH enabled	Activation globale de SFTP/SSH
Enable manufacturer SSH access	Activation SSH pour les besoins du fabricant (utilisation en usine uniquement)
Enable archive SSH access	Activation de l'accès SSH pour l'archivage des perturbations
Remote logging	Validation d'envoyer des messages syslog, plus de détails voir chapitre 0

Client Whitelist

L'accès à l'appareil peut être réservé à des adresses IP spécifiques. La fonctionnalité de *Client whitelist* disponible dans l'appareil sous **Security** > **Security settings** > onglet **Client whitelist**, est utilisée à cette fin. Lorsque la fonction est activée, jusqu'à huit clients peuvent être configurés avec des rôles différents.
Les paramètres suivants peuvent être définis pour la configuration de la Client whitelist.

Paramètres de la Client whitelist

TITRE	EXPLICATION
Enable	La fonctionnalité de liste blanche de clients peut être activée
Client 1..8 IP	L'adresse IPv4 du client peut être définie
Client 1..8 Rôle	Les privilèges autorisés peuvent être définis pour le client : • Les deux : tous les privilèges sont autorisés. • SCADA : Tous les protocoles de communication avec l'application SCADA sont autorisés. • Gestion : HTTP /HTTPS est autorisé .

Authentification

Les types d'authentification suivants sont pris en charge par les relais des Gammes PROTECTA et SMARTLINE S24 :

- Authentification de l'appareil (authentification locale de l'appareil)
- Authentification du serveur (serveur LDAP)

Aucun mot de passe ou information de sécurité n'est affiché en texte clair par l'interface web de l'appareil, et ces informations ne sont jamais transmises sans protection cryptographique.
Le nombre d'utilisateurs/mots de passe individuels pris en charge est de 32.

Contrôle d'accès basé sur les rôles (RBAC)

Avec RBAC, les utilisateurs peuvent voir les fonctionnalités qui sont autorisées à des rôles qui leur ont été attribués dans l'IHM. Les rôles et les droits appliqués sont harmonisés avec les normes et les lignes directrices suivantes : IEC 62351-8, IEEE 1686, BDEW Whitepapers.

Rôles des utilisateurs

Les conditions préalables suivantes sont requises pour ajouter/modifier le rôle d'un utilisateur :

- Le droit utilisateur "Manage users" doit être attribué à l'utilisateur.

REMARQUE : L'appareil est initialement configuré avec des droits utilisateur invité où tous les droits sont autorisés à l'invité. Les droits de l'utilisateur invité doivent être limités après la configuration de la sécurité.

Des rôles d'utilisateur prédéfinis avec différents droits d'utilisateur sont disponibles dans le menu **Security** > **User manager** > onglet **Roles.**

Rôles de l'utilisateur prédéfinis conformément à la norme IEC 62351-8 :

VIEWER :
Un observateur peut voir quels objets sont présents dans un IED.
OPERATOR :
Un opérateur peut voir quels objets et quelles valeurs sont présents dans un IED et peut effectuer des actions de contrôle.
ENGINEER :
Un ingénieur peut voir quels objets et quelles valeurs sont présents dans un IED et peut initier des actions de contrôle. De plus, un ingénieur a un accès complet pour configurer l'équipement localement ou à distance (paramétrage, mise à jour de la configuration).
INSTALLER :
Un installateur peut voir quels objets et quelles valeurs sont présents dans un IED en présentant le type et l'ID de ces objets. En outre, un installateur peut écrire des fichiers et configurer le serveur localement ou à distance.
SECADM :
L'administrateur de sécurité peut modifier l'attribution des rôles et des droits et gérer les utilisateurs. En outre, il a accès à la gestion des certificats et au menu Alarme / Journalisation.
SECAUD :
L'auditeur de sécurité peut consulter les journaux d'audit et les alarmes.
RBACMNT :
La gestion RBAC peut modifier l'attribution des rôles et des droits et gérer les utilisateurs. Notez que le RBACMNT constitue une sous-fonctionnalité du rôle SECADM.

Le rôle de l'utilisateur prédéfini suivant est spécifique au fournisseur et n'est pas défini dans la CEI 62351-8 :

Guest :
Par défaut, l'appareil attribue le rôle d'invité à l'utilisateur, avant toute exigence de connexion.

NOTE **:** Initialement, tous les droits sont attribués à l'utilisateur invité. Il est important de limiter les droits de l'utilisateur invité après la mise en place de la sécurité du réseau.

Emergency :
Dans le cas d'une authentification par serveur LDAP, l'utilisateur d'urgence propose comme alternative d'authentification, si, pour une raison quelconque, le serveur LDAP n'est pas disponible.

Full access :
Tous les droits sont accordés à l'utilisateur.
Erreur ! Source du renvoi introuvable. ci-dessous rassemble les attributions de droits de rôle prédéfinies en usine dans l'appareil :

Attributions prédéfinies de rôles et de droits sans CyberProtect

Rôle	Type	View data	View settings	Manage settings	Control	Manage configuration	Update firmware	Manage users	Audit	Log	Edit
Guest	Guest	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Edit
Full acces		Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	
Viewer		Web, Lcd									
Operator		Web, Lcd	Web, Lcd								
Engineer		Web, Lcd	Web, Lcd	Web, Lcd		Web, Lcd					
Installer		Web, Lcd	Web, Lcd	Web, Lcd		Web, Lcd	Web, Lcd				
SECADM		Web, Lcd	Web, Lcd	Web, Lcd				Web, Lcd			
SECAUD		Web, Lcd	Web, Lcd	Web, Lcd					Web, Lcd		
RBACMNT		Web, Lcd						Web, Lcd			

Refresh

Fonctionnalité CyberProtect

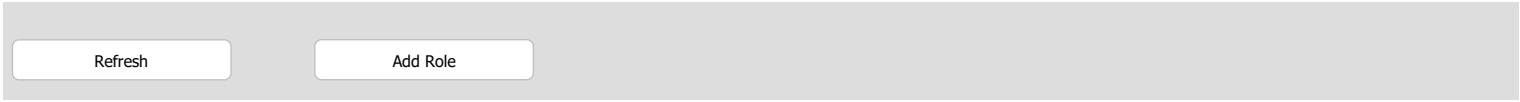
La fonctionnalité *CyberProtect* permet une gestion avancée des utilisateurs avec des rôles définis par l'utilisateur. Autrement, les rôles des utilisateurs sont définis par la norme IEC 62351-8 comme expliqué ci-dessus.
Notez les deux caractéristiques suivantes :

- Dans la dernière colonne, tous les rôles ont un bouton "Edit" pour permettre une gestion personnalisée des droits. Voir tableau ci-dessous.
- D'autres rôles personnalisés peuvent être créés à l'aide du bouton "*Add Role*".

NOTE : Le rôle "*Emergency*" ne peut être configuré que lorsque CyberProtect est activé. En effet, la pertinence du rôle "*Emergency*" n'entre en jeu que lorsque LDAP (une sous-fonctionnalité de *CyberProtect*) est activée.

Attributions prédéfinies des rôles et des droits avec la fonction CyberProtect

Rôle	Type	View data	View settings	Manage settings	Control	Manage configuration	Update firmware	Manage users	Audit	Log	Edit
Guest	Guest	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Edit
Emergency	Emergency	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Edit
Full access		Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Web, Lcd	Edit
Viewer		Web, Lcd									Edit
Operator		Web, Lcd	Web, Lcd								Edit
Engineer		Web, Lcd	Web, Lcd	Web, Lcd		Web, Lcd					Edit
Installer		Web, Lcd	Web, Lcd	Web, Lcd		Web, Lcd	Web, Lcd				Edit
SECADM		Web, Lcd	Web, Lcd	Web, Lcd				Web, Lcd			Edit
SECAUD		Web, Lcd	Web, Lcd	Web, Lcd					Web, Lcd		Edit
RBACMNT		Web, Lcd						Web, Lcd			Edit



NOTE : Les rôles "*Guest*" et "*Emergency*" ne peuvent pas être supprimés. Seul le nom du rôle peut être modifié. Les colonnes "*Type*" du tableau ci-dessus indiquent le nom original de ces rôles non effaçables.

Les droits définis en usine sont présentés dans le tableau ci-dessous :

Définition des droits

TITRE DES DROITS	EXPLICATION
View data	Visualiser les données opérationnelles de l'équipement (tension, courant, puissance, énergie, état, alarmes ...) qui ne sont pas destinées à être disponibles en tant qu'affichage d'informations générales.
View settings	Visualiser les paramètres de configuration de l'équipement, tels que la mise à l'échelle, l'adressage des communications, les routines logiques programmables et les numéros de version du micrologiciel.
Manage settings	Gestion des paramètres de réglage
Control	Accès à la manipulation d'objets contrôlables
Manage configuration	Téléchargement et chargement de fichiers de configuration dans l'IED
Update firmware	Mise à jour du firmware (micrologiciel)
Manage users	Création, suppression ou modification d'identifiants d'utilisateurs, de mots de passe, de rôles et/ou d'autorisations de rôles et configuration de l'accès LDAP
Audit	Visualisation et téléchargement de la trace d'audit
Log	Accès au menu Status/log

Gestion des rôles

Les conditions suivantes doivent être remplies pour pouvoir gérer les rôles :

- Le droit utilisateur "*Manage users*" doit être attribué à l'utilisateur.

Ajouter un nouveau rôle

Pour ajouter un nouveau rôle :

1. Dans le menu **Security** > **User manager**, onglet **Role**, sélectionnez le bouton "Ajouter un rôle".
2. Dans la fenêtre contextuelle "*Add role*", définissez les éléments suivants :
   - Rôle : désignation du rôle.
   - Groupe LDAP : définition du groupe LDAP appliqué lors de l'utilisation de l'authentification utilisateur LDAP.
   - Permissions : sélection des droits appliqués au nouveau rôle. Ici, les permissions pour l'accès web et l'accès local au LCD peuvent être sélectionnées séparément.
3. Cliquez sur le bouton "*Add role*" pour ajouter le rôle au réseau ou sur le bouton "*Cancel*" pour annuler la procédure d'ajout d'un nouveau rôle.

Modifier le rôle

Pour modifier un rôle existant :

1. Le rôle existant peut être modifié en cliquant sur le bouton "*Edit*" dans l'entité de rôle sélectionnée.
2. Dans la fenêtre contextuelle "*Edit role*" :
   - Le nom du rôle peut être modifié.
   - Le groupe LDAP peut être modifié.
   - L'attribution des droits peut être modifiée.
3. Cliquez sur le bouton "*Save*" pour sauvegarder la modification du rôle, sur le bouton "*Cancel*" pour annuler la modification, sur le bouton "*Reset*" pour rétablir les valeurs d'origine ou sur le bouton "*Remove role*" pour supprimer le rôle de la liste des rôles.

Gestion des utilisateurs

Le menu "*User manager*" permet de modifier les profils utilisateurs de l'équipement sélectionné. Il est possible de créer de nouveaux utilisateurs, de supprimer des utilisateurs existants et de modifier les membres de différents groupes d'utilisateurs. Les conditions préalables suivantes sont requises pour ajouter des comptes d'utilisateurs au système de gestion de la sécurité des utilisateurs :

- Le droit d'utilisateur "*Manage users*" doit être attribué à l'utilisateur.

REMARQUE : L'appareil est initialement configuré avec un utilisateur "*admin*" auquel est attribué le rôle "*Full Access*". Le mot de passe "*admin*" par défaut : C1b3rS3c!

Il est important de supprimer l'utilisateur "*admin*" ou de modifier le mot de passe par défaut "*admin*" après la mise en place de la sécurité du réseau.

Ajouter un nouvel utilisateur

Pour ajouter un compte d'utilisateur :

1. Dans l'onglet **Security** > **User manager** > **Users**, sélectionnez le bouton "*Add user*".
2. Dans la fenêtre contextuelle "*Add user*", définissez les éléments suivants :
   - Nom d'utilisateur :
   - Rôle : sélectionnez le rôle requis dans la liste Rôles. Les rôles définis sont visibles sous l'onglet **Users.**
   - Mot de passe : pour plus de détails sur les exigences en matière de mot de passe,
   - Confirmer le mot de passe
3. Cliquez sur le bouton "*Add user*" pour ajouter le compte d'utilisateur au réseau ou sur le bouton "*Cancel*" pour annuler la procédure d'ajout d'un nouvel utilisateur.

Modifier l'utilisateur

Pour modifier un utilisateur existant :

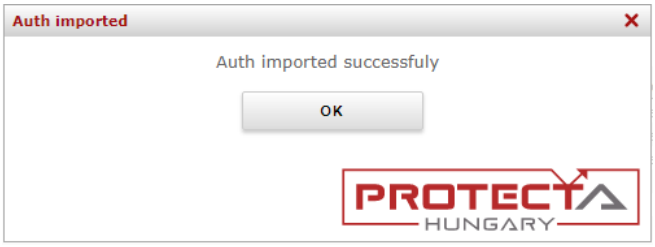
1. L'utilisateur existant peut être modifié en cliquant sur le bouton "*Edit*" dans l'entité utilisateur sélectionnée.
2. Dans la fenêtre contextuelle "*Edit user*" :
   - Le nom d'utilisateur peut être modifié.
   - L'attribution des rôles peut être modifiée. Les rôles définis sont visibles sous l'onglet **Role** .
3. Cliquez sur le bouton "Enregistrer" pour sauvegarder la modification du compte d'utilisateur, sur le bouton "Annuler" pour annuler la modification, sur le bouton "Réinitialiser" pour rétablir les valeurs initiales des champs ou sur le bouton "Supprimer l'utilisateur" pour supprimer l'utilisateur de la liste des utilisateurs.

NOTE : Toute modification de l'utilisateur actif n'entre en vigueur qu'après une nouvelle session de connexion.

Importer / Exporter des utilisateurs

Dans l'onglet **Security** > **User manager** > **Import / Export**, les utilisateurs peuvent être importés ou exportés vers un autre IED.
Pour ajouter des utilisateurs d'un autre IED :

1. Cliquez sur le bouton "*Import*".
2. Dans la fenêtre contextuelle de l'explorateur, sélectionnez le fichier *pgf* exporté de l'autre IED.
3. Si l'importation est réussie, la fenêtre contextuelle suivante s'affiche :



Pop-up montrant une importation réussie d'utilisateurs à partir d'un fichier pgf

4. Dans l'onglet **User**, les utilisateurs nouvellement ajoutés apparaissent.

Pour exporter un fichier *pgf* depuis l'IED :

1. Cliquez sur le bouton "*Export*".
2. Le fichier *pgf* est sauvegardé sur le PC, après quoi il peut être utilisé dans un autre IED.

Exigence d'un mot de passe

L'appareil permet la saisie de mots de passe à partir d'une connexion locale ou à distance. Les mots de passe créés par l'utilisateur suivent un ensemble de règles qui doivent être respectées lors de la création de chaque mot de passe.
Un minimum de huit (8) caractères doit être utilisé et le mot de passe doit être sensible à la casse. Les caractères du mot de passe doivent contenir les éléments suivants :

- Au moins une lettre majuscule et une lettre minuscule
- Au moins un chiffre
- Au moins un caractère non alphanumérique (par exemple, @, %, &, *, etc.)

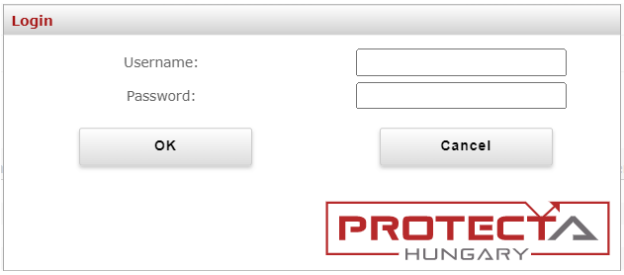
Toute tentative de création d'un mot de passe qui enfreint ces règles sera détectée au moment de la tentative de création, et l'utilisateur en sera informé et invité à choisir un autre mot de passe conforme aux règles.

Connexion de l'utilisateur

Pour se connecter à l'interface web :

1. Cliquez sur le menu **Login**
2. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter

REMARQUE : La fenêtre contextuelle "*Login*" apparaît sur en accédant à l'appareil, si tous les droits pour le rôle d'invité sont désactivés. Le rôle d'invité est désactivé.



"Fenêtre contextuelle "Login

Traitement des sessions

Les propriétés de gestion des sessions Web et LCD se trouvent dans le menu **Security** > **User manager** , onglet "**Session Handling**".

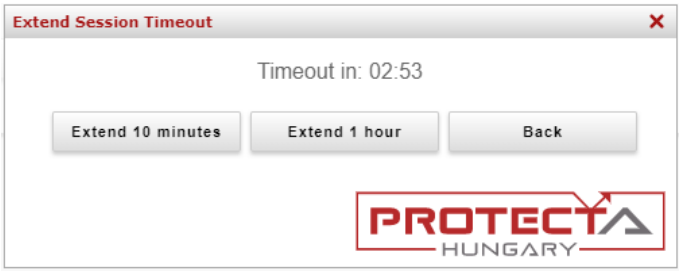
Propriétés de l'onglet “Gestion des sessions”

TITRE	WEB/LCD	EXPLICATION
Number of login attempts	WEB&LCD	Nombre maximum de tentatives de connexion infructueuses autorisées à la fois.
Lock time	WEB&LCD	Après le nombre maximum de tentatives de connexion infructueuses effectuées à un moment donné , l'utilisateur sera bloqué pendant une période définie ici.
Default timeout for session	WEB&LCD	Le compteur de temps d'attente démarre à partir de cette valeur après l'ouverture d'une session ou toute autre activité de l'utilisateur.
Maximum timeout for session	WEB&LCD	Valeur maximale jusqu'à laquelle le délai d'attente peut être prolongé au cours d'une session
Maximum number of sessions	WEB&LCD	Maximum nombre de connexions autorisées à l'appareil (sessions de connexion) à la fois
Maximum number of users	WEB&LCD	Nombre maximal d'utilisateurs autorisés à se connecter à l'appareil à la fois

Le temps restant de la session est indiqué dans la barre de menu de gauche.

Pour prolonger la session :

1. Cliquez sur "*User/Role*" dans la barre de menu.
2. Prolongez la durée de la session active dans la fenêtre contextuelle "Extension Session Timeout". *REMARQUE* : la durée maximale de la session ne peut pas dépasser le paramètre "*Maximum timeout for session*".

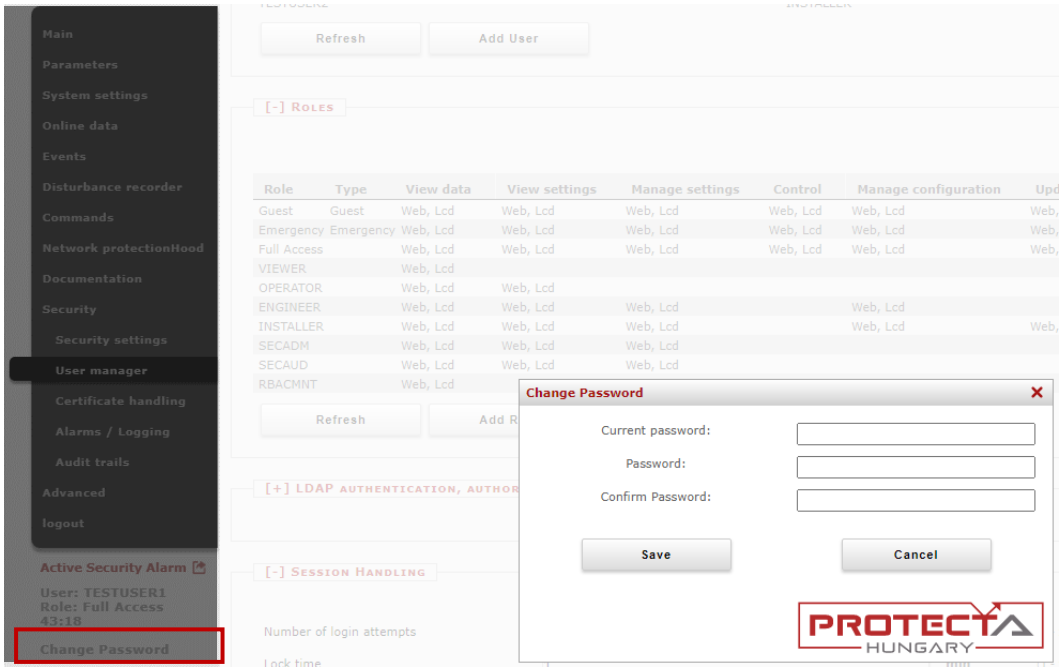


"Fenêtre contextuelle "Extension Session Timeout

REMARQUE : L'accès revient automatiquement au niveau invité en fonction des valeurs du délai d'attente du niveau d'accès.

Gestion du mot de passe

Pour changer le mot de passe, l'utilisateur actif doit cliquer sur la section "*Change password*" dans la barre de menu de gauche.



Section "Modifier le mot de passe" et fenêtre contextuelle "Modifier le mot de passe".

REMARQUE : le mot de passe de l'utilisateur authentifié par LDAP ne peut pas être modifié !

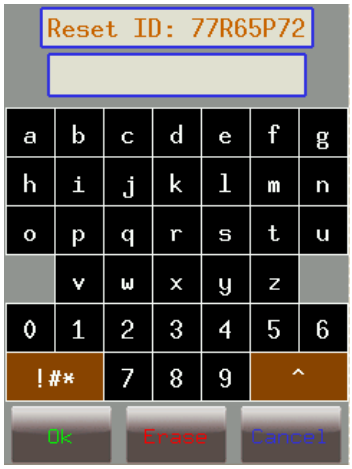
Mot de passe perdu

En cas de perte d'un mot de passe principal avec le menu "*Manage users*", il est possible de le récupérer en réinitialisant l'unité aux valeurs par défaut et en rétablissant l'attribution des droits de rôle par défaut.

REMARQUE : A Tous les paramètres des relais seront réinitialisés aux valeurs d'usine à la du processus de réinitialisation des mots de passe, et pas seulement les mots de passe !

Pour rétablir la configuration par défaut de l'attribution des droits et des rôles :

1. Appuyez sur le bouton "*O*' accessible à l'avant de la protection six fois en l'espace de 10 secondes lorsque l'écran LCD principal est actif. L'identifiant de réinitialisation apparaît en haut de l'écran LCD.
2. Créez un ticket d'assistance sur le site internet MICROENER en indiquant le numéro de série de l'appareil et le code de réinitialisation affiché . Le support client MICROENER fournira en retour un code de réinitialisation permettant de rétablir les paramètres d'usine du relais.
3. Répétez l'étape no . 1 et entrez le mot de passe de réinitialisation reçu.
4. Le processus de réinitialisation dure environ 8 secondes. Sur l'écran, une boîte de dialogue s'affiche : "*Factory default in 8 seconds* !". Appuyez sur "Ok". L'appareil redémarre automatiquement et rétablit les paramètres d'usine par défaut.



Fenêtre de réinitialisation du mot de passe sur l'écran LCD

Authentification du serveur (serveur LDAP)

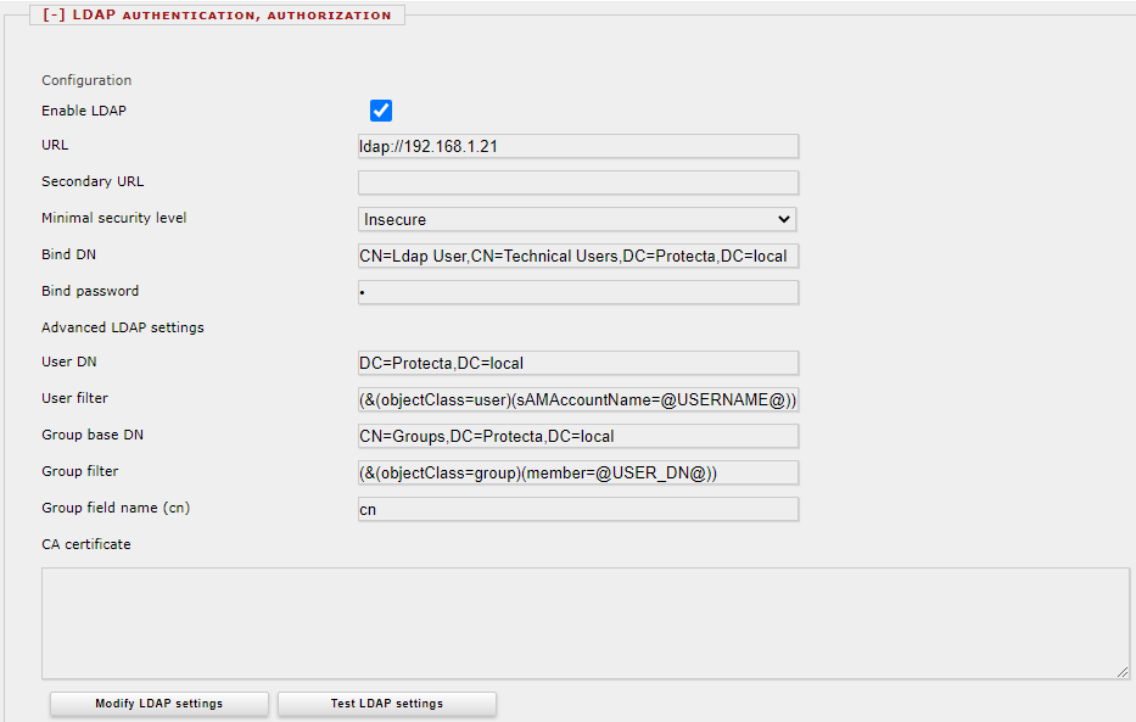
Les conditions suivantes doivent être remplies pour configurer l'authentification du serveur :

- Le droit utilisateur "Manage users" doit être attribué à l'utilisateur.

Le relais prend en charge le protocole LDAP (Lightweight Directory Access Protocol) pour permettre les fonctions d'authentification et d'autorisation pour le serveur Authentication Authorization Accounting (AAA).

NOTE : L'authentification par serveur LDAP n'est disponible que lorsque la fonctionnalité optionnelle CyberProtect est activée. Dans le cas contraire, seule l'authentification locale est possible.

Tous les paramètres pertinents pour la configuration de LDAP sont rassemblés dans le menu **Security** > **User manager,** onglet **LDAP authentication, authorization**.
Si le serveur LDAP préconfiguré n'est pas disponible, il est possible d'accéder à l'appareil avec des droits d'utilisateur d'urgence.



Onglet LDAP montrant un exemple de configuration LDAP

"Propriétés de l'onglet "Authentification et autorisation LDAP

TITRE DU PARAMÈTRE	EXPLICATION
Enable LDAP	Activer l'authentification et l'autorisation LDAP
URL	Adresse ou nom du serveur sur lequel LDAP est hébergé.
Secondary URL	Adresse ou nom du serveur LDAP de sauvegarde
Minimal security level	Activation/désactivation de TLS sur LDAP. Les options sont les suivantes : *Insecure, TLS/SSL - No CERT Check, TLS/SSL*
Bind DN	DN utilisé pour une connexion protégée par un mot de passe (ignorée en 'Bind passw ord' est vide)
Bind password	Mot de passe utilisé pour se connecter au serveur (vide signifie que le serveur n'est pas protégé par un mot de passe)
Advanced LDAP settings	
User DN	DN de base pour la recherche des utilisateurs
User filter	Expression de filtre utilisée pour la recherche de l'utilisateur ('@USERNAME@' sera remplacé par le nom d'utilisateur saisi)
Group base DN	DN de base pour la recherche de groupe
Group filter	Expression de filtre utilisée pour la recherche de groupe '@USER_DN@' sera remplacé par le DN renvoyé par la recherche d'utilisateur)
Group field name (cn)	Nom du champ contenant le nom du groupe
CA certificate	Certificat CA du serveur au format PEM

Pour configurer la connexion LDAP et l'authentification des utilisateurs enregistrés :

1. Remplissez l'onglet **LDAP authentication, authorization** ci-dessus avec les données pertinentes obtenues auprès de votre administrateur réseau et cliquez sur le bouton "*Modify LDAP settings*".
2. Sous l'onglet **Roles** , une nouvelle colonne "*LDAP Group*" apparaît après actualisation de la page web.
3. Sélectionnez le rôle souhaité pour l'authentification LDAP et remplissez le champ "*LDAP Group*" avec l'ID de groupe approprié obtenu auprès de votre administrateur réseau.

Role	Type	LDAP Group	View data	View settings
Guest	Guest		Web, Lcd	Web, Lcd
Emergency	Emergency		Web, Lcd	Web, Lcd
Full Access			Web, Lcd	Web, Lcd
VIEWER			Web, Lcd	
OPERATOR			Web, Lcd	Web, Lcd
ENGINEER			Web, Lcd	Web, Lcd
INSTALLER		AddressBook	Web, Lcd	Web, Lcd

Exemple de définition d'un groupe Role-LDAP

Définition de l'utilisateur d'urgence :
Le rôle d'utilisateur d'urgence peut être utilisé pour accéder à l'appareil lorsque LDAP est activé mais que les serveurs LDAP configurés par ne sont pas disponibles.

Pour tester la connexion LDAP et l'authentification des utilisateurs enregistrés :

4. Cliquez sur le bouton "*Test LDAP settings*" dans l'onglet **LDAP authentication, authorization** pour tester la connexion LDAP et l'authentification et l'autorisation.
5. Saisissez le nom d'utilisateur et le mot de passe pour la connexion au serveur LDAP et cliquez sur le bouton "*OK*".
6. La fenêtre contextuelle "*LDAP test result*" affiche le résultat réel de la connexion au serveur LDAP et le résultat de la procédure d'authentification et d'autorisation.

Exemple de résultat pour "Test des paramètres LDAP" :
Tue Jun 28 07:40:55 2022 : Starting RESOLVE test with username 'zsarnaisz'...
Tue Jun 28 07:40:55 2022 : ---
Tue Jun 28 07:40:55 2022 : SECURITY WARNING : Using insecure connection
Tue Jun 28 07:40:55 2022 : Connecting to to to ldap://192.168.1.21...
Tue Jun 28 07:40:55 2022 : Setting LDAPv3 client version...
Tue Jun 28 07:40:55 2022 : Setting timeouts to 2 second(s)...
Tue Jun 28 07:40:55 2022 : Connexion avec authentification
simple...
Tue Jun 28 07:40:55 2022 : LDAP connection successful
Tue Jun 28 07:40:55 2022 : ---
Tue Jun 28 07:40:55 2022 : Lookup user - base :
DC=Protecta,DC=local filter : (&(objectClass=user)(sAMAccountName=zsarnaisz))
Tue Jun 28 07:40:55 2022 : User found ! dn is : CN=Zsarnai Szabolcs,OU=Users,OU=Application,DC=Protecta,DC=local
Tue Jun 28 07:40:55 2022 : ---
Tue Jun 28 07:40:55 2022 : Lookup group - base :
CN=Groups,DC=Protecta,DC=local filter : (&(objectClass=group)(member=CN=Zsarnai
Szabolcs,OU=Users,OU=Application,DC=Protecta,DC=local))
Tue Jun 28 07:40:55 2022 : Checking group CN=GitLab-Users,CN=Groups,DC=Protecta,DC=local
Tue Jun 28 07 :40:55 2022 : Member of 'GitLab-Users'
Tue Jun 28 07:40:55 2022 : Checking group CN=AddressBook,CN=Groups,DC=Protecta,DC=local
Tue Jun 28 07:40:55 2022 : Member of 'AddressBook'
Tue Jun 28 07:40:55 2022 : Found LDAP 2 group(s)

Resolved to role : Accès complet

Les conditions préalables suivantes sont requises pour mettre en place le service de journalisation :

- Les droits d'utilisateur "View settings, Manage settings" doivent être attribués à l'utilisateur.

Le relais peut utiliser un System Logging Protocol (Syslog) pour communiquer avec un serveur de journalisation (serveur syslog). Syslog server est spécialement conçu pour faciliter la surveillance des périphériques sur le réseau. Un Syslog server peut être un serveur physique, une machine virtuelle autonome ou un service logiciel.

Les paramètres pertinents pour la configuration de syslog se trouvent dans le menu **Security** > **Security parameters** > **System services.** Il est possible d'activer jusqu'à deux serveurs Syslog à l'aide des paramètres "server1" et "server2".

Paramètres de configuration de syslog

TITRE	EXPLICATION
Remote logging	Activation du protocole du serveur syslog.
Log server1 IP address	L'adresse IP du serveur syslog1 peut être définie ici.
Log server1 UDP port	Les messages Syslog sont envoyés via le protocole UDP (User Datagram Protocol), le numéro de port par défaut étant 514.
Log server2 IP address	L'adresse IP du serveur syslog2 peut être définie ici.
Log server2 UDP port	Les messages Syslog sont envoyés via le protocole UDP (User Datagram Protocol), le numéro de port par défaut étant 514.

Propriétés des messages Syslog : facilité, gravité et priorité

Le fichier de configuration du récepteur Syslog traite les messages principalement en fonction de l'évènement signification et de leur gravité. Cependant, lorsque le message Syslog est généré, il est envoyé avec une valeur de priorité qui a été calculée à partir de la facilité et de la gravité plutôt que des propriétés individuelles.

La facilité et la gravité peuvent être définies dans le menu **Security** > **Alarms / Logging** sous l'onglet **Syslog level settings.**
Chaque évènement et chaque niveau de gravité ont un nom et une valeur numérique.

Le tableau suivant répertorie les valeurs numériques, les noms et les abréviations couramment utilisés dans les fichiers de configuration syslog :

Liste d'évènements

CODE NUMÉRIQUE	ÉVÉNEMENT	TITRE
0	messages du noyau	Kernel
1	messages au niveau de l'utilisateur	User
2	réseau de messagerie	Mail
3	les démons du réseau	Daemon
4	messages de sécurité/autorisation	Auth
5	messages générés en interne par syslogd	Syslog
6	sous-système d'impression de ligne	Lpr
7	sous-système d'information en réseau	News
8	Sous-système UUCP	Uucp
9	horloge	Cron
10	messages de sécurité/autorisation	Authpriv
11	Démon FTP	Ftp

Les degrés de gravité vont de 0 (urgence) à 7 (débogage) :

Liste d'importance

CODE NUMÉRIQUE	SÉVÉRITÉ	TITRE
0	Urgence : le réseau est inutilisable	Urgence
1	Alerte : des mesures doivent être prises immédiatement	Alerte
2	Critique : conditions critiques	Critique
3	Erreur : conditions d'erreur	Erreur
4	Avertissement : conditions d'avertissement	Avertissement
5	Avis : état normal mais significatif	Avis
6	Informatif : messages d'information	Info
7	Debug : messages de niveau débogage	Débogage

La priorité est calculée comme suit :
Priorité = Facilité * 8 + Importance (niveau de gravité)

Traces d'audit

La fonction "Trace"sd'audit" peut stocker au moins 2048 événements avant que la mémoire tampon circulaire ne commence à remplacer l'événement le plus ancien par le dernier événement . Il n'est pas possible d'effacer ou de modifier la "Traces d'audit". Il n'est pas possible de retirer le support de stockage de la Trace d'audit sans endommager de façon permanente l'EEI au-delà de la capacité de réparation sur le terrain.
En outre, les opérations relatives à la sécurité, telles que les échecs de connexion, les changements de mot de passe, etc. sont enregistrées et ne peuvent pas être supprimées dans l'appareil. La structure de la "Traces d'audit" et les messages enregistrés sont conformes à la norme IEEE 1686.
Les entrées de la piste d'audit se trouvent dans le menu **Security** > **Audit trails.**
Les conditions préalables suivantes sont requises pour ajouter/modifier le rôle d'un utilisateur :

- Le droit d'utilisateur "Audit" doit être attribué à l'utilisateur

Chaque événement de la piste d'audit comprend les paramètres suivants :

- Numéro d'enregistrement de l'événement - ID de l'événement : Numéro séquentiel généré automatiquement pour l'événement.
- Facilité et gravité en fonction de l'onglet **Syslog level settings**.
- Heure et date : l'heure et la date de l'événement, y compris l'année, le mois, le jour, l'heure, la minute et la seconde.
- Utilisateur : l'identifiant de l'utilisateur connecté à l'équipement au moment de l'événement.
- Source : adresse IP du client distant qui demande l'événement dédié.
- Destination : IP de l'appareil
- Activité : plusieurs activités sont à l'origine d'une entrée dans l'enregistrement de la piste d'audit. Elles sont classées en fonction du ci-dessous.

Détails : informations détaillées relatives à l'entrée.

Catégories d'activités

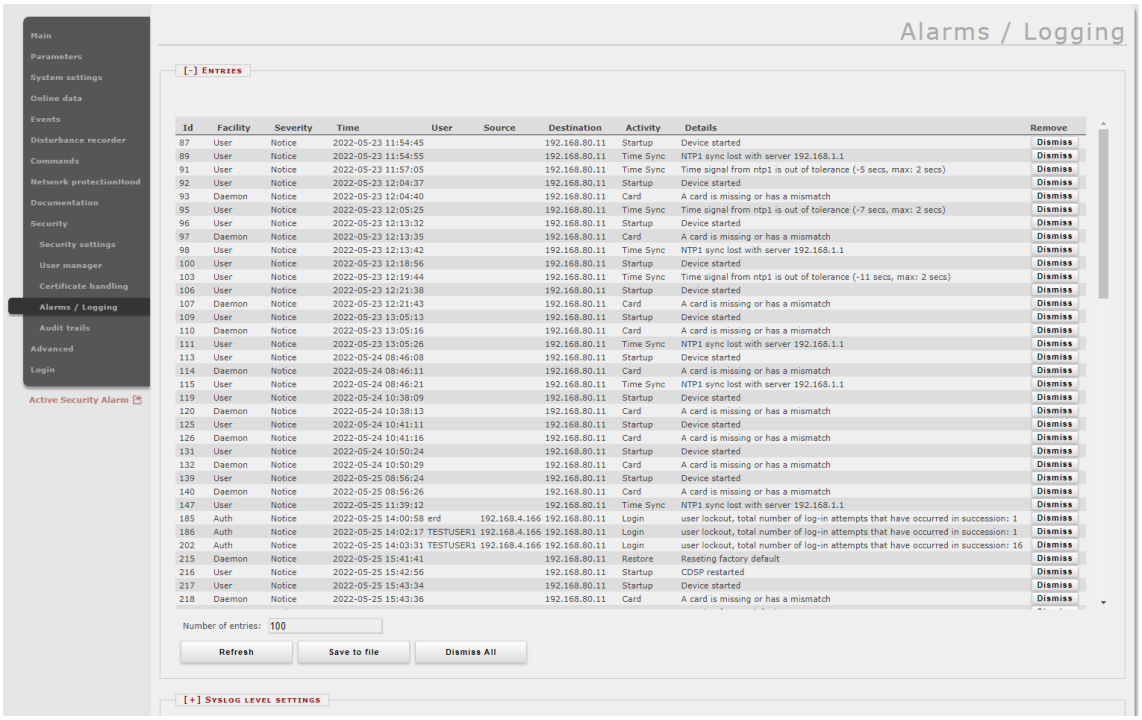
TITRE	EXPLICATION
Login	Résultat d'une tentative de connexion locale ou à distance (succès/échec)
Logout	Déconnexion initiée par l'utilisateur ou automatique (en raison de l'expiration du temps de session).
Upload	Téléchargement de fichiers
Settings	Paramètres modifiés
Parameters	Paramètres modifiés
Options	Options modifiées
User Manager	Ajouter / supprimer / modifier des utilisateurs ou changer le mot de passe d'un utilisateur
Role Manager	Ajouter / supprimer / modifier des rôles
Pfw Upload	Résultat d'un téléchargement de pfw (succès/erreur)
Psp Upload	Résultat d'un téléchargement PSP (succès/erreur)
Epcs Upload	Résultat d'un téléchargement epcs (succès/erreur)
Restore	Résultat d'un processus de restauration (succès/erreur)
Command	Résultat d'une commande adressée à l'appareil à partir de la page web
Download	Résultat du téléchargement d'un fichier par un client à partir de l'appareil
Audit	Résultat du téléchargement ou de la visualisation des entrées d'audit/d'alarme à partir de la page web
Time Sync	Résultat d'un événement lié à la synchronisation temporelle
Startup	Device starting
Card	Différence entre la carte/module configurée et la carte/module installée
IO Simulator	Les entrées de simulation d'entrées/sorties binaires sont enregistrées via cette balise.
Nameplate	Résultat des événements liés à la plaque signalétique, tels que la suppression, etc.

Alarmes

Les alarmes sont définies comme des activités qui peuvent indiquer une activité non autorisée. Les entrées du menu des alarmes sont un sous-ensemble des événements de la "Trace d'audit". Alors que ces dernières ne peuvent pas être supprimées, les entrées d'alarme peuvent être supprimées/effacées en cliquant sur "*Dismiss*". Les événements d'alarme suivants sont enregistrés :

User locked out
Les utilisateurs peuvent se bloquer eux-mêmes lorsque des tentatives de saisie de mot de passe incorrect sont effectuées successivement au cours d'une session de connexion de l'utilisateur - les paramètres correspondants sont présentés dans ce document
Attempted use of unauthorized configuration file or firmware
La détection par l'IED d'une tentative d'utilisation d'un fichier de configuration ou d'un micrologiciel, d'un ordinateur d'accès ou d'une combinaison de ceux-ci qui n'est pas enregistré comme pouvant être légitimement utilisé pour la configuration de l'IED.
Device start or restart
Tous les cas de démarrage ou de redémarrage de l'appareil seront enregistrés dans cette entrée.
Time sync signal loss
Les événements de synchronisation du temps tels que la perte de la connexion NTP, le signal de temps hors tolérance, etc. seront enregistrés dans la liste des alarmes.
Missing I/O module
Ce type d'alarme est déclenché en cas de non-concordance entre les cartes configurées et les cartes détectées dans l'appareil.

L'activité de l'alarme de sécurité indique un message d'alarme de sécurité sur le web. Le message "*Active Security Alarm*" apparaît dans la barre de menu de gauche. En cliquant sur le message, l'utilisateur est dirigé (lorsque le niveau d'accès lui permet de voir les messages d'alarme) vers l'onglet **Security > Alarm /Logging** onglet **Entries**.



Le menu Alarmes/Enregistrements visualise les entrées d'alarmes.

Traitement des certificats

Les conditions préalables suivantes sont requises pour le traitement des certificats :

- Le droit utilisateur "*Manage settings*" doit être attribué à l'utilisateur.

Certificat HTTPS

HTTPS comprend une authentification via le protocole SSL/TLS. Le certificat SSL/TLS du relais comprend une clé publique, qu'un navigateur web peut utiliser, pour confirmer que les données envoyées par le serveur ont été signées numériquement par une personne en possession de la clé privée correspondante.
Par défaut, le certificat du serveur est un certificat auto-signé, fourni par le relais et généré par l'appareil lui-même, et non émis par une autorité de certification (CA).

REMARQUE : un certificat auto-signé crypte les communications entre votre serveur et tous les clients. Cependant, comme il n'est pas signé par l'une des autorités de certification de confiance incluses dans les navigateurs web, les utilisateurs ne peuvent pas utiliser le certificat pour valider automatiquement l'identité de votre serveur.

Il est possible de télécharger le certificat d'un serveur, qui a été signé par une autorité de certification (AC) publiquement reconnue. Par conséquent, le navigateur peut accepter que toute information d'identification incluse dans le certificat ait été validée par un tiers de confiance.
Le certificat peut être téléchargé sous l'onglet **Security** > **Certificate handling** > onglet **HTTPS Certificate**

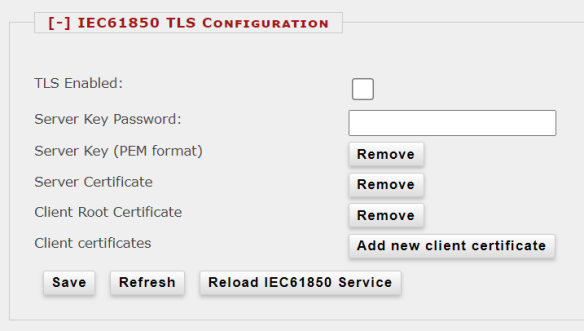
Fenêtre de gestion des certificats HTTPS

IEC 61-850 TLS Configuration

La communication IEC 61-850 peut être sécurisée à l'aide de TLS. Les vulnérabilités de la communication IEC 61-850 peuvent être résolues en activant TLS et en téléchargeant les certificats requis. Le tableau ci-dessous indique les paramètres TLS relatifs à la norme IEC 61-850. Deux paramètres peuvent être définis et les certificats peuvent être téléchargés. Ces paramètres se trouvent sous l'onglet **Security** > **Certificate handling** > **IEC 61850 TLS Configuration**.

IEC 61850 TLS Paramètres de configuration

TITRE	EXPLICATION
TLS Enabled	Activation/désactivation de la norme IEC 61850 TLS
Server key password	Mot de passe pour la clé privée du serveur
Server key (PEM format)	Téléchargement/suppression de la clé privée du serveur, nécessaire au fonctionnement
Server Certificate	Télécharger/supprimer le certificat du serveur, requis pour le fonctionnement
Client Root Certificate	Téléchargement/suppression du certificat racine pour les clients, facultatif
Client certificates	Télécharger/supprimer les certificats individuels des clients. S'il y en a, seuls les clients qui les possèdent peuvent s'inscrire

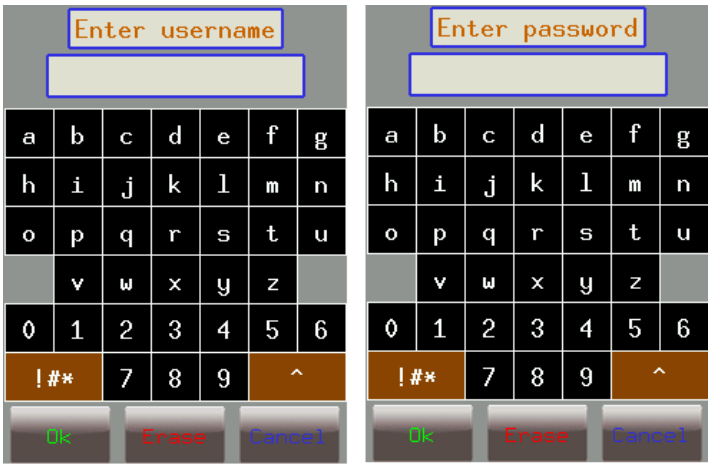


Onglet des paramètres IEC 61850 sur la page web

Utilisation de l'IHM locale

Gestion des utilisateurs

Pour se connecter à l'IHM locale, l'utilisateur doit toucher l'icône  sur l'écran principal. Lorsque la fenêtre de connexion apparaît, le nom d'utilisateur et le mot de passe doivent être saisis l'un après l'autre.

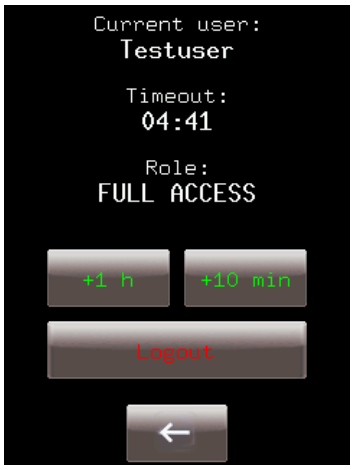


Authentification de l'utilisateur sur l'IHM locale

La session IHM locale peut être gérée dans la fenêtre suivante en fonction des paramètres de gestion de la session locale LCD.

Pour accéder à la fenêtre de gestion de la session IHM locale, appuyez sur l'icône  .

Dans la fenêtre de gestion de la session, l'utilisateur peut prolonger le délai d'expiration de la session de l'IHM locale (Timeout) et se déconnecter (Log out). Le symbole de la "flèche de retour" permet à l'utilisateur de revenir à l'écran principal.



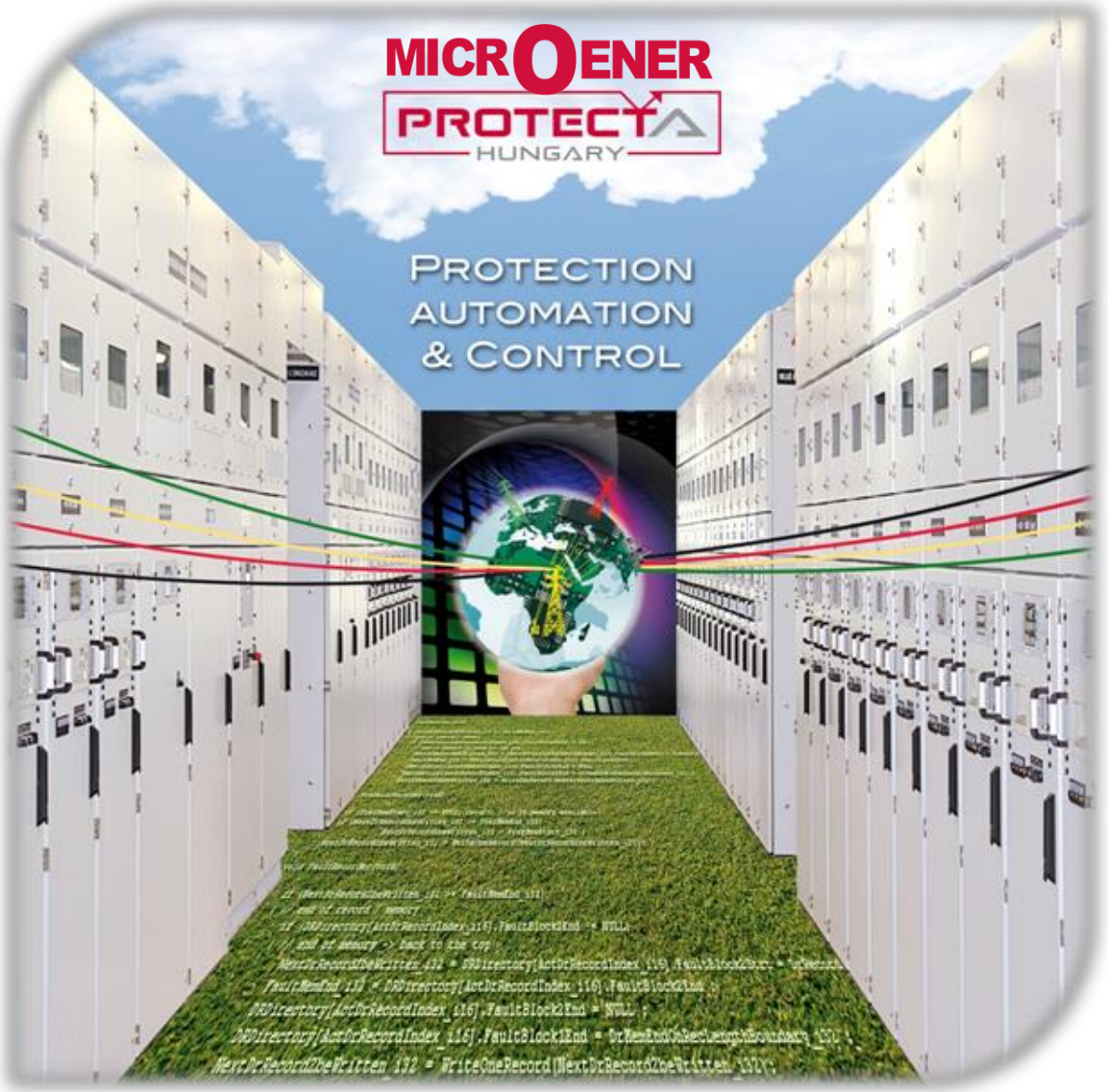
Gestion de la session locale de l'écran LCD

Paramètres de sécurité

Les paramètres de sécurité, similaires à ceux de l'interface web, sont accessibles à partir de l'écran LCD.

Écran des paramètres de sécurité à partir de l'écran LCD

Les paramètres figurant sous les trois menus sont les mêmes que ceux de l'interface web.


MICROENER
PROTECTA
HUNGARY
PROTECTION
AUTOMATION
& CONTROL

MICROENER 49 rue de l'Université - 93160 Noisy le Grand – Tél : +33 1 48 15 09 01 – Fax : +33 1 43 05 08 24
info@microener.com – www.microener.com