



Link.net

Contrôle d'accès

Gestion du temps de présence

Gestion d'évacuation d'urgence

Gestion de visiteurs

Gestion de biens

**Manuel d'opération de l'utilisateur et guide d'installation
technique**



Ouverture de session	5
Menu principale	5
Afficheur d'événements	5
Afficheur de mise à jour directe du personnel	6
Afficheur d'alarmes	6
Afficheur de pistage	6
Afficheur d'alarmes de biens	7
Afficheur de mise à jour directe des biens	7
Boîte de dialogue d'alarme de biens	7
Afficheur d'image	7
Touches de raccourci	8
Utilisateurs	9
Ajout d'un nouveau port de carte	9
Liste du personnel	10
Suppression d'un détenteur de carte	11
Planning	11
Modification d'un horaire de planning	11
Groupes de contrôle d'accès	12
Modification d'un groupe d'accès	12
Changement de nom d'un groupe d'accès	13
Attribution d'un horaire de planning aux capteurs de groupe	13
Jours fériés	14
Paramétrage des jours fériés	14
Édition des jours fériés	14
Ajout ou modification d'un bien	14
Registre des biens	14
Sortie/entrée de biens	15
Le client autonome de sortie de biens	14
Utilisation d'un poste de sortie à écran tactile	16
Rapports Link.net	16
Rapport des événements contenus en historique	16
Rapport par SQL	17
Exécution d'une requête de l'historique à partir des archives de la bibliothèque	17
Rapport de la période sur les lieux et de l'emplacement d'individus	18
Création d'une base de données dédiée à la période sur les lieux	19
Rapport d'emplacement	19
Rapport de biens disparus	21
Automatisation du rapport de biens perdus	21
Rapport d'inventaire de biens	21
Rapport des biens sortis	22
Rapport de l'historique des biens	22
Gestion des alarmes	22
Définition des types d'alarmes	23
Diffusion par courrier	23
Définition d'une session de courrier IP	23
Contenu du message	24
Gestion des données	24
Copie de la totalité du programme et fichiers de soutien	24
Compréhension de la structure de la base de données	24
Gestion du tableau d'événements principaux	25
Étape 1 – Création d'un archive de bibliothèque d'événements	25
Étape 2 – Purge des événements subsistants de la base de données	25
Étape 3 – Compression de la base de données d'événements	26
Zones	23
Création de zones	27
Définition d'une zone en tant que lieu sécurisé	28
Attribution de zones aux capteurs d'accès et de biens	28
Travail hors ligne	29
Mise à jour de contrôleurs avec les données hors lignes	29
Récupération d'événements hors ligne	30
Travail en ligne par l'utilisation de contrôleurs hors ligne choisis	30
Récupération d'événements à partir de contrôleurs hors ligne exclus	30

Fenêtre « Options »	31
Options de démarrage	31
Utilisation du signal sonore	31
Utilisation d'images graphique pour les alarmes	31
Importation d'un arrière plan graphique personnel	31
Positionnement des objets d'alarme	31
Options de capteur longue portée de contrôle d'accès	32
Options de liste d'appel	32
Sélection d'une imprimante à distance	32
Filtrage temporisé de contrôle d'accès (TACF)	33
Ignorer les ID de cartes inconnus	33
Options de la base de données	33
Fonctions avancées en échange de données	33
Exportation d'événements à accès accordés	33
Information sur le fichier d'exportation	35
Module VIP d'échange de données	35
Tableau d'importation VIPDATA	35
Tableau d'exportation EVENTDATA	36
Annexe A:	37
Matériel Link.net	37
Planification de l'installation	37
Produits de connectivité IP LAN/WAN	37
Travail hors ligne	37
Contrôleurs Link.net	38
Généralités	38
Caractéristiques de bloc d'alimentation intégré	39
Information d'installation	39
Installation d'un contrôleur d'accès Link (LT-20AC)	39
Capteurs de contrôle d'accès	39
Interface standard de capteur Horloge et Données Link (par défaut)	40
Capteur de proximité Link LT-100R	40
Lecteur à puce intelligente Mifare LT-8000	40
Lecteur à bande magnétique CDV DGLM/L Externe ou Interne	40
Lecteur d'accès à bande magnétique MR 4130 Interne	40
Lecteur d'accès à bande magnétique MR 51T2B Externe	40
Capteur longue portée d'étiquettes actives XTAG XT200A	41
Étiquettes actives XTAG	42
Interface de capteur 26 bits Wiegand de qualité industrielle (en option)	42
Capteurs de proximité CDV DGLI/W, DGLP/W & DGLP/TW	42
Lecteur biométrique d'empreinte digitale CDV DGID/W	42
Connexion de boutons de sortie, contacts de porte et entrées générales	43
Connexion de dispositifs de verrouillage	43
Grille d'arrêt de verrou	43
Test d'un contrôleur d'accès Link.net	44
Installation de verrouillage entre deux portes	44
Installation d'un contrôleur d'accès IP LAN (LT-20IP)	44
Connexion LAN	45
Réglage de contrôleur pour MAC	45
Utilitaire d'activation du réseau	45
Changement dynamique des réglages du contrôleur	46
Réglages du contrôleur de serveur IP Link.net	46
Installation d'un contrôleur d'accès Wavetrend (LT-20WAC)	48
Câble du lecteur	48
Opération appropriée du lecteur	49
Réglages du lecteur LRX-201	49
Installation d'un contrôleur de gestion de biens (LT-30AM2)	50
Connexions	50
Câble du lecteur	50
Opération appropriée du lecteur	51
Réglages du lecteur LRX-201	51
Création automatique d'adresses	52
Réglage de la surveillance rétroactive par contrôleur	52
Test du contrôleur de gestion de biens Link.net	52
Création d'adresse pour un contrôleur Link.net	52
Connexion à un ordinateur personnel	53
Réseau de contrôle d'accès par câblage à canal unique	53
Réseau de contrôle d'accès par câblage multi canal multiple	54
Connexion de réseau de contrôle d'accès par câblage et IP	54
Techniques de réseautage Link.net	55
Câble blindé ou UTP	55
Interface PC RS232 pour réseau	55

<u>Interface PC Amplicon, modèle 485HF9</u>	55
<u>Méthode de connexion 1 – Réseau alimenté par contrôleur 485HF9 (Recommandée)</u>	56
<u>Méthode de connexion 2 – Réseau alimenté localement 485HF9</u>	56
<u>Interconnexion des contrôleurs</u>	58
<u>Terminaison des lignes de réseau RS485</u>	58
<u>Utilisation d'un système de lecture comme lecteur d'entrée de badge</u>	58
<u>Installation d'une carte d'interface pour lecteur LT-RIB</u>	58
<u>Installation du logiciel Link.net</u>	58
<u>Première ouverture du logiciel</u>	59
<u>Installation du contrôleur Plug&Play</u>	58
<u>Installation manuelle du contrôleur</u>	59
<u>Modification des paramètres du contrôleur</u>	60
<u>Attribution d'une sortie locale de relais pour alarmes de biens</u>	61
<u>Choix du type d'interface globale en contrôle d'accès</u>	62

Ouverture de session

L'ouverture de session est utilisée pour activer le logiciel [Link.net](#) et identifier l'utilisateur pour vérifier ses droits pour modification, configuration du système et génération de renseignements à partir de l'historique. Consultez la référence sur l'attribution des droits des utilisateurs.

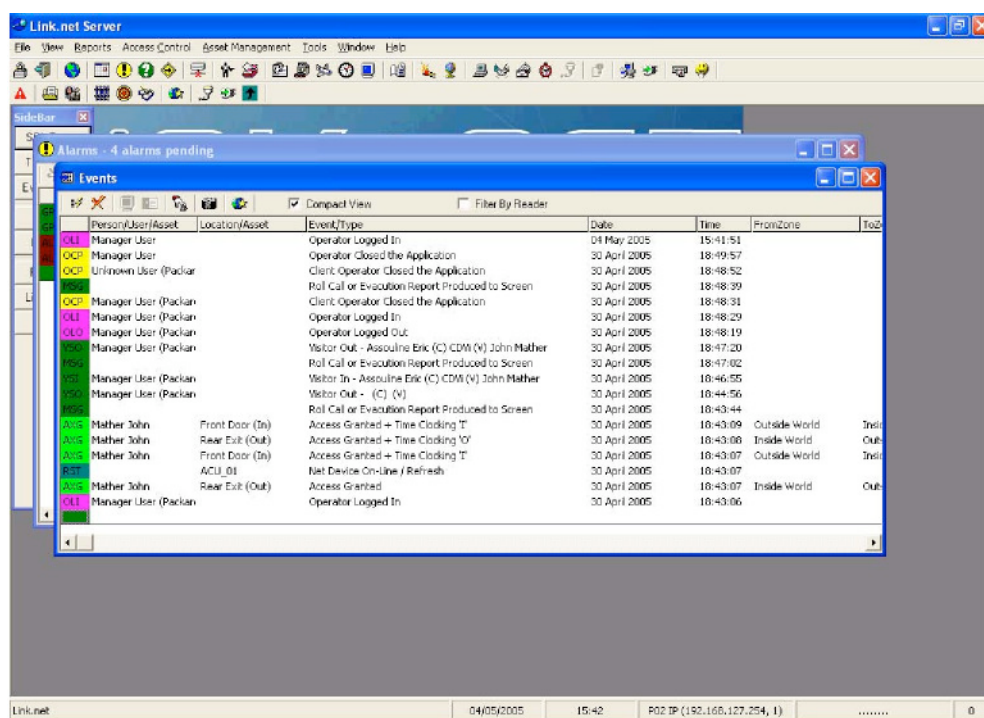


La boîte de dialogue illustrée à gauche s'affiche après le lancement du programme [Link.net](#) à partir du menu de démarrage Windows. Cette boîte permet à l'utilisateur de s'identifier en saisissant son nom dans le champ supérieur de la boîte et ensuite en inscrivant son mot de passe personnel. Assurez-vous que le mot de passe corresponde bien à celui choisi par l'utilisateur et selon la casse requise pour permettre l'ouverture de la session. Par défaut, le nom de l'utilisateur ainsi que le mot de passe sont « **Manager** ». Ceux-ci peuvent être modifiés ultérieurement. Un nombre illimité d'utilisateurs peut être inscrits.

À partir de l'option de préférence de langue, vous pouvez choisir votre langue de travail. Les langues standards incluent l'Anglais et le Français et d'autres langues s'ajouteront dans des versions à venir. Lorsque votre choix est fait, cliquez OK pour ouvrir votre session.

Menu principale

Le Menu principale permet à l'utilisateur (qui a les droits appropriés) de visualiser, modifier et générer des rapports à partir du Système de contrôle d'accès et gestion de biens [Link.net](#). Nous devons mentionner à ce point-ci que toutes les décisions d'ouverture de portes pour des détenteurs de badges de localisation précis ainsi que les fonctions d'alarmes sont exécutées par des zones de protections autonomes de portes et de biens. Le logiciel [Link.net](#) est un outil qui permet d'effectuer des changements et surveiller en temps réel les événements et les alarmes. De plus, Il est un composant important à la solution globale de sécurité et il est recommandé qu'il soit fonctionnel et contrôlé.



Vue du menu principale

Le menu principal inclut les menus déroulants traditionnels pour accéder à toutes les fonctions disponibles du logiciel [Link.net](#). Deux barres d'outils existent dans ce logiciel. Ils permettent un accès rapide aux fonctions les plus utilisées. Le menu supérieur est très utilisé pour le contrôle d'accès et celui du bas pour la gestion des biens (si installé). Au bas de l'écran des événements, vous trouvez la « barre d'état ». La « barre d'état » fournit les détails de l'état de la procédure en cours d'exécution et affiche aussi la date et l'heure actuelle.

Afficheur d'événements

L'afficheur d'événements est une fenêtre qui affiche les mille (1000) derniers événements qui ont eu lieu dans tout le système. Cet afficheur doit fonctionner en tout temps s'il y a nécessité de surveillance en temps réel.

The screenshot shows a Windows XP desktop environment. The taskbar at the top includes icons for Logon Tools, Internet Explorer, Outlook Express, Access Control, Asset Management, and a Start menu button. The Logon Tools application window is open, displaying a table titled "Records in the Viewed Database: 43". The table has columns for Event Name, Location Host, Event Type, Logon Date, Time, EndTime, and IDValue. It lists various logon events, including successful logons, failed logons, and logon attempts from different locations like "Asset Reader 1".

Event Name	Location Host	Event Type	Logon Date	Time	EndTime	IDValue
Manage User		Operator Logged In	17 August 2002	21:13:09		
Manage User		Operator Closed the Application	11 August 2002	18:24:57		
Manage User		Operator Logged In	11 August 2002	18:24:14		
Manage User		Operator Closed the Application	11 August 2002	18:13:04		
Manage User		Operator Logged In	10 August 2002	17:26:04		
Manage User		Operator Closed the Application	10 August 2002	22:17:39		
Manage User		Operator Logged In	10 August 2002	21:16:28		
Manage User		Operator Logged Out	10 August 2002	21:16:19		
Manage User		Operator Logged In	10 August 2002	21:15:45		
Manage User		Operator Logged Out	10 August 2002	21:15:43		
Manage User		Operator Logged In	10 August 2002	21:14:54		
Manage User		Operator Closed the Application	08 August 2002	22:25:20		
Manage User		Operator Logged In	08 August 2002	22:19:58		
Pack it Bell-Laptop	Asset Reader 1	Asset "ASLAPR" - TAMPER	08 August 2002	21:19:17	Retention	
Manage User		Operator Closed the Application	08 August 2002	21:19:16		
Pack it Bell-Laptop	Asset Reader 1	Asset "ASLAPR" - TAMPER	08 August 2002	21:19:16	Retention	
Manage User		Operator Closed the Application	08 August 2002	21:19:10		
Manage User		Operator Logged In	08 August 2002	21:18:44		
Pack it Bell-Laptop	Asset Reader 1	Asset "ASLAPR" - TAMPER	08 August 2002	21:17:36	Retention	
Manage User		Operator Closed the Application	08 August 2002	21:17:34		
Manage User		Operator Logged In	08 August 2002	21:17:06		
Manage User		Operator Closed the Application	08 August 2002	21:16:44		
Manage User		Operator Logged In	08 August 2002	21:16:42		
Manage User		Operator Closed the Application	08 August 2002	21:16:40		
Manage User		Operator Logged In	08 August 2002	21:14:59		
Manage User		Operator Closed the Application	08 August 2002	21:14:14		
Manage User		Operator Logged In	08 August 2002	21:14:05		
Manage User		Operator Closed the Application	08 August 2002	21:11:32		
Manage User		Operator Logged In	08 August 2002	21:10:31		
Pack it Bell-Laptop	Asset Reader 1	Asset "ASLAPR" - TAMPER	08 August 2002	21:09:16	Retention	
Manage User		Operator Closed the Application	08 August 2002	20:59:40		
Pack it Bell-Laptop	Asset Reader 1	Not Device On-Line	08 August 2002	20:25:21		
Manage User		Asset "ASLAPR" - TAMPER	08 August 2002	20:24:29	Retention	
Manage User		Operator Logged In	08 August 2002	20:14:22		

At the bottom left, there is a status bar showing "Status: Normal" and a date/time indicator "17/08/2002 21:27".

Events Viewer Window

Les événements qui suivent sont énumérés dans la fenêtre de l'afficheur d'événements :

- Activité du contrôle d'accès ainsi que les alarmes
- Activité des biens
- Infractions en contrôle d'accès ainsi que les alarmes
- Infractions sur les biens ainsi que les alarmes
- Activités d'ouverture et de fermeture de session par les utilisateurs locaux et ceux de postes de travail Link Messages et information du système

Afficheur de mise à jour directe du personnel

Cet afficheur montre le dernier état actuel connu pour la totalité du personnel. Les renseignements tels que le dernier emplacement connu, l'heure, la date et l'état actuel (entrée/sortie) s'affichent. Toutes les 30 secondes (5 secondes si la fonction mise à jour rapide est utilisée), cet afficheur est mis à jour selon l'état d'ENTRÉE ou par ordre de nom de famille. Si vous le souhaitez, vous pouvez effectuer un tri temporaire de la liste selon les colonnes désirées en utilisant le bouton d'outil situé au haut de cette fenêtre.

Afficheur d'alarmes

L'afficheur d'alarmes est une fenêtre qui affiche toute alarme immédiate déclenchée par une ouverture forcée des portes ou si des portes sont laissées ouvertes et non sécurisées après une procédure d'accès normal (contrôle d'accès) et aussi à partir de capteurs externes et des tentatives d'accès non autorisées. Consultez votre fournisseur CDV pour vous renseigner sur la possibilité d'installation de capteurs (appelés aussi GPI).

The screenshot displays the Link-net software interface. At the top, a menu bar includes 'File', 'View', 'Reports', 'Access Control', 'Asset Management', 'Utilities', and 'Help'. Below the menu is a toolbar with various icons. The main window is titled 'Alarms - 0 alarms pending'. It features a table with the following columns: 'Alarm Type', 'Date', 'Time', 'Source', and 'Manager'. The table is currently empty. To the left of the table is a vertical list of devices with status indicators (green for OK, red for Alarm, yellow for Warning). The bottom status bar shows 'Status: Normal', '17/08/2002', and '21:44'.

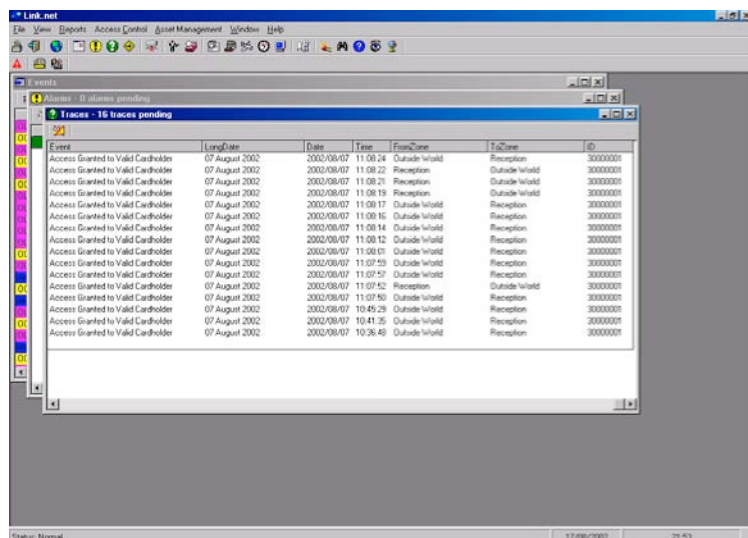
The Alarms Viewer Window

La fenêtre de l'afficheur est disponible à partir du menu **View_Events**.

L'afficheur d'alarmes est disponible à partir du menu **View Alarms.**

Afficheur de pistage

La fenêtre de l'afficheur de pistage s'utilise pour localiser, selon les besoins, tout détenteur de bouton de localisation en activité. L'utilisation de cette fonction permet le signalement de la présence d'un individu sur le site ou la vérification des habitudes d'accès d'un individu. Vous pouvez donc surveiller un individu ou un groupe.

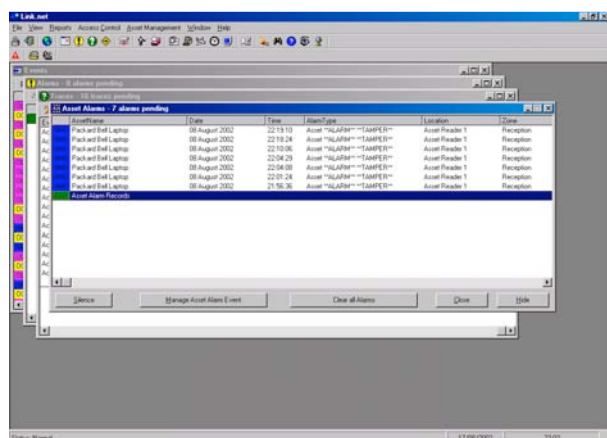


The Traces Viewer Window

L'afficheur de pistage est disponible à partir du menu **View_Traces**.

Afficheur d'alarmes de biens

L'afficheur pour les alarmes de biens montre tous les déplacements de biens ou signale une alarme lors d'infractions sur les biens. Cette fenêtre est activée uniquement si le matériel requis pour la gestion de biens est installé dans vos bureaux et activé.



The Asset Alarms Viewer Window

L'afficheur d'alarmes de biens est disponible à partir du menu **Alarmes View_Asset**.

Afficheur de mise à jour directe de biens

Cet afficheur montre le dernier état actuel connu pour la totalité des ensembles de biens contenus dans le registre des biens. Les renseignements tels que le dernier emplacement connu, l'heure, la date et l'état actuel (entrée/sortie) s'affichent. Cet afficheur est mis à jour régulièrement.

Boîte de dialogue d'alarmes de biens

Le logiciel inclut, en plus de l'afficheur d'alarmes, une boîte de dialogue qui affiche la dernière infraction de déplacement de biens. La boîte de dialogue est qualifiée de **'modale'** et requiert un nettoyage avant que s'affichent des messages supplémentaires ou qu'elle procède à un autre processus du programme. Les messages à venir seront mis en file d'attente cachée et ils doivent être traités de la même façon que les messages précédents.



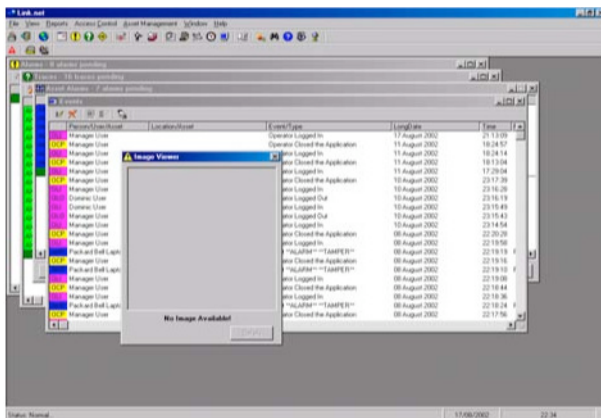
The Asset Dialog Alarm Box

L'importance des messages supplémentaires est d'assurer que toute alarme, lors d'infraction de déplacement, est traitée selon la priorité appropriée.

Afficheur d'image

La vue à l'écran de l'image de détenteurs de badges de localisation s'affichera en temps réel lors d'accès par une porte précise. Sa fonction est d'activer la transmission de l'image au bureau de sécurité pour ainsi comparer la transaction en cours avec l'identité réelle du détenteur de badges de localisation pour éviter les prêts de cartes ou autres infractions à la sécurité de contrôle d'accès. D'autres utilisations peuvent inclure la validation d'abonnement et des comparaisons par CCTV. L'image de l'écran affichera aussi l'image de tout bien ayant déclenché une alarme.

Vous pouvez sélectionner un lecteur précis en contrôle d'accès là où vous voulez capter des images. L'écran d'image affichera aussi tout message indiquant la raison pour le déclenchement de l'alarme pour un bien accompagné de son image.



L'écran d'image est disponible à partir de l'écran **View_Image**

L'afficheur de l'écran d'images

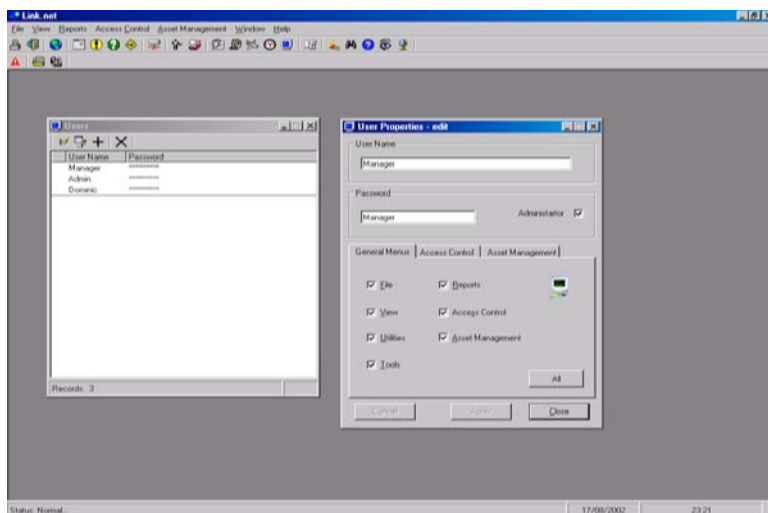
Touches de raccourci

Les touches de raccourcis Link.net s'utilisent pour ajuster rapidement les fenêtres lors de visualisations et aussi pour retrouver une fenêtre qui est cachée par une autre. La liste qui suit indique les fonctions des touches (liste partielle):

- F1 – Menu d'aide à l'écran
- F2 – Affiche toutes les fenêtres en mode cascade (tel un jeu de cartes)
- F3 – Juxtaposition verticale
- F4 – Juxtaposition horizontale (lorsque possible)
- F5 – Ferme toutes les fenêtres
- F6 – Lance la liste d'inventaires de biens
- F7 – Lance le rapport de biens perdus
- F11 – Affiche l'utilitaire de localisation du personnel
- F12 – Lance les rapports de suppression ou d'appel par liste

Utilisateurs

La définition d'un utilisateur est un individu qui a des droits d'accès au logiciel [Link.net](#). Des droits d'accès conditionnels sont établis pour chaque utilisateur. Un « administrateur » se définit comme un individu ayant la capacité de définir des utilisateurs supplémentaires. Il existe un réglage par défaut pour la création d'un nouvel utilisateur qui inclut un descripteur ainsi qu'un mot de passe qui est « Gestionnaire ». Comme suite à la création de nouveaux utilisateurs, nous recommandons que soit supprimé le descripteur puisque cela peut présenter un risque potentiel en sécurité.

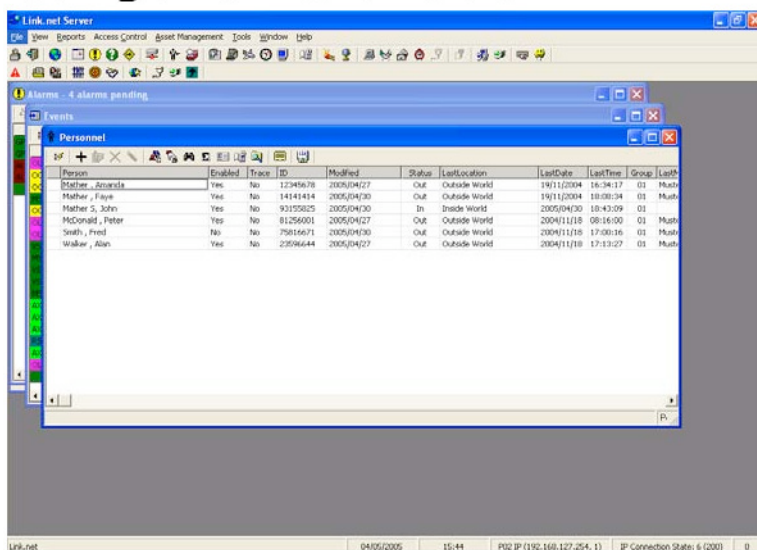


The Users Windows

L'écran d'utilisateur est disponible à partir de **View_Users**

Ajout d' un nouveau port de carte

Adding a new card holder



L'écran du personnel est disponible à partir de l'accès **Control_Personnel**

Liste du personnel

La fenêtre du personnel inclut des options d'édition et d'ajout de nouveaux détenteurs de carte (individu). Cliquez la touche « Ajouter » pour créer un nouveau dossier :

LastDate	LastTime	Group	LastH
19/11/2004	16:24:17	01	Mush
19/11/2004	18:08:34	01	Mush
2005/04/30	18:43:09	01	
2004/11/19	00:16:00	01	Mush
2004/11/19	17:00:16	01	Mush
2004/11/19	17:13:27	01	Mush

Personnel Add View

Les champs requis incluent :

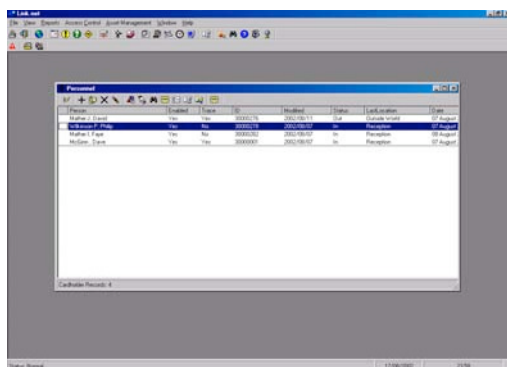
- Nom de famille
- Prénom
- Numéro unique de carte (ID)

Vous pouvez remplir d'autres champs incluant ceux définis par l'utilisateur, disponibles à partir de l'onglet « Champs supplémentaire ». De plus, une image peut s'attacher à un dossier.

Si la fonctionnalité « Lecteur de bureau de saisie de badges de localisation » est installée par votre fournisseur, vous pouvez soit, inscrire le numéro à 8 chiffres directement ou sélectionner la touche « ? » située à la droite du champ. Une fois choisie, insérez le badge requis dans « Lecteur de bureau de saisie de badges de localisation » et après quelques instants les données pour ce badge seront saisies. Si vous utilisez des badges de localisation sécurisés par un numéro à notation hexadécimale de 10 chiffres (19F02356B6) vous pouvez, alors, sélectionner la touche « H » pour inscrire ce numéro crypté à 10 chiffres et le système le décodera pour vous. Notez qu'il est normal qu'un autre numéro soit placé dans le champ d'identification du badge.

À ce moment si vous sélectionnez « **OK** » le nouveau dossier sera créé. Ce détenteur de badges de localisation aura donc des droits de contrôle d'accès pour toutes les portes et en tout temps. La liste sous-jacente sera rafraîchie pour inclure cette nouvelle entrée.

Suppression d'un détenteur de carte



Personnel View

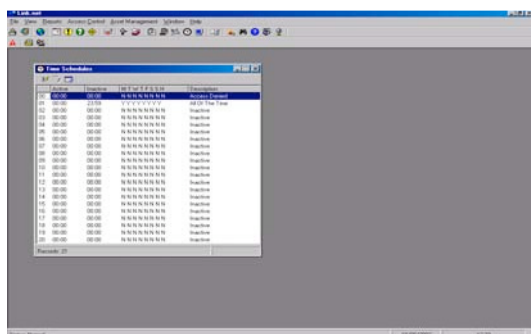
Deux méthodes existent pour retirer des droits de contrôle d'accès pour tout détenteur de carte. Vous pouvez supprimer complètement le dossier (détenteur de carte) ou sinon les droits peuvent être désactivés (recommandé). Les deux activités sont disponibles à partir de la barre d'outils « Personnel ».

CONSEIL : Restez quelques moments sur toute touche de la barre outils et une fenêtre contextuelle de conseils s'affichera!

Planning

Le planning se compose de fonctions qui activent ou désactivent les événements selon certaines périodes. Il s'utilise pour deux raisons principales :

- La configuration de spécifications à un groupe d'accès pour permettre/interdire l'accès selon l'heure et le jour.
- La configuration des lecteurs de contrôle d'accès pour automatiquement déverrouiller/verrouiller à nouveau des portes par le contrôle de période d'accès non sécurisés lors de périodes d'accès à haute activité.

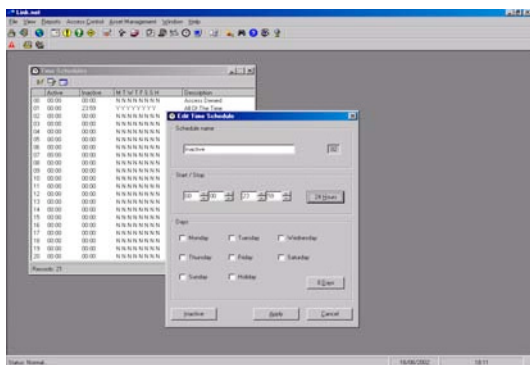


The Time Schedules Window

La fenêtre de planning est disponible à partir de l'**Accès Schedules Control_Time**

21 horaires de planning sont disponibles pour utilisation. Les horaires 00 & 01 sont des horaires de base du système et peuvent être alloués, mais non modifiés. Les horaires de planning 02-20 peuvent être édités. **Notez que :** des précautions doivent être prises lors de la modification d'un horaire de planning qui est en utilisation dans un autre emplacement puisque vos modifications affecteront son attribution.

Modification d'un horaire de planning



Time Schedule Modify View

Une fois choisi, l'heure de planning peut se régler selon une heure de début et de fin ainsi que selon des journées de la semaine ou elle sera en activité. Sa période d'activité est la minute de début jusqu'à la minute de fin. L'heure de début doit toujours être antérieure à l'heure de fin!

Un titre indiquant sa fonction d'utilisation devrait être inscrit. Cliquez « Attribuer » lorsque vous avez terminé et la liste sous-jacente se met à jour.

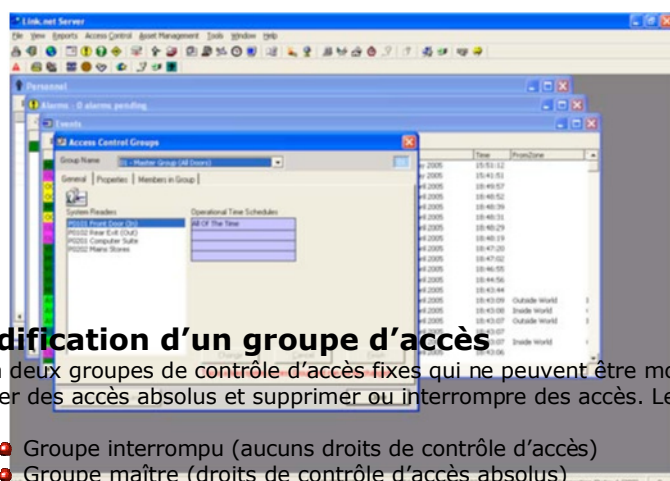
Groupes de contrôle d'accès

Les groupes de contrôle d'accès permettent l'attribution de droits de contrôle d'accès à des zones et heures précises par un label. Cela permet l'attribution rapide de droits de contrôle d'accès à tout individu nouveau (détenteur de carte). Si une nouvelle catégorie est requise une nouvelle définition en contrôle d'accès est, alors, aussi requise.

CONSEIL : Créez le moins de groupes de contrôle d'accès que vous le pouvez. Réfléchissez « Combien d'individus requiert vraiment des droits d'accès différents ? » – cela définira vos besoins continus en groupes d'accès!

Par définition tout individu (détenteur de carte) qui est un membre d'un groupe de contrôle d'accès précis détient des droits de contrôle d'accès identiques aux autres membres. Si vous changez les droits de contrôle d'accès pour un groupe de contrôle d'accès vous changez, alors, tous les droits pour les membres du groupe. Il existe 30 groupes d'accès pour édition et ils sont disponibles à partir du menu **Accès Control_Groups**.

L'écran de groupes de contrôle d'accès est disponible à partir de l'accès **Control_Groups**

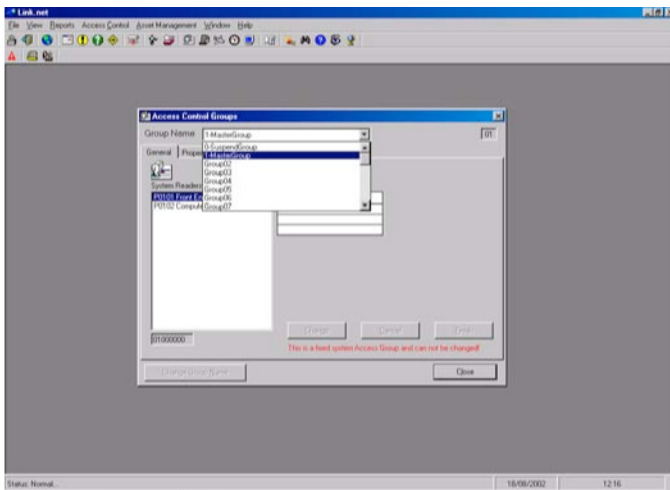


Modification d'un groupe d'accès

Il y a deux groupes de contrôle d'accès fixes qui ne peuvent être modifiés puisqu'ils sont utilisés par Link.net pour allouer des accès absolus et supprimer ou interrompre des accès. Les groupes fixes se définissent comme suit :

- Groupe interrompu (aucuns droits de contrôle d'accès)
- Groupe maître (droits de contrôle d'accès absolus)

Pour sélectionner un groupe d'accès de réserve, sélectionnez-le à partir de la boîte de liste de défilement à partir du menu situé dans la partie supérieure de la fenêtre de groupe d'accès.

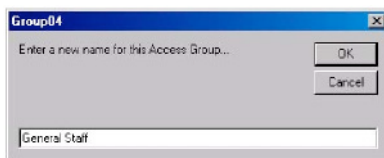


Access Group selection

Une fois que vous avez choisi une liste de tous les lecteurs disponibles en contrôle d'accès (portes) s'affichera ainsi que les horaires de planning qui sont opérationnel pour chaque lecteur. Le choix du lecteur à partir de la liste énumérera les horaires de planning dans la partie adjacente. Vous pouvez connecter jusqu'à 4 horaires de planning à tout lecteur à l'intérieur des spécifications du groupe d'accès. Dès que les groupes d'accès sont établis, ils peuvent être attribués aux détenteurs de carte en utilisant l'onglet « Groupe » à partir des dossiers personnels.

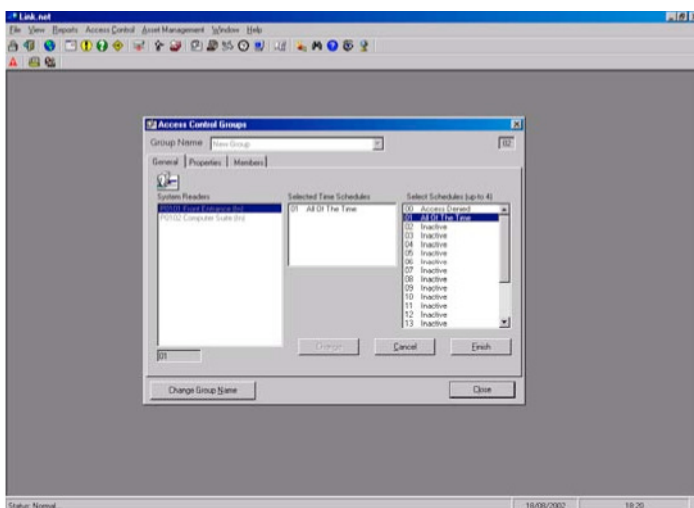
Changement de nom d'un groupe d'accès

En choisissant la touche appropriée dans la fenêtre « Groupe », vous pouvez changer le label du groupe d'accès pour un label qui indique plus précisément son utilité.



Cliquez « OK » pour enregistrer le nom modifié ou si vous ne voulez pas l'enregistrer cliquez « Annuler ».

Attribution d'un horaire de planning aux lecteurs de groupes



Access Group Time Schedule View

À partir de la liste de lecteurs du système, mettez le lecteur approprié en surbrillance et cliquez « Changer ». Les

horaires de planning disponibles s'affichent à droite. Vous pouvez choisir jusqu'à 4 horaires de mise à l'heure pour chaque lecteur et une copie de votre choix s'affichera dans la liste du milieu. Si vous voulez annuler les changements, choisissez « Annuler ». Continuez la sélection de lecteurs à partir de la liste de gauche et procédez à tout changement, tel que requis.

CONSEIL : Un seul clic sur le lecteur de la liste de gauche et il en résultera un affichage du nom des horaires attribuées à la liste du milieu. Rappelez-vous que pour chaque lecteur, vous pouvez allouer quatre réglages divers d'heure de planning.

Jours fériés

Généralement le système de contrôle d'accès fonctionne sur un cycle de 7 jours. Normalement il y a un niveau de sécurité plus élevé pendant le week-end puisqu'il y a moins d'individus sur les lieux. Cependant, cela crée un trouble potentiel, puisque quelques jours fériés se fêtent à certains jours ou une sécurité normale serait en place. Les jours fériés se déterminent par une liste de dates (JJMM) ayant loi de précedence lors de l'analyse pour d'accorder au détenteur de carte l'accès à une porte ou si une porte doit être déverrouillée automatiquement. Parfois cette situation est considérée comme le huitième jour. Vous avez peut-être constaté que dans un planning il y existe un choix pour un huitième jour. Si, dans un planning, il y a la présence d'un jour férié, alors, c'est à partir des spécifications de ce dernier par lequel la requête ainsi que la mise en activité sont effectués et non selon le jour de la semaine en cours.

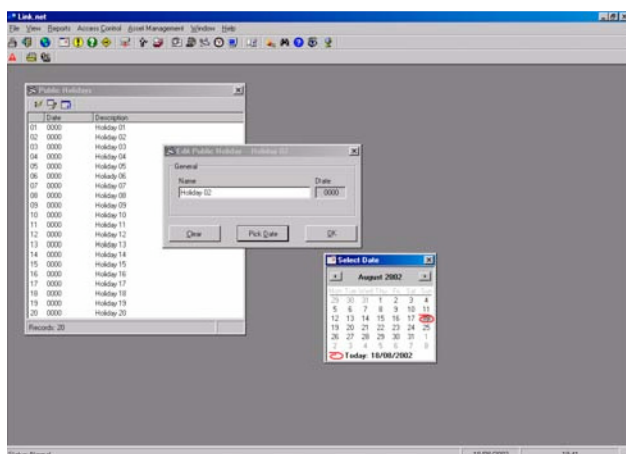
Paramétrage des jours fériés

Sélectionnez la première rangée de congés à partir de la liste et ouvrez le dossier. Inscrivez un nom descriptif pour cette date (p. ex. Noël). Sélectionnez la touche « Choix de date » et naviguer jusqu'à la bonne date et double cliquez dessus. Sélectionnez « OK » et la liste sous-jacente est mise à jour. Fermez la fenêtre de jours fériés.

Édition de jours fériés

Pour éditer ou retirer un jour férié, suivez le même chemin pour ainsi ouvrir le dossier existant pour soit le retirer ou l'attribuer à une nouvelle date.

CONSEIL : Les dates ne s'identifient pas par année, donc assurez-vous que le tableau est mis à jour au début de chaque nouvelle année.



Selecting a list of Public Holidays

L'écran des jours fériés est disponible à partir de l'**Accès Control_Public Holidays**

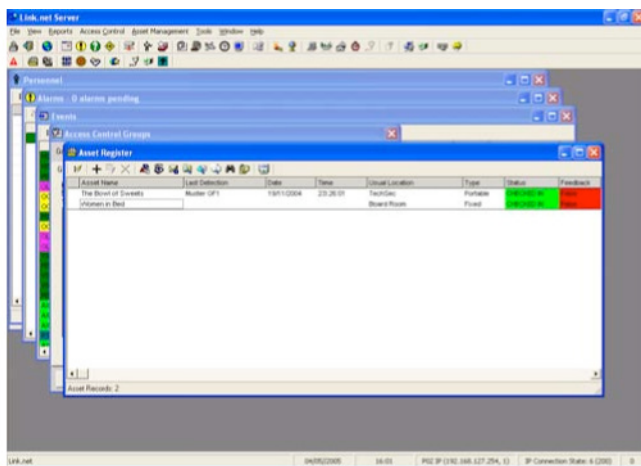
Ajout ou modification d'un bien

Le module de gestion de bien s'utilise pour surveiller les biens portant une étiquette Wavetrend sans fil pour biens actifs. Les propriétés ou fonctions sont disponibles à partir du menu déroulant de « Gestion de biens » et aussi à partir de la deuxième barre d'outils.

Note: Si vous n'avez pas le matériel de support pour la gestion de bien il est probable que l'installateur de votre Link.net n'a pas encore installé tous les éléments de cette fonction et conséquemment ne sera pas visible dans votre version du logiciel Link.net.

Registre des biens

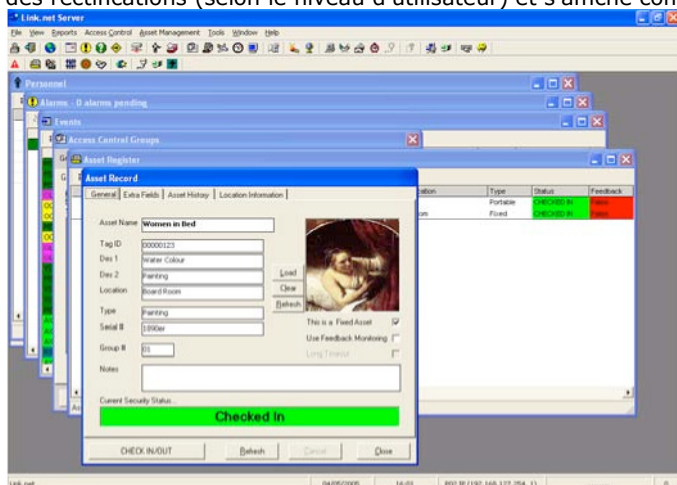
Le registre de biens est une liste qui comporte tous les dossiers et toutes les informations du bien sous protection ainsi que les spécifications opérationnelles. Le registre des biens peut contenir jusqu'à 3000 dossiers.



The Asset Register

L'écran de registre de biens est disponible à partir du **Registre de biens**
Management_Asset

De plus, le registre des biens inclut une vue en direct de l'emplacement et la dernière date que ce bien a été aperçut ainsi que son état actuel. Si vous désirez mettre à jour cette visualisation, cliquez simplement sur la touche de rafraîchissement de la barre d'outils du registre de biens. Pour aider à extraire de l'information, vous pouvez sélectionner la vue à partir de la plupart des colonnes de cette barre d'outils. L'ouverture du dossier de biens permet des rectifications (selon le niveau d'utilisateur) et s'affiche comme suit :



An individual Asset Record

Le dossier de biens comporte trois onglets. L'onglet général fournit le nom, la description, l'ID d'étiquette (TAGID, qui se retrouve sur l'étiquette du bien actif) son emplacement accoutumé ainsi que les paramètres individuels pour ce bien. Les paramètres se définissent comme suit :

Biens immobilisés – s'utilise lorsque le bien ne se déplace jamais de son emplacement p. ex. un tableau peint, une exposition ou biens commerciaux qui ne doivent normalement pas être retirés de leur emplacement désiré.

Utilisation de surveillance rétroactive – s'utilise lorsque l'emplacement du bien doit être surveillé en permanence. La rétroactivité s'utilise pour mettre à jour le dossier de registre de bien. À partir de la liste du registre de biens, vous pouvez voir le dernier état connu (pistage) de tous les biens sous surveillance. Cette fonction s'utilise conjointement avec le rapport de biens perdus. Il existe une option qui peut s'installer (vérifiez avec votre installateur) et qui permet au système de vérifier la présence permanente de biens précis dans un emplacement. Cette fonction s'appelle « Surveillance par contrôle de rétroactivité ». Les alarmes locales reliées aux fonctions d'alarmes centrales se déclenchent si un bien disparaît pour un laps de temps de sa zone d'emplacement (résidence).

Des champs supplémentaires sont disponibles pour obtenir plus d'information en ce qui concerne les biens et incluent la capacité d'ajout d'une image du bien. Si une image est requise, Link.net supporte les images de format JPEG qui sont facilement obtenues à partir d'une caméra numérique bon marché.

Sortie/entrée de biens

- Si vous désirez déplacer ou exclure un bien sans déclencher une alarme, un utilisateur privilégié ayant les droits appropriés peut utiliser, alors, la fonction « entrée/sortie de biens ». Si l'état du bien est modifié pour « sortie » il ne sera plus, alors, sous la surveillance du système et aucune alarme ne se déclenchera. Il est important que seuls les utilisateurs de haut niveau détiennent des droits d'accès dans le menu de gestion de biens pour éviter que des biens soient exclus par erreur.

- Pour changer l'état d'un bien, veuillez sélectionner la touche ENTRER/SORTIR.



La boîte de dialogue illustrée ci-dessus vous demandera de confirmer la modification.

Le client autonome de sortie de biens

Il existe une fonction additionnelle du logiciel qui est disponible pour la gestion quotidienne de biens. Il s'agit d'une petite fonction qui s'installe sur un poste de travail pour permettre à plusieurs individus l'entrée ainsi que la sortie de biens sans avoir de véritables autorisations. Cette application est disponible pour les PC et aussi comme un dispositif à écran tactile qui peut s'installer à la réception ou dans d'autres points stratégiques. La fonction est renvoyée par le réseau au serveur principal du logiciel Link.net selon la configuration du serveur client. Veuillez contacter votre fournisseur CDV pour en savoir plus.

Utilisation d'un poste dédié à « écran tactile » pour la sortie de biens



S'il est nécessaire que certains individus entrent et sortent certains de leurs biens et qu'ils ont les autorisations prédéfinies appropriées, cette option peut être, alors, utile pour vous.

Une console dédiée à écran tactile peut reposer sur un piédestal ou se fixer au mur pour servir de « Poste de sortie ». Toutes les activités sont enregistrées dans le serveur Link.net. Cela permet une procédure rapide par l'utilisation d'un menu pour encourager la prise en charge par les individus de leurs biens alloués.

Touch Screen option.

Le « Poste de travail à écran tactile pour sortie de biens » peut se brancher à l'infrastructure TCP/IP existante ou branchée par câble au poste de travail principal. Des postes de travail additionnels peuvent s'ajouter pour permettre un plus grand débit d'activité.

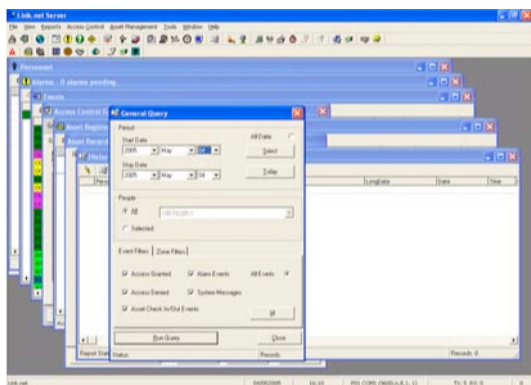
Rapports Link.net

Une fonction vitale du système est sa capacité de faire des requêtes pour l'obtenir de l'information sur l'historique ainsi que l'état en cour du bien. Ces fonctions se retrouvent sur le menu déroulant « Rapports » et sont aussi disponibles à partir de la barre d'outils. On y retrouve ce qui suit :

- **Événements dans l'historique** – un rapport défini par utilisateur pour la production de données sur tous les événements archivés dans la base de données actuelle. Vous pouvez aussi produire des rapports pour une période définie qui indiquent la période de présence sur les lieux des individus ou un rapport qui indique la zone précise où les individus se retrouvent. Prenez note que l'utilisation de cette fonction dépend de la fonctionnalité de caractéristiques précises, si vous avez des doutes concernant l'installation de cette fonction, vérifiez la, alors, avec votre installateur.
- **Requête SQL** – un outil pour les utilisateurs chevronnés en bases de données, qui veulent lancer des rapports bruts des événements principaux de la base de données. La connaissance du langage SQL est requise.
- **Emplacement** – un rapport détaillé basé sur le dernier emplacement connu de tous les individus selon certaines zones précises. Les utilisateurs peuvent choisir autant d'emplacements voulus.
- **Appel par liste** – selon l'information du registre d'urgence cette fonction génère tous les détails sur les individus présents dans la bâtisse. Ce rapport exclut les individus présents dans les « zones sécuritaires ». Consultez la section de contrôle d'accès de zones pour obtenir plus d'information. Ce rapport peut générer en continue des impressions à distance à partir d'un lieu d'impression prédéfini tel qu'un point de rassemblement.
- **Rapport de biens perdus** – fournit tous les détails d'une liste de biens et inclut la surveillance rétroactive d'événements non détectés pendant la journée en cours (à partir de minuit). Ce rapport fournit pour l'utilisateur toute information sur des alertes de surveillance des biens ainsi que des déplacements sporadiques du bien. Peu importe les événements, une investigation est requise. De plus, ce rapport indique que la cellule d'alimentation des étiquettes est en panne.
- **Rapport de biens exclus** – fournit des détails de la liste des biens exclus de leur emplacement normal. Ce rapport inclut l'information du « qui » et du « quand ».
- **Rapport de l'inventaire de biens** – fournit les détails d'une liste d'« où » et « quand » les biens ont été vus pour la dernière fois. Le rapport peut être trié selon la plupart des champs.
- **Rapport de période sur les lieux** – génère le calcul de la présence sur les lieux d'un individu ou groupe et inclut une période totale calculée de temps productif de présence sur les lieux pour une période précise.

Rapport des événements contenus dans l'historique

Ce rapport s'utilise pour générer, par une requête, une liste à partir d'un « historique sur mesure ». Choisissez le rapport d'événements en historique, et pressez la touche « Requête générale » affichée dans cette fenêtre.



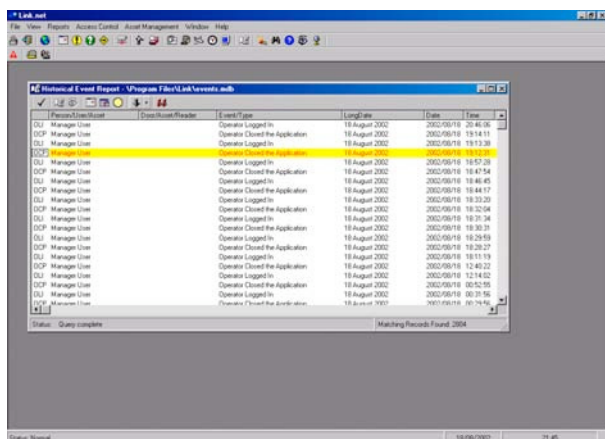
The General Query View

La fenêtre « Requête générale » fournit par défaut les détails de la date en cours, mais elle peut être personnalisée selon une date pour obtenir les résultats d'une période précise. Si un rapport est requis pour un individu précis (contrôle d'accès) vous pouvez choisir, alors, l'individu à partir de la liste de sélection d'individus. Vous pouvez filtrer des événements divers à volonté. Les genres d'événements sont :

- Accès accordé – toute transaction réussie en contrôle d'accès
- Accès refusé – toute infraction en contrôle d'accès
- Événements d'alarmes – toute alarmes déclenchées par les portes, déplacements de bien ainsi que tous les changements de l'état d'entrée
- Messages du système – toute information concernant le système ainsi que les opérations effectuées par les utilisateurs
- Événements d'entrée et de sortie de biens – tout événement en changement d'état de la gestion de biens

Lorsque les critères souhaités sont en place, cliquez la touche « Exécuter requête » ce qui lance la génération du rapport.

CONSEIL: Le rapport peut prendre quelque temps avant de compléter la compilation, surtout si la base de données est volumineuse. La barre d'état au bas de l'écran de la fenêtre de l'historique d'événements suivra le progrès de la génération du rapport.



The completed Report View

Vous pouvez trier le rapport final selon toutes les colonnes et imprimer une partie ou la totalité du rapport et l'envoyer vers l'imprimante de votre choix. Pour imprimer une partie du rapport, mettez en surbrillance un bloc continu de lignes d'événements et uniquement ce bloc sera imprimé.

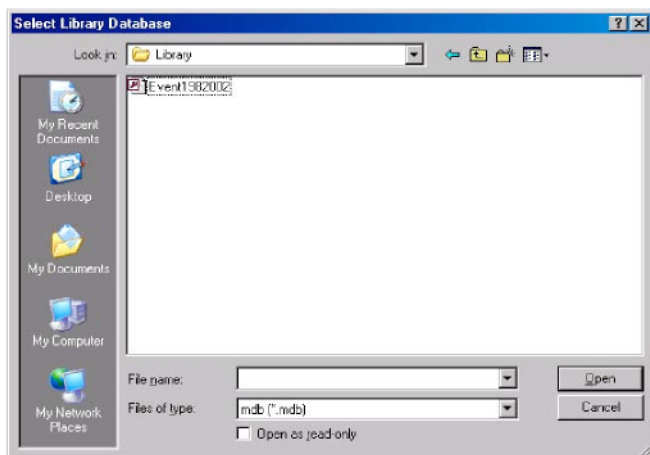
Rapport par SQL

En plus, vous pouvez effectuer par SQL une requête « Historique d'événements locaux ou à distance ». Ce sujet est étendu et dépend de la connaissance de l'utilisateur en langage de base de données standard et n'est donc pas traité dans ce manuel. Un utilisateur ayant les connaissances requises en utilisation du SQL peut effectuer des requêtes avec ce langage ce qui génère des résultats plus rapidement et fournit des détails plus complexes. Si vous désirez plus d'information ou de la formation en ce qui concerne cette fonction puissante du module, consultez votre fournisseur du logiciel Link.

Exécution d'une requête de l'historique à partir des archives de la bibliothèque

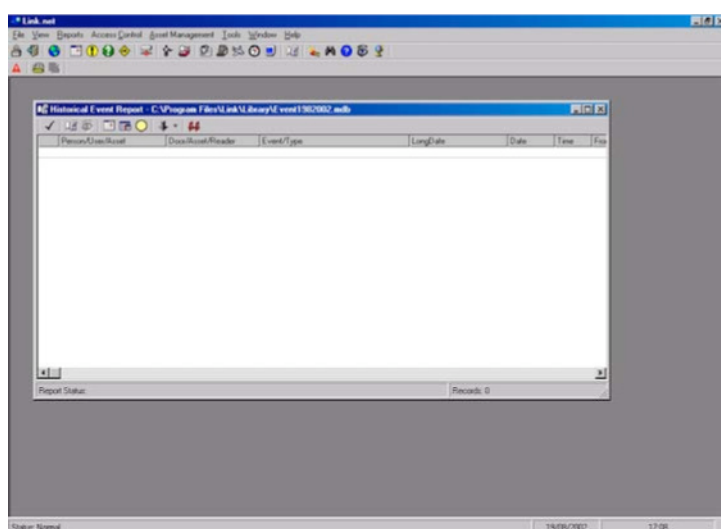
Lorsque la gestion de données est utilisée, les bases de données archivées sont créées dans le dossier **Program**

Files\Link\Library. Ces fichiers saisissent automatiquement la date selon le protocole d'attribution de nom. La date indique que la bibliothèque contient des événements jusqu'à cette date. Pour exécuter une requête dans la bibliothèque à partir de la fenêtre « Historique d'événements » choisissez la touche « Sélectionner bibliothèque » et une boîte de requête de fichier s'ouvrira :



Allez au dossier recherché et ouvrez le fichier pertinent contenu dans la bibliothèque. La fenêtre « Historique d'événements » inclura et effectuera des requêtes à partir de cette base de données et cela jusqu'à ce que la fenêtre se ferme et que vous retourniez à la base de données en cours.

CONSEIL : La base de données d'événements en cours auxquels la fenêtre « Historique d'événements » est actuellement connectée est précisée dans le titre de l'écran, tel qu'illustré ci-dessous.



Fenêtre « Historique d'événements » qui précise la base de données à laquelle elle est connectée

Rapport de la période sur les lieux et de l'emplacement d'individus

Des rapports standard génèrent une liste d'événements qui ont lieu pendant une période précise. Cela est utile pour des raisons de sécurité, mais peut aussi être utile pour le calcul de la période de présence d'individus dans certaines zones (emplacement) ou pour surveiller la totalité de l'emplacement (site) selon une période précise. Cela peut se faire si le matériel approprié de lecture de sortie est installé et configuré.

À partir de la fenêtre principale « Historique d'événement », choisissez l'option « Période sur les lieux et l'emplacement d'individus » et une fenêtre s'affiche pour vous permettre de choisir vos critères. Vous pouvez générer un rapport sur un individu précis ou sur un groupe d'individus.

Pour générer un rapport individuel, vous devez choisir des dates, l'individu qui est l'objet du rapport et vous devez décider si le rapport doit englober le site complet ou une zone (emplacement) précise. Ensuite, choisissez la touche « Lancer rapport ». Le rapport produira tous les détails de transactions pertinentes pour la période choisie et au bas de la liste vous verrez le calcul du temps total passé sur et hors emplacement des individus.

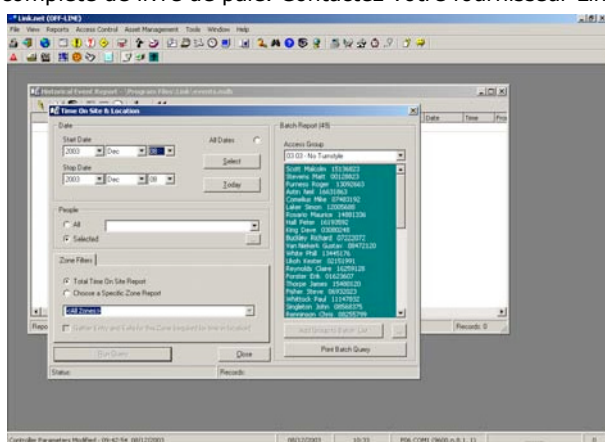
En plus, vous pouvez regrouper un groupe d'individus selon les groupes d'accès pour augmenter la vitesse de génération du rapport. Si cette fonction est utilisée, le rapport sera imprimé directement sur l'imprimante choisie à moins que la boîte « Prévisualiser » soit cochée. Dans ce cas une prévisualisation du rapport s'affiche à l'écran. Il est possible de générer ce rapport en format long ou court et aussi le faire sortir en tant que fichier de valeur séparé par virgule (CSV).

Création d'une base de données dédiée à la période sur les lieux

Vous pouvez lancer ce rapport directement à partir de la base de données d'événement principal. Cependant, par définition, la génération de ce rapport est lente puisque la requête doit naviguer dans une accumulation d'informations non pertinentes. Nous recommandons l'utilisation d'une base de données dédiée pour filtrer le signal d'heure de l'horloge système puisque cela donne de meilleurs résultats et est beaucoup plus rapide pour générer le rapport. Pour régler cette option à partir de l'onglet dans le menu d'options général, sélectionnez l'option « Utiliser base de données dédiée de période sur les lieux (TA) ». Tout signallement d'heure à l'horloge système suivante sera transmis au tableau de base de données dédiée TA.mdb dans le fichier Link. En plus, il est bon de choisir l'option « Indiquer uniquement les changements d'état » puisque cela stockera uniquement les transactions de sortie à entrée ainsi que d'entrée à sortie.

Lorsque cette option est choisie, vous pouvez définir les lecteurs du système qui effectueront un signal d'heure. Comme exemple, le lecteur qui conduit du monde extérieur vers la réception peut être un signal d'heure d'entrée et le lecteur à partir de la réception vers le monde extérieur peut être un signal d'heure de sortie. Nous pouvons aussi fournir des lecteurs additionnels pour signaler les heures de sortie ou d'entrée. Lors de la génération d'un rapport, toute période de sortie est déduite du total de temps sur les lieux. Pour configurer tout lecteur comme un point de signal d'heure, choisissez le contrôleur approprié et ouvrez-le. Ensuite, choisissez l'option « T/A » à partir du nœud du lecteur pertinent.

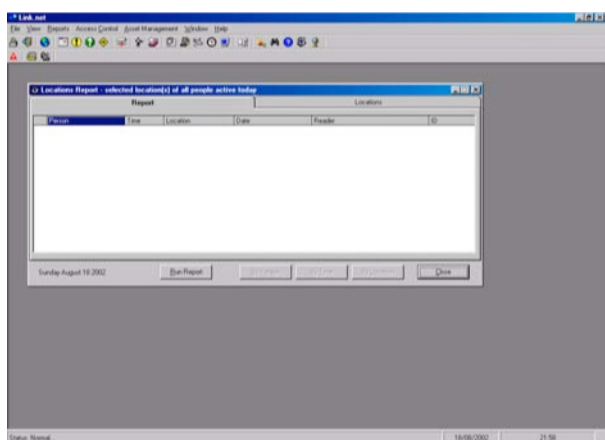
CONSEIL: La base de données dédiée peut se connecter à d'autres utilisations de réseau LAN ou WAN et elle peut aussi exécuter des requêtes par SQL. Des utilisateurs habilités en technologie de l'information peuvent créer des rapports améliorés permettant ainsi la génération de rapports personnalisés selon vos besoins précis. La connexion ODBC est soutenue dans ce logiciel. L'utilisation de l'information générée par le système Link peut mener à une solution complète de livre de paie. Contactez votre fournisseur Link pour obtenir plus d'information.



Tel que stipulé pour un rapport individuel, sélectionnez les critères pour les dates ainsi que les zones pour ce rapport. L'option désirée de la section « Individu » doit être sélectionnée. Dans la section « rapport par lot », vous pouvez choisir des groupes d'accès individuels et les inclure dans la liste de lots. Sélectionnez les groupes désirés et pressez la touche « Ajouter un groupe à la liste de lots ». Tous les membres de ce groupe seront ajoutés à la liste du lot et seront inclus dans le rapport.

Lorsque tous les individus sont inclus dans la liste, choisissez la touche « Imprimer lot » pour amorcer le processus. Une prévisualisation du rapport par lot s'affichera en premier. Vous serez alors en mesure d'imprimer le rapport à partir de votre imprimante ou générer un fichier de données.

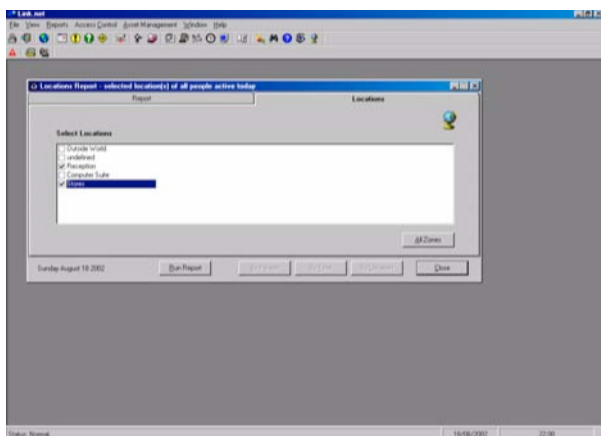
Rapport d'emplacement



The Locations Report

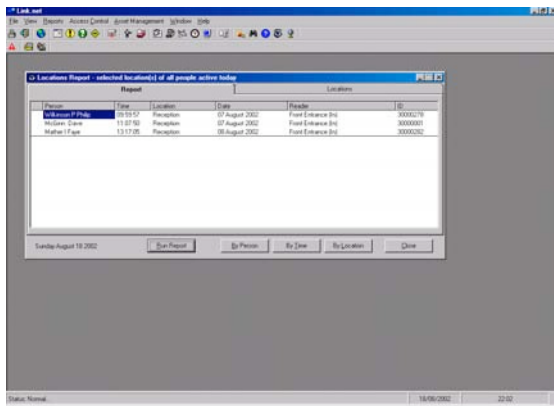
L'utilisateur peut choisir l'onglet « Emplacement » et inclure et exclure certains emplacements (zones) pour produire un rapport plus personnalisé. Ce rapport peut se générer selon deux procédures. Vous pouvez saisir l'information absolue du dernier emplacement connu. Cela peut se faire par roulement ou optionnellement par réinitialisation à minuit. Cette

fonction est choisie à partir du menu « Affichage d'options » sous l'onglet « Appel par liste ». Cochez la boîte « Absolue » pour générer un rapport par déroulement.



The Locations Tab

Lorsque vous avez choisi les emplacements qui vous intéressent, cliquez la touche « Lancer rapport » et le rapport se générera.

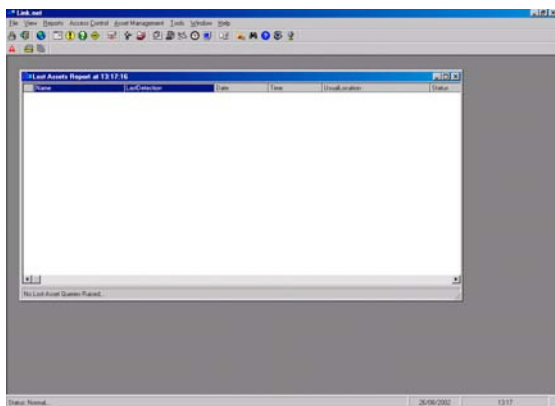


The Report

Initialement, le rapport est trié par individu, mais peut ultérieurement être trié par les touches disponibles.

Rapport de biens disparus

Le rapport de biens disparus est activé lorsque vous le sélectionnez dans « Rapport de biens disparus » Reports_Lost à partir du menu à déroulement. Cela générera un rapport qui comportera les biens réglés par l'option « Rétroaction de surveillance » dans le dossier des biens. Tous les biens non détectés depuis minuit, à la date en cour, seront listés et doivent faire l'objet d'investigations plus soutenues.



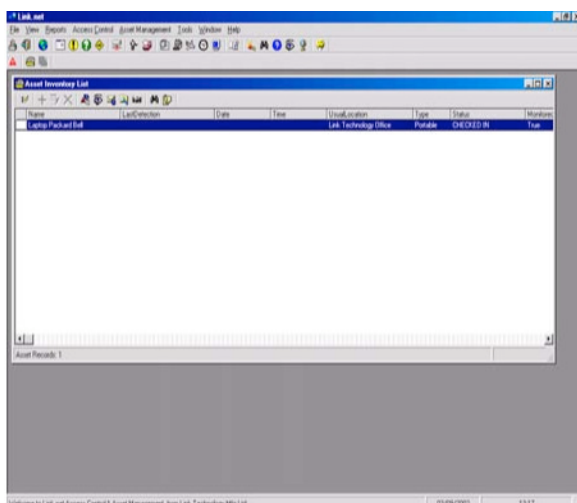
Lost Assets Report (showing no observations)

Automatisation du rapport de biens disparus

Ce rapport peut être automatisé pour qu'il soit lancé à chaque changement d'heure. Pour activer cette fonction, sélectionnez le menu « Options » à partir du menu déroulant View_Options. Sélectionnez l'onglet « Procédures lors d'alarmes pour biens » et cochez l'option « Activer le rapport de surveillance rétroactif hôte ». Ainsi, le rapport sera lancé à 1h00, mais peut être activé manuellement en tout temps.

Rapport d'inventaire des biens

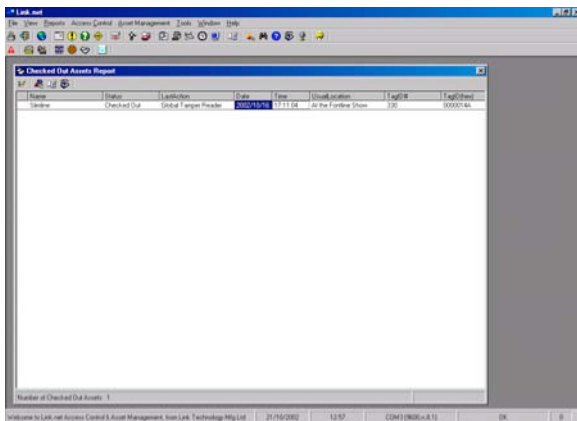
Le Rapport d'inventaire de biens est s'active lors de la sélection « Rapport d'inventaire Reports_Asset » à partir du menu déroulant. Un rapport basé sur tous les biens sera alors généré. Uniquement les biens qui comportent réglage pour la surveillance rétroactive auront des valeurs qui sont à jour. Utilisez les options de tri pour travailler dans la liste.



Asset Inventory Report

Rapport de biens sortis

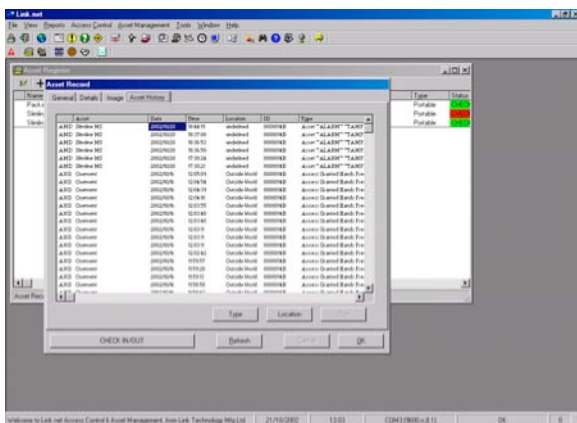
Ce rapport est utile pour garder un œil sur les biens sortis. Il générera en détail les informations sur qui a sorti le bien de son site et à quel moment. Pour activer ce rapport, choisissez « Rapport de biens sortis Reports_Checked ».



Rapport de biens sortis

Rapport de l'historique des biens

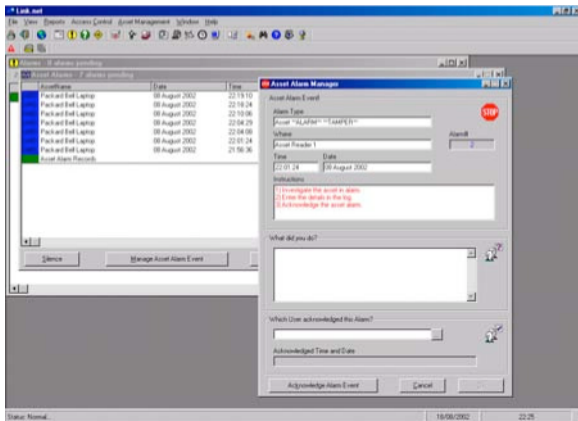
Ce rapport fournira en détail l'historique des biens individuels. Pour sélectionner le rapport, ouvrez « Registre de biens », choisissez le bien et à partir de l'onglet « Historique des biens » sélectionnez « Exécuter ». Ce rapport peut être long à générer, puisqu'il s'agit d'une liste exhaustive de la totalité de son historique. Un rapport plus personnalisé peut se faire à partir de la fenêtre « Écriture de rapport d'historique des événements ».



Rapport de l'historique des biens

Gestion des alarmes

Link.net mène la gestion des alarmes à partir de deux endroits clés : l'Afficheur général d'alarmes ainsi que l'Afficheur d'alarmes de bien. Le but de l'option gestion d'alarmes est de permettre à l'utilisateur de prendre connaissance d'un événement d'alarmes et de fournir les détails pour la procédure à prendre lors de ces circonstances. Vous pouvez autoriser des droits pour qu'un utilisateur ne puisse supprimer les alarmes ou allouer des droits de suppression d'alarmes à un utilisateur d'un niveau supérieur. L'importance de cela est que les alarmes peuvent être vérifiées et ultérieurement supprimées par un utilisateur de niveau supérieur. Retirez les alarmes périodiquement et ne laissez pas des alarmes multiples s'empiler puisque cela nuira au rendement de l'application conformément à la mémoire que vous avez dans votre PC.



Vue de l’Afficheur général d’alarmes et de l’Afficheur d’alarmes de bien lors d’une opération de la procédure de gestion

Vous pouvez gérer l’alarme en la choisissant dans la fenêtre de l’afficheur et en cliquant sur la touche « Gérer ». La fenêtre « Gestion d’alarme » s’affiche. Les instructions pour l’utilisateur lors de ce type d’événement s’affichent en rouge. Vous pouvez personnaliser cette fonction à partir de l’écran du menu « Options ».

Ce qui suit est un exemple d’un processus normal :

- Activez "Gestion d’alarmes à partir de l’événement d’alarme en direct
- Suivez les procédures inscrites en rouge
- Enregistrez les détails des activités que vous avez effectuées
- Sélectionnez votre ID à partir de la liste d’utilisateurs
- Cliquez la touche « Enregistrer » pour compléter le processus

La date ainsi que l’heure de l’enregistrement s’ajoutent aux événements d’alarmes pour vérification ultérieure.

CONSEIL : Les alarmes enregistrées ne peuvent se modifier – ils ne peuvent qu’être révisés.

Vous pouvez supprimer des alarmes (si vous avez les droits appropriés) à partir de la fenêtre appropriée d’alarmes.

Définition de types d’alarme

Les alarmes sont des événements critiques que nous pouvons diviser en deux utilisations précises :

- Procédure de traitement d’alarmes
- Diffusion par courrier MAPI

Des exemples d’alarmes sont : une porte forcée ou maintenue ouverte, une infraction en déplacement de bien ou une entrée indiquant un changement de l’état général du bien. Vous pouvez choisir à partir des fenêtres « Options et diffusion par courrier », quels types d’alarmes peuvent se déclencher lors d’événements décrits ci-dessus. Une infraction pour un bien est toujours traitée comme une alarme. Si vous désirez qu’un type d’événement soit diffusé par une session de courrier MAPI, l’événement doit être, alors, classé comme un type alarme.

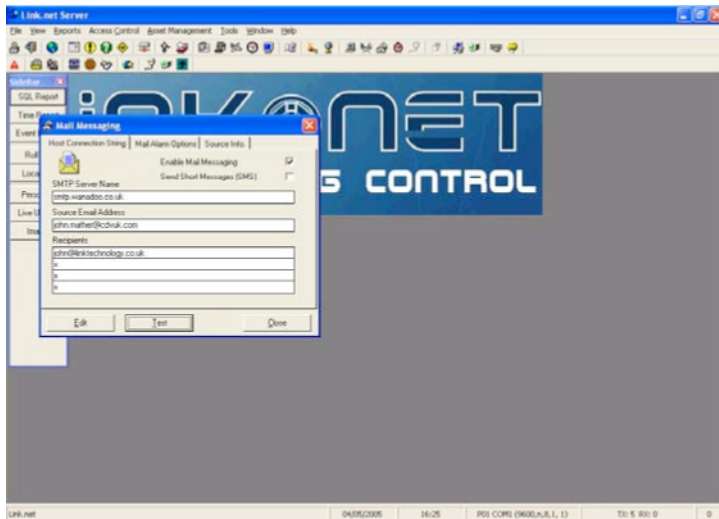
Diffusion par courrier

Le logiciel Gestion de bien et contrôle d’accès Link.net soutien les Emails IP de certains types d’événements. Link.net utilise et communique avec un serveur de courrier SMTP existant qu’il soit situé à l’extérieur ou l’intérieur du site. Les fonctions dans ce secteur sont immenses puisque SMS (service de courts messages) ainsi que les services de radiomessagerie sans fil sont compris dans le domaine IT. Pour utiliser la fonction de courrier par IP, vous aurez besoin de ce qui suit:

- Un serveur conforme au protocole de courrier SMTP
- Un groupe de courrier prédéfini et réglé pour la diffusion d’alarmes
- La diffusion de courrier par IP Link.net est réglée pour rencontrer vous besoins précis.

Définition d’une session de courrier IP

Pour commencer la définition d’une connexion IP, veuillez choisir l’outil de courrier de Tools_Link et l’écran qui suit s’affichera :



The Alarm Mail Messaging Window

Les réglages disponibles incluent le nom de serveur SMTP, p. ex. smtpmail.btopenworld.com ou tout autre nom par lequel vos emails sont diffusés. En plus, vous aurez à fournir une adresse valide d'email en tant qu'expéditeur de tous les messages. Si vous le souhaitez, vous pouvez fournir jusqu'à 4 adresses d'email qui recevront les événements d'alarmes spécifiques.

Les autres onglets vous permettent de configurer quel message doit être diffusé par email IP et ceux qui seront classés comme alarme. Les onglets permettent aussi de configurer un emplacement additionnel pour permettre l'étiquetage du lieu d'expédition des messages.

Contenu du message

Le contenu du message doit inclure l'information importante qui suit lors d'alarmes :

- En tête du message à définir par l'utilisateur
- Type d'alarme
- Emplacement
- Raison du déclenchement de l'alarme
- Date et heure de l'alarme
- Source

Ces paramètres ne sont pas tous appropriés aux différents types d'alarmes.

Gestion des données

Tout logiciel qui contient des bases de données essentielles doit absolument inclure une fonction qui exécute une sauvegarde régulière de la gestion de données. CDV recommande que vous suiviez une stratégie en deux étapes, p. ex.

- Une copie de la totalité du répertoire cible ainsi que tous ses sous répertoires doivent être stocké fréquemment dans un lecteur à stockage massif.
- L'exécution régulière d'un archivage dans la bibliothèque de la base de données principale d'événements Link.net et ensuite une purge (compression) régulière de la base de données d'origine des événements principaux.

Les bases de données Link.net sont compatibles avec le programme Microsoft Access de Microsoft Office et comportent une extension de fichier .mdb. Les fichiers peuvent être compressés et réparés en utilisant Microsoft Access. Consultez votre division de soutien IT avant d'entreprendre ce genre de procédure.

Copie de la totalité du programme et fichiers de soutien

Fermez tous les programmes ainsi que Link.net et redémarrez votre PC (poste de travail). En utilisant l'explorateur Windows, allez au dossier **Program Files\Link** et copier la totalité du contenu de ce dossier ainsi que ses sous dossiers vers un lecteur de réseau ou autre dispositif à distance tel qu'un CD-ROM, etc. Dans l'éventualité qu'un événement désastreux se produise, cette procédure vous permettra d'avoir en main une copie des données du programme pour réinstallation sur le PC (poste de travail) d'origine.

Compréhension de la structure de la base de données

Il existe cinq fichiers de base données essentielles (également appelé tableau) associés à cette application. Ils sont :

- **Événements** – base de données des événements. Ce fichier devrait être archivé dans la bibliothèque et ensuite purger régulièrement de l'application puisqu'il peut devenir très volumineux et difficile à gérer. Lorsque le fichier est archivé dans la bibliothèque il est comprimé par date. Cela vous permettra de faire des requêtes à une date ultérieure à partir du rapport d'historique d'événements.
- **Actuel** – ce tableau temporaire stocke les 1000 dernières transactions et se gère de façon autonome.
- **Alarmes** – stocke tous les événements associés à une alarme et se gère de façon quasi autonome, mais

- doit être purgé périodiquement par un utilisateur de haut niveau.
- **Groupes** – stocke toutes les informations associées au système, tel que la configuration, les biens et les détenteurs de carte.
- **Système** – stocke les informations de modification du système ainsi que la personne qui les a exécutés. Nous recommandons que cette application soit purgée périodiquement à partir de la fenêtre « Afficheur des événements du système » dans l'application principale.

Gestion du tableau d'événements principaux

La procédure qui suit doit être exécutée périodiquement pour compresser la base de données **d'événements** principaux et créer un archive des événements antérieurs pour pouvoir exécuter des requêtes à partir de la fenêtre « Historique d'événements ». Vous devez effectuer cette procédure en trois étapes :

Étape 1 – Création d'un archive de bibliothèque d'événements

À partir du menu « Outils », sélectionnez le fichier « Bibliothèque de tableau d'événements Utilities_1_Create ».

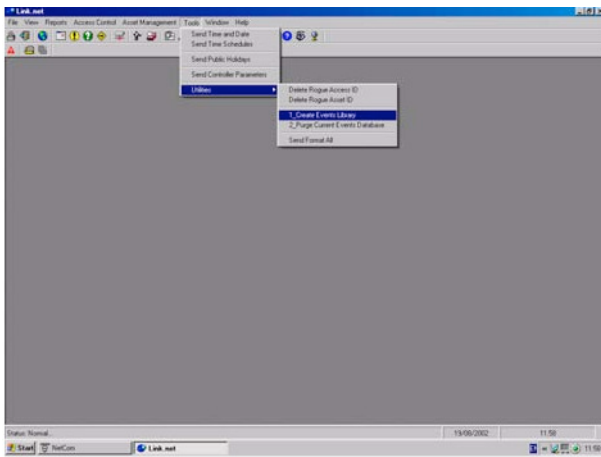
CONSEIL : Ne créez pas plus qu'une bibliothèque d'événements par jour.



Suivez les directives du message-guide qui s'affiche à l'écran et fermez tous les applications et ensuite redémarrez l'ordinateur. Lancez l'application [Link.net](http://link.net) telle que vous le faites normalement. Une copie de la base de données **Événements** est créée dans le dossier **\Program Files\Link\Library** et vous y retrouverez la date courante dans sa description.

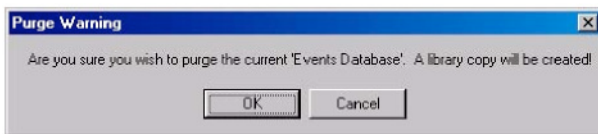
Étape 2 – Purge des événements subsistants de la base de données

Après terminaison de l'étape un, vous devez maintenant sélectionner « Option 2_Purge de la base de données des événements courants ».



À partir du menu
« Outils » sélectionnez
**Base de données
d'événements
actuels Utilities_
2_Purge**

The following prompt appears:



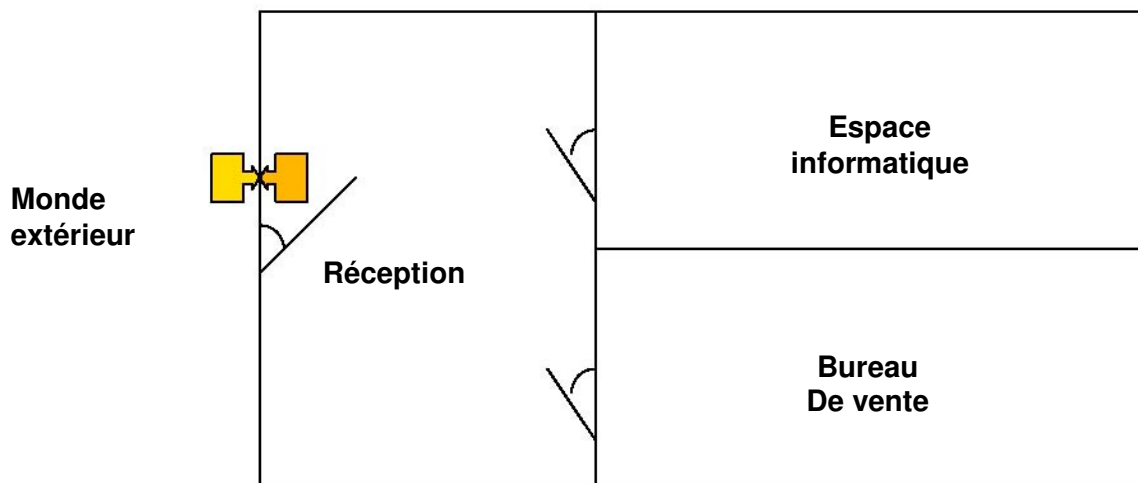
Sélectionnez "OK" et la base de données des événements courants sera compressée laissant les archives de bibliothèque dans le dossier bibliothèque. En plus, vous pouvez choisir l'option « Purger le tableau des événements par date », ce qui permet uniquement la purge ou la suppression d'événements jusqu'à une date précise.

Étape 3 – Compression de la base de données d'événements

Comme suite à la purge de la base de données d'événements selon une des options mentionnée à l'étape deux, nous conseillons de compresser la base de données. Les bases de données de style Microsoft Access 2000 demeurent volumineuses après suppression de rangées d'événements. Donc, pour conserver de l'espace précieux du disque et pour améliorer la vitesse d'exécution ou améliorer le tableau de la base de données d'événements, sélectionnez l'option quarte après un processus de purge. L'application vous demandera de fermer et redémarrer l'application Link suite à cette procédure. À partir de l'explorateur Windows ou à partir de Mon ordinateur vous verrez que la taille du fichier\Program Files\Link\Events. mdb est grandement diminuée.

Zones

Les zones ou emplacements se définissent comme des lieux qui mènent de et à d'autres emplacements à l'intérieur d'un bâtiment. Comme exemple : une porte est placée à l'entrée d'une bâtisse, donc deux lecteurs de contrôle d'accès se retrouvent sur chaque côté de la porte avant.

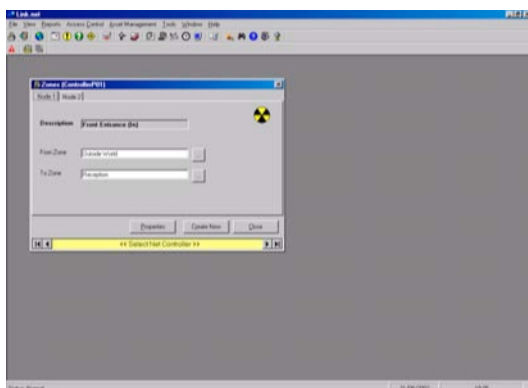


Le plan du bâtiment montre 4 espaces

Lorsque les détenteurs de carte transitent par le capteur situé dans la zone « Monde extérieur » pour se rendre dans la zone « Réception », leur présence est détectée dans cette zone et cela est de même lors d'un transit en sens inverse. Leur présence demeure à cet emplacement jusqu'à ce qu'ils se déplacent vers une autre zone branchée à un capteur. Si vous avez besoin de rapports de type « Emplacement » et « Liste d'appel » un contrôle d'accès selon la zone doit, alors, être utilisé. Les zones peuvent aussi servir pour la gestion des biens. Ils fournissent une référence supplémentaire du lieu protégé par les capteurs actifs de biens.

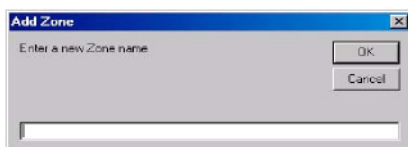
Création de zones

La création de zones est tout simplement un nom qui est donné à un lieu spécifique pour servir de capteur de contrôle d'accès ou de bien actif à une date ultérieure. Un capteur de contrôle d'accès requiert deux noms de zone, un pour indiquer la destination d'où provient l'individu et l'autre pour indiquer la destination vers laquelle l'individu se rend. Un capteur actif de biens ne requiert que la spécification « Provenance ». Sélectionnez l'option « Zone » à partir des menus de contrôle d'accès ou de gestion de biens.

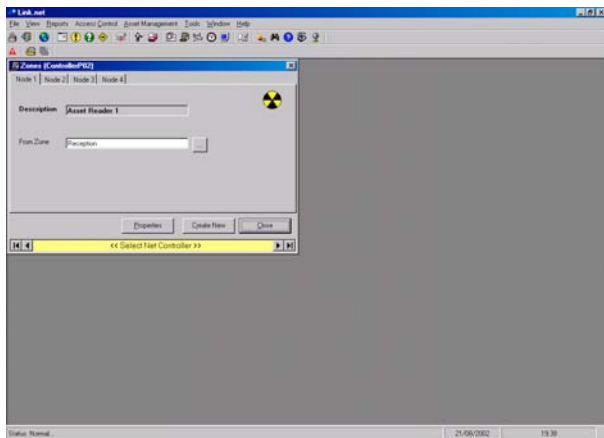


The Zones Menu for creating and applying Zones

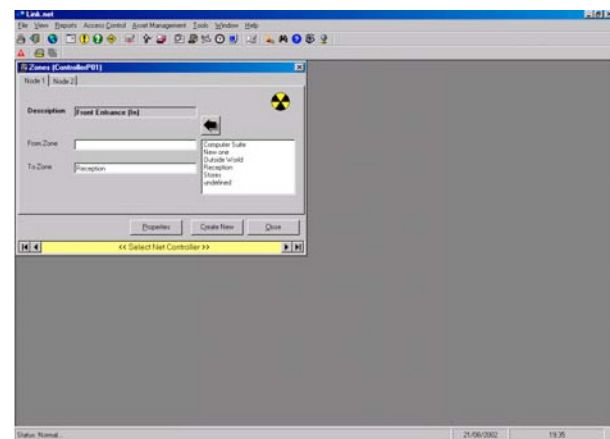
Pour créer une spécification pour une nouvelle zone, sélectionnez la touche « Créer ».



Inscrivez le nom de la nouvelle zone et ensuite cliquez « OK ».



Vue d'une application de capteur actif de zone pour un bien (uniquement une spécification)



Adding a Zone to a reader

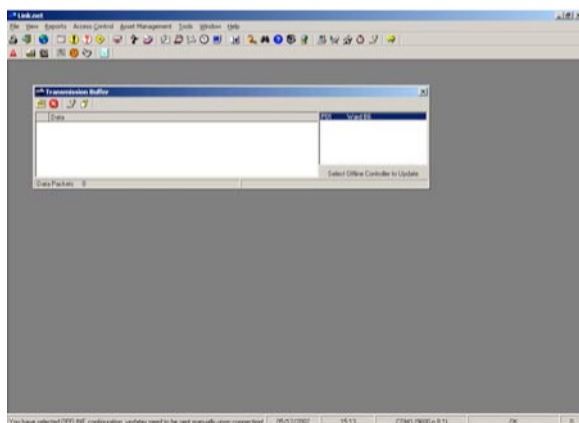
Travail hors ligne

Il est normal que tous les contrôleurs soient redirigés par réseau vers un seul PC (mode en ligne). Vous pourriez souhaiter dans certains cas, gérer les modifications apportées à votre système en étant HORS LIGNE. Dans ce cas, chaque contrôleur sera autonome et isolé l'un de l'autre. Les conséquences sont que toutes les modifications faites à partir de votre PC ne mettraient pas à jour les contrôleurs concernés puisqu'il n'existe plus aucune connexion physique. Les modifications que vous faites sont stockées dans la mémoire tampon et doivent donc être appliquées au contrôleur, tel qu'expliqué ci-dessous :

Mise à jour de contrôleur avec les données hors ligne

Un processus typique serait comme suit :

1. Lancez le logiciel [Link.net](http://link.net).
2. Faites toutes les modifications d'administratives.
3. Prenez l'ordinateur ou portable et branchez-le au contrôleur en utilisant le raccord fourni par l'installateur.
4. Sélectionnez la touche « Envoyer les données hors ligne ».
5. La fenêtre « Mémoire tampon de transmission » s'affiche.
6. Sélectionnez le contrôleur auquel vous êtes branché (les noms descriptifs apparaissent dans la liste de droite).
7. Sélectionnez « Mettre à jour les informations hors ligne maintenant ».
8. L'information est envoyée. Les données qui subsistent dans la liste s'appliquent à d'autres contrôleurs. Allez au contrôleur suivant.
9. Répétez le processus à partir de l'étape 5.



The 'Transmission Buffer' Window (Data should appear in the left hand list)

Récupération d'événements hors ligne

Chaque contrôleur comporte une capacité en stockage de 450 événements hors ligne. Lorsque sa capacité de stockage est atteinte, l'événement le plus ancien est perdu irrévocablement et libère ainsi de l'espace pour faire place à des événements plus récents. Si, pour vous, la perte d'événements est critique le mode hors ligne ne doit, alors, pas être utilisé et tous les contrôleurs doivent donc être retournés au PC par réseau, utilisation du réseau de câblage, modem radio ou protocole TCP/IP.

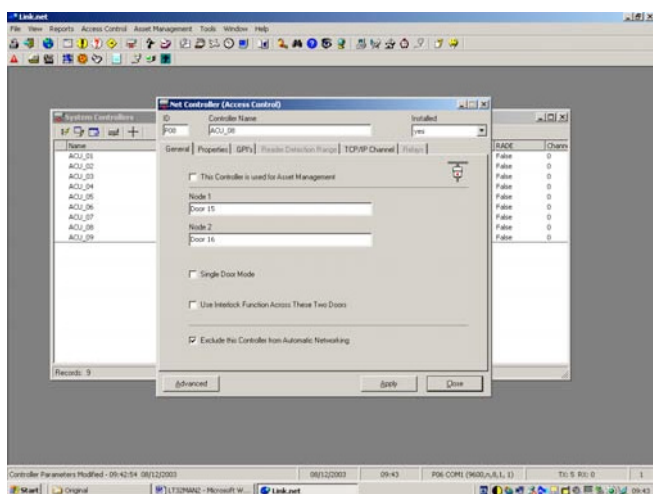
Pour récupérer des événements hors ligne, vous devez suivre le procédure suivante :

- 1 Lancez le logiciel [Link.net](#).
- 2 Branchez l'ordinateur ou portable au contrôleur en utilisant le raccord fourni par l'installateur.
- 3 Sélectionnez la touche « Envoyer les données hors ligne ».
- 4 La fenêtre « Mémoire tampon de transmission » s'affiche.
- 5 Sélectionnez le contrôleur auquel vous êtes branché (les noms descriptifs apparaissent dans la liste de droite).
- 6 Sélectionnez « Importer les informations hors ligne maintenant ».
- 7 L'information reçue sera stockée dans le journal d'événements. Allez au contrôleur suivant.
- 8 Répétez le processus à partir de l'étape 5.

CONSEIL : Ce mode d'opération doit normalement être sélectionné pour vous par votre installateur!

Travail en ligne avec des contrôleurs hors ligne choisis

Un système de réseautage standard (en ligne) peut s'utiliser avec un nombre de contrôleurs choisis situés à distance et qui fonctionnent en mode autonome (hors ligne). Pour exclure des contrôleurs du système de réseautage standard en ligne, sélectionnez le contrôleur correspondant à partir de la liste des contrôleurs.



Choisissez l'option « Exclure » située au bas de la fenêtre « Contrôleur réseau ». Le système de réseautage standard en ligne tentera d'établir une connexion avec ce contrôleur. Répétez cette procédure pour tous les contrôleurs hors ligne.

Récupération d'événements à partir de contrôleurs hors ligne exclus

Les contrôleurs hors ligne généreront tout de même des données ainsi que des événements. Ceux-ci sont stockés dans la mémoire tampon local du contrôleur. Tous les événements sont stockés avec la date et l'heure précise de la survenance de l'événement. Jusqu'à 450 événements sont automatiquement stockés dans cette mémoire tampon et lors de l'entrée du 451e événement cela supprime l'événement le plus ancien.

Pour récupérer les données du contrôleur hors ligne, branchez le PC au contrôleur à distance cible et sélectionnez la touche « Importer données du contrôleur exclu » situé sur la deuxième barre d'outils identifiés par une flèche noire sur

fond vert. Après quelques instants, les événements seront importés vers le logiciel. Après la fin du premier processus, répétez-le pour tous les contrôleurs hors ligne.

CONSEIL : Rappelez-vous que la capacité de la mémoire tampon du contrôleur hors ligne est de 450 événements.

Fenêtre « Options »

Le menu « Options » s'utilise pour établir des méthodes de travail et aussi pour choisir le mode d'opération de votre système. Pour accéder à la fenêtre "Options", sélectionnez View_Options. La fenêtre "Options" est composée d'onglets et ce qui suit donne une description sommaire de leur utilité :

- Général – réglages d'initialisation et d'opérations de vos applications.
- Champs OD – des champs définis par les utilisateurs présents dans le dossier « Personnel »
- Liste d'appel – s'utilise pour définir le rendement et l'opération du rapport « Liste d'appel », et fournit aussi la liste du personnel sur les lieux selon une période choisie.
- Procédures à suivre lors du déclenchement d'alarmes de portes – permet à l'utilisateur de définir des instructions pour l'opérateur lors d'un déclenchement d'alarme de portes.
- Procédures à suivre lors du déclenchement d'alarmes de biens – permet à l'utilisateur de définir des instructions pour l'opérateur lors d'un déclenchement d'alarme pour une infraction envers un bien.
- Procédures GPI – permet à l'utilisateur de définir des instructions pour l'opérateur lors d'un changement dans l'état de l'entrée général.
- Graphiques – permet à l'utilisateur le réglage d'un arrière plan graphique qui affiche les alarmes vectorisées pour raisons d'avertissement lors de déclenchement d'alarmes.
- Options de lecteurs – configuration d'opérations précises en ce qui concerne les lecteurs d'ID ainsi que les protocoles.
- MySQL – format optionnel de base de données pour traiter des activités d'événements d'envergures (installation optionnelle)

Options de mise en service

Vous pouvez configurer les fenêtres qui s'affichent lors du démarrage du logiciel. Pour configurer l'affichage de la fenêtre "Alarmes générales" au démarrage, sélectionnez l'onglet « Général » et cochez l'option appropriée. Vous pouvez aussi configurer l'affichage des fenêtres « Pistage » et « Alarmes de biens ». Nous devons préciser que ces deux fenêtres s'affichent automatiquement lors de l'apparition d'un événement.

Utilisation du signalement sonore

Lorsque des alarmes se déclenchent vous pouvez faire entendre un fichier externe de son, dont le fichier se situe dans le dossier « Par défaut ». Le son associé avec les alarmes générales se retrouve dans le fichier **Program Files\Link\Alarm.wav**. Vous pouvez enregistrer votre propre fichier de son (.wav) et le renommer, si vous désirez qu'un son ou des paroles distinctes soit entendus. La fonction « Pistage d'alarmes » comporte aussi un fichier associé à un son différent à partir de **Program Files\Trace.wav**. Ce fichier peut aussi être personnalisé. Pour activer et désactiver les sons, sélectionnez l'option appropriée à partir de l'onglet « Général ».

Utilisation d'images graphiques des alarmes

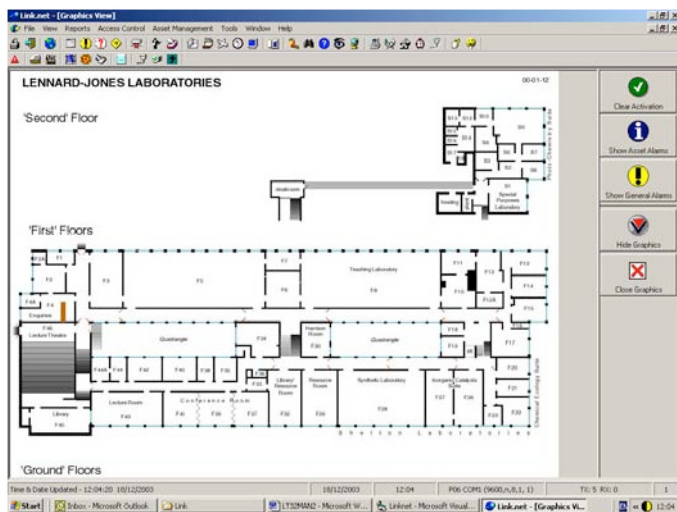
Les graphiques à couche simple sont intégrés dans [Link.net](#) et peuvent être affichés ou non à partir de l'onglet « Général » de la fenêtre « Options ». L'image graphique des alarmes est utile pour délimiter rapidement le type et l'emplacement de l'alarme qui est déclenché.

Importation d'un arrière plan graphique personnel

Pour utiliser les graphiques d'alarmes vous devez dessiner une maquette de votre bâtiment à partir de l'ensemble CAD externe et l'enregistrer en format de fichier bitmap. Vous pouvez utiliser la fonction résidente Microsoft Paint qui est livrée sans frais avec votre système d'exploitation Microsoft. Les dimensions du graphique personnalisé doivent être 940 pixels par 600 pixels pour remplir complètement la vue. Après la configuration des dimensions et du format de votre arrière plan graphique, vous devez l'importer dans le logiciel [Link.net](#). Pour ce faire, sélectionnez l'onglet « Graphique » à partir de la fenêtre « Option » et sélectionnez la touche « Sélectionner graphique ». Une boîte de fichier s'affiche et vous demande de choisir le bitmap cible. Une fois choisie, cliquez « Ouvrir ». Si vous le désirez, vous pouvez prévisualiser le graphique comme une vignette.

Positionnement d'objets d'alarmes

Après la configuration de l'arrière plan graphique, vous devez maintenant mettre en place les objets sur le graphique pour en connaître les emplacements lors de l'affichage du graphique d'alarmes. Sélectionnez « Visualiser graphique » tel qu'illustré ci-dessous:



Les graphiques remplissent la quasi-totalité de l'écran, tout en gardant un espace libre du côté droit. Les alarmes d'objets comportent des références vectorisées pour les dispositifs d'opérations. Les objets [Link.net](#) sont :

- Positions de capteur de contrôle d'accès
- Données d'entrée universelle
- Positions de capteur de gestion de biens
- Bien

Un objet se place par la fonction glisser-déposer et lorsqu'un tout objet est déposé cela déclenche la connexion de la référence vectorisée (de la partie supérieure gauche du bitmap) à cet objet pour le signalement d'alarmes tardives. Vous pouvez positionner tous nos objets de la même manière, mais l'exemple qui suit s'applique aux objets de capteur de contrôle d'accès.

- 1) Sélectionnez la fenêtre "Graphique"
- 2) À partir du menu « Outils ». sélectionnez les positions des capteurs sur le graphique à partir de Tools_Access.

Une liste de tous les capteurs de contrôle d'accès configurés s'affiche du côté droit.

- 3) Sélectionnez le premier objet de la liste et une icône apparaît sur les graphiques.
- 4) Glissez cet objet dans sa position adéquate sur l'image du graphique.
- 5) Sélectionnez l'objet suivant de la liste et répétez la procédure.
- 6) Lorsque tous les objets sont sélectionnés, vous pouvez fermer la fenêtre « Graphique ».

Répétez ce processus pour tous les autres objets tel que requis.

CONSEIL : Pour appeler la signalisation graphique d'alarme, sélectionnez l'onglet « Général View_Options » et sélectionnez la boîte à cocher « Graphique d'appel d'alarme ».

Option de capteur longue portée de contrôle d'accès XTAG

Lorsque vous utilisez les capteurs de longue portée de contrôle d'accès de biens et du personnel XTAG, nous recommandons que le réglage de l'option « Ignorer les ID d'accès inconnus » soit sélectionné. Cela évitera la consignation dans la base de données de toutes les étiquettes actives n'appartenant pas au système. Si vous utilisez un capteur pour la saisie rapide d'ID tel que la surveillance du personnel ou des applications véhiculaires nous recommandons, alors, l'utilisation du réglage "Filtrage temporisé de contrôle d'accès ». Cela réduira la quantité d'étiquettes actives d'ID connu qui sont stockées par filtrage pendant un laps de temps de 2 à 9 minutes. Vous trouverez ces contrôles sur l'onglet « Options » VIEW_OPTIONS_READER.

Options de liste d'appel

[Link.net](#) peut fournir une liste de tous les individus sur les lieux en instantané. La présence sur les lieux se détermine par la dernière transaction faite par l'individu à partir d'un point de contrôle d'accès. Si l'individu présent au point de contrôle d'accès se déplace vers une zone sécurisée (consultez la section Zone) leur état passe, alors, hors lieux et ils ne sont donc pas inclus dans la liste.

La liste peut s'imprimer automatiquement à partir d'une imprimante locale ou à distance et imprimera 15 listes en contenu toutes les 10 minutes. Cela s'utilise pour rapporter le point de rassemblement dans l'éventualité de la survenance d'une évacuation d'urgence. En plus, cette fonction est améliorée par l'utilisation de la technologie de capteur longue portée XTAG. Le rapport peut être déclenché automatiquement par un changement d'état à distance, par une alarme de feu ou par un autre appareil.

Sélection d'une imprimante à distance

À partir de l'onglet "Liste d'appel" dans "option", sélectionnez le nom de l'imprimante appropriée en utilisant les contrôles de déplacement vers le haut ou le bas. Le nom de l'imprimante choisie apparaît dans la boîte adjacente. Il faut savoir que si vous utilisez une imprimante à distance sur un réseau, elle doit être visible lors de la mise en place

de ces réglages. L'installation de partage d'imprimante ainsi que les autres modifications requises, pour votre poste de travail pour permettre la visualisation de l'imprimante ainsi que l'impression à partir de l'imprimante choisie, doit se faire par la division IT. Vous pouvez imprimer une page test vers l'imprimante locale ou à distance en sélectionnant cette touche.

Nous recommandons la sélection de l'option « Absolue » qui permet le stockage du dernier emplacement connu d'un individu à partir du dossier de la base de données des détenteurs de carte. Cela produira des résultats précis lors de la génération du rapport « Liste d'appel ». Si vous désirez que le rapport s'imprime automatiquement, sélectionnez cette option.

Filtrage temporisé de contrôle d'accès (TACF)

Le filtrage temporisé de contrôle d'accès est une fonction qui s'utilise normalement lorsque vous utilisez les capteurs de longue portée pour le contrôle d'accès et le pistage du personnel. Puisqu'il est possible de capter des étiquettes dans une zone à partir d'une certaine distance, nous devons filtrer et éliminer quelques données inutiles. Comme exemple : si un individu traverse une porte d'entrée couverte par un capteur longue portée XTAG ou Wavetrend, nous avons besoin d'uniquement un événement dans un laps de temps à partir de cet emplacement (zone). Le filtrage temporisé de contrôle d'accès (TACF) éliminera par filtrage les données indésirables selon une période de temps programmable (2 à 9 minutes). Pour activer le TACF, sélectionnez l'onglet "Fonction avancé pour capteur" dans le menu "Option". Sélectionnez l'option et réglez une période en minutes à partir du contrôle à défilement (2 à 9). Dès que TACF est globalement réglé comme décrits ci-dessus, nous pouvons exclure ce filtrage pour certains points (zone) de captage. Cela peut être des zones à portée courte passive ou des zones actives à courte portée. Pour configurer cette fonction, ouvrez le dossier du contrôleur approprié et sélectionnez « Désactiver le filtrage d'accès » pour les capteurs choisis.

Ignorer l'ID de carte inconnue

Vous pouvez filtrer indéfiniment l'information générée à partir de cartes ou étiquettes n'appartenant pas au système. Cela ne peut être non important qu'un ID de carte n'appartenant pas au système soit enregistré. Si cela est le cas, sélectionnez cette option à partir de l'onglet « Fonction avancé pour capteur » dans le menu « Option ».

Options de la base de données

Les bases de données utilisées dans le logiciel Link sont par défaut de type Microsoft Access (*.mdb). Ces types de tableaux de base de données fournissent un stockage flexible, compact et accessible de quantités importantes de données. [Link.net](http://link.net) utilise également des structures de bases de données MySQL. Cela permet aussi des opérations de réseautage. Les utilisateurs intéressés par cette fonction peuvent contacter directement CDV pour obtenir plus de renseignements.

Fonctions avancées en échange de données

Exportation d'événements à accès accordé

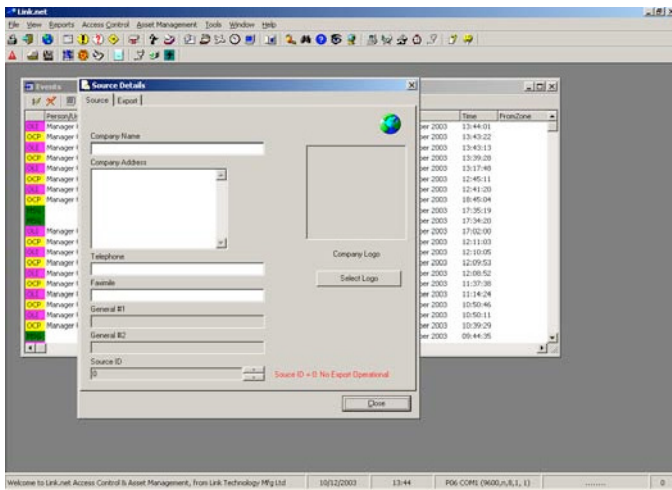
Toutes les données générées et stockées dans ce logiciel sont stockées dans des bases de données de type Microsoft Access. La communication peut être activée par l'interface ODBC ou une requête peut se faire directement avec les applications comme Microsoft Access.

Dans certains cas, vous pouvez souhaiter un autre format pour les rapports et la génération de données à partir de l'application. Vous pouvez alors exporter tous les événements à accès accordés à un fichier à distance pour être traité à une date ultérieure par des applications tiers ou logiciel personnalisé. Le fichier de base de données cible est stocké dans le répertoire par défaut du logiciel Link, mais peut être déplacé vers tout autre chemin sur ou hors de l'ordinateur source. Ce type d'échange de données est Simplex, ce qui indique le flot de données se fait uniquement dans un sens et dans ce cas cela se fait à partir de la source vers la cible.

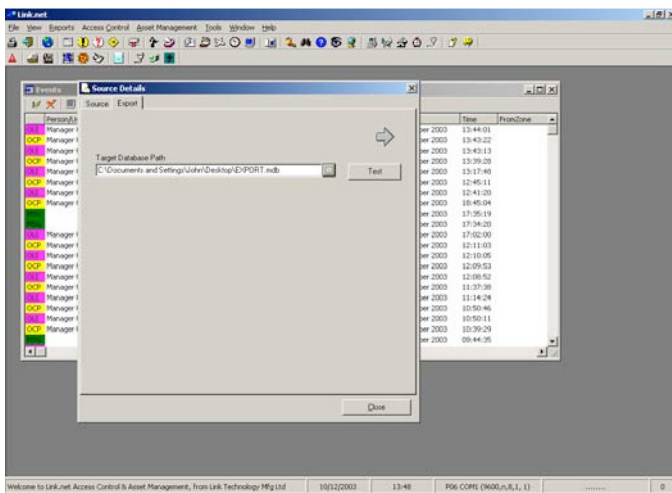
Les utilisations de cette fonction sont:

- La fusion des données de sortie à partir de plusieurs systèmes (sources) Link dans un fichier unique de base de données Microsoft Access.
- La création d'une base de données locale secondaire comportant uniquement les événements d'accès accordés pour analyse ultérieure.
- Le stockage à distance et la protection de l'information d'événements à accès accordés pour des raisons de sécurité et d'information.

Pour créer une exportation à distance des messages à accès accordés, en premier lieu vous devez faire une copie du fichier vide export.mdb situé dans le dossier source Link et le stocker dans le lieu cible. Le lieu cible est l'endroit où les sources chercheront à placer l'information. À partir du menu du fichier de chaque source (système Link), sélectionnez « Détails de source » et la fenêtre suivante s'affichera :



Remplissez les champs de détails de source qui identifie l'origine des données sources dès leurs enregistrements dans le fichier cible à distance (export.mdb). Sélectionnez un numéro d'ID unique de source pour la source du système. En sélectionnant 0 (chiffre par défaut) cela assure qu'aucune exportation de données ne survient. Assurez-vous que toute source comporte un numéro d'ID unique, sauf pour 0 pour empêcher aucune fonction d'exportation à partir de cette source. Sélectionnez l'onglet « Exporter ».



À partir de la touche ... sélectionnez l'emplacement du fichier cible. Vous pouvez tester la connexion en utilisant la touche de source pour vous assurer que le lien approprié est établi.



La connexion au fichier de la base de données cible à distance est réussie.

Information sur le fichier d'exportation

Le fichier cible export.mdb est un tableau de base de données de format Access 2000 (ODBC) Les champs ainsi que leurs types sont expliqués dans le tableau ci-dessus :

Nom du tableau: Global1

Nom de champ	Type de données	Description
RECORDID	Champ AutoNuméro	Numéro unique de rangée
SID	Chaîne	Numéro ID de source
SNAME	Chaîne	Nom de source
ST1	Chaîne	Source champ 1
ST2	Chaîne	Source champ 2
TYPEID	Chaîne	Code à 3 chiffres de type d'événement
TYPE	Chaîne	Description de l'événement
DATE	Chaîne	Date de l'événement
LDATE	Chaîne	Date de l'événement – format long
TIME	Chaîne	Heure de l'événement
READER	Chaîne	Nom et emplacement du capteur
RID	Chaîne	ID du capteur
FROM	Chaîne	Information à partir de la zone
TO	Chaîne	Information vers la zone
PERSON	Chaîne	Individu, si applicable
TID	Chaîne	ID unique de jeton, 8 chiffres
STATUS	Chaîne	ENTRÉE ou SORTIE
ARRIVAL DATE	Chaîne	Date d'événement source (arrivé)
ARRIVAL TIME	Chaîne	Heure d'événement source (arrive)

Ce logiciel permet la génération de requêtes personnalisées à partir de plusieurs applications, incluant Microsoft Access (intégré à Microsoft Office suite). Des programmeurs d'expérience peuvent générer des rapports comportant de l'information exhaustive à partir de sites Link.net individuels ou multiples.

Module VIP d'échange de données

Link.net v4.20 CDV ou les versions ultérieures du logiciel incluent un module qui permet l'échange de données avec des logiciels tiers. Cela se fait par l'intermédiaire d'une base de données Microsoft Access 2000 (VIP_LINK.mdb). Ce fichier se situe dans le dossier cible Link et doit y demeurer pour fonctionner correctement. Des programmes externes doivent localiser ce fichier pour accéder à la fonction d'importation/exportation de données.

Cette base de données contient deux tableaux VIPDATA dont les fonctions sont l'importation de données vers le logiciel Link et EVENTDATA, et l'exportation de données à partir du logiciel Link. Pour activer ce module, sélectionnez View_Options_Advance Reader et sélectionnez l'option « Utiliser le protocole VIP d'importation et exportation à distance ». Vous devez quitter et lancer le module pour compléter la procédure d'activation. L'échange de données peut se faire à partir d'une base de données MySQL. Consultez votre détaillant Link pour obtenir plus de renseignements.

Tableau d'importation VIPDATA

Le tableau d'importation VIPDATA permet par les applications de tiers, l'ajout, l'édition et la suppression de détenteurs de carte dans le système de contrôle d'accès Link par l'intermédiaire de ce tableau de base de données. Les données sont présentées sous forme de rangées dans le tableau d'importation et périodiquement (toutes les 10 secondes) le logiciel Link consulte et entre en action sur ces rangées en fonction des besoins de sa base de données personnelle ainsi que le contrôle du réseau. Le respect de certaines règles de placement de données dans le tableau est important pour que les données erronées soient éliminées. Le tableau qui suit définit les champs ainsi que leur état du tableau d'importation VIPDATA :

Nom du champ	Type de données/caractères	Description	Essentiel
Séquence	Champ AutoNumber	Numéro unique de rangée/lecture seulement	
RECORDTYPE	Chaîne (1)	N = Ajouter, E = Éditer et D = Supprimer	OUI
TOKEN	Chaîne (8)	Numéro de carte à 8 chiffres	OUI
GROUP	Chaîne (2)	Accès de groupe 01-99 (00 = annuler). Corresponds aux définitions de groupe de Link.net . Groupe "01" permet l'accès à toutes les portes et en tout temps. Les autres groupes sont définis dans le logiciel Link.net .	OUI
TITLE	Chaîne (5)	M, Mlle, Mme, etc.	NON
FNAME	Chaîne	Prénom	OUI
MI	Chaîne	Initiale	NON
SNAME	Chaîne	Nom de famille	OUI
IMAGE	Chaîne	Chemin vers l'image jpg pour le jeton	NON

ACTION ED	Chaîne (1)	Toujours « N » lorsque vous le créez. Inactivé. Après le traitement de la rangée Link la supprime	OUI
-----------	------------	--	-----

Pour créer et enregistrer une nouvelle carte dans le logiciel Link vous devez en premier lieu remplir les champs minimum requis d'une rangée du tableau:

RECORTYPE: « N »
 FNAME « John »
 SNAME « SMITH »
 TOKEN « 12345678 »
 GROUP « 01 »
 ACTION ED « N »

Pour éditer un dossier, vous devez remplir la rangée comme suit :

RECORTYPE: « E »
 FNAME « John »
 SNAME « SMITH »
 TOKEN « 12345678 »
 GROUP « 02 »
 ACTION ED « N »

Pour supprimer une carte dans le logiciel Link vous devez remplir la rangée comme suit :

RECORTYPE: « D »
 TOKEN «12345678 »
 ACTION ED « N »

Vous pouvez tester la fonctionnalité du tableau par une entrée manuelle de données à partir de Microsoft Access dans le tableau.

Tableau d'exportation EVENTDATA

Le tableau d'exportation remplit automatique les rangées à partir du logiciel Link.net pendant que et lorsque les événements d'accès accordé sont reçus à partir du réseau de contrôle d'accès. Ces événements peuvent être traités ultérieurement par un logiciel. Link.net ne supprime aucune rangée de ce tableau, puisqu'il est de la responsabilité du logiciel de réception de supprimer les rangées du tableau en activité et indésirable. Le tableau suivant définit les champs ainsi que leur état du tableau d'exportation EVENTDATA:

Nom du champ	Type de données/caractères	Description
<i>EVENTNO</i>	<i>Champ AutoNumber</i>	<i>Numéro unique de rangée</i>
TOKEN	Chaîne (8)	Jeton/numéro de carte unique
DATE	Chaîne (8)	Date en format MMDDYYYY
TIME	Chaîne (8)	Temps en format HH:MM:SS
ZONE	Chaîne	Nom du lecteur utilisé (Link)
STATUS	Chaîne (1)	« I » ou « O » = à l'intérieur ou l'extérieur de la bâtisse/lieu
FROM_ZONE	Chaîne	Emplacement du capteur de carte
TO_ZONE	Chaîne	Emplacement la où le capteur vous suit
ACTIONED	Chaîne (1)	Toujours « N »

Les événements générés par le logiciel Link.net de ce tableau peuvent s'utiliser pour la génération de rapports selon le temps et peut aussi afficher à un logiciel tiers l'information d'événement et d'accès

Annexe A : [Link.net](#) Matériel

Le concept [Link.net](#) est que les systèmes divers autonomes (contrôleur à distribution intelligente) soient tous branchés à une sortie réseau (jusqu'à 1200m) gérée par le logiciel [Link.net](#) installé sur votre PC ou par interface (normalement RS232) à votre poste de travail. Chaque contrôleur gère les biens qui y sont attribués ainsi que les individus. À l'intérieur de chaque contrôleur, nous retrouvons ce qui suit :

- Une base de données qui inclut tous individus et biens
- Une horloge et calendrier de traitement en temps réel (autonome)
- Une mémoire pour stocker les événements et activités (500)
- Une structure de mémoire globale non volatile de 10 ans
- Une source d'alimentation avec surveillance de défaillances (en option)
- Un sous-système de l'horloge de surveillance (Watchdog)
- Communications bidirectionnelles simultanées RS485 comportant un débit en bauds de 8 entrées et 4 sorties à relais

S'il y a une défaillance du réseau, le logiciel [Link.net](#) se ferme, ou le câble de branchement réseau entre les contrôleurs est perturbé. Chaque contrôleur individuel (net) demeure en opération et les événements seront stockés localement dans la mémoire tampon de chaque base de données non volatile de contrôleur.

Planification de l'installation

Lorsque vous projetez une installation, installez et testez chaque contrôleur comme s'ils étaient des systèmes individuels.

Par lui-même le contrôleur requiert une connexion par fusible non commuté d'un ampère, installé par un électricien qualifié. Telle qu'il a été spécifié dans les réglementations de l'IEEE 16, la connexion doit se composer d'un câblage principal d'une classification appropriée. Lors de l'installation d'un contrôleur pour contrôle d'accès vous devez porter attention à la pose des verrous électromécaniques. Les points à examiner doivent inclure :

- Si deux verrous sont en utilisation sur un réseau de contrôle d'accès à partir d'un bloc d'alimentation (PSU), chaque verrou ne doit pas excéder une consommation en courant de crête de 500m Ampère.
- Chaque verrou doit comporter un « para-surtenseur » ou « diode » de polarité appropriée qui se fixe sur les terminaux de verrouillage pour ainsi éviter des dommages aux commandes électroniques pouvant être déclenchées par une force contre-électromotrice en différence de potentiel. Utilisez ces dispositifs même si vous avez des PSU dédiés pour le verrouillage.
- Installez toujours des verrous de qualité et si vous avez des doutes à ce sujet, consultez un serrurier qualifié en installation de verrous électromagnétiques.
- Si le dispositif de verrouillage est de type sécurité intégré (auto-blocage), alors fixez toujours un interrupteur en série vert de relâchement de disjoncteur avec l'alimentation en électricité du verrou située du côté sécurisée de la porte pour assurer le bon fonctionnement de la sortie d'urgence. Si vous utilisez une version à émission double, vous pouvez alors surveiller le risque potentiel en sécurité par l'interface GPI de chaque contrôleur.

Produits de connectivité IP LAN/WAN

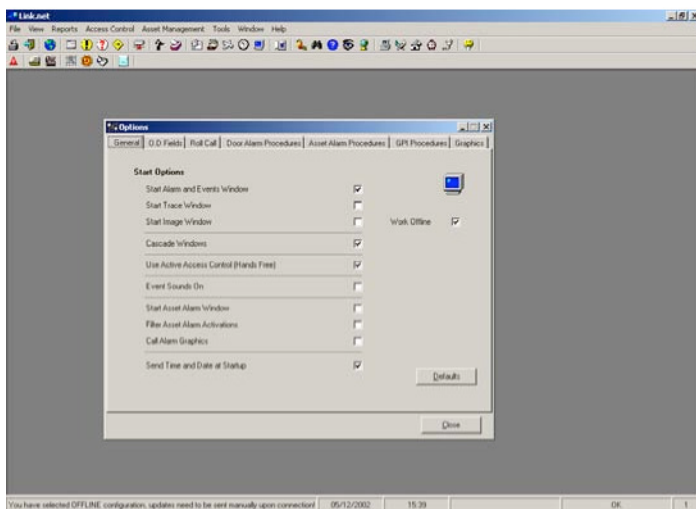
Nous pouvons utiliser le LAN ou WAN existant du client lors de la connexion des contrôleurs. Cela permet l'utilisation de l'infrastructure de câblage existante, ce qui réduit énormément les coûts et la durée de mise en service. De plus, cela permet une installation plus aisée des contrôleurs dans divers emplacements géographiques ainsi que dans les bâtisses. Pour se faire, vous pouvez utiliser la gamme de produits de contrôleurs avec protocole internet (IP) du logiciel Link. Ces produits s'identifient par les lettres IP inscrites à la fin du numéro de la pièce, p. ex. LT-20IP est une version de connexion IP/LAN/WAN pur une unité standard LT-20AC en contrôle d'accès.

Les produits IP se branchent directement au LAN existant du client par un système structuré de câblage et s'installe avec un type de câblage CAT5 ou CAT5E et des prises RJ45. Tous les produits IP sont offerts avec une prise de courant RJ45 supplémentaire intégrée pour permettre une connexion rapide par un cordon de raccordement CAT5. Le logiciel [Link.net](#) soutient la connexion du matériel par IP ou/et par un câblage local conventionnel.

De plus, les contrôleurs IP peuvent s'utiliser comme passerelle vers des contrôleurs additionnels LT-20AC et LT-30AM à câblage standard. Cela est idéal pour lors d'un besoin de transfert d'une bâtisse à l'autre puisque la version IP agit comme plate-forme. Le contrôleur IP se branche à une prise de LAN locale et des contrôleurs standards subséquents sont câblés à partir de cette unité Belden 8723 comme s'ils étaient branchés directement au PC par un réseau câblé de contrôleurs de lieu.

Travail hors ligne

Il est normal que tous les contrôleurs soient retournés par réseau vers un seul PC (mode en ligne). Vous pourriez souhaiter dans certaines circonstances, gérer les modifications apportées à votre système en étant HORS LIGNE. Dans ce cas, chaque contrôleur sera autonome et ne sera plus en réseau. Les conséquences sont que toutes les modifications faites à partir de votre PC ne mettront pas à jour les contrôleurs concernés puisqu'il n'existe plus aucune connexion physique. Les modifications que vous faites sont stockées dans la mémoire tampon et doivent donc être appliquées au contrôleur, tel qu'expliqué dans la section « Utilisateur » de ce manuel. Pour régler cette fonction, sélectionnez View_Options et cochez la boîte « Travail hors ligne » si vous désirez utiliser ce mode de travail. Si un travail en ligne est requis, alors ne cochez pas la boîte.



Cochez la boîte « Travail hors ligne » si vous n'êtes pas en réseau avec les contrôleurs.

Contrôleurs Link.net

Les contrôleurs Link.net sont fournis dans une large enceinte métallique avec un bloc d'alimentation contrôlé par un microprocesseur de 2.5 ampères. Les caractéristiques du bloc d'alimentation sont comme suit :

- Capacité de 2.5 ampères (2 ampères pour verrouillage)
- Circuit de charge de batterie pour une batterie plomb-gel de 7Ah
- Protection de décharge profonde de batterie à <10.7 volts, LED principale « En marche »
- Batterie OK / LED actuel
- LED general pour défaillance
- Défaillance de la batterie / arrêt du relais de sortie de l'alarme du réseau électrique
- Fusible à 4 point de contact

Lorsque le contrôleur est mis sous tension le LED vert du réseau électrique s'allume. Le PSU géré par microprocesseur vérifie la batterie ainsi que les autres paramètres et allumera le voyant de défaillance s'il y a existence d'un trouble. De plus, le relais d'alarme changera d'état s'il y a présence de troubles. Le relais pour l'alarme ainsi que l'interrupteur de violation du couvercle peuvent être supervisés dynamiquement par les Entrées générales du système permettant une supervision par l'opérateur de toute panne de l'enceinte ou tout bloc d'alimentation. Pour les unités comportant un PSU intégré, il y a une fonction d'autoanalyse étendue pour les pannes. La batterie est supervisée en continuellement pour assurer et afficher un état adéquat de charge.

Généralités

L'unité est réglée en usine pour fournir une sortie nominale de 13.86 VDC. Lors du réglage de l'accumulateur au plomb-acide, il peut être chargé et ensuite avoir une charge d'entretien pour maintenir un état optimal de fonctionnement. Les batteries ayant une fourniture en voltage supérieur à 9 VDC sont nécessaires pour activer le circuit de charge. Sur le panneau avant, vous retrouvez Les LED suivants :

LED VERT = bon fonctionnement du réseau électrique
 LED ROUGE = état de panne générale
 LED JAUNE = batterie en cours de chargement/charge basse

Lors de défaillances du réseau électrique, le système est alimenté par une batterie rechargeable (si elle est en place). Un circuit de déconnexion automatique (protection de la batterie lors de décharge importante) s'activera lorsque la borne de réseau en tension perturbatrice devient trop basse pour protéger la batterie. Le relais de panne change d'état lors de toute occurrence de panne. Ces conditions sont : batterie manquante, court circuit ou une panne totale du réseau électrique, défaillance du fusible de sortie, ou un court circuit de la charge de sortie. Conjointement avec le relais, le LED ROUGE clignotera pour indiquer le niveau et la raison de la panne. Le niveau et la raison des pannes sont indiqués comme suit :

Alarme Niveau 1 = Défaillance du réseau électrique
 Alarme Niveau 2 = Batterie en panne
 Alarme Niveau 3 = Fusible sauté

Note: Le niveau d'alarme fait référence au nombre de clignotements du LED ROUGE. Les niveaux s'allument par ordre de priorité de façon tel que s'il y a existence d'une alarme de niveau 2 et 3, alors uniquement l'alarme de niveau 2 est affichée. Lorsque le LED du réseau principal s'allume, cela indique un manque du réseau électrique. Le LED ROUGE clignotera et le relais sera activé après approximativement une minute.

Caractéristiques du bloc d'alimentation intégré

Entrée du réseau principal	230/240 Volts AC 50Hz
Sortie de charge	2 Amp à 13.8 VDC
Variation de tension de charge	0.9% maximum
Fluctuation de sortie	50mV RMS maximum
Niveau de déconnexion de la batterie	10 VDC nominal
Période de recharge de la batterie	24 heures à 80% de sa capacité (7Ah cellule)
Environnement	-10 à + 40 C jusqu'à 95% d'humidité relative
Fusible FS1 d'entrée secondaire AC	F5A
Fusible FS2 sortie DC	F4A
Fusible FS3 Charge de batterie	F4A
Bloc du réseau électrique	F2A

Information d'installation

Lors de la mise sous tension, le LED ROUGE passe par une séquence de clignotements. Si la batterie n'est pas réglée ou si elle est sous la différence de potentiel requise, le LED ROUGE restera allumé. Si une batterie de qualité est mise en place le LED ROUGE se fera et le LED JAUNE s'allumera, pour indiquée qu'elle est en cours de chargement. Pendant les cinq premières minutes après la mise sous tension initiale, vous pouvez tester le fonctionnement de la batterie. La déconnexion de la batterie pendant cette période déclenchera le clignotement du LED ROUGE et le relais d'alarme changera d'état après une minute de déconnexion. Suite à cette période initiale, de test de fonctionnement la batterie revient au mode normale et sera testé à tous les quatre heures pour vérification de pannes. La fonction de panne de batterie peut se vérifier en tout temps soit par la simulation d'une panne du réseau électrique ou d'un fusible sauté. Le test de panne de batterie est disponible pour 5 minutes pour la simulation et correction de la panne, et ensuite retournera à la normale selon les caractéristiques décrites dans le paragraphe précédant

Installation d'un contrôleur d'accès Link (LT-20AC)

La carte de circuit intégré (PCB) Link.net est normalement placée à l'Intérieur, dans l'enceinte en métal accompagné de son bloc d'alimentation (PSU) ainsi que le chargeur. Le PCB Link.net est situé dans le coin droit inférieur de cette enceinte. Les groupes de terminaux ainsi que leurs fonctions sont indiqués ci-dessous :

Groupe du terminal	Terminaux	Type de câble	Description
MON1	DC1, DC1	CAT5 sécuritaire	Porte magnétique à contrôle numérique 1contact (Link hors usage si non utilisé)
MON2	DC2, DC2	CAT5 sécuritaire	Porte magnétique à contrôle numérique 2 contacts (Link hors usage si non utilisé)
RELAY1	C, NO, NC	CAT5 sécuritaire	Relais pour verrou de la porte 1
RELAY2	C, NO, NC	CAT5 sécuritaire	Relais pour verrou de la porte 2
RELAY3	C, NO, NC	CAT5 sécuritaire	Relais pour alarme de porte 1
RELAY4	C, NO, NC	CAT5 sécuritaire	Relais pour alarme de porte 2
CARDREADER1	5,0, CL, DL, GL	Belden 9536	Lecteur de carte 1 (porte 1)
CARDREADER2	5,0, CL, DL, GL	Belden 9536	Lecteur de carte 2 (porte 2, porte 1 sortie)
Link.net COM	TX+,TX-,RX+,RX-	Belden 9503, CAT5	Réseau de communication 4-fils
EXIT1	EX1, EX1	CAT5 sécuritaire	Bouton à pression de sortie de porte 1
EXIT2	EX2, EX2	CAT5 sécuritaire	Bouton à pression de sortie de porte 2
GP INPUTS	GPI1-4 et une reprise commune pour tous	CAT5 sécuritaire	4 entrées d'usage général pour surveillance de lieu. Interrupteur ouvert/fermé pour tous les moniteurs d'entrée. Aucune différence de potentiel ne doit être appliquée à ces terminaux.

Capteurs de contrôle d'accès

Ci-dessous sont listés des capteurs de contrôle d'accès variés que vous retrouverez dans notre système. Si vous avez besoin d'un autre type de capteur qui n'est pas dans la liste, consultez votre fournisseur CDV pour obtenir plus de renseignements. Les dernières versions des contrôleurs Link (micrologiciel séries 10) soutiennent les interfaces Wiegand et Horloge & Données des standards dans l'industrie. Le type d'interface est choisi à partir du logiciel soit par réglage global ou par niveau de contrôleur individuel. Les réglages par défaut sont Horloge & Données Standards Link.

Interface standard de capteur Horloge et Données Link (par défaut)

Capteur de proximité Link LT-100R	Couleur de câble du capteur	Terminal PCB Link
5-12V DC	ROUGE	5V (capteur 1 ou 2)
0V	NOIR/NOIR	0V (capteur 1 ou 2)
HORLOGE	BLANC	CL (capteur 1 ou 2)
DONNÉES	VERT	DA (capteur 1 ou 2)
LED VERT	BRUN	GL (capteur 1 ou 2)
SORTIE OPTIQUE D'INVOLABILITÉ*	VIOLET	(bas lorsque fixé au mur)

* Le signal de la sortie optique sera bas (fermé) lorsque fixé contre une surface. Si vous utilisez cette fonction, assurez-vous que le capteur est bien fixé, mais pas trop fortement. La distance entre le câble Belden 9536 et tout port de capteur doit être au maximum 75 mètres. Veuillez prendre note que le capteur de proximité LT-100R est doté d'un connecteur de style Molex qui doit se fixer à une connexion male appropriée pour allonger le câble du capteur. Optionnellement, vous pouvez en couper une partie et faire une terminaison câble à câble. L'utilisation de carte blanche de style ISO en contrôle d'accès LT-100C ainsi que des capteurs éloignés de surfaces ou structures métalliques, offre le meilleur rendement en captage. Ne fixez jamais des capteurs de proximité dos à dos sur la même porte, car cela pourrait perturber leurs champs mutuels engendrant une performance médiocre. Prenez l'habitude de fixer les capteurs sur les côtés opposés d'une entrée.

Lecteur de cartes à puce intelligente Mifare LT-8000	Terminaux de lecteurs	Terminal PCB Link
12V	1	12V DC
0V	2	0V (lecteur 1 ou 2)
D0/STROBE	3	CL (lecteur 1 ou 2)
DONNÉES D1	4	DA (lecteur 1 ou 2)
FORMAT	5	0V (lecteur 1 ou 2)
LED	6	GL (lecteur 1 ou 2)

La distance maximale du câble Belden 9536 est de 75 mètres.

Lecteur à bande magnétique CDV DGLM/L externe ou interne	Couleur du lecteur	Terminal PCB Link
Alimentation 4.5 – 5.5 V	Brun	5V (lecteur 1 ou 2)
GND	Gris	0V (lecteur 1 ou 2)
Horloge	Orange	CL (lecteur 1 ou 2)
Données	Jaune	DA (lecteur 1 ou 2)
LED de contrôle*	Blanc (Résistance en série 220)*	GL (lecteur 1 ou 2) *
	Vert	Non utilisé

La distance maximale de prolongement de câble Belden 9536 est de 50 mètres. Le fil blanc du LED de contrôle doit avoir une résistance en série de 200 ohms rendus au terminal (GL). Le LED du lecteur est rouge en tout temps et lorsqu'une carte valide est utilisée pour ouvrir une porte le voyant rouge s'éteint. Si une carte non valide est glissée dans le lecteur, le LED demeure ROUGE.

LED Fil blanc (DGLM-L)

220 Terminal GL (Contrôleur Link)

Lecteur d'accès à bande magnétique MR 4130 Interne	Couleur du lecteur	Terminal PCB Link
Alimentation 4.5 – 5.5 V	Rouge/Orange	5V (lecteur 1 ou 2)
GND	Noir/écran	0V (lecteur 1 ou 2)
Présence de carte	Bleu	Non utilisé
Impulsion	Jaune	CL (lecteur 1 ou 2)
Données	Brun	DA (lecteur 1 ou 2)
LED de contrôle	Vert	GL (lecteur 1 ou 2)

La distance maximale du câble Belden 9536 est de 75 mètres. Le LED demeure éteint jusqu'à la lecture d'une carte valide et s'allumera de vert pour la période de verrouillage.

Lecteur d'accès à bande magnétique MR 51T2B externe	Couleur du lecteur	Terminal PCB Link
Alimentation 4.5 – 5.5 V	Rouge	5V (lecteur 1 ou 2)
GND	Noir/écran	0V (lecteur 1 ou 2)
Présence de carte	Bleu	Non utilisé
Impulsion	Jaune	CL (lecteur 1 ou 2)
Data	Brun	DA (lecteur 1 ou 2)
Commande numérique	Vert	Non utilisé
LED de contrôle	Orange	GL (lecteur 1 ou 2)

La distance maximale du câble Belden 9536 ou CAT5 est de 75 mètres. Le LED du lecteur est rouge en tout temps jusqu'à utilisation d'une carte valide et s'allumera de vert pour la période de verrouillage.

Capteur longue portée d'étiquette active XTAG XT200A	Terminal de contrôle	Couleur de câble Belden 9535
5V	5V	Rouge
D1	DA (capteur 1 ou 2)	Brun
D0	CL (capteur 1 ou 2)	Blanc
GND	0V (capteur 1 ou 2)	Noir/écran
GLED	GL (capteur 1 ou 2)	Vert (ne branchez pas ce contrôleur lorsqu'y a des étiquettes multiples sur les
	Réglages d'interrupteur DIP lors d'opérations normales : SW1-SW5 FERMÉ. Consultez la fiche du SW3 sur les lecteurs jumelés sur un à deux contrôleurs de capteur comme le Link LT-20AC.	SW5 lorsque OUVERT est en mode de réglage pour tester la portée

Le capteur longue portée de capteur d'étiquette active XT-200A détectera et décodera des étiquettes individuelles ou multiples à partir de son champ omni directionnel. Le champ peut se régler pour une portée de 4 à 25 mètres. La portée exacte dépend des conditions environnementales ainsi que l'emplacement du capteur. Une petite vis de réglage situé sur la partie inférieure droite du capteur règle le champ à partir d'aucune perception jusqu'à une pleine portée de perceptions.

Montage

Le capteur XTAG XT-200A est conçu pour se fixer à proximité d'une porte ou ouverture d'une hauteur comprise entre 1200 à 1400 mm. Nous ne recommandons pas que le capteur soit fixé au-dessus de la porte, mais plutôt dans le même emplacement qu'un lecteur de contrôle d'accès conventionnel. Le capteur doit toujours être fixé en station verticale. Le capteur XT-200A est doté d'une antenne interne qui perçoit plus efficacement des étiquettes à partir de l'arrière et l'avant de l'unité. Évitez le montage du capteur sur ou près de larges surfaces métalliques puisque cela peut être la cause d'une performance médiocre en captage. Le XTAG XT-200A ne peut capter des étiquettes actives à travers d'objets en métal et sa performance de captage des étiquettes sera perturbée par de larges obstacles denses. Donc, lors de l'installation considérez la ligne de mire pour assurer une performance optimale de captage.

Test et réglage de la portée

Le capteur XTAG XT-200A peut se régler pour capter des rayons variables par son fonctionnement omni directionnel. Nous ne recommandons pas un réglage inférieur à 4 m (diamètre 8 m) du rayon d'action puisque des variations de puissance du rayon d'action ainsi que l'orientation de l'étiquette peuvent diminuer la performance en captage. Après la mise en place du câblage Belden 9535 entre le capteur et le contrôleur hôte, tout en respectant une distance de moins que 30 mètres, réglez l'option du capteur à « Réglage de test de portée » en plaçant l'interrupteur SW5 en position OUVRETE. Pour tester la portée de perceptions d'étiquettes, utilisez toujours une étiquette uniquement tout en conservant les autres à bonne distance de la zone de test pour ainsi éviter des données de perception erronées. Des étiquettes additionnelles peuvent être testées pour confirmer que le réglage de la portée désirée est approprié lorsque la portée initiale de perceptions est réglée. Lorsque ce test est complété assurez-vous que l'interrupteur du SW5 soit FERMÉ pour désactiver l'option *Test de réglage de la portée*.

Lorsqu'en mode de *Test de réglage de la portée* le LED du capteur est vert et le relais interne émettra un **déclat d'une seconde** lorsqu'une étiquette est perçue. Aucune donnée à partir de l'étiquette n'est décodée ni transmise au contrôleur lorsqu'en mode *Test de réglage de la portée*. Utilisez un potentiomètre d'ajustement et réglez et testez à nouveau les ajustements. **L'ajustement de la portée est de 25 rotations bout à bout dans le sens des aiguilles d'une montre, ce qui engendre un accroissement de la portée et un ajustement de la portée dans le sens contraire des aiguilles d'une montre produisant l'effet contraire.** Lorsque la portée approximative est réglée alors des rotations d'un ou un demi-tour dans la direction appropriée donneront un réglage de précision. Prenez note que le capteur peut prendre 2 secondes ou plus pour se stabiliser après un ajustement, procédez, alors, à un test soigneux tout en tenant compte de ce délai.

Options d'opération du capteur XT-200A

Le capteur d'étiquette active XTAG XT-200A comporte des modes d'opérations varies qui se configurent par les commutateurs DIP à cinq directions situés sur l'unité. Le réglage par défaut pour le mode d'opération standard lorsque branché à un contrôleur d'accès est que tous les interrupteurs sont en position FERMÉ. Les utilisations précises des interrupteurs sont décrites ci-dessous, pour ajustement par le client, si requis :

Interrupteur XT200	Opération	Ouvert	Fermé	Notes	Link (par défaut)
SW1	Interface	Wiegand 26Bit	Horloge et données		FERMÉ
SW2	Vérification de bits LRC	Transmission des bits LRC	Bits LRC non transmis	Aucun fonctionnement	FERMÉ
SW3 **	Dispositifs jumelés à un contrôleur	Une entrée du capteur lors de délai de pré-transmission	Capteur à deux entrées avec délai de post transmission		Capteur 1 FERMÉ Capteur 2 OUVERT

SW4	Verrouillage de portée d'étiquettes	Lorsqu'une étiquette n'est plus perçue un avertissement est transmis 4 fois et puis verrouillé	Envoie par transparence de l'étiquette	Verrouillage de 8 secondes après déplacement de l'étiquette de la portée (OUVERT).	FERMÉ
SW5	Mode test	Réglage de test portée, en opération	Mode d'opération normale		FERMÉ

**** Une bonne procédure à suivre en réglage est de faire des réglages contraires pour les interrupteurs DIP du SW3 pour chaque capteur jumelé, lorsque deux capteurs sont branchés à un seul contrôleur d'accès à partir d'entrées de captage indépendantes.**

La distance maximale de câblage Belden 9535 à partir du capteur jusqu'au contrôleur hôte est de 30 mètres. Ne branchez jamais l'écran à la terminaison du capteur et éboutez et isolez le câble. L'écran ainsi que le conducteur noir doivent se brancher à 0V à l'entrée du contrôleur du capteur.

Étiquettes actives XTAG

Les étiquettes actives XTAG sont conçues pour les individus et les véhicules. **Lors d'une mise en place dans un véhicule, évitez que la fonction de filtrage ne se fasse à partir de la carrosserie en métal.** Placez les étiquettes actives sur le pare-brise ou derrière les grilles à air ou sur les pare-chocs ou la carrosserie en plastique. Lorsque des individus doivent porter des étiquettes, l'efficacité de la perception dépend grandement du rayon de perception. Lorsqu'un rayon de perception est plus large que 10m les étiquettes peuvent, alors, se porter sur l'individu ou dans des portefeuilles ou poches. Lorsqu'un rayon de perception plus petit est requis nous recommandons, alors, l'utilisation de cordons de cou à décrochage, des chaînes de cou sans nickel ou des clips de revers de chemise. Les étiquettes actives sont conçues pour offrir un meilleur rendement lorsqu'en **position à plat et tombant vers le bas et à une distance supérieure par rapport à la rainure de montage.** L'étiquette active standard XTAG transmet un signal codé sécurisé toutes les 2 secondes, alors quand rayon de perception est plus petit, des portées différentes peuvent être captées lors d'une avance vers le capteur. Le tout dépend du temps de transmission de l'étiquette et aussi si son fonctionnement est parfaitement normal.

Interface de capteur 26 Bits Wiegand de qualité industrielle (en option)

Vous pouvez sélectionner cette option dans le logiciel à partir du menu « Options » Options Reader. Vous devez aussi transmettre cette information à partir de la commande « Format du capteur de contrôle d'accès », lorsque tous les contrôleurs sont en ligne. Le logiciel vous demandera alors d'indiquer le type d'interface qui sera configuré.

Capteurs de proximité CDV DGLI/W, DGLP/W & DGLP/TW	Connexion du capteur	Terminal PCB Link
+	+	Bloc d'alimentation 12VDC
-	-	0V & Écran (capteur 1 ou 2)
H	H	
D0	D0	CL (capteur 1 ou 2)
D1	D1	DA (capteur 1 ou 2)
R	R	
V	V	GL (reader 1 or 2)

Sélectionnez la fonction de captage de 26 bits sur l'unité en plaçant le pont ST5 à la position 3 (puisque la documentation du lecteur peut être trompeuse, sélectionnez toujours la position 3). De plus, sélectionnez les résistances 5V internes de rappel vers le niveau haut sur le pont ST4. Utilisez une longueur maximale de 100m de câblage Belden 9536 pour chaque capteur.

Lecteur biométrique d'empreinte digitale CDV DGID/W	Connexion du lecteur	Terminal Link PCB
+	+	Bloc d'alimentation 12VDC
-	-	0V & Écran (lecteur 1 ou 2)
H	H	
D0	D0	CL (lecteur 1 ou 2)
D1	D1	DA (lecteur 1 ou 2)
R	R	
V	V	
P	Interrupteur à pression N/O (Avertissement)	
M	Interrupteur à pression N/O (Avertissement)	

Les terminaux P et M permettent l'envoi d'un appel d'avertissement à partir de l'interrupteur local jusqu'au logiciel Link. Cette fonction est optionnelle, mais peut s'utiliser si un utilisateur rencontre des troubles lors de l'utilisation de son modèle d'empreinte digitale biométrique. De plus, vous devez fixer le connecteur RS232 fourni à l'intérieur d'une distance de 15m pour le téléchargement vers le lecteur d'empreinte digitale biométrique. Lorsque vous effectuez ce

type de connexion entre le lecteur et le contrôleur Link, n'utilisez jamais le relais intégré du dispositif de verrouillage puisque ce dernier est branché directement au contrôleur Link. Sélectionnez la fonction de lecteur 26 bits en plaçant le pont ST1 à la position 3. Choisissez aussi, les résistances 5V internes de rappel vers le niveau haut en laissant le pont ST2 ouvert. Utilisez une longueur maximale de 100m de câblage Belden 9536 pour chaque lecteur. Nous recommandons que vous lisiez et compreniez la documentation précise du lecteur d'empreinte digitale biométrique DIGI/ID/W.

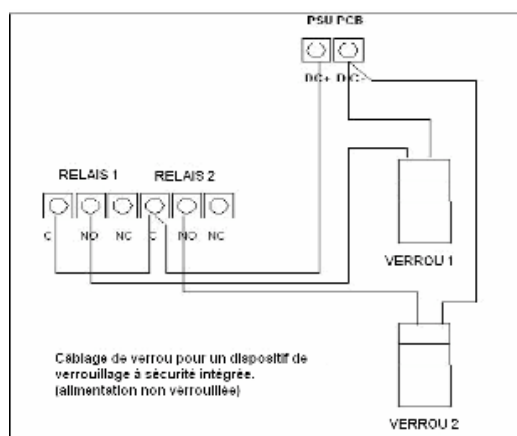
Connexion de boutons de sortie, contacts de portes et entrées générales

Les dispositifs ci-dessus sont tous branchés par une connexion à deux fils aux connexions des terminaux appropriés du PCB (carte de circuit intégrée) principale Link.net. Vous pouvez utiliser des câbles standards, CAT5 ou blindés pour ces connexions et en plus vous pouvez les rassembler ensemble à l'intérieure d'une même gaine (multiconducteur).

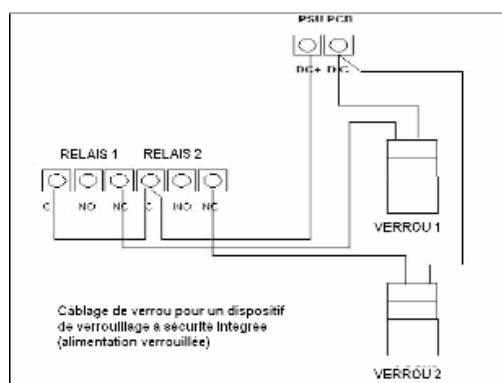
Pour toutes circonstances la distance maximale entre toutes entrées à partir de son terminal est 50 mètres.

Note : Aucune différence de potentiel ne doit être appliquée à ces entrées, car cela causerait des dommages irréparables au PCB. Surveillez l'état d'entrée/de sortie pour vous assurez qu'il n y aucune différence de potentiel (interrupteurs).

Connexion de dispositifs de verrouillage



Câblage à sécurité intégrée (branchez toujours une grille d'arrêt directement au dispositif de verrouillage)



Câblage à sécurité intégrée (branchez toujours une grille d'arrêt directement au dispositif de verrouillage)

Grille d'arrêt de verrou

Le branchement d'un dispositif de grille d'arrêt dédiée ou une diode directement au réseau des terminaux de verrou est essentiels pour éviter un retour EMP de différence de potentiel vers le dispositif de verrouillage inductif causant des dommages aux composants électroniques. Des dispositifs appropriés sont :

Numéro de pièce	Type	Connexion	Détails
IN4001/2/3/4	Diode	Polarisée	Faible coût et disponible, mais doit se brancher correctement à la cathode (délimité par une ligne autour du corps) qui est branchée au coté positif de différence de potentiel du verrou.

PKE36V	Tension résiduelle transitoire	Non polarisée	Plus dispendieux, mais fournit un meilleur rendement et est plus rapide. Capacité de connexion bidirectionnelle.
--------	--------------------------------	---------------	--

Test d'un contrôleur d'accès [Link.net](#)

Avant de brancher le réseau, [Link.net](#) quelques tests de bases peuvent se faire pour vérifier l'installation du réseau. Mettez le contrôleur sous tension à partir du **fusible non commuté de l'embase du poteau du réseau électrique**.

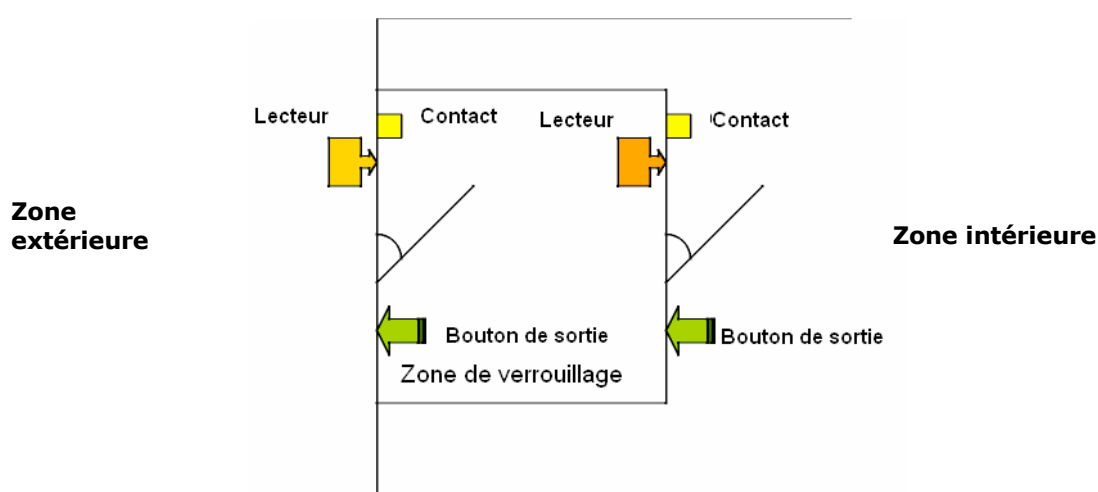
1. **Testez pour obtenir environ 13.6VDC** aux terminaux PSU PCB DC.
2. Assurez-vous que le LED vert du PCB principal est allumé.
3. Chaque lecteur de cartes doit s'allumer en rouge (type dépendant).
4. Lorsqu'un jeton y est présenté, il peut émettre un bip sonore (type dépendant).
5. Assurez-vous que les boutons de sorties déverrouillent la porte pour une période d'environ 7 secondes et qu'ensuite elle se verrouille.
6. Déverrouillez le verrou de la porte et ensuite ouvrez le contact du moniteur de porte pour vérifier que les relais d'alarme fonctionnent pendant que la porte est ouverte de force. Les LED sur le PCB principal de [Link.net](#) montrent l'état des sorties de relais.

Si vous découvrez des troubles, vérifiez à nouveau tout le câblage et effectuez de nouveaux tests. Procédez de la même manière pour tous les autres contrôleurs et si tout est conforme vous pouvez amorcer la procédure de mise en place du réseau.

Installation de verrouillage entre deux portes

Un seul contrôleur vous permet d'établir un système de verrouillage (ou sas) pour traverser deux portes. Un verrouillage se compose d'une porte extérieure et intérieure avec un espace vide entre les deux.

Un seul individu à la fois peut traverser les deux portes, mais la porte extérieure doit être physiquement fermée et verrouillée avant que la porte intérieure puisse s'utiliser et ouvrir. La même procédure s'applique pour une traversée en sens inverse. Les boutons de sortie sont normalement utilisés pour un déplacement dans la direction contraire.



Pour que le verrouillage fonctionne correctement le contrôleur doit être réglé à la position 0 (interrupteur DIP 6, fermé). Normalement les contacts de portes fermées devraient s'utiliser sur les deux portes. Si la sortie se fait en le lecteur (au lieu des boutons) vous devez en plus installer des **contacts bipolaires** ainsi qu'ajouter un contrôleur LT-XXAC.

utilisant

Installation d'un contrôleur LAN IP (LT-20IP)

Le LT-20IP consiste en un contrôleur LT-20AC qui comporte un PBC de connectivité LAN additionnelle ainsi qu'un port secondaire [Link.net](#) pour permettre le câblage d'un contrôleur local de réseau aux contrôleurs LT-20AC standard subséquents. Tous les branchements pour des lecteurs, du verrouillage et des aménagements pour l'alimentation pour le contrôleur d'accès standard LT-20AC se font de la même manière que décrite dans les sections précédentes. Cependant, la configuration d'une adresse unique de contrôleur Link sur le PCB principal demeure essentielle (consultez la section « adresse de contrôleurs »). Cette section traitera de la connectivité et de la **d'adresses** pour la carte LAN dans l'infrastructure existante LAN/WAN. Pour la compréhension de cette section, supposons que vous ayez des connaissances de base en réseau local et création d'adresse IP et que vous avez sécurisé en fonction. Pour établir une connexion entre le LT-20IP et le logiciel [Link.net](#), vous devez suivre les étapes qui suivent :

qu'un
sections
création
nous
un LAN
étapes

- Branchez le contrôleur IP au LAN/WAN avec un câble de raccordement CAT5 et mettez-le sous tension.
- Prenez en note l'adresse MAC unique, l'emplacement et l'adresse du contrôleur Link de la carte LT-20IP LAN.
- Installez et utilisez l'utilitaire du logiciel « Configuration de l'activation de réseau » pour communiquer et réglez l'adresse IP et le masque de sous-réseau pour chaque contrôleur IP.
- Attribuez et configurez une référence pour le contrôleur sur le logiciel [Link.net](#).
- Vérifiez le fonctionnement de la connectivité à partir du serveur [Link.net](#).

Connexion LAN

Le PCB LAN sur le contrôleur LT-20IP accepte un câble de raccordement standard RJ45 UTP d'une longueur maximale de 305 mètres à partir d'un port d'échange LAN ou 30 mètres **à partir d'une interface de connexion RJ45**. Les raccords de fil fabriqués commercialement sont recommandés et sont exactement du même type que ceux utilisés pour brancher un PC à un relais LAN.

Réglages de contrôleur pour MAC

Chaque LT-20IP qui est fabriqué porte une adresse unique MAC, imprimée sur une petite étiquette argentée. Une adresse MAC est un nombre qui est unique à chaque dispositif LAN et est utilisé par le LAN pour trouver des **dispositifs à niveau bas de logiques pour des raisons de mise en service**. Vous devez garder ce numéro en dossier, ainsi que l'adresse unique du contrôleur Link et l'emplacement physique du contrôleur avant de procéder à la configuration du logiciel. Comme exemple :

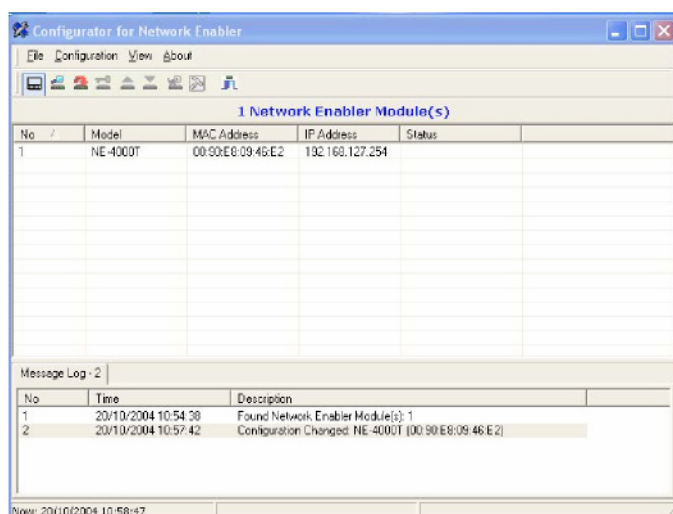
MAC: 00:90:E8:09:46:E2

Link: 01

Emplacement : Front Dr Ctrl

Utilitaire d'activation de réseau

Pour installer l'utilitaire d'activation de réseau, insérez le CD Link et lancez l'application « Utility_Setup.exe » à partir du dossier « Activation IP ». Le programme d'installation vous demandera d'exécuter l'installation. Ne faites aucun changement aux réglages par défaut de l'installation et lancez l'utilitaire, lorsque demandé. En plus, une icône de lancement rapide s'installera sur votre bureau pour utilisation ultérieure. Lorsque vous ouvrez l'utilitaire, sélectionnez l'option de recherche « Configuration Broadcast » pour trouver et lister selon leurs adresses MAC uniques tous les contrôleurs IP qui existent **sur le réseau accessible**. L'affichage ressemble à ceci :

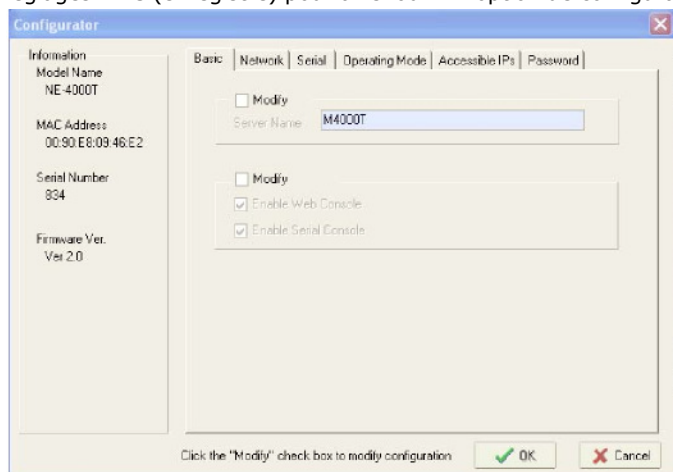


Si vous avez plus d'un contrôleur IP, ils devraient apparaître dans la liste. Si aucun contrôleur n'est trouvé, cela signifie qu'il y a un trouble en ce qui concerne la création d'adresse IP ou un trouble avec le LAN qui doit être corrigé par les administrateurs du LAN.

Par défaut, l'adresse IP installée en usine pour tous les contrôleurs LT-20IP est 192.168.127.254 et le masque de sous réseau est 255,255,0,0. Consultez la partie de votre manuel (page 28) 'manual_1st.pdf' sur le CD pour obtenir de l'information plus détaillée sur la création d'adresses IP et la résolution de troubles. Cependant, les réglages TCP/IP de votre adaptateur LAN au niveau du PC hôte local (serveur link.net) comporte le réglage du masque de sous-réseau suivant : 255.255.0.0.

Changement dynamique des réglages du contrôleur IP

Avant de pouvoir effectuer des changements au contrôleur, vous devez en premier déverrouiller le contrôleur pour que les changements soient stockés dans chaque LT-20IP. Sélectionnez le LT-20IP que vous voulez déverrouiller par l'adresse MAC que vous avez enregistrée plus tôt et cliquez à droite sur la souris. Sélectionnez-le à partir de la liste à défilement. Un mot de passe peut être demandé, mais sélectionnez tout de même « OK » puisque, par défaut, le réglage en usine ne comporte pas de mot de passe. Vous pouvez alors double cliquer sur l'entrée qui correspond aux réglages MAC (enregistré) pour ainsi ouvrir l'option de configuration pour contrôleur individuel :



Vous devez choisir l'onglet approprié et vérifier la boîte de modification de chaque section, lorsque vous faites des changements de réglages. Lorsque vous avez terminé, sélectionnez « OK » pour mettre à jour les changements dans le LT-20IP à distance. Les sections (onglet) que nécessitent des changements sont « Base » et « Réseau ».

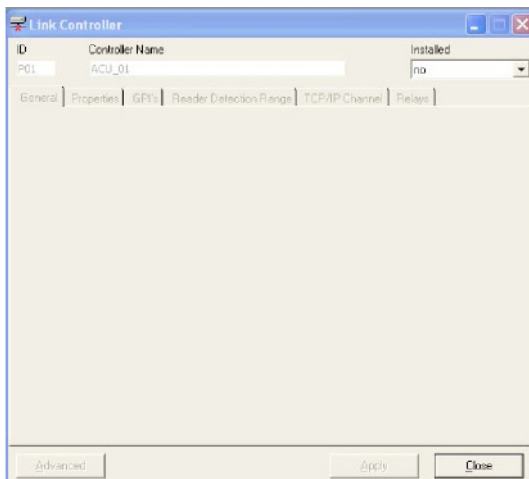
L'onglet « Base » comporte le nom du serveur (LT-20IP), ainsi que tous les autres réglages. Ces données doivent apparaître telles qu'illustrées ci-dessus et doivent demeurer inchangées. Pour régler le nom du serveur, cochez la boîte appropriée, soit « Modifier » et inscrivez le nom enregistré du contrôleur p. ex. Front Dr Ctrl. Le champ du nom est limité à 17 caractères incluant les espaces, soyez alors concis et précis sur les détails de l'emplacement du LT-20IP. L'onglet « Réseau » comporte les réglages d'importances de l'IP unique pour ce contrôleur LT-20IP. Vous devez les utiliser correctement et en conformité avec les normes utilisées sur le LAN précis auquel vous vous connectez. Veuillez demander à l'administrateur du LAN, une adresse IP pour chaque contrôleur LT-20IP. Pour obtenir de l'information plus détaillée à ce sujet, consultez la section 'manual_1st.pdf' (page 35) du manuel sur le CD Link. Nous supposons que vous avez des connaissances en création d'adresses IP et en masques de sous-réseau.

Lorsque les réglages précis du LT-20IP sont effectués, sélectionnez la touche « OK » pour enregistrer les changements. Si vous devez sélectionner un autre contrôleur dans la liste ou si vous devez en ouvrir un à nouveau pour effectuer d'autres changements, n'oubliez pas de le déverrouiller tel que décrit plus tôt pour que tous changements subséquents soient stockés en permanence. Lorsque tous les contrôleurs sont configurés, vous pouvez fermer l'utilitaire.

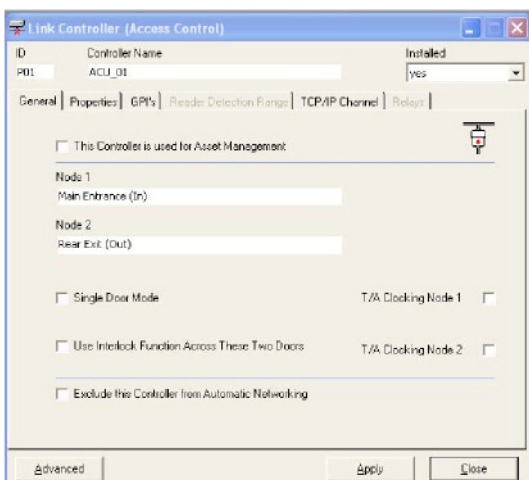
Réglages du contrôleur du serveur IP [Link.net](http://link.net)

Lorsque tous les contrôleurs LT-20IP sont dotés d'une adresse IP unique compatible ainsi qu'un masque de sous-réseau, alors vous pouvez régler les spécifications du contrôleur dans le serveur du logiciel [Link.net](http://link.net). Pour commencer, installez en premier le logiciel tel que décrit un peu plus loin dans ce manuel et prenez note que vous ne pouvez utiliser l'option d'installation « Plug & Play » pour trouver les dispositifs IP. Nous recommandons que tous contrôleurs sur circuit en fil métallique soient mis en service selon la procédure normale et que les dispositifs IP additionnels soient ajoutés manuellement ultérieurement.

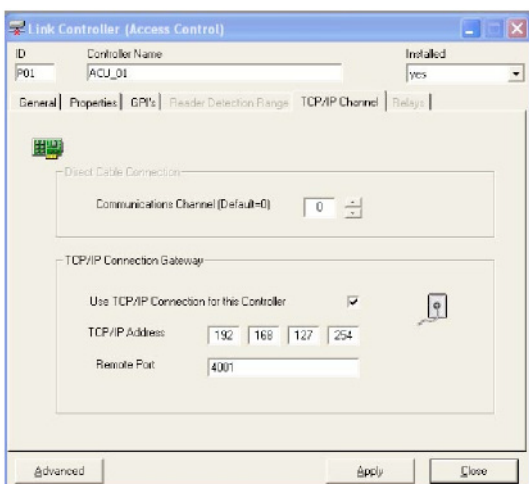
Sélectionnez l'article du menu « Contrôle d'accès et contrôleurs ». Ensuite, sélectionnez la touche d'option « Lister les contrôleurs disponibles » et mettez en surbrillance le contrôleur que correspond à votre EID (l'EID est l'adresse électronique unique enregistrée sur le circuit de commande principale par l'interrupteur DIP) p. ex. P01. Ouvrez le menu des spécifications du contrôleur en choisissant « Éditer » ou en double cliquant avec votre souris.



Pour installer le contrôleur, sélectionnez « Oui » à partir de l'option d'installation.



Sélectionnez l'onglet « Canal TCP/IP » et cochez l'option « Utiliser connexion TCP/IP ». Inscrivez les réglages IP appropriés pour ce contrôleur ainsi que le numéro de port 4001. Par défaut, le numéro de port pour tous les contrôleurs LT-20IP est 4001 et c'est ce numéro qui doit être utilisé. Si votre administrateur de réseau est d'avis contraire pour l'utilisation de numéro de port, par défaut, 4001, demandez, alors, l'attribution d'un nouveau numéro et faites les changements requis dans cette section ainsi que dans les réglages du LT-20IP en utilisant l'utilitaire 'Configuration de réseau' décrit plus tôt.

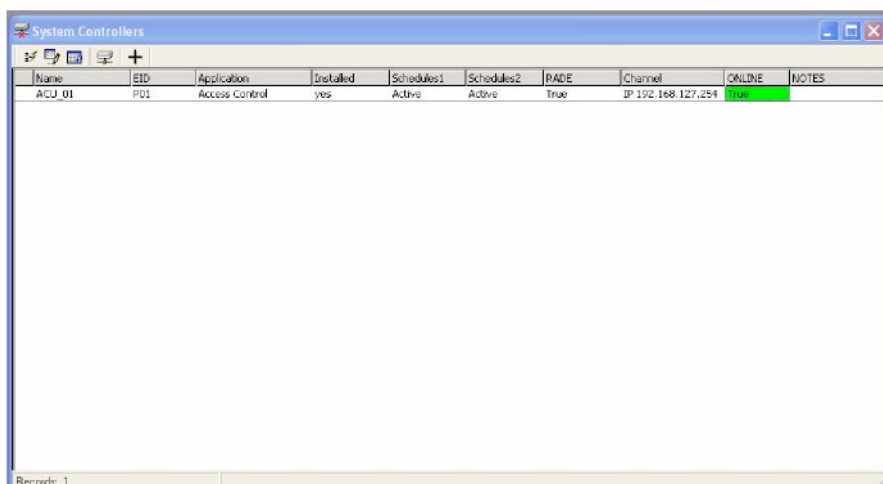


Lorsque les réglages appropriés sont en place, sélectionnez "Appliquer" et ensuite "Fermer". Pour définir des contrôleurs additionnels, répétez la procédure.

Si des contrôleurs LT-20AC standard individuels ou en réseau sont câblés à un **contrôleur LT-20IP répéteur bus Link.net**, configurez-le, alors, comme passerelle IP. Les réglages IP ainsi que le numéro de port doivent être les mêmes que **celui du contrôleur de passerelle** dans la **définition du LT-20AC**. L'unique différence sera l'EID unique (ID) de ce **contrôleur**. Cela indique au système qu'il doit tenter une connexion au contrôleur standard en passant par un contrôleur LT-20IP configuré comme passerelle IP.

Lorsque toutes les définitions des contrôleurs sont choisies, la liste des contrôleurs devrait afficher une boîte verte

« En ligne » pour chaque contrôleur IP qui est connecté, chaque passerelle IP connectée ou connectée par circuit en fil métallique au PC.



Name	EID	Application	Installed	Schedules1	Schedules2	PADE	Channel	ONLINE	NOTES
ACU_01	PD1	Access Control	yes	Active	Active	True	IP 192.168.127.254	True	

Records: 1

Installation d'un contrôleur d'accès Wavetrend (LT-20WAC)

Le contrôleur LT-20WAC de CDV est compatible avec jusqu'à 2 lecteurs actifs longue portée Wavetrend LRX-201. En plus, il est compatible avec la version LRX-200 cependant, pour ce modèle de lecteur plus ancien, le réglage de la portée active doit s'effectuer manuellement avec l'ensemble de programmation de lecteur Wavetrend.

Les applications incluses avec ce lecteur sont :

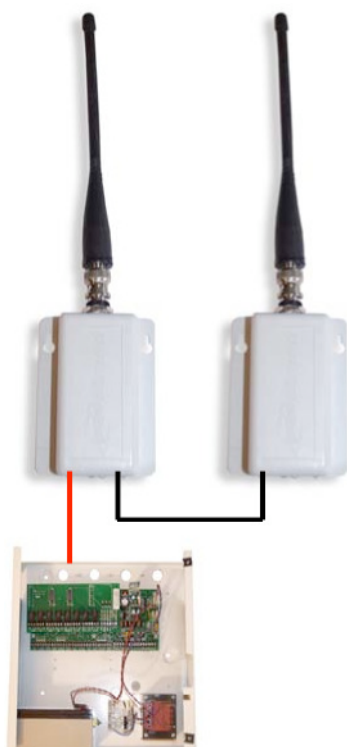
- Contrôle d'accès main libre pour les portes
- Fonction main libres pour le contrôle des portails et barrières
- Contrôle d'accès et pistage du personnel
- Liste d'appel et contrôle pour évacuation d'urgence

Les connexions de base pour le lecteur sont illustrées ci-dessous. Toutes les autres connexions locales pour les verrous et boutons de sortie sont décrites dans la section de contrôle d'accès précédente de ce manuel. Cette version soutient toutes les autres fonctionnalités standards en contrôle d'accès.

Le fil rouge est le fil de sortie principale qui est composée d'une fiche de raccordement standard CAT5 UTP (STP) ce qui signifie que toutes les 8 broches de raccordement se branche broche à broche. La distance maximum autorisée pour ce branchement est jde 15 mètres.

Le fil noir est la connexion entre le premier lecteur et le deuxième et dernier lecteur. La distance de fonctionnalité est de 300 mètres. Les données ainsi que l'alimentation sont transmises par le même câble CAT5 UTP ou câble STP. Le branchement de ce deuxième câble est non standard puisque la connexion n'utilise que les quatre broches centrales du connecteur RJ45. Ne faites pas de connexions supplémentaires, car cela pourrait endommager les lecteurs Wavetrend.

Lecteurs LRX-201



LT-20WAC

Câble du lecteur

Nous recommandons l'utilisation d'un câble CAT5 STP (blindé) pour le lecteur. Un câble non blindé peut agir en tant qu'antennes et par ce fait peut capter des fréquences radios (RF) indésirables à partir des lecteurs. Cela présente un problème puisque les prises RJ45 du lecteur ne soutiennent pas les connecteurs blindés RJ45. Des connexions blindées s'utilisent uniquement pour la connexion du PCB principale et le premier lecteur (en presumant que deux lecteurs doivent être branchés). À partir de la connexion principale PCB, dénudez le blindage avant de procéder au sertissage sur une fiche de connexion RJ45 et à partir de cet endroit soudez un petit fil de raccord afin qu'il se termine à la position 0V du port du terminal du premier lecteur. Avant de brancher les connexions RJ45 sur le lecteur (principal) dénudez le blindage sur le port d'entrée

(gauche) et sur le fil de sortie tout en le laissant en place dans le port de sortie (droite) et joignez-les ensemble à proximité des connexions RJ45. Ces mesures assureront un blindage efficace de la totalité du câblage et cela jusqu'au dernier lecteur.

CONSEIL : Lorsque la position ou l'ordre des lecteurs est réglé, vous devez les garder dans la même position puisque lors de la mise sous tension le premier lecteur physique est choisi par le système comme le lecteur principal. Si des lecteurs sont remplacés ou leurs positions interchangées, leurs drapeaux d'appel sélectif automatique doivent être reconfigurés pour « Ouvert » à partir de l'ensemble de programmation de lecteur Wavetrend.

Opération appropriée du lecteur

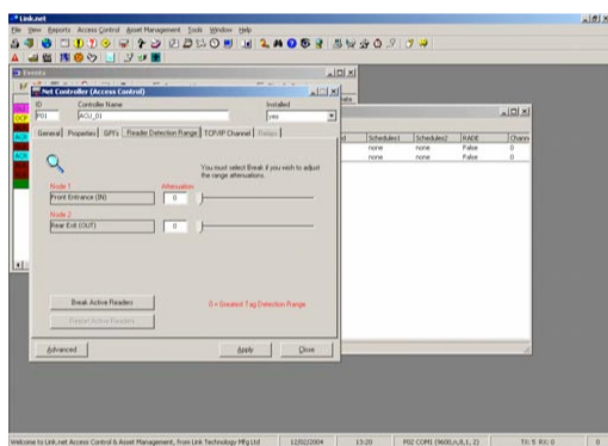
Pour déterminer l'exécution appropriée du lecteur comme suite à sa mise sous tension, vous devez vérifier que les LED jaune et vert de gauche sont allumés sur les deux lecteurs. Cela signifie que les données d'étiquettes reçues seront transmises à partir des lecteurs au contrôleur LT-20WAC pour traitement (appel sélectif automatique, en fonction). Si après 20 secondes ces LED ne s'allument pas comme suite à la mise sous tension, débranchez et vérifiez les connexions du lecteur, par la comparaison avec les spécifications de base de l'usine (énumérés ci-dessous). Chaque fois qu'une étiquette est perçue dans le rayon d'action de tous les lecteurs, le troisième LED (à partir de la gauche) clignote en jaune. Le quatrième LED des deux lecteurs doit aussi être allumé. Le retrait ainsi que le rebranchement du fil de sortie principal à partir de la prise de contrôle, engendreront un redémarrage. Un redémarrage peut prendre jusqu'à 20 secondes.

Réglages du lecteur LRX-201

Il faut savoir que le lecteur LRX-201 Wavetrend contient plusieurs paramètres internes qui doivent être soit réglés à l'usine Wavetrend ou par l'utilisation de l'ensemble de programmation de lecteur Wavetrend. Les réglages doivent être configurés sur le lecteur avant l'installation.

- Débit en bauds 9600 Baud
- Appel sélectif automatique – ouvert
- Appel sélectif manuel – fermé
- RSSI - 100 *
- Le code du site doit correspondre avec le code du site de l'étiquette pour l'installation Type de portée LR ou SR pour convenir à l'application (normalement SR)

* Le réglage de la portée de perceptions RSSI peut se faire manuellement avec l'ensemble de programmation de lecteur Wavetrend ou par le logiciel Link. Il est parfois plus facile de tester chaque lecteur dans son contexte pour s'assurer que les réglages RSSI sont appropriés. Les réglages de portée RSSI peuvent s'effectuer pour chaque paire de lecteurs à partir de leurs emplacements en utilisant le programme Link depuis un portable branché au réseau ou temporairement à chaque point du contrôleur. Vous pouvez aussi utiliser l'ensemble de programmation de lecteur Wavetrend. Le troisième LED de gauche de lecteur Wavetrend clignote chaque fois qu'une étiquette est perçue dans son rayon d'action. Cela vous donne une indication sur les réglages appropriés de la portée RSSI. En suivant une des procédures mentionnées ci-dessus, vous pouvez faire les ajustements nécessaires pour le bon fonctionnement du lecteur. Lorsque vous utilisez la procédure Link, assurez-vous que le programme communique avec le contrôleur qui gère les deux lecteurs pour lesquels vous voulez faire des réglages. Sélectionnez l'option « Contrôleur » à partir du menu contrôle d'accès et ensuite sélectionnez l'onglet « Portée du lecteur » L'écran qui suit s'affiche :



Lorsque vous utilisez la procédure Link de réglage de la portée RSSI vous devez en premier sélectionner le contrôleur approprié à partir de la liste et ouvrir l'onglet « Portée de perception du capteur ». La procédure de base est comme suit :

- Assurez-vous que vous êtes branché et en communication avec le contrôleur sélectionné (parmi les autres, si vous êtes complètement en réseau).
- Sélectionnez une fois la touche « Interrompre les lecteurs actifs ». Après quelques secondes les deux LED de gauche se ferme ce qui signifie que la fonction d'appel sélectif automatique est fermée et que les lecteurs et prêt à recevoir les nouvelles données RSSI.
- Sélectionnez le lecteur désiré et la portée à partir de la barre de défilement appropriée (Nœud 1 est le premier lecteur physique sur le contrôleur). Lors de relâchement du contrôle de défilement, le logiciel vous demandera si vous voulez modifier les réglages du lecteur sélectionné. En suite, l'information est transmise au contrôleur et la

mise à jour du lecteur survient peu de temps après. Les deux LED de gauches clignoteront brièvement pendant la mise à jour des nouveaux réglages RSSI. Testez la portée avec une seule étiquette tout en observant le troisième LED pour vérifier la perception d'étiquette et ajustez la barre de défilement convenablement. N'oubliez pas d'attendre quelques secondes pour que les changements soient en vigueur.

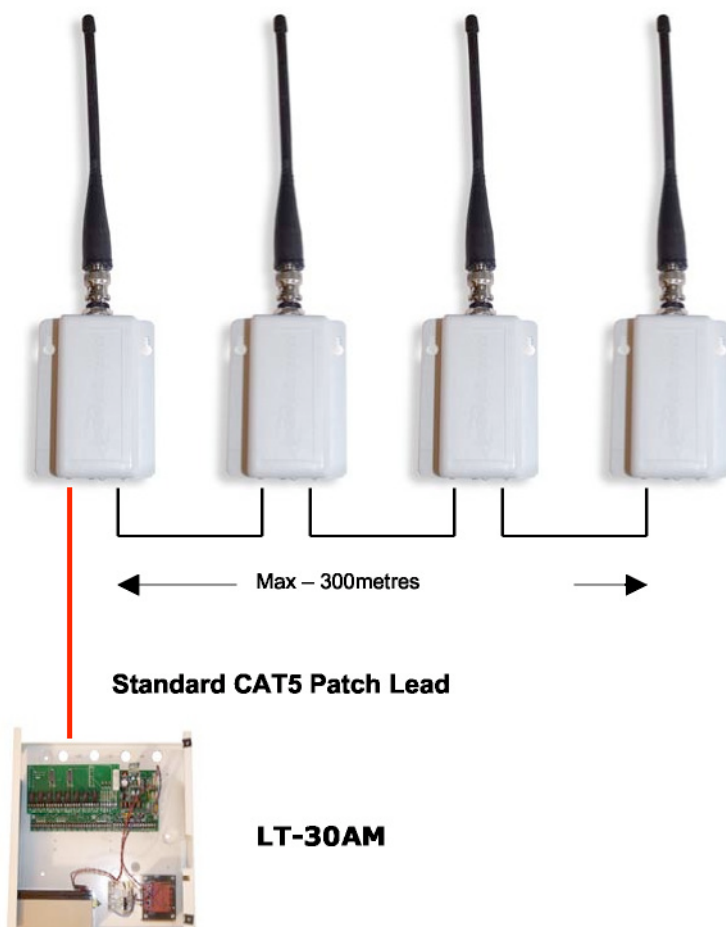
- Lorsque la portée désirée est réglée pour les deux lecteurs, sélectionnez la touche « Redémarrer les lecteurs actifs » et ensuite fermez la fenêtre de contrôle. Après quelques secondes, tous les LED concernés s'allumeront à nouveau signalant ainsi que le tout est opérationnel. Si vous avez des doutes sur le l'ouverture appropriée des lecteurs, vous pouvez retirez la connexion RJ45 du contrôleur et le rebrancher (réinitialisations à froid du lecteur). Après quelques secondes, les lecteurs redémarreront en mode appropriée d'appel sélectif automatique.

CONSEIL : Les réglages de la portée du lecteur sont compris entre 0 et 250, 250 étant la portée la moins longue et 0 la plus longue. Les réglages **linéaires en temps réel** sont compris entre 60 et 200. Notez que la portée précise pour toute valeur attribuée, dépend du type de lecteur (LR, SR ou PR), de type d'antenne qui s'y rattache ainsi que l'environnement. Par conséquent, il est impossible de trouver la distance exacte de toute valeur de portée (RSSI) donnée.

Installation d'un contrôleur de gestion de biens Link (LT-30AM2)

Les lecteurs de biens actifs se branchent directement au PCB principal Link.net par le câble principal qui est fourni. Il se branche à la prise RJ45 de réserve. Toute la source d'alimentation des lecteurs est fournie par cette connexion.

Connections



Le fil rouge est le fil de sortie principale qui est composée d'une fiche de raccordement standard CAT5 UTP (STP) ce qui signifie que toutes les 8 broches de raccordement se branche broche à broche. La distance autorisée pour ce branchement est de 15 mètres maximum

Le fil noir est la connexion entre le premier lecteur et le deuxième et dernier lecteur. La distance de fonctionnalité est de 300 mètres. Les données ainsi que l'alimentation sont transmises par le même câble CAT5 UTP ou câble STP. Le branchement de ce deuxième câble est non standard puisque la connexion n'utilise que les quatre broches centrales du connecteur RJ45. Ne faites pas de connexions supplémentaires, car cela pourrait endommager les lecteurs Wavetrend.

Diagramme du contrôleur de gestion de biens

Câble du lecteur

Nous recommandons l'utilisation d'un câble CAT5 STP (blindé) pour le lecteur un câble non blindé peut agir en tant qu'antennes et par ce fait peut capter des fréquences radios (RF) indésirables à partir des lecteurs. Cela présente un problème puisque les prises RJ45 du lecteur ne soutiennent pas les connecteurs blindés RJ45. À partir de la connexion principale PCB, dénudez le blindage avant de procéder au sertissage sur une fiche de connexion RJ45 standard et à partir de cet endroit soudez **un petit fil de jonction** pour qu'il se termine à la position 0V du port du terminal du premier lecteur. Avant de brancher les connexions RJ45 sur le lecteur (principal), dénudez le reillis sur le port d'entrée (gauche) et sur le fil de sortie tout en le laissant en place dans le port de sortie (droite) et joignez-les ensemble à proximité des connexions RJ45. Continuez ainsi pour tous les lecteurs restants. Le blindage n'a pas à être terminé physiquement sur le dernier lecteur. Ces mesures assureront un blindage efficace de la totalité du câblage et cela jusqu'au dernier lecteur.

CONSEIL : Lorsque la position ou l'ordre des lecteurs est réglé, vous devez les garder dans la même position puisque lors de la mise sous tension le premier lecteur physique est choisi par le système comme le lecteur principal. Si des lecteurs sont remplacés ou leurs positions interchangées, leurs drapeaux d'appel sélectif automatique doivent être reconfigurés pour « Ouvert » à partir de l'ensemble de programmation de lecteur Wavetrend.

Opération appropriée du lecteur

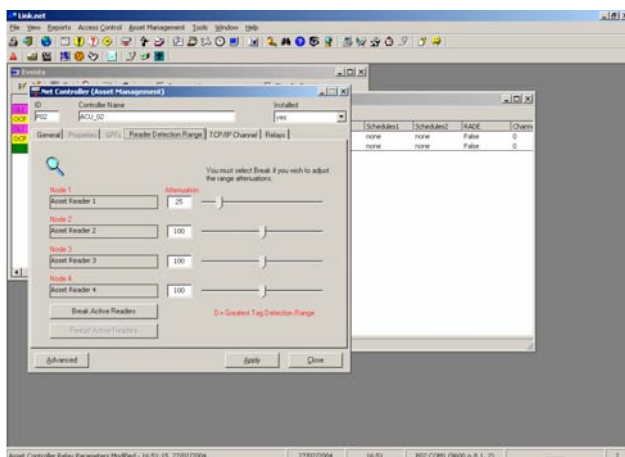
Pour déterminer l'exécution appropriée du lecteur à la suite de sa mise sous tension, vous devez vérifier que les LED jaune et vert de gauche sont allumés sur les deux lecteurs. Cela signifie que les données d'étiquettes reçues seront transmises à partir des lecteurs au contrôleur LT-30AM pour traitement (appel sélectif automatique, en fonction). Si après 20 secondes ces LED ne s'allument pas à la suite de la mise sous tension, débranchez et vérifiez les connexions du lecteur, en comparaison avec les spécifications de base de l'usine (énumérés ci-dessous). Chaque fois qu'une étiquette est perçue dans le rayon d'action de tous les lecteurs, le troisième LED (à partir de la gauche) clignote en jaune. Le quatrième LED des deux lecteurs doit aussi être allumé. Le retrait ainsi que le rebranchement du fil de sortie principal à partir de la prise de contrôle, engendreront un redémarrage. Un redémarrage peut prendre jusqu'à 20 secondes.

Réglages du lecteur LRX-201

Vous devez comprendre que le lecteur LRX-201 Wavetrend contient plusieurs paramètres internes qui doivent être soit réglés à l'usine Wavetrend ou par l'utilisation de l'ensemble de programmation de lecteur Wavetrend. Les réglages doivent être configurés sur le lecteur avant l'installation.

- ❖ Débit en bauds 9600 Baud
- ❖ Appel sélectif automatique – ouvert
- ❖ Appel sélectif manuel – fermé
- ❖ RSSI - 100 *
- ❖ Le code du site doit correspondre avec le code du site de l'étiquette pour l'installation Type de portée LR ou SR pour convenir à l'application (normalement SR)

* Les réglages de portée RSSI peuvent s'effectuer pour chaque paire de lecteurs à partir de leurs emplacements en utilisant le programme Link à partir d'un portable branché au réseau ou temporairement à chaque point du contrôleur. En plus, vous pouvez utiliser l'ensemble de programmation de lecteur Wavetrend. Le troisième LED de gauche du lecteur Wavetrend clignote chaque fois qu'une étiquette est perçue dans son rayon d'action. Cela vous donne une indication sur les réglages appropriés de la portée RSSI. En suivant une des procédures mentionnées ci-dessus, vous pouvez faire les ajustements nécessaires pour le bon fonctionnement du lecteur. Lorsque vous utilisez la procédure Link, assurez-vous que le programme communique avec le contrôleur qui gère un des quatre lecteurs pour lequel vous voulez faire des réglages. Sélectionnez l'option « Contrôleur » à partir du menu contrôle d'accès et ensuite sélectionnez l'onglet « Portée du lecteur » L'écran qui suit s'affiche :



Lorsque vous utilisez la procédure Link de réglage de la portée RSSI vous devez en premier sélectionner le contrôleur approprié à partir de la liste et ouvrir l'onglet « Portée de perception du capteur ». La procédure de base est comme suit :

- ❖ Assurez-vous que vous êtes branché et en communication avec le contrôleur sélectionné (parmi les autres, si vous êtes complètement en réseau).
- ❖ Sélectionnez une fois la touche « Interrompre les lecteurs actifs ». Après quelques secondes les deux LED de gauche se ferme ce qui signifie que la fonction d'appel sélectif automatique est fermée et que les lecteurs et prêt à recevoir les nouvelles données RSSI.

- Sélectionnez le lecteur désiré et la portée à partir de la barre de défilement appropriée (Nœud 1 est le premier lecteur physique sur le contrôleur et ensuite le nœud 2, 3 et 4). Lors de relâchement du contrôle de défilement, le logiciel vous demandera si vous voulez modifier les réglages du lecteur sélectionné. En suite, l'information est transmise au contrôleur et la mise à jour du lecteur survient peu de temps après. Les deux LED de gauches clignoteront brièvement pendant la mise à jour des nouveaux réglages RSSI. Testez la portée avec une seule étiquette tout en observant le troisième LED pour vérifier la perception d'étiquette et ajustez la barre de défilement selon le besoin. N'oubliez pas d'attendre quelques secondes pour que les changements soient effectifs
- Lorsque la portée désirée est réglée pour les deux lecteurs, sélectionnez la touche « Redémarrer les lecteurs actifs » et ensuite fermez la fenêtre de contrôle. Après quelques secondes, tous les LED appropriés s'allumeront à nouveau signalant ainsi que tout est opérationnel. Si vous avez des doutes sur le l'ouverture appropriée des lecteurs, vous pouvez retirez la connexion RJ45 du contrôleur et le rebrancher (réinitialisations à froid du lecteur). Après quelques secondes, les lecteurs redémarreront en mode appropriée d'appel sélectif automatique.

CONSEIL : Les réglages de la portée du lecteur sont compris entre 0 et 250, 250 étant la portée la moins longue et 0 la plus longue. Les réglages **linéaires en temps réel** sont compris entre 60 et 200. Prenez note que la portée précise pour toute valeur attribuée, dépend du type de lecteur (LR, SR ou PR), de type d'antenne que s'y attache ainsi que l'environnement. Par conséquent, il est impossible de trouver la distance exacte de toute valeur de portée (RSSI) donnée.

Création automatique d'adresses

Lorsqu'un réseau de 4 lecteurs ou moins (4 zones) est branché à l'hôte LT-30AM et ensuite mis sous tension, le système d'appel sélectif automatique lance l'attribution des adresses de noeuds selon l'emplacement physique du lecteur sur le réseau. Les règlements qui régissent la création d'adresse automatique sont les suivantes :

- Les adresses du réseau sont configurées de gauche à droite (1 à 4)
- Une fois réglé, le premier lecteur physique (1) ne doit jamais être déplacé de son ordre dans le réseau, car il est créé en tant que lecteur maître. Les autres lecteurs peuvent être déplacés.
- Si le réseau est hors service lorsqu'il est alimentée en courant, l'alimentation doit être, alors, débranchée et ensuite rebranchée lors de la remise en service du réseau pour réinitialiser la configuration d'adresses.

Réglage de surveillance rétroactive par contrôleur

Si la fonction « Surveillance rétroactive par contrôleur » est nécessaire à vos opérations pour surveiller continuellement la présence des biens à partir du contrôleur concerné, réglez, alors, l'interrupteur DIP 6 pour qu'il soit en position « Ouvert ». Cela activera la transmission par le contrôleur d'un message d'alarme pour signaler un bien manquant dans une zone surveillée à la suite à une temporisation de la sécurité. La surveillance rétroactive par contrôleur fonctionne uniquement pour les applications en surveillance.

Test du contrôleur de gestion de biens [Link.net](#)

Avant de brancher [Link.net](#) au réseau, quelques tests de bases doivent être effectués pour vérifier l'installation du réseau. Mettez le contrôleur sous tension depuis **l'embase du poteau du réseau électrique à fusible non commuté**.

1. Test à 13.6VDC aux terminaux PSU PCB DC.
2. Assurez-vous que le LED d'alimentation PCB principal est allumé.
3. Les LED des lecteurs de biens actifs devraient clignoter.
4. Lorsque qu'une étiquette est visualisée ou activée à partir du code de site approprié, le troisième LED de gauche devrait clignoter pour chaque étiquette perçue par le capteur.

Création d'adresse pour un contrôleur [Link.net](#)

Chaque PCB principal [Link.net](#) comporte un interrupteur DIL à 6 directions. Pour que le contrôleur soit reconnu par le réseau [Link.net](#) il doit avoir une adresse unique. Les interrupteurs DIP 1 à 5 créent l'adresse électronique unique (EID) comme suit :

CONSEIL : **Chaque contrôleur doit avoir une adresse unique et les messages doivent toujours être transmis par ordre chronologique.**

Adresse	S1	S2	S3	S4	S5
1	OUVERT	FERMÉ	FERMÉ	FERMÉ	FERMÉ
2	FERMÉ	OUVERT	FERMÉ	FERMÉ	FERMÉ
3	OUVERT	OUVERT	FERMÉ	FERMÉ	FERMÉ
4	FERMÉ	FERMÉ	OUVERT	FERMÉ	FERMÉ
5	OUVERT	FERMÉ	OUVERT	FERMÉ	FERMÉ
6	FERMÉ	OUVERT	OUVERT	FERMÉ	FERMÉ
7	OUVERT	OUVERT	OUVERT	FERMÉ	FERMÉ
8	FERMÉ	FERMÉ	FERMÉ	OUVERT	FERMÉ
9	OUVERT	FERMÉ	FERMÉ	OUVERT	FERMÉ
10	FERMÉ	OUVERT	FERMÉ	OUVERT	FERMÉ
11	OUVERT	OUVERT	FERMÉ	OUVERT	FERMÉ
12	FERMÉ	FERMÉ	OUVERT	OUVERT	FERMÉ
13	OUVERT	FERMÉ	OUVERT	OUVERT	FERMÉ
14	FERMÉ	OUVERT	OUVERT	OUVERT	FERMÉ

15	OUVERT	OUVERT	OUVERT	OUVERT	FERMÉ
16	FERMÉ	FERMÉ	FERMÉ	FERMÉ	OUVERT
17	OUVERT	FERMÉ	FERMÉ	FERMÉ	OUVERT
18	FERMÉ	OUVERT	FERMÉ	FERMÉ	OUVERT
19	OUVERT	OUVERT	FERMÉ	FERMÉ	OUVERT
20	FERMÉ	FERMÉ	OUVERT	FERMÉ	OUVERT
21	OUVERT	FERMÉ	OUVERT	FERMÉ	OUVERT
22	FERMÉ	OUVERT	OUVERT	FERMÉ	OUVERT
23	OUVERT	OUVERT	OUVERT	FERMÉ	OUVERT
24	FERMÉ	FERMÉ	FERMÉ	OUVERT	OUVERT
25	OUVERT	FERMÉ	FERMÉ	OUVERT	OUVERT
26	FERMÉ	OUVERT	FERMÉ	OUVERT	OUVERT
27	OUVERT	OUVERT	FERMÉ	OUVERT	OUVERT
28	FERMÉ	FERMÉ	OUVERT	OUVERT	OUVERT
29	OUVERT	FERMÉ	OUVERT	OUVERT	OUVERT
30	FERMÉ	OUVERT	OUVERT	OUVERT	OUVERT
31	OUVERT	OUVERT	OUVERT	OUVERT	OUVERT

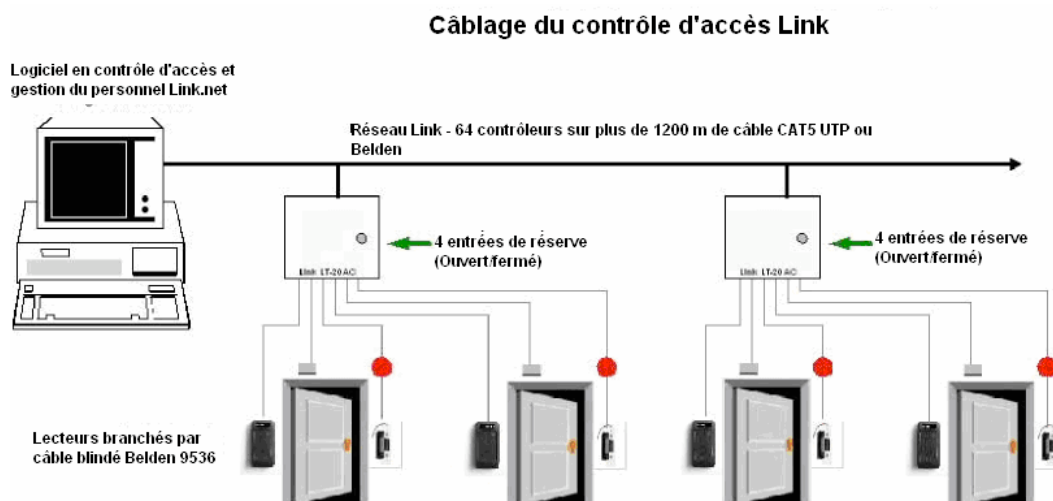
Les interrupteurs DIP 6 règlent le mode d'opération des contrôleurs comme suit :

Interrupteur 6 (LT-20AC, LT-20I/FD, LT-20IP)	Adressage étendu de réseau
FERMÉ	Sélection standard d'adresse
OUVERT	Décalage standard d'adresse +32 (p. ex O, O, O, O, O, O est 63)
Interrupteur 6 (LT-30AM2 gestion de biens)	Mode opérationnel
FERMÉ	Mode standard de biens
OUVERT	Surveillance rétroactive par contrôleur

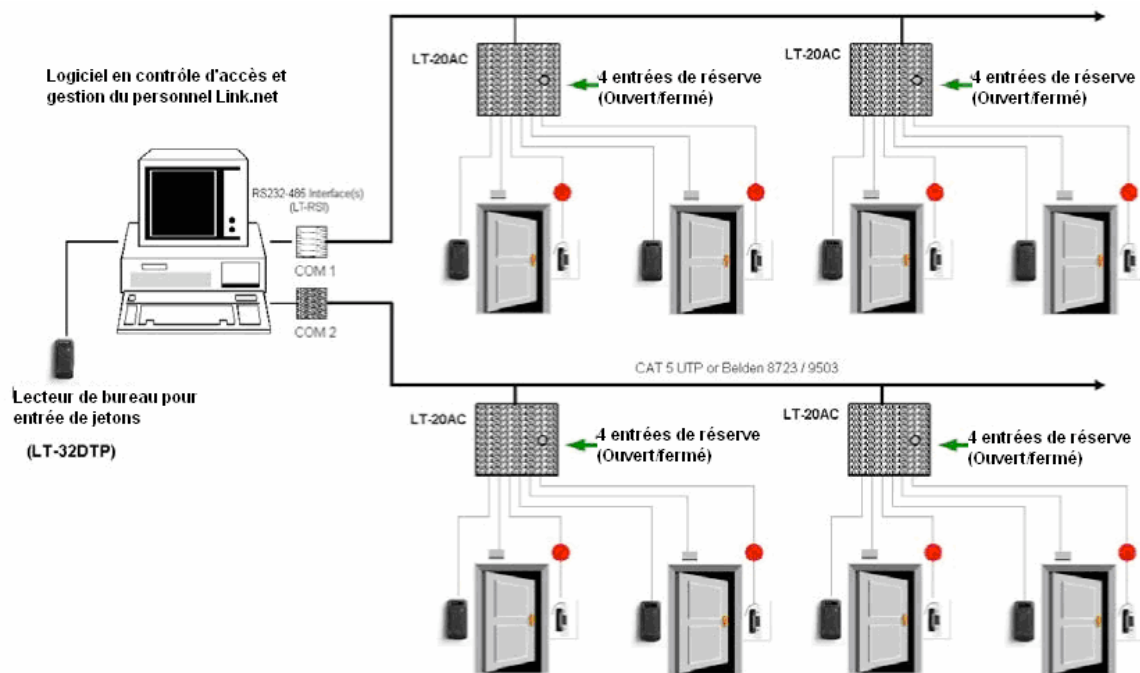
Connexion à un ordinateur personnel

Lorsque tout le matériel est installé et testé tel que décrit précédemment, vous pouvez maintenant connecter les contrôleurs au réseau et sur un ordinateur personnel (PC). Les sections suivantes expliquent la procédure pour une mise en réseau à fiabilité maximale et qui est efficace. Les schémas de principes, qui suivent expliquent les options diverses pour la mise en place des contrôleurs Link.net :

Réseau de contrôle d'accès par câblage à canal unique



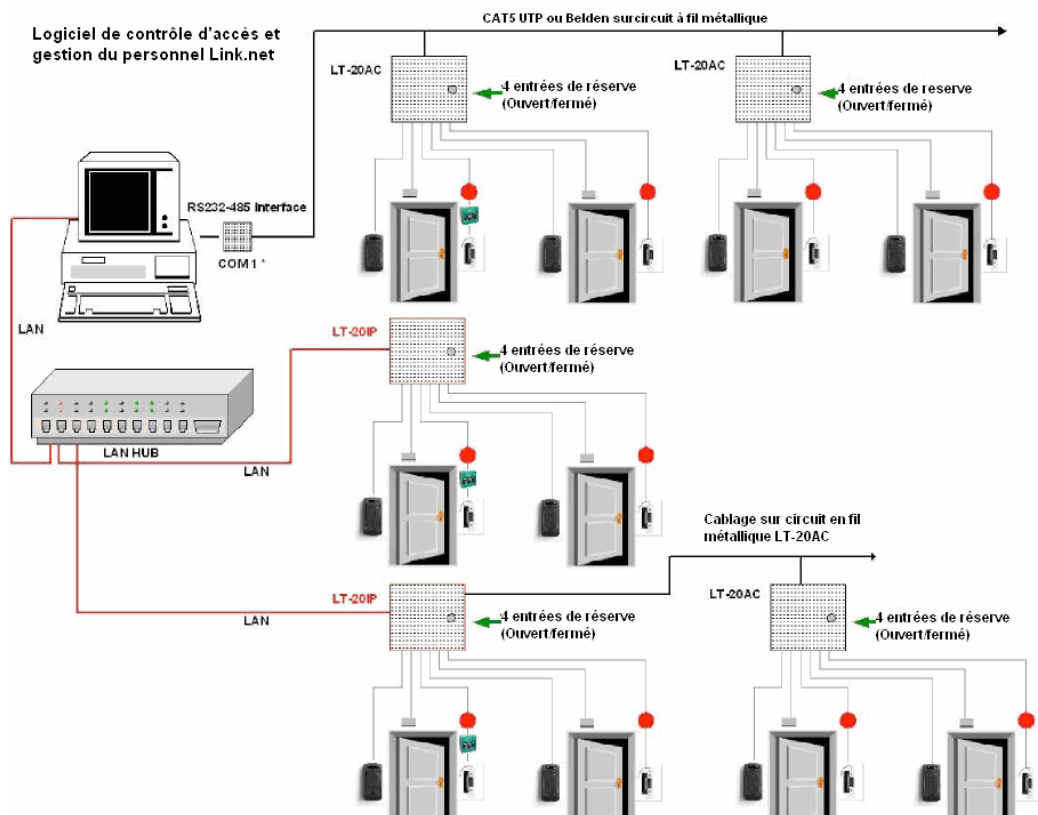
Réseau de contrôle d'accès à câble multi canal



Link.net Cable Channel (2 of 8) - 64 Controllers on each over 1200M of CAT5 / UTP or Belden Cable

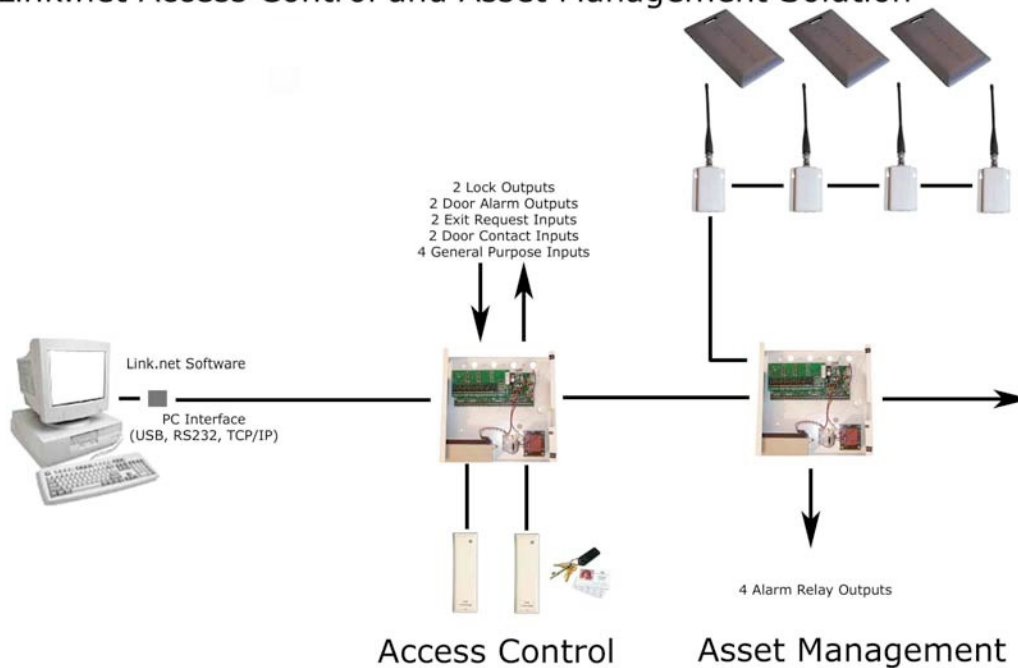
L'illustration ci-dessus montre l'utilisation des réseaux à câblage de canal unique et à câblage multi canal. Chaque réseau de câblage peut atteindre 1.2 kilomètres en utilisation des câbles CAT5 UTP ou Belden 8723/9503 à faible coût. [Link.net](#) peut soutenir jusqu'à 8 canaux direct de câblage à partir de ports séries RS232. En plus il peut soutenir des connexions pour des réseaux et contrôleurs additionnels par TCP/IP LAN (contrôleur IP requis) tel qu'illustré ci-dessous :

Connexion de réseau de contrôle d'accès par câblage et IP



Veuillez noter l'utilisation de LT-20IP inférieur comme passerelle IP vers les contrôles câblés de manière traditionnelle. Un schéma général montrant un mélange de contrôle d'accès et de gestion de biens est illustré ci-dessous :

Link.net Access Control and Asset Management Solution



Techniques de réseautage [Link.net](#)

Lorsque vous êtes prêts à établir un réseau, vous devez tenir compte de ce qui suit :

- Choisissez l'interface réseau appropriée (RS232, USB ou TCP/IP)
- **Créez toujours vos adresses par ordre chronologique**
- Ne créez jamais des numéros d'adresses en double
- Les terminaux doivent se connecter par, p. ex. TX+ à TX+, etc.
- Employez toujours un seul fil pour la mise à la terre (cinquième fil).
- Utilisez dans câbles CAT5 UTP ou Belden 9503 (blindé) dans des **environnements rigoureux à distance**
- Utilisez toujours des **paires jumelées de câbles pour le TX et pour le RX**
- Ne dépassez jamais 1200m de distance en câblage
- N'utilisez jamais un système de câblage en étoile **ou par antenne**

Câble blindé ou UTP

La décision d'utiliser des câbles blindés (Belden 9503/8723), ou CAT5 UTP se fait par l'évaluation des trois facteurs, qui suivent :

- Distance de câblage de réseau
- Quantité de contrôleurs du réseau
- Environnement

Utilisez toujours un système de câblage blindé lorsque la longueur du câblage réseau excède 500m. Si la quantité de contrôleurs du réseau excède 10 , vous devez, alors, utiliser un câble blindé, peu importe la distance. Si vous tenez compte de l'environnement dans lequel le système se retrouve et qu'il y existe des risques d'interférences, un câble blindé est la meilleure solution pour vous. Peu importe la raison pour laquelle vous utilisez du câblage blindé, le rendement du réseau sera meilleur, mais à un coût plus élevé. Cependant, vous devez parfaire soigneusement le câble dans tout le réseau, car une mauvaise installation engendrera une perte de performance du câble blindé (consultez les instructions à venir).

Interface PC RS232 pour réseau

Lorsque vous branchez le réseau [Link.net](#) à un port de connexion d'ordinateur, vous devez le faire soigneusement par l'attribution du port appropriée ainsi que l'utilisation du bon câblage, ce qui assurera la rapidité et l'efficacité de votre réseau local de contrôleurs.

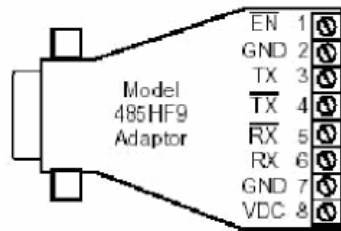
Interface PC Amplicon, modèle 485HF9

Ci-dessous un schéma de câblage de l'interface de réseau local par contrôleur Amplicon 485HF9. Cette interface est conçue pour convertir des signaux RS232 PC à transmission basse à des signaux RS485 à transmission étendue de liaison multipoints, nécessaires au bon fonctionnement du système [Link.net](#). Le succès de tout fonctionnement d'un système dépend de l'installation appropriée du réseau. Auparavant, dans ce manuel vous avez lu la description des règlements en réseautage par RS485, maintenant nous expliquerons l'implantation. Il existe deux méthodes de connexion.

Méthode de connexion 1 – Réseau alimenté par contrôleur 485HF9 (recommandée)

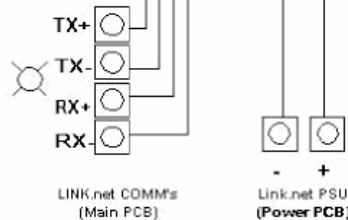
La méthode de connexion standard, comporte une interface RS232 alimentée et référencée **pour mise à la terre** par le premier contrôleur du réseau. Cela est illustré dans le schéma qui suit.

Modèle 485HF9
Connexion port série
RS 232 sur un PC



Avertissement - Les connexions pour l'alimentation sont susceptibles à la polarité. Vérifiez toujours que le terminal 7 est (-) et 8 (+). Une connexion inappropriée aura comme résultat la destruction de l'interface.

1. La distance maximale à partir du PC et le premier contrôleur Link est de 150 m
2. Utilisez le câble de raccordement CAT5 ou un mylar à paire blindée Belden 9503, si un système de blindage est requis
3. Pour le raccord CAT5 utilisez les paires pour (3, 4), (5, 6) et (7, 8)



Méthode 1 : La connexion au premier contrôleur alimente l'interface RS232 - RS485

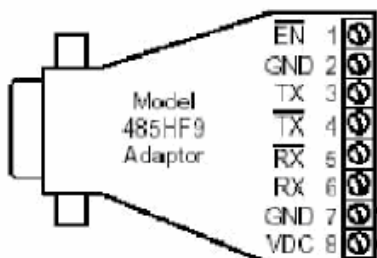
Premier contrôleur (Adresse 01)

Méthode de connexion 2 – Réseau alimentée localement 485HF9

Cette méthode de connexion comporte une interface RS232 alimentée par une source locale DC individuelle (PSU à **connexion directe**). La référence de mise à la terre est employée dans la totalité du réseau. La connexion alternative pour PC est illustrée dans le schéma ci-dessous.

Utilisez toujours une source d'alimentation périphérique STABILISÉE 9-13VDC et notez que le **Terminal 8 est +V**.

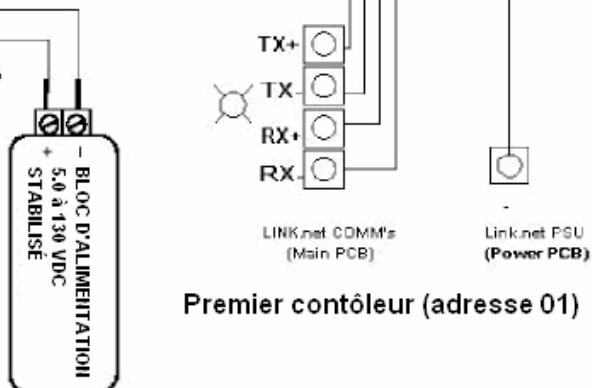
Modèle 485HF9
Connexion port série
RS232 sur un PC



Avertissement - Les connexions pour l'alimentation sont susceptibles à la polarité. Vérifiez toujours que le terminal 7 est (-) et le 8 (+). Une connexion inappropriée aura comme résultat la destruction de l'interface.

Méthode 2 - Alimentation locale PSU de l'interface RS232 - RS485

1. La distance maximale entre l'interface du PC et le premier contrôleur est limité par la distance globale du réseau à 1200 m
2. Utilisez le câble CAT5 ou un mylar à paire blindée Belden 9503 si un système de blindage est requis.
3. Pour le raccord CAT5 utilisez les paires (3, 4), (5, 6) et une paire de réserve pour la connexion de mise à la terre. (-GND)



Premier contrôleur (adresse 01)

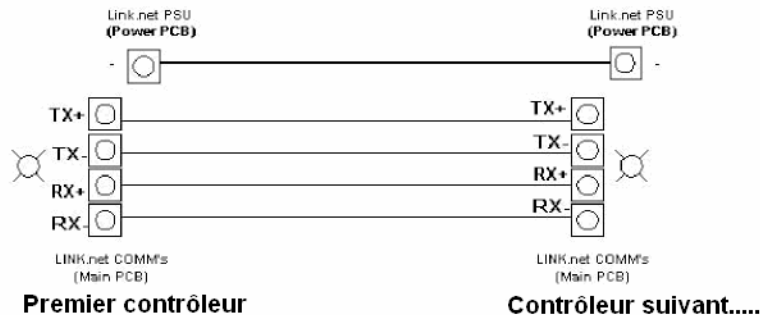
Cette méthode est moins utilisée car les risques de pertes d'alimentation à partir de l'interface sont plus élevées. Cependant, sa capacité de transmission au premier contrôleur sur de plus longues distances offre un avantage

(>150M).

Interconnexion de contrôleurs

INTERCONNEXION DE CONTRÔLEURS

1. La distance maximale entre le premier contrôleur et le dernier est de 1200 m.
2. Utilisez le câble de raccordement CAT5 ou un mylar à paire blindée Belden 8132 si un système de blindage est requis. Utilisez le blindage pour le conducteur (-) à (+).
3. Pour le câble de raccordement CAT5 utilisez les paires pour (3, 4), et (5, 6)
4. Ne faites jamais une interconnexion du (+) à partir du contrôleur PSU de port au contrôleur.



Lorsque vous installez le réseau de câbles, évitez toujours l'installation de longs câbles en parallèle entre les centrales électriques. Si vous le pouvez, faites passer les câbles dans des conduits individuels ou conservez les câbles éloignés les uns des autres. Utilisez toujours une paire jumelée pour la paire TX et pour la paire RX. Si vous utilisez des câbles blindés (recommandés pour les environnements industriels hostiles ou pour des réseaux à plusieurs dispositifs), branchez le blindage à la connexion GND du convertisseur électronique (terminal 8) et terminez-le à la position de point de volt 0 (-) de chaque contrôleur tel qu'illustré. Si vous utilisez un câble de raccordement CAT 5, utilisez alors un conducteur de réserve.

CONSEIL : Le fil négatif (-) doit se terminer sur tout le réseau de contrôleurs, ce qui fournit une référence commune de mise à la terre pour la totalité du réseau.

Terminaison de lignes de réseau RS485

Lorsque la longueur du câble excède 200 mètres, la bonne procédure est d'utiliser une terminaison de ligne de réseau. En plus, cette procédure peut être nécessaire si le réseautage se fait dans des environnements bruyant ou si vous utilisez des câbles CAT5 UTP, peu importe la distance. La terminaison s'effectue par le branchement d'une résistance à couche métallique 120R sur le dernier contrôleur pour les terminaux RX+ et RX- uniquement.

Utilisation d'un système de lecture comme lecteur d'entrée de badges

Certains types de contrôle d'accès par badge ne comportent pas l'impression du numéro de badge. Cela crée un problème lors d'une tentative de validation. Pour contourner ce problème, vous pouvez utiliser le lecteur de contrôle d'accès pour valider le badge directement à partir de la base de données. Cette fonction doit se faire à partir de la première position « 01 » de lecture du contrôleur. Vous pouvez tout de même l'utiliser comme lecteur de contrôle d'accès de la porte. Cette option s'utilise fréquemment lorsqu'un petit nombre de détenteurs de carte doit être géré quotidiennement. Si une gestion supplémentaire est requise, alors un réseau dédié de lecteurs d'entrée de badge est plus approprié.

Installation d'une carte d'interface pour lecteurs LT-RIB

L'installation d'un bureau dédié d'accès de lecteur situé sur le côté du PC simplifie la gestion des badges. Vous aurez besoin d'un lecteur supplémentaire que vous utiliserez pour les portes de contrôle d'accès et une carte d'interface de LT-RIB. Les instructions de LT-RIB détailleront comment relier et configurer cette unité pour l'opération.

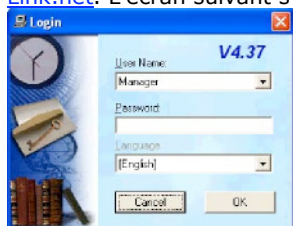
Installation du logiciel [Link.net](#)

Le logiciel d'application [Link.net](#) s'installe à partir du CD ressource de CDV. Insérez le CD dans le lecteur du PC à partir duquel vous voulez installer l'application. À partir du répertoire de route du CD, vous trouverez le fichier Setup.EXE. Lancez ce fichier et suivez les instructions spécifiées par les messages guides qui s'affichent à l'écran.

Première ouverture du logiciel

Le logiciel [Link.net](#) permet l'utilisation de profils d'utilisateur. Lorsqu'il est expédié, le logiciel comporte un utilisateur

par défaut « Manager ». Lorsque des utilisateurs sont ajoutés, vous pouvez alors supprimer cet utilisateur par défaut. Sélectionnez « Démarrer » et ensuite « Programmes » Link et contrôle d'accès et gestion de biens Link.net. L'écran suivant s'affiche pour l'ouverture de session :

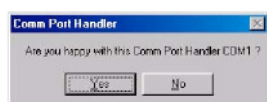


Inscrivez « Manager » dans le champ du mot de passe (tenez compte du M majuscule) et sélectionnez « OK ». Si ce logiciel est utilisé pour la première fois, il lancera automatiquement l'application « Gestion du contrôleur Plug & Play ». Si vous n'utilisez pas le dispositif en série par défaut, « Gestionnaire COM » (COM1) vous devez donc utiliser la fonction « Changer gestionnaire COM ».

Installation du contrôleur Plug & Play

Lorsque le système est lancé pour la première fois et que le logiciel ne comporte aucune installation en matériel (hardware), le « Gestionnaire Plug & Play » s'active automatique par l'utilisation du message guide suivant :

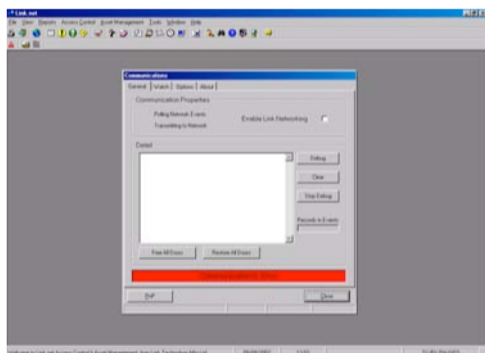
1



Si vous utilisez des dispositifs de type FD comme le LT-20I/FD (remarquez la présence du suffixe FD) vous devez donc utiliser le protocole le plus rapide en vitesse de communication. Si vous utilisez des dispositifs standards, passez à l'étape 2. Pour les dispositifs « FD », sélectionnez « Non » et la fenêtre de communications s'affiche. Sélectionnez l'onglet « Option » et cochez boîte « Protocole rapide ». En plus, sélectionnez le port de communication approprié, là où votre matériel est installé. Passez à l'étape 3.

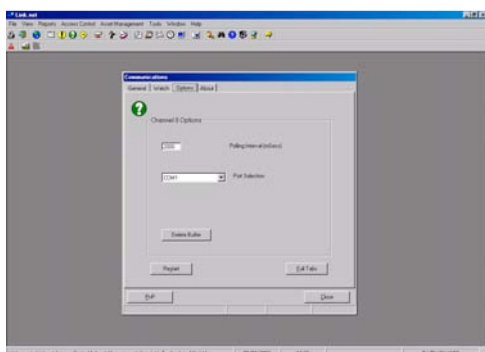
2

Sélectionnez « Oui » si vous êtes satisfait de l'utilisation du port par défaut (Gestionnaire COM) ou « Non » si vous voulez en configurer un autre. La fenêtre de dialogue s'affiche automatiquement, comme illustré ci-dessous:



Sélectionnez l'onglet "Option" pour sélectionner le port approprié. Si vous utilisez un port USB de connexion, alors, c'est à partir de cet endroit que vous sélectionnez le « Gestionnaire virtuel de port com ».

3



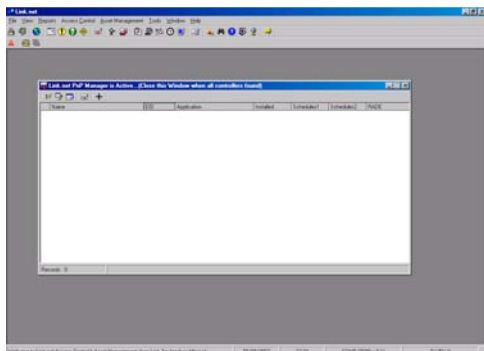
Lorsque vous avez terminé, retournez à l'onglet général et cochez la boîte « Activer réseautage Link ». Cela configurer le nouveau port COM et créera le réseautage. Le matériel Link.net peut maintenant se brancher sur le PC par l'utilisation de l'interface. Assurez-vous que le matériel est installé et testé en conformité avec les instructions d'installations fournies dans ce manuel et en plus assurez-vous que vous êtes branché au port COM adéquat.

Le gestionnaire Plug & Play Manager affichera le message guide suivant :



Si toute installation est conforme et que le matériel est branché, alors sélectionnez "Oui". En quelques instants, le gestionnaire Plug & Play détectera le matériel.

4

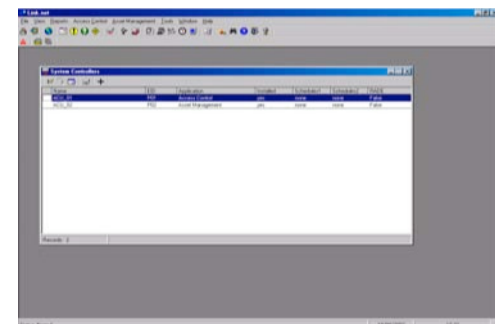


*Le gestionnaire
Plug & Play est
automatiquement
lancé.*

Le logiciel localisera le matériel individuel et ajoutera leurs détails dans la liste. En plus, un bip sonore se fait entendre chaque fois qu'un nouveau matériel est localisé.

5

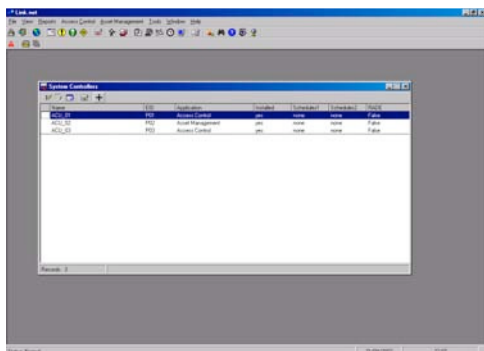
Lorsqu'un nouveau dispositif en matériel est localisé, une zone de texte s'affiche vous demandant **si le contrôleur doit être utilisé**. Répondez "Oui" uniquement si ce N'EST PAS une application de gestion de biens (LT-30AM). Lorsque tout le matériel est localisé, fermez la fenêtre "Contrôleurs du système de réseau" pour terminer la procédure. Cela peut prendre quelques minutes avant que tous les contrôles soient localisés, alors soyez patient.



*Deux contrôleurs localisés s'affichent sur 2
rangées*

Installation manuel du contrôleur

Lorsque vous installez des contrôleurs supplémentaires dans le réseau existant [Link.net](http://link.net), **une installation P & P n'est pas requise une installation manuelle s'applique alors**. Vous pouvez aussi utiliser la fonction « Installer nouveau matériel » à partir du menu « Outils ». Sélectionnez « Contrôleur » à partir des menus « Contrôleur d'accès » ou « Gestion de biens ». Ensuite, sélectionnez la touche « Installer nouveau contrôleur ».



Un nouveau dossier de contrôleur est créé

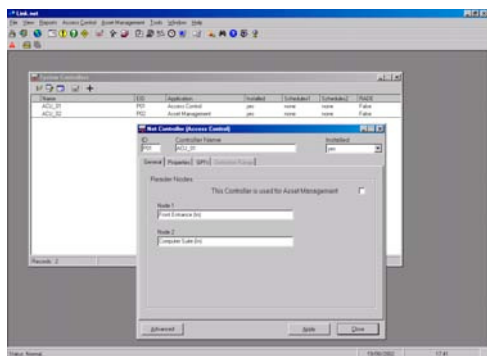
CONSEIL : Le nouveau dossier est créé. Prenez note que la première adresse libre du réseau y est allouée, ainsi, attribuez toujours physiquement les adresses de contrôleurs par ordre chronologique.

Modification des paramètres du contrôleur

Lorsque vous avez localisé la quantité appropriée de contrôleurs, vous devez configurer ce qui suit :

- La fonction – contrôle d'accès ou gestion de biens
- Les paramètres – caractéristiques opérationnels

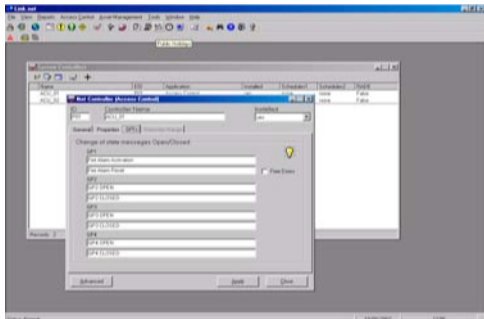
Sélectionnez le dossier du premier contrôleur de la liste et ouvrez-le.



Dossier du contrôleur Link.net (Contrôle d'accès)

Cochez la boîte "Gestion de biens" si ce contrôleur n'est pas utilisé pour le contrôle d'accès (s'il est utilisé pour le contrôle d'accès, ne cochez pas cette boîte). Suivez la procédure qui suit pour configurer un contrôleur d'accès :

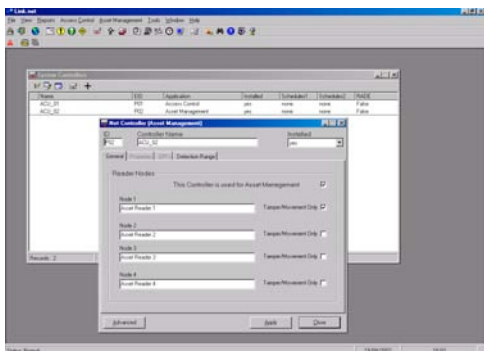
1. À partir de l'onglet Général, allouez des noms aux nœuds 1 et 2 (lecteur de carte 1 et 2) utilisez des noms qui décrivent la porte ainsi que la direction.
2. En plus, vous pouvez allouer un nom plus pertinent pour le contrôleur. Pour un bon choix, nous suggérons son emplacement physique.
3. Sélectionnez l'onglet "Propriétés" et réglez la période de temps (en secondes) requis pour que la porte où sont installés les contrôleurs demeure déverrouillée. Une période de 5 secondes est standard et est le réglage par défaut dans les propriétés.
4. Si ce contrôleur est utilisé pour un contrôle par sas verrouillé entre deux portes, alors, cochez la boîte appropriée pour **activer la fonction logique du** contrôleur (l'interrupteur DIP 6 doit être fermé).
5. Si l'onglet « Entrée universelle » est branché, cela permet l'affichage de messages personnalisés dans l'afficheur « Événements et alarmes » vous pouvez donc vérifier l'état de fermeture et ouverture de portes. Ajoutez simplement ceux-ci dans les champs.
6. Lorsque vous avez terminé, cliquez « Appliquer » et « Fermer ».



The General Inputs TAB

Contrôleur de gestion de biens

Les onglets et afficheurs pour configurer le contrôleur de gestion de biens sont comme suit :

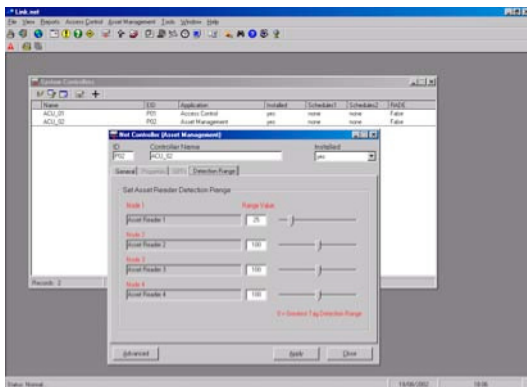


Net Controller Record (Asset Management)

1. À partir de l'onglet "Général" allouez des noms au nœud 1, 2, 3 et 4 (s'il existe une pleine gamme de lecteurs actifs de bien), utilisez des noms représentatifs de leurs zones de couverture.
2. Si l'option « Inviolable/déplacement » est utilisée lorsque pour un lecteur actif de biens précis cela ne sert uniquement qu'à surveiller les déplacements et la violation des étiquettes de biens (si équipé). Si la boîte

n'est pas cochée, la transmission normale de l'étiquette sera signalée comme une alarme. Choisissez cette option si requise.

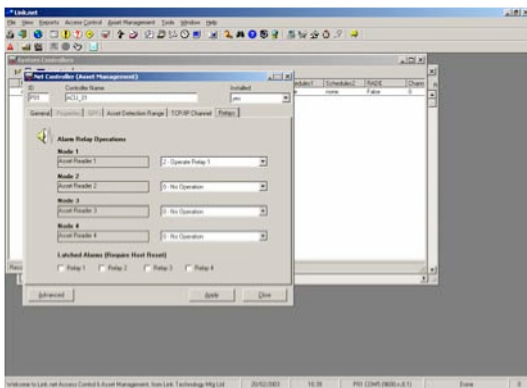
3. Lorsque vous avez terminé, cliquez « Appliquer » et « Fermer ».



The Active Asset Reader Detection Range TAB

Attribution d'une sortie locale de relais pour alarmes de biens

Vous pouvez sélectionner un des relais de contrôleur de gestion de biens pour qu'il opère lors d'une alarme générée par un des lecteurs actifs du contrôleur. De plus, vous pouvez vérifier si la raison de l'alarme est le verrouillage. À partir de la fenêtre « Contrôleur », sélectionnez l'onglet « Relais ».



The Asset Alarm Relay Assignment Tab

Les modes d'opérations ainsi que leurs caractéristiques sont comme suit :

Mode 0 – Aucune opération - aucune activité de relais ne survient même lors d'alarmes à partir de ce lecteur actif.

Mode 1 – Suivi d'alarme de nœud - le relais correspondant du l'alarme du lecteur actif se déclenche si l'alarme est en mode non verrouillé. Cela survient en dépit du réglage du drapeau de relais de verrou correspondant (coché).

Mode 2, 3, 4, 5 – Opère les relais correspondants. Si le drapeau de verrou est coché, peu importe le relais, il restera en position « Ouvert » jusqu'à réinitialisations à partir du PC hôte par l'opérateur détenteur de droits appropriés.

Choix du type d'interface globale en contrôle d'accès

Les micrologiciels en contr le d'acc s les plus r cents : LT-20AC (s rie 10) soutiennent les standards Wiegand ainsi que ceux d'Horloge et Donn es. L'utilisation de l'option 26 bits Wiegand permet la connexion de plusieurs types de lecteur de contr le d'acc s. L'utilisation de l'option Horloge et Donn es standard configur e par d faut offre un protocole plus s curitaire sans erreurs. Que ce soit en usine ou apr s un formatage, le contr leur est r gl  par d faut au standard Horloge et Donn es. Pour modifier le type d'interface en connexion pour les dispositifs Wiegand, premi rement, s lectionnez la section d'options View_Options_Reader et cochez ou d cochez l'option « Utiliser protocole de lecteur de cartes 26 bits Wiegand. Deuxi mement, vous devez acheminer l'information aux contr leurs   partir du format de lecteur de contr le d'acc s Tools_Advanced Controller_Set. Cette fonction est non volatile et ne changera pas m me si le contr leur est sans alimentation  lectrique.

CDV (UK) Ltd, tous droits r serv s, V4.37 ao t 2005.