

AccessLog

EVO/PRO



Configuration de base



6, Rue de l'Industrie
BP130 SOULTZ
68503 GUEBWILLER Cedex

Fax.: 03 89 62 13 31
support@telmatweb.com

Comment contacter notre Support

Tél : 0 367 350 830

1 CONTENU DE VOTRE PACKAGE ACCESSLOG-EVO/PRO	4
2 CONTENU DE VOTRE PACKAGE ACCESSLOG PRO	5
3 CONNEXION DE L'ACCESSLOG-EVO/PRO AU RESEAU	6
4 PRINCIPE DE FONCTIONNEMENT	8
4.1 MODES D'ACCES :	8
4.2 PROFILS D'ACCES :	8
5 ACCES A L'INTERFACE DE CONFIGURATION	9
6 ASSISTANT DE CONFIGURATION	11
7 ASSISTANT DE CONFIGURATION WIFI :	15
8 CONFIGURATION RESEAU	16
9 CONFIGURATION DES ACCES INTERNET :	20
9.1 MODE D'ATTRIBUTION DES IDENTIFIANTS :	20
9.2 MODE ACCES LIBRE AVEC OU SANS DEMANDE D'INFORMATION :	23
9.2.1 Mode accès libre avec code d'accès	26
9.3 PARAMETRAGE DE LA CREATION D'UN IDENTIFIANT PAR L'UTILISATEUR :	27
9.4 CONFIGURATION EMISSION DE MAIL ET DE SMS :	28
9.5 CREATION D'IDENTIFIANT PAR L'ADMINISTRATEUR PAR ENVOI DE MAIL ET DE SMS :	30
9.6 CONFIGURATION DES ACCES RESEAUX SOCIAUX	30
9.6.1 Connexion via le Portail	31
10 PROFIL INTERNET	32
11 CONTROLE PARENTAL ET TEMPS DE MAINTIEN DE LA CONNEXION AU PORTAIL :	35
12 MEMORISATION DES IDENTIFIANTS	36
13 CHANGEMENT DE MOT DE PASSE UTILISATEUR PAR L'UTILISATEUR :	36
14 SUPPRESSION DU COMPTE PAR L'UTILISATEUR :	37
15 ACCES SANS AUTHENTIFICATION	39
15.1 POSTES SANS AUTHENTIFICATION :	39
15.2 RESEAUX SANS AUTHENTIFICATION :	39
16 DECLARATION D'UN NOUVEL IDENTIFIANT PAR L'ADMINISTRATEUR	40
16.1 CHOIX DES INFORMATIONS A SAISIR	40
16.2 PERSONNALISATION DU TICKET UTILISATEUR	40
16.3 CREATION D'UN UTILISATEUR	43
16.4 VISUALISATION DES UTILISATEURS/POSTES CONNECTES	43
17 CREATION D'ADMINISTRATEURS DELEGUES ET MODIFICATION MOT DE PASSE ADMINISTRATEUR	44
18 PERSONNALISATION DU PORTAIL CAPTIF	45
18.1 DESIGN DU PORTAIL CAPTIF AVEC ASSISTANT	45
18.2 DESIGN DU PORTAIL CAPTIF EN MODE EXPERT	47
18.3 DEMANDE D'IDENTIFIANT UTILISATEUR	48
18.4 CHAMPS DE CONFIGURATION POUR LA CREATION D'UN UTILISATEUR	48
19 ADMINISTRATION CLOUD :	51
19.1 INTRODUCTION :	51
19.2 CREATION D'UN COMPTE :	52
19.3 SYNCHRONISATION DES MACHINES RATTACHEES :	55
19.4 LISTE DES MACHINES ASSOCIEES AU COMPTE :	56
19.5 CONFIGURATION REDIRECTION PORTAIL AVANT AUTHENTIFICATION :	56

20 LES TRACES ENREGISTREES PAR ACCESSLOG-EVO/PRO	58
20.1 TRACES D'ACCES.....	58
20.2 LA SAUVEGARDE DES TRACES D'ACCES.....	58
20.3 EXTERNALISATION PERIODIQUE DES TRACES	58
21 RESEAUX PRIVES VIRTUELS (V.P.N.).....	21-1
21.1 INTRODUCTION	21-1
21.2 ACCES AU MENU DE CONFIGURATION.....	21-1
21.3 VPN POUR POSTE DE TRAVAIL DISTANT (PPTP)	21-2
21.3.1 Démarrage du service :.....	21-2
21.3.2 Configuration du serveur VPN PPTP	21-2
21.3.3 Configuration Client PPTP :.....	21-5
21.3.4 Connexion en cours :.....	21-7
21.3.5 Prise en compte des modifications :.....	21-7
21.4 VPN L2TP / IPSEC :.....	21-7
21.4.1 Configuration du service et création du compte PPTP/L2TP :.....	21-7
21.4.2 Configuration du service IPSEC pour L2TP :	21-9
21.4.3 Visualisation des connexions en cours :.....	21-11
21.4.4 Configuration Client de Connexion :	21-12
21.5 CLIENT OPENVPN :	21-14
22 STATISTIQUES	17
22.1 ACTIVITES RESEAU :	17
22.2 ACCES INTERNET :	17
22.3 STATISTIQUES PAR USAGE :.....	19
22.4 CHARGE MACHINE :	19
23 ADMINISTRATION AVANCEE.....	20
23.1 SAUVEGARDE/RESTAURATION DE LA CONFIGURATION	20
23.2 RESTAURATION DE LA CONFIGURATION USINE	21
23.3 MISE A JOUR LOGICIELLE	21
23.4 SAISIE LICENCE :	21
24 ACTIVATION LICENCE OLFE0, FILTRAGE :.....	22
24.1 SOUSCRIPTION NOUVELLE LICENCE OLFE0 :	22
24.2 RESTAURATION CONFIGURATION UTILISATEUR ET USINE :.....	23
24.3 FILTRAGE :	23
ANNEXE 1 : VERIFICATION DU BON FONCTIONNEMENT DU PORTAIL CAPTIF	26
ANNEXE 2 : SUPERVISION DES FONCTIONS	27
ANNEXE 3 : GESTION DES MOTS DE PASSE DES ADMINISTRATEURS	27
ANNEXE 4 : COMPLEMENTS DE CONFIGURATION ET DOCUMENTATION DETAILLEE.....	29

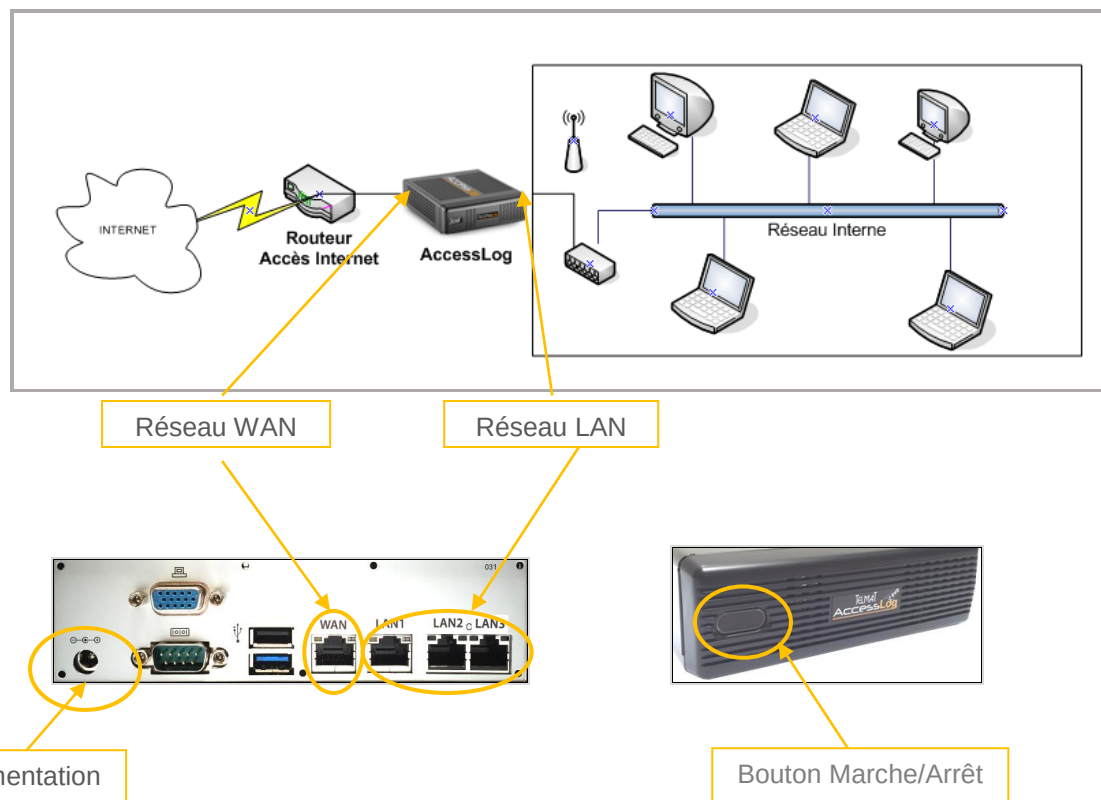
1 Contenu de votre package AccessLog-Evo/Pro

 AccessLog-Evo/Pro	
 Bloc Alimentation	
 Cordon Secteur	
 2 x Câbles Réseaux RJ45 longueur 2 mètres	

2 Contenu de votre package AccessLog Pro

 AccessLog-Pro	
 Cordon Secteur	
 2 x Câbles Réseaux RJ45 longueur 2 mètres	

3 Connexion de l'AccessLog-EVO/Pro au réseau

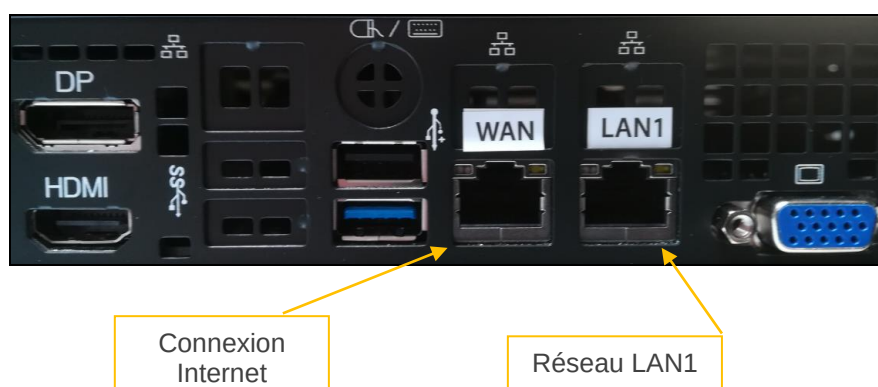


Connecter l'Alimentation, le câble réseau WAN (réseau internet) et LAN (réseau local).

Appuyer sur le bouton Marche/Arrêt pour démarrer la machine. A la fin du démarrage la machine émet **Trois Bips consécutifs**.

Pour **AccessLog Pro** la connectique est la suivante, La connexion internet est sur l'interface WAN et la connexion réseau local sur l'interface LAN1.

En fonction de la configuration matérielle acquise, des extensions réseaux complémentaires sont disponibles. Elles seront référencées LAN2, LAN3



Pré-Requis

Pour configurer la connexion de l'**AccessLog-Evo/Pro** à internet ainsi qu'à votre réseau local, il est nécessaire de disposer des informations suivantes :

Informations relatives à votre connexion Internet

Ces informations vous sont fournies par votre Fournisseur d'Accès Internet (FAI)

- ▶ Adresse IP du routeur
- ▶ Adresse IP du ou des serveurs de nom (DNS primaire et secondaire)
- ▶ Le nom du serveur SMTP pour l'envoi d'emails.

Informations relatives au réseau local

- ▶ Adresse IP et masque associé l'**AccessLog-Evo/Pro**
- ▶ Type Adressage des postes de travail (statique ou dynamique)

4 Principe de fonctionnement

4.1 Modes d'Accès :

Le principe repose sur la capture et la redirection des requêtes internet vers le portail captif. Dès la détection de la demande, l'**AccessLog-Evo/Pro** agira en fonction du paramétrage du portail. Quatre modes sont ainsi disponibles sur la machine.

<u>Authentifié Web / Log</u>	Lors de l'accès à internet une demande d'authentification est présentée. L'utilisateur doit pour continuer saisir dans les champs appropriés les informations demandées. Le filtrage est réalisé en fonction du <i>Code Parental et des horaires</i> . En mode Authentifié Web Les traces sont conservées dans <i>connexions externes et traces proxy</i> En mode Authentifié Log les traces sont conservées dans <i>connexions externes</i> .
<u>Libre / URL</u>	Mode de fonctionnement transparent pour l'utilisateur. Aucune information de connexion au portail n'est demandée. Les restrictions d'accès sont exécutées en fonction du profil associé au réseau. Le filtrage d'accès est réalisé par le proxy. Les traces sont conservées dans <i>connexions externes et traces proxy</i>
<u>Libre /Log</u>	Mode de fonctionnement transparent pour l'utilisateur. Aucune information de connexion au portail n'est demandée. Les restrictions d'accès sont exécutées en fonction du profil associé au réseau. Les traces sont conservées dans <i>connexions externes</i> .

4.2 Profils d'Accès :

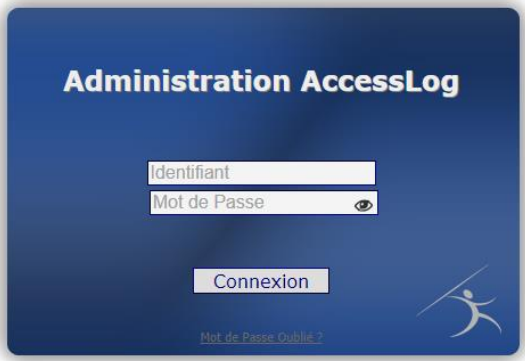
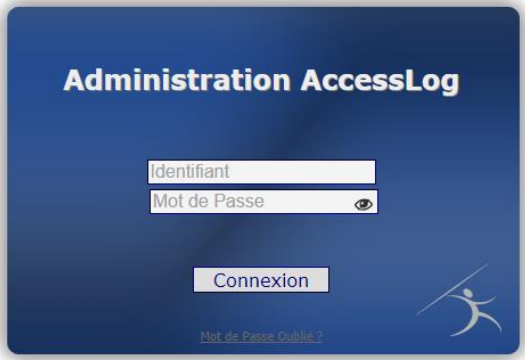
Deux profils, **Base** et **Sécurisé**, sont disponibles. Ils permettent de définir des restrictions différentes en fonction des modes d'Accès et aux utilisateurs lors de leurs créations.

- ✓ **Mode Accès Authentifié Web et Log** : Le profil **Base** ou **Sécurisé** est associé à l'utilisateur au moment de sa création. Si l'utilisateur est créé avec le profil **Base**, celui-ci basculera en profil **Sécurisé** si le code parental est actif et s'il n'est pas saisi correctement au moment de l'authentification. Il basculera également dans ce profil si celui-ci se connecte en dehors des plages horaires autorisées dans le profil de base.
- ✓ **En mode Web** la connexion http (80) est filtrée par le Proxy et les autres connexions par le DNS. En mode **Log** le filtrage de sites est uniquement basé sur le DNS.
- ✓ **Enregistreur de Site Web et de Log** : Le profil est associé au réseau complet sur lequel le portail dans ce mode est en écoute. Si l'interface est configurée en profil **Base**, le basculement en profil **Sécurisé** se fera en fonction des plages horaires autorisées

Multi connexion : Uniquement utilisable en **Mode Accès Authentifié**. Cela permet, en utilisant le même identifiant de se connecter à partir de plusieurs postes simultanément. Peut être utilisé avec ou sans le mode parental. Ce dernier se configure dans le **profil de base/ nouvel utilisateur et Design du portail captif**

La configuration du nombre de connexions se fait par l'onglet Accès **Internet/Accès internet de Bas**

5 Accès à l'interface de configuration

	La configuration et l'administration de l'AccessLog-Evo/Pro se font depuis un poste de travail disposant d'un simple navigateur Web. La connexion est réalisée du côté LAN L'adressage du poste de travail doit être configuré : ▶ Soit en Mode dhcp ▶ Soit avec une adresse IP fixe - Adresse IP de type : 192.168.0.xxx - Masque se sous-réseau : 255.255.255.0 - Passerelle par défaut : 192.168.0.254
	Le lien d'accès à l'interface d'administration est ▶ <u>https://192.168.0.254:99</u> C'est une interface sécurisée, suivre les informations affichées par le navigateur pour accéder à la mire d'authentification
	Les champs à saisir ont les valeurs par défaut suivantes : ▶ Nom d'utilisateur : admin ▶ Mot de passe : webctrl ▶  Permet de visualiser le mot de passe Nous vous recommandons de modifier le mot de passe rapidement ▶ Mot de passe oublié : Possibilité de réinitialiser le mot de passe – uniquement depuis la version TAL_20200730 – Se reporter à l'Annexe 3 du présent document

Si l'authentification est réussie vous accédez aux menus d'administration de l'**AccessLog-Evo/Pro**. Les menus se déploient suite à la sélection d'une entrée. Vous pouvez afficher la barre de menu gauche en cliquant sur  ou la faire disparaître en cliquant sur . Le nom du menu sélectionné est affiché dans cette barre de menu gauche.



L'AccessLog-Evo/Pro dispose d'un assistant de configuration, pour y accéder cliquer sur



. Reportez-vous au chapitre Assistant de Configuration pour plus d'information.

6 Assistant de Configuration

L'AccessLog-Evo/Pro inclut un Assistant de Configuration permettant le paramétrage rapide. Il est décomposé en 13 tableaux qui sont différents en fonction de la configuration désirée. Un redémarrage de la machine est réalisé à la fin du paramétrage. Pour passer au tableau suivant cliquer



sur

Dans chaque tableau ou avant le redémarrage en toute fin de la configuration, il est possible de



revenir en arrière pour réaliser une ou plusieurs modifications. Le paramétrage ne sera pris en compte qu'après le redémarrage.

Pour démarrer l'assistant cliquer sur le titre **AccessLog Administration** ou sur

l'icône .

	Quatre choix sont possibles DEMARRER Lancer l'assistant IMPORT Permet d'importer un fichier de configuration ou de charger la configuration usine. ASSISTANT WIFI Permet la configuration de base de certaines bornes WIFI. La liste est affichée en accédant à la fonction ABANDONNER Pour arrêter l'assistant et revenir dans les menus standards
	Paramétrage du nom de la machine. Pas de caractères spéciaux type, accents, blancs, symboles ... L'email de l'administrateur est l'adresse de messagerie avec laquelle les emails d'administration seront envoyés. Elle doit être valide car certains serveurs de messagerie vérifient cela.
	Paramétrage de la passerelle par défaut, DNS primaire et secondaire – privilégier ceux de votre FAI – Pour l'émission de message, la configuration d'une passerelle SMTP valide est requise

Paramètres Réseaux

Interface	Adresse IP	Masque Réseau	Accès
Wan	192.168.1.254	255.255.255.0 (24)	
Lan1	192.168.0.254	255.255.255.0 (24)	Authentifié / URL
Lan2	192.168.2.254	255.255.255.0 (24)	Inactif
Lan3	192.168.3.254	255.255.255.0 (24)	Inactif



Saisir l'adresse IP et le masque de l'interface WAN, C'est l'interface du côté internet qui est connectée au routeur.

Saisir l'adresse IP et le masque associé du côté LAN. C'est l'interface connectée au réseau interne. Vous sélectionnez le mode de fonctionnement.

Les VLANs ne peuvent être configuré par l'assistant. Utiliser le menu de *Configuration Général*

Configuration du Service DHCP

Interface	Service Actif	Adresse IP de Début	Adresse IP de Fin
Lan1	☒	192.168.0.10	192.168.0.250
Lan2	☒	192.168.2.1	192.168.2.253
Lan3	☒	192.168.3.1	192.168.3.253



Configuration du *dhcp* du côté réseau internet. S'assurer que les adresses à distribuer ne recouvrent pas des IP statiques du réseau. La cohérence de la classe d'adresses avec l'interface LAN est vérifiée lors de l'enregistrement.

ASSISTANT DE CONFIGURATION ÉTAPE 5 / 13

PROFIL D'ACCÈS INTERNET

Selection (Base)

Filtrage des Sites Internet

- Risque Pénal ☒
- Diversissements et Société ☒
- Contenu Adulte ☒
- Bande Passante ☒
- Risque de Sécurité ☒
- Confidentialité ☒
- Services aux Particuliers ☒
- Services aux Entreprises ☒
- Éducation ☒
- Catégories obsolètes ☒
- Autres ☒

Accès Réseau Étendu

- fullaccess ☒
- port_systeme ☒
- port_applicatif ☒
- port_dynamique ☒
- mail ☒
- ftp ☒
- instantmessaging ☒
- microsoftnetwork ☒
- remoteaccess ☒
- http ☒
- sftp ☒
- telnet ☒
- admin ☒
- printers ☒
- phone ☒

Contrôles Horaires

	Début	Fin
Dimanche	00:00	00:00
Lundi	00:00	00:00
Mardi	00:00	00:00
Mercredi	00:00	00:00
Jeudi	00:00	00:00
Vendredi	00:00	00:00
Samedi	00:00	00:00

Profil de Repli ☒

Filtrage des Connexions

Connexions Simultanées par Identifiant (1)

Gestion de la Bande Passante

Débit Maximum (1) Mb

Protocoles Autorisés

- Streaming ☒
- Gaming ☒
- Peer to Peer ☒

MODIFIER



Configuration des deux profils existants : **Base et Sécurisé**.

- ✓ Accès réseau étendu : Ce sont les ports de communications que vous désirez ouvrir lors de la connexion
- ✓ Horaire de connexions :
 - ✗ : tout le temps interdit
 - ✓ : tout le temps autorisé
 - 🔒 Contrôle sur plage horaire
- ✓ Protocole autorisé : Filtrage de protocole en fonction du service utilisé – Le système reconnaît et bloque automatiquement certaines communications
- ✓ Bande passante : Limitation appliquée à tous les utilisateurs connectés via ce profil.
- ✓ Nombre de connexions par identifiant autorisé : uniquement sur *le profil de base*
- ✓ Code parental si activé dans le **Design du portail Captif**
- ✓ Profil de repli : En dehors des plages horaires :
 - ✗ : blocage en dehors des horaires
 - ✓ : basculement en profil **Sécurisé**

Maintien de la Connexion Internet

Par Fenêtre de Présence (Gestion des temps) ✗

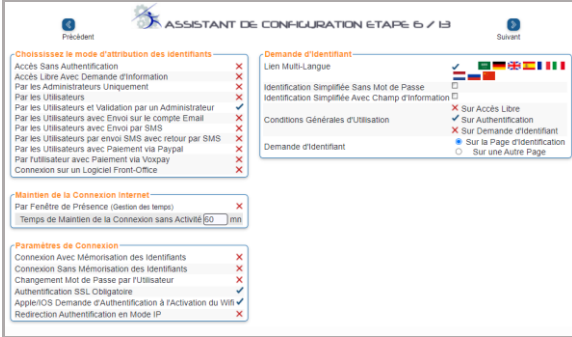
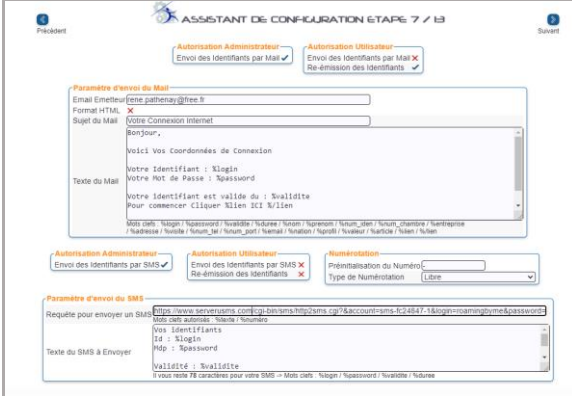
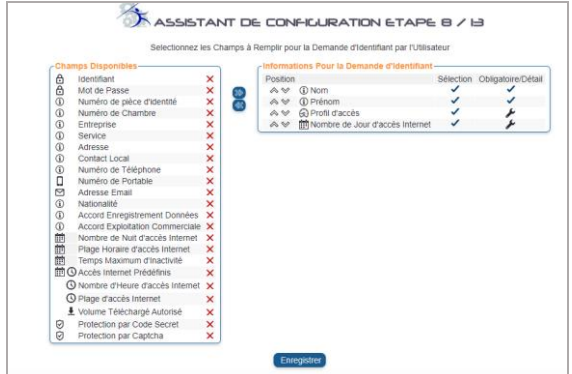
Temps de Maintien de la Connexion sans Activité (2) mn

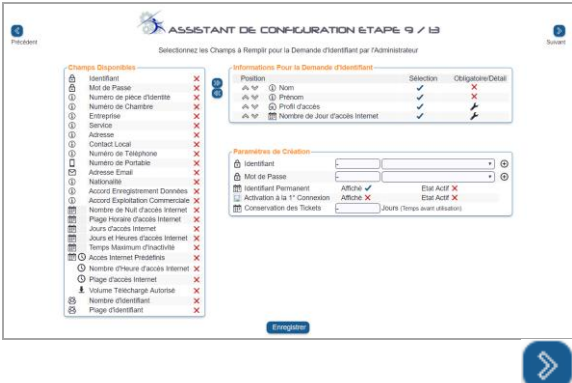
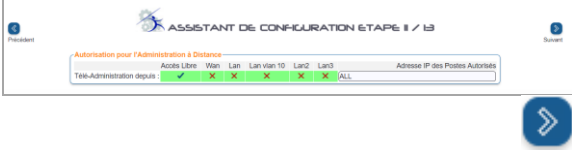
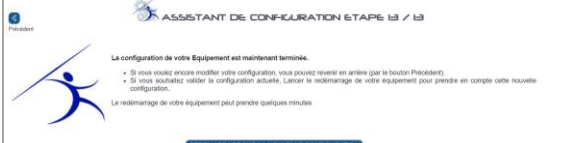
Paramètres de Connexion

- Connexion Avec Mémoire des Identifiants ☒
- Temps de Mémoire (1) Jour(s)
- Mémoire par Cookie ☒
- Connexion Sans Mémoire des Identifiants ☒
- Changement Mot de Passe par l'utilisateur ☒
- Authentification SSL Obligatoire ☒
- Apple/iOS Demande d'Authentification à l'Activation du Wifi ☒
- Redirection Authentification en Mode IP ☒

La mode maintien de la connexion au portail est valide pour tous les utilisateurs.

- ✓ Par Fenêtre de Présence : Gestion des temps de connexion
- ✓ Sans fenêtre de présence : paramétrage du temps de déconnexion
- ✓ Avec ou Sans Mémoire des identifiants : Mémoire de la connexion adresse MAC et IP avec l'identifiant

	✓ Possibilité à l'utilisateur de modifier son mot de passe via le portail de connexion. ✓ Authentification SSL obligatoire ✓ IOS ouverture automatique de la demande d'identification suite à l'obtention d'une adresse IP ✓ L'activation/ désactivation d'une ou plusieurs langues se paramètre en sélectionnant/désélectionnant le drapeau de la langue (colorisation) ✓ L'accès libre avec ou sans demande d'information peut être activé conjointement avec d'autres modes ✓ Condition Générales d'Utilisation : Configuration indépendante sur chaque mode de connexion authentifié.
	Menu présent si le mode attribution par email et/ou SMS validés Envoi Mail/SMS par l'administrateur : L'Administrateur/ Administrateur délégué peut envoyer les identifiants. Autorisation Utilisateur/Envoi des identifiants par mail/SMS : Permet à l'utilisateur d'envoyer son code par email ou SMS suite à sa création via le portail de connexion Ré-émission d'identifiant : permet à l'utilisateur (uniquement) connecté au portail de se rémettre son identifiant : même adresse email ou même numéro de téléphone utilisé lors de la création. Paramétrage des informations d'émission email et/ou SMS
	Configuration de la page de saisie des informations lors de la création d'un identifiant par l'utilisateur qui désire utiliser le portail captif. Ces informations sont affichées sur la page de création de l'utilisateur du portail captif. Possibilité de rendre des champs de saisie obligatoire en cochant la case <i>obligatoire</i> en face du champ. Les paramètres des informations demandées dans le cas de l'accès libre sont sélectionnés spécifiquement Paramétrage du temps de connexion et durée de vie du ticket. L'incompatibilité des champs est visualisé par ■

	Configuration de la page de saisie de l'administrateur ou de l'administrateur délégué. Les champs cochés et paramétrés sont ceux qui s'affichent lors de la création de l'identifiant. Certains champs sont pré paramétrables comme le temps de conservation. Possibilité de rendre des champs de saisie obligatoire en cochant la case <i>obligatoire</i> en face du champ Paramétrage du temps de connexion et durée de vie du ticket. L'incompatibilité des champs est visualisée par ■
	Permet de créer un administrateur délégué. Il dispose de droits spécifiques et a une visibilité restreinte sur les menus.
	Configuration des restrictions de connexions à l'administration de la machine. Ces accès peuvent être soit autorisés ou interdits. Ils peuvent être restreints en configurant dans le champ « adresse Ip et poste autorisé » la classe de réseau ou l'adresse IP du poste. Les adresses ou classes sont séparées par des blancs dans le cas d'une saisie multiple.
	L'administrateur choisit la présentation de la page d'accueil affichée lors de la connexion de l'utilisateur à internet. Elle peut être ensuite remaniée dans la page de configuration du portail.
	Dès que vous cliquez sur le bouton, la machine redémarre pour la prise en compte des modifications.

L'assistant de configuration ne crée pas les utilisateurs – Pour cela, se reporter au chapitre sur la création des utilisateurs.

7 Assistant de Configuration WIFI :

A travers l'assistant de configuration, il est possible de configurer l'accès direct de bornes sur un contrôleur WIFI externe.

L'assistant vous guide au long de la configuration

Assistant de Configuration de Borne Wifi :

Cette fonction permet de déployer rapidement un réseau Wifi dans une configuration basique.

ASSISTANT WIFI

Pour la recherche de bornes, saisissez dans la fenêtre de saisie l'adresse MAC complète ou partielle du contrôleur.

Cliquez sur RECHERCHER

Le contrôleur trouvé suite au scan est affiché –

Remplissez le champ *localisation* (impératif) et pour mettre en place l'exception cocher *Visibilité*

Sélectionnez également le Profil pour le filtrage à appliquer.

Configuration bornes sur contrôleur WIFI Externe

ASSISTANT DE CONFIGURATION WIFI

Cet Assistant permet de configurer les bornes Wifi suivantes :

- Dlink DAP2230
- Dlink DAP2310
- Dlink DAP2310B
- Dlink DAP2360
- Dlink DWL3600AP
- Dlink DAP3662
- Dlink DWL6600AP
- Dlink DAP2660

- Dlink DAP2690
- Dlink DWL3200AP
- Dlink DWL3260AP
- Dlink DAP2360B
- Dlink DAP2590
- Dlink DWL2600AP
- Dlink DAP2610

Les bornes doivent d'abord être connectées au réseau, sous tension et SNMP doit être actif sur celles-ci

Pour les Bornes Pilotées par un Contrôleur Externe, Adresse MAC

RECHERCHE DES BORNES

ASSISTANT DE CONFIGURATION CONTRÔLEUR WIFI EXTERNE

Pour chacune des bornes, vous pouvez configurer les informations suivantes :

- Visibilité : Rend votre borne visible par le contrôleur externe
- Localisation : Information **obligatoire** qui facilite le repérage de la borne
- Adresse IP : Modifiable uniquement si votre borne est en mode DHCP
- DHCP : Si votre borne est en mode DHCP, Pour un fonctionnement plus fiable, Activez cette fonction (case cochée), sinon, ne pas activer cette fonction

Etat	Suppression	Visibilité	Adresse Mac	Localisation	Adresse	Interface	dhcp
■	✗	✓	04:a8:1d:90:07:28	ETAGE 2	192.168.0.50	Lan1	✗

Nouvelle Adresse Scannée

Selection	Visibilité	Adresse Mac	Localisation	Adresse	Interface	dhcp
■	✓	04:a8:1d:90:07:28	ETAGE 2	192.168.0.50	Lan1	✗

Filtré Adresse MAC (04:a8:1d:90:07:28) Profil de Visibilité : [] Scan Réseau ✗ **ENREGISTRER**

8 Configuration Réseau

Après la connexion au service d'administration, le Menu de *Configuration Générale* permet de configurer les interfaces réseau et les services qui s'exécutent sur l'**AccessLog-Evo/Pro**.

AccessLog Administration 192.168.26.16

Utilisateur Accès Internet Statistiques Configuration Administration avancée

CONFIGURATION GÉNÉRALE

Informations Générales

Identifiant AccessLog AccessLog64-142 Email Administrateur rpa@telmat.fr
Niveau de Log 1 Cryptage des Logs

Paramètres de Connexion

Passerelle Par Défaut 192.168.26.254
Adresse DNS FAI primaire 8.8.4.4
Adresse DNS FAI secondaire 8.8.8.8
Passerelle SMTP smtpauth.orange.fr

Paramètres Réseaux

Interface	DHCP	Adresse IP	Masque
Wan		192.168.26.142	255.255.255.0
Lan1		192.168.0.254	255.255.255.0
Lan1 vlan id 10		192.168.10.254	255.255.255.0
Lan1 vlan id 20		192.168.20.254	255.255.255.0
Lan2		192.168.2.254	255.255.255.0
Lan3		192.168.3.254	255.255.255.0

Services Réseaux

- Proxy Web
- Proxy DNS
- Proxy SMTP
- Serveur DHCP
- Serveur FTP
- Serveur VPN PPTP
- Serveur VPN IPSEC
- Client OpenVPN
- Firewall

Administration Serveur

- Administration Web
- Administration Cloud
- Connexion Telnet
- Connexion SSH

Services Réseaux

Interface	Service DHCP	IP Début	IP Fin	Accès	Enregistreur	DNS	SMTP	ZeroConf	Service Web
Wan									
Lan1									
Lan1 vlan id 10									
Lan1 vlan id 20									
Lan2									
Lan3									

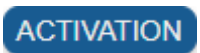
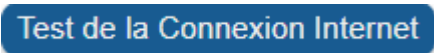
Test de la Connexion Internet

Les interfaces réseaux électriquement connectées sont détectées automatiquement par le système

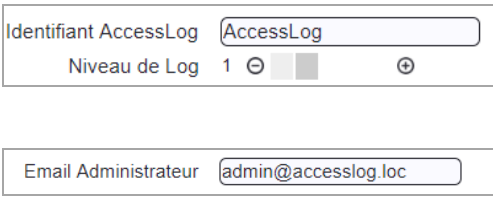
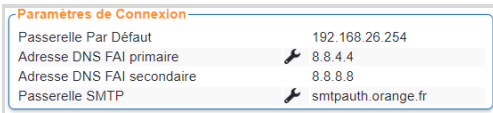
Paramètres Réseaux

Interface	DHCP	Adresse IP	Masque
Wan		192.168.26.135	255.255.255.0
Lan1		192.168.0.254	255.255.255.0
Lan1 vlan id 10		172.16.20.254	255.255.255.0
Lan1 vlan id 20		172.16.200.254	255.255.255.0
Lan1 vlan id 30		10.0.30.254	255.255.255.0
Lan2		192.168.20.254	255.255.255.0
Lan3		192.168.30.254	255.255.255.0

Procédure de Configuration du Réseau

	▶ Cliquer sur l'icône pour passer en mode édition
1 6	▶ Configurer les zones 1, 2, 3, 4, 5, 6
	▶ Enregistrer la Configuration
	▶ Activer la configuration
	▶ Tester la Connexion Internet ▶ Permet de récupérer l'adresse IP publique 2 ▶ Si vous avez une erreur, vérifiez la zone
	▶ Reportez-vous à l'Annexe 1 pour vérifier le fonctionnement de votre réseau local

Détail des informations à configurer

1 	Identifiant AccessLog-Evo/Pro : C'est le nom que vous donnez à la machine. Email Administrateur : Email pour l'émission des emails. Cette adresse doit être valide et acceptée par le serveur SMTP du FAI Niveau de Log : Permet d'ajuster la quantité de traces de Connexions Externes en cliquant sur + ou -.
2 	Passerelle par Défaut : adresse IP et interface réseau du routeur connecté à l'AccessLog-Evo/Pro. Adresse DNS : Ce sont les adresses IP des Serveurs de Nom (DNS) du FAI. Pour ajouter des nom de machines au DNS local cliquer sur  en face de DNS FAI primaire. Passerelle SMTP : Nom ou adresse IP de la passerelle de messagerie du FAI (sinon les mails peuvent ne pas aboutir). Cliquez sur  pour configurer le mode authentifié et une autre adresse d'émission des emails

3

Services Réseaux

Proxy Web	▶ 🔄
Proxy DNS	▶ 🔄
Proxy SMTP	▶ 🔄
Serveur DHCP	▶ 🔄
Serveur FTP	▶ 🔄
Serveur VPN PPTP	▶ 🔄
Serveur VPN IPSEC	▶ 🔄
Client OpenVPN	▶ 🔄
Firewall	▶ 🔄
Filtre URL Cyren	▶ 🔄

Tableau de pilotage des services.

Ne pas modifier les services en cours d'exécution.

▶ || 🔄 : Démarrage, Arrêt, Rechargement du service local

4

Services Réseaux

Interface	Service DHCP	IP Début	IP Fin
Wan			
Lan1	🔧	192.168.0.10	192.168.0.250
Lan2	🔧	192.168.2.10	192.168.2.250
Lan3	🔧	192.168.3.10	192.168.3.250

DHCP : Mise en DHCP client de l'interface. **Attention**, l'interface attend une adresse IP distribuée par un système.

Adresses IP et Masque : Adresse et masque de l'adresse IP fixe de l'interface. Celle pour la connexion internet et celle du réseau local

VLAN ID : C'est l'identifiant VLAN (non l'ID) de l'équipement connecté (borne WIFI Multi-SSID par exemple)

🔧 pour configurer la vitesse de l'interface réseau

5

Administration Serveur

Administration Web	🔧	▶ 🔄
Administration Cloud		▶ 🔄
Connexion Telnet	🔧	▶ 🔄
Connexion SSH	🔧	▶ 🔄

En cliquant sur cette icône 🔧 vous accédez à la configuration des restrictions d'accès. Le firewall est automatiquement réglé et relancé après ACTIVATION de la configuration.

Administration Web	✓	×	×	×	×	×	
Connexion Telnet	×	×	×	×	×	×	212.103.26. 192.168.
Serveur SSH	×	×	×	×	×	×	212.103.26. 192.168.

▶ || 🔄 : Démarrage, Arrêt, Rechargement du service local

Administration Cloud : Se reporter au chapitre **Administration Cloud (9)**

6

Interface	Service DHCP	IP Début	IP Fin	Accès	Enregistreur	DNS	SMTP	ZeroConf	Demande SMS
Wan									
Lan1	🔧	192.168.0.10	192.168.0.250	Authentifié	URL	■	-	-	■
Lan2	🔧	192.168.2.10	192.168.2.250	Authentifié	URL	■	-	-	■
Lan3	🔧	192.168.3.10	192.168.3.250	Authentifié	URL	■	-	-	■

Service DHCP : Démarrage du service DHCP sur l'interface cochée. Déclaration de la plage d'adresses IP distribuées

Portail Captif : Vous choisissez le mode de fonctionnement – se reporter au § Principe de Fonctionnement.

Case DNS : Autorisation de relayage des requêtes DNS sur cette interface.

Case SMTP : Autorisation de relayage des requêtes SMTP sur cette interface.

Cryptage des logs: Permet de crypter les logs contenant les informations de connexions internet des utilisateurs; Se fait à travers une clé générée directement à partir du menu. Cette clé est unique.

Il est impératif de conserver cette clé dans un endroit sûr. Elle est nécessaire pour la lecture des logs archivés. En cas de perte, le déchiffrement est impossible.

Email Administrateur rpat@telmat.fr Cryptage des Logs CRYPTAGE DES LOGS CERTIFICAT DE L'AUTORITE Taille de Clé 2048 ▼ Pays FR ▼ Province France Localité Local Organisation Entreprise Unité AccessLog Nom Usuel (cn) gateway.intranet.loc Adresse Email admin@intranet.loc ENREGISTRER GENERER Cryptage Actif Nombre de Jour d'Archive 3 Nombre de Jour d'Archive Cryptée 0 Cryptage de tous les Logs Importez une Clé  Test de Votre Clé Arrêt du Cryptage	Cocher Cryptage des logs pour la mise en route Générer la clé et conservez la précieusement en cliquant sur Export à la fin de la génération. Elle est téléchargée sur le poste de l'administrateur Cryptage de tous les logs : Démarre le cryptage des logs non cryptés Test de la clé : Permet de charger et de tester la clé. Il faut la charger pour chaque lecture de logs Arrêt du Cryptage : Arrêt du mécanisme soit définitivement ou temporairement
--	--

9 Configuration des Accès Internet :

Le paramétrage dépendra du mode de déclaration d'un nouvel utilisateur ainsi que des champs nécessaires à la création de l'utilisateur.

9.1 Mode d'attribution des Identifiants :

- ✓ Dans les modes avec SMS et/ou email, les champs *adresse email et/ou numéro de portable* sont obligatoires lors de la demande d'identifiant
- ✓ Il est possible d'utiliser simultanément les modes retour par SMS et par Email.

Mode de Déclaration d'un Nouvel Utilisateur <table border="1"> <tbody> <tr><td>Accès Libre</td><td>×</td></tr> <tr><td>Accès Libre Avec Demande d'Information</td><td>×</td></tr> <tr><td>Par les Administrateurs Uniquement</td><td>×</td></tr> <tr><td>Par l'utilisateur</td><td>×</td></tr> <tr><td>Par l'utilisateur et Validation</td><td>✓</td></tr> <tr><td>Par l'utilisateur avec retour par Email</td><td>×</td></tr> <tr><td>Par l'utilisateur avec retour par SMS</td><td>×</td></tr> <tr><td>Par l'utilisateur par envoi SMS avec retour par SMS</td><td>×</td></tr> <tr><td>Par l'utilisateur avec Paiement via Paypal</td><td>×</td></tr> <tr><td>Par l'utilisateur avec Paiement via Voxpay</td><td>×</td></tr> <tr><td>Connexion à un Front Office</td><td>×</td></tr> </tbody> </table>	Accès Libre	×	Accès Libre Avec Demande d'Information	×	Par les Administrateurs Uniquement	×	Par l'utilisateur	×	Par l'utilisateur et Validation	✓	Par l'utilisateur avec retour par Email	×	Par l'utilisateur avec retour par SMS	×	Par l'utilisateur par envoi SMS avec retour par SMS	×	Par l'utilisateur avec Paiement via Paypal	×	Par l'utilisateur avec Paiement via Voxpay	×	Connexion à un Front Office	×	<u>Accès Libre</u> : L'utilisateur peut accéder à Internet en validant la connexion et sans authentification. <u>Accès Libre avec demande d'information</u> : L'utilisateur devra remplir les champs demandés lors de la demande de connexion au portail. Les champs à remplir correspondent à ceux demandés dans la configuration de l'écran de saisie utilisateur. Ce sont les champs infos ⓘ, mail, téléphone paramétrés dans le champs affichés. <i>Les modes Accès Libre ou Accès Libre Avec Demande d'Information peuvent être utilisés conjointement avec les autres modes</i> <u>Par les Administrateurs Uniquement</u> : Seuls les administrateurs définis sont autorisés à créer un nouvel utilisateur. <u>Par l'utilisateur</u> : A la première connexion sur le portail, l'utilisateur devra saisir les informations demandées pour obtenir ses identifiants. <u>Par l'utilisateur et validation</u> : A la première connexion l'utilisateur devra saisir les informations demandées. La demande est alors en attente de validation par l'Administrateur. Suite à l'acceptation les identifiants sont affichés sur le navigateur client. <u>Par l'utilisateur avec retour par Email</u> : A la première connexion l'utilisateur devra saisir les informations demandées (dont son adresse email). Il dispose d'un temps paramétrable pour accéder à sa messagerie et récupérer ses identifiants. <u>Par l'utilisateur avec retour par SMS</u> : A la première connexion l'utilisateur devra saisir les informations demandées (dont son numéro de portable). Ses identifiants de connexion lui seront envoyés par SMS. Sur son téléphone portable. L'administrateur doit souscrire un abonnement auprès d'un fournisseur de SMS. <u>Par l'utilisateur par Envoi SMS et retour par SMS</u> : Pour obtenir un identifiant retourné par SMS, Le client doit envoyer un SMS particulier vers un serveur de SMS. L'administrateur doit souscrire un abonnement auprès d'un fournisseur de SMS.
Accès Libre	×																						
Accès Libre Avec Demande d'Information	×																						
Par les Administrateurs Uniquement	×																						
Par l'utilisateur	×																						
Par l'utilisateur et Validation	✓																						
Par l'utilisateur avec retour par Email	×																						
Par l'utilisateur avec retour par SMS	×																						
Par l'utilisateur par envoi SMS avec retour par SMS	×																						
Par l'utilisateur avec Paiement via Paypal	×																						
Par l'utilisateur avec Paiement via Voxpay	×																						
Connexion à un Front Office	×																						

	<u>Par l'utilisateur avec Paiement via Paypal</u> : lors de sa connexion le client se voit proposer plusieurs choix de durée de connexion. Pour récupérer son identifiant, il doit procéder au paiement via Paypal en suivant les instructions. L'Administrateur doit avoir un compte de type boutique existant chez Paypal. <u>Par l'utilisateur avec Paiement via VoxPay/Monético</u> : lors de sa connexion le client se voit proposer plusieurs choix de durée de connexion. Pour récupérer son identifiant, il doit procéder au paiement via Voxpay en suivant les instructions. L'Administrateur doit avoir un compte de type boutique existant chez Voxpay. La configuration Monético se fait à partir de l'environnement Voxpay en cliquant sur  <u>Connexion sur un Logiciel Front-Office</u> : Permet l'interconnexion sur certains systèmes de réservation d'hôtels. L'Administrateur choisit entre AGSCOM et Meteor.
Maintien de la Connexion Internet Par Fenêtre de Présence (Gestion des temps)  Maintien de la Connexion Internet Par Fenêtre de Présence (Gestion des temps)  Temps de Maintien de la Connexion sans Activité 5 mn	Le choix applicable à tous les utilisateurs en mode authentifié permet de définir le maintien de la connexion <u>Par la fenêtre de présence</u> : le temps de connexion est calculé depuis l'acceptation de l'authentification jusqu'à la fermeture de la fenêtre de présence (forcée ou par le bouton) <u>En mode Sans fenêtre de présence</u> vous pouvez spécifier le temps du maintien de la connexion après la dernière activité sur le poste. Suite à ce temps le poste est déconnecté et une demande d'identification est demandée suite à la reconnexion. <u>Sans fenêtre de présence et mémorisation des identifiants</u> : Dans ce mode, suite à la première identification le système mémorise la connexion provenant du poste. L'utilisateur doit s'authentifier à la première connexion. Le choix lui est laissé pour la mémorisation ou non de la connexion (se souvenir de moi) L'utilisateur n'aura plus à s'authentifier pendant toute la durée d'existence de son identifiant avec le même poste s'il change de poste il devra s'authentifier.

Paramètres de Connexion

Connexion Avec Mémoire des Identifiants	✓
Temps de Mémoire	1 Jour(s)
Mémoire par Cookie	✗
Connexion Sans Mémoire des Identifiants	✓
Changement Mot de Passe par l'Utilisateur	✓
Authentification SSL Obligatoire	✓
Apple/iOS Demande d'Authentification à l'Activation du Wifi	✓
Redirection Authentification en Mode IP	✗

Connexion Avec ou Sans Mémoire des identifiants

Affiche un des deux ou les deux boutons lors de la connexion au portail captif

Se connecter : ne mémorise pas les identifiants ; ils seront demandés à chaque connexion.

Se connecter et se souvenir de moi : Les identifiants sont mémorisés par rapport aux postes. Ceux-ci seront automatiquement affichés dans le portail à toute nouvelle détection de connexion.

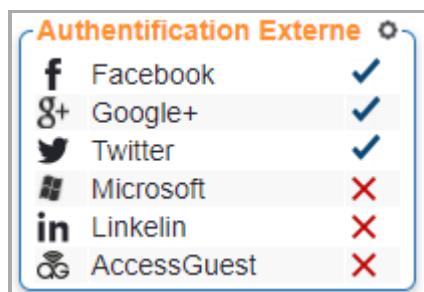
Authentification SSL Obligatoire : Force le mode d'authentification en SSL pour les utilisateurs se connectant au portail

Changement du Mot de Passe par L'Utilisateur : Si activé, donne la permission à l'utilisateur après connexion de modifier son mot de passe : 5 caractères mini. L'utilisateur a la possibilité de supprimer son compte via le portail.

En fonction de la version de l'iOS : la connexion au portail peut, lors de la récupération de l'adresse IP via le DHCP ouvrir automatiquement la demande d'authentification ou pas. Pour mettre en œuvre ou arrêter cette option il suffit de cocher ou de décocher l'option

Temps de Mémoire des identifiants : C'est le temps de mémorisation des identifiants conservé par le système lorsque le mode *Connexion Avec Mémoire des Identifiants* est cochée. A 0 par défaut, correspond à un temps de conservation infini.

Redirection Authentification IP : L'accès au portail se fait par son adresse IP. Pas de résolution DNS effectuée lors de la connexion



L'utilisateur devra cliquer sur l'icône correspondant au réseau social qu'il désire utiliser avant de saisir l'identifiant du réseau social concerné.

- ✓ **f** : utilisation du compte Facebook® de l'utilisateur
- ✓ **Twitter** : utilisation du compte Twitter® de l'utilisateur
- ✓ **g+** : utilisation du compte Google+® de l'utilisateur
- ✓ **in** : utilisation du compte Linkelin® de l'utilisateur
- ✓ **Microsoft** : utilisation du compte MicroSoft® de l'utilisateur
- ✓ **AccessGuest** : se reporter sur le site <https://accessquest.fr>

La configuration des couleurs se fait dans le **design du portail captif** : Onglet et texte choix identifiant. La durée de connexion se paramètre dans l'écran de saisie utilisateur : *Nombre d'heures d'accès Internet*. Les valeurs mini et maxi doivent être identiques.

9.2 Mode Accès libre avec ou sans Demande d'Information :

Le mode - Accès Libre ou Accès Libre Avec Demande D'Information peut être utilisé conjointement avec un des autres modes de déclaration.

Accès Libre sans demande d'information

Paramétrage du mode

Le mode de déclaration doit être paramétré en conséquence.

Mode de Déclaration d'un Nouvel Utilisateur	
Accès Libre	✓
Accès Libre Avec Demande d'Information	✗
Par les Administrateurs Uniquement	✗
Par l'utilisateur	✗
Par l'utilisateur et Validation	✗
Par l'utilisateur avec retour par Email	✓
Par l'utilisateur avec retour par SMS	✗
Par l'utilisateur par envoi SMS avec retour par SMS	✗
Par l'utilisateur avec Paiement via Paypal	✗
Par l'utilisateur avec Paiement via Voxpay	✗
Connexion à un Front Office	✗

Aucune information n'est demandée à l'utilisateur. Lors de cette connexion, une validation des conditions générales d'utilisation d'internet peut être demandée (cf Design Portail Captif)
Dans la fenêtre de connexion, l'utilisateur doit cliquer sur le bouton **SE CONNECTER**.

Dans les Utilisateurs Actifs, l'accès libre est visible par l'adresse IP du poste.

Utilisateur Accès Internet Statistiques Configuration Administration avancée									
LISTE DES UTILISATEURS									
Nombre d'utilisateur Déclarés : 0 Connectés : 1 Nombre de Licence : 1 / 50									
192.168.0.107	✓	Base	14/01/2019 11:47	14/01/2019 19:47	30.3Ko	10s /-			
MODIFIER									

Paramétrage des limites :

Le paramétrage des limites se fait par le menu d'*Ecran de saisie Utilisateur*.

Limitation des Connexions Libres		
Période de Supervision	1	Jour(s) ▼
Temps Maximum de Connexion	10	Minute(s) ▼
Nombre Maximum de Connexion	2	

Période de Supervision : Durée de mémorisation du compteur et du temps de connexion par poste ; Remis à zéro après chaque fin de période.

Temps maximum de connexion : C'est le temps alloué au poste pour se connecter pendant toute la Période de supervision.

Nombre Maximum de connexions : Nombre maximum de connexions possibles pendant le temps maximum de connexion paramétré.

Accès Libre Avec demande d'Information :

Le mode de déclaration doit être paramétré en conséquence.

Mode de Déclaration d'un Nouvel Utilisateur	
Accès Libre	✗
Accès Libre Avec Demande d'Information	✓
Par les Administrateurs Uniquement	✗
Par l'utilisateur	✗
Par l'utilisateur et Validation	✗
Par l'utilisateur avec retour par Email	✓
Par l'utilisateur avec retour par SMS	✗
Par l'utilisateur par envoi SMS avec retour par SMS	✗
Par l'utilisateur avec Paiement via Paypal	✗
Par l'utilisateur avec Paiement via Voxpay	✗
Connexion à un Front Office	✗

L'utilisateur devra remplir les champs demandés lors de la demande de connexion au portail.

Paramétrage des champs :

Les champs à remplir correspondent à ceux demandés dans la configuration de l'écran de saisie utilisateur.

Ce sont les champs infos ① mail, téléphone paramétrés dans le champs affichés.

Champs Obligatoire :

Les champs peuvent être rendus obligatoires. En cas d'omission un message d'erreur est affiché.

Informations Pour la Demande d'Identifiant			
Position		Actif	Obligatoire/Détail
Identifiant	✓	✓	✗
Mot de Passe	✓	✓	✗

Welcome

Demande d'Utilisation Internet

Adresse Email : Informations incomplètes !

Merci d'indiquer vos Coordonnées

Nom : bon

Prénom : jean

Adresse Email :

☒ J'accepte l'enregistrement de mes données personnelles

☒ J'accepte l'exploitation commerciale de mes données personnelles

VALIDER

La raison de l'échec est consignée dans les traces de Gestion de Utilisateurs.

Sélection / Filtre			
Début		Fin	
14/Jan/2019:11:55:41	Base	192.168.0.107	Erreur email : Pb Taille / Format
14/Jan/2019:11:55:18	Base	free-access	deconnect [-] [192.168.0.107] [9c:
14/Jan/2019:11:47:17	Base	free-access	connect [-] [192.168.0.107] [9c:

Lorsque l'utilisateur se connecte au portail il doit saisir les informations requises.

Dans la fenêtre de connexion, l'utilisateur doit cliquer sur le bouton **SE CONNECTER**.
Les connexions en cours sont affichées dans liste d'utilisateur. Seule l'adresse IP du poste est affichée.

LISTE DES UTILISATEURS									
Nombre d'utilisateur Déclarés : 4 Connectés : 1 Nombre de Licence : 1 / 50									
Identifiant	Profil d'accès	N° de Portable	Adresse Email	Début d'autorisation	Fin d'autorisation	Volume	Temps	IP	
sa	Base	-	-	22/07/2021 15:48	-	-	1h06m	-	A341
sg1	Base	0679973197	spathenay@gmail.com	26/07/2021 09:27	-	-	-	-	A346
jms2	Sécurisé	0679973197	rene.pathenay@laposte.net	26/07/2021 09:27	-	-	-	-	A347
tpa	Sécurisé	0679973197	rpa@telmat.fr	26/07/2021 09:27	-	-	-	-	A348

MODIFIER

Les informations de connexions - champs complémentaires sont récupérées dans les traces de gestion utilisateur

- - - - - 1547463558 1547467158 0 1 A110 jean.bon@email.dom - - y y - -									
Début Fin Toutes Filtre VALIDER									
14/Jan/2019:11:55:18	Base	dslog15e	create	[admin_user]	[192.168.0.107]	[192.168.0.107]	[14/Jan/2019:11:55:18]	[14/Jan/2019:11:55:18]	[14/Jan/2019:11:55:18]

Paramétrage des limites :

Le paramétrage des limites se fait par le menu d'Ecran de saisie Utilisateur.

Informations Pour la Connexion Libre		Limitation des Connexions Libres	
Position	Actif	Obligatoire/Détail	
① Nom	✓	✓	Période de Supervision 1 Jour(s)
① Prénom	✓	✓	Temps Maximum de Connexion 10 Minute(s)
✉ Adresse Email	✓	✓	Nombre Maximum de Connexion 2
① Accord Enregistrement Données	✓	✓	
① Accord Exploitation Commerciale	✓	✓	

Période de Supervision : Durée de mémorisation du compteur et du temps de connexion par poste ; Remis à zéro après chaque fin de période.

Temps maximum de connexion : C'est le temps alloué au poste pour se connecter pendant toute la Période de supervision.

Nombre Maximum de connexions : Nombre maximum de connexions possibles pendant le temps maximum de connexion alloué.

9.2.1 Mode accès libre avec code d'accès

Ce mode de configuration permet de demander un code d'accès lors de la connexion en mode libre. Permet en fonction du code d'affecter un profil à l'utilisateur/poste qui se connecte. C'est une protection qui permet de mettre en place un contrôle sur les connexions sans avoir à créer d'utilisateur.

Il faut être en mode **Accès libre avec demande d'information** pour utiliser cette fonction.

Champs Disponibles		Informations Pour la Demande d'Identifiant		Protection Contre les Demandes Abusives d'Identifiant	
		Position	Actif	Obligatoire/Détail	
① Nom	✗	✗			Temps de Relevé de Mail 0 mn
① Prénom	✗	✗			Temps entre Deux Demandes 1 mn
① Identifiant	✗	✗			Limitation des Demandes par Inactif
① Mot de Passe	✗	✗			Adresse Mac
① Profil d'accès	✗	✗			
① Numéro de pièce d'identité	✗	✗			
① Numéro de Chambre	✗	✗			
① Entreprise	✗	✗			
① Service	✗	✗			
① Adresse	✗	✗			
① Contact Local	✗	✗			
① Numéro de Téléphone	✗	✗			
① Numéro de Portable	✗	✗			
✉ Adresse Email	✗	✗			
① Nationalité	✗	✗			
① Accord Enregistrement Données	✗	✗			
① Accord Exploitation Commerciale	✗	✗			
① Nombre de Jour d'accès Internet	✗	✗			
① Nombre de Nuit d'accès Internet	✗	✗			
① Plage Horaire d'accès Internet	✗	✗			

Informations Pour la Connexion Libre	
Position	Actif
✗ Protection par Code Secret	✓

PARAMETRE DÉTAILLÉ	
Protection par Code Secret	
En Cas d'erreur de Mot de Passe	Refus
Mot de Passe	Moncode
Mot de Passe	Sécurisé
Mot de Passe	Défaut
Mot de Passe	Base
Mot de Passe	Sécurisé
VALIDER	

Sélectionner **Protection par Code Secret** en l'affectant à **Informations Pour la Connexion Libre**.

Cliquer sur 

PARAMETRE DÉTAILLÉ	
Protection par Code Secret	
En Cas d'erreur de Mot de Passe	Refus
Mot de Passe	Moncode
Mot de Passe	Sécurisé
Mot de Passe	Défaut
Mot de Passe	Base
Mot de Passe	Sécurisé
VALIDER	

Paramétrer le code et affecter le profil.

Toute erreur de saisie de code par l'utilisateur refuse la connexion.

9.3 Paramétrage de la création d'un identifiant par l'utilisateur :

Seuls ces modes de création nécessitent un paramétrage de l'interface de saisie utilisateur.

Les modes de déclaration ainsi que les types de connexions autorisées sont définis dans ce menu. Après modification cliquez sur **MODIFIER** pour enregistrer et la prise en compte des valeurs.

- ✓ Temps de relevé : Temps imparti à l'utilisateur pour lire son email sans passer par une authentification
- ✓ Temps entre demandes : Temps minimum entre deux demandes d'identifiant.
- ✓ Limitation des demandes : Permet de restreindre le nombre de demandes faites par l'utilisateur sur le portail. Un filtrage peut être réalisé en fonction du champ paramétré et du nombre de demandes.
- ✓ Format Identifiant : possibilité de choisir le format de l'identifiant créé (caractères, chiffres, champs ...) - S'il n'y a pas de saisie de valeurs, l'identifiant et le mot de passe sont générés de manière aléatoire.

9.4 Configuration Emission de Mail et de SMS :

Seuls ces trois modes ont un menu spécifique de configuration pour le portail captif en mode identifié

Mode de Déclaration d'un Nouvel Utilisateur	
Accès Libre	×
Accès Libre Avec Demande d'Information	✓
Par les Administrateurs Uniquement	×
Par l'utilisateur	×
Par l'utilisateur et Validation	×
Par l'utilisateur avec retour par Email	✓
Par l'utilisateur avec retour par SMS	✓
Par l'utilisateur par envoi SMS avec retour par SMS	×
Par l'utilisateur avec Paiement via Paypal	×
Par l'utilisateur avec Paiement via Voxpay	×
Connexion à un Front Office	×

CONFIGURATION POUR L'ENVOI DE MAIL

Autorisation Administrateur : Envoi des identifiants par Mail ✓

Autorisation Utilisateur : Envoi des identifiants par Mail ×, Ré-émission des identifiants ✓

Paramètres d'envoi du Mail

Email Emetteur : rene.patheray@free.fr

Format HTML : ✓

Sujet du Mail : Votre Connexion Internet

Texte du Mail :

Bonjour,

Voici Vos Coordonnées de Connexion

Votre Identifiant : %login

Votre Mot de Passe : %password

Votre Identifiant est valide du : %validite

Pour commencer Cliquez Xlien ICI %lien

Mots Clés : %login / %password / %validite / %adresse / %nom / %prenom / %num_dan / %num_chambre / %entreprise / %adresse / %ville / %num_tel / %num_port / %email / %fonction / %profil / %valeur / %article

MODIFIER

L'émission des emails peut se faire en mode texte ou html.

Attention, l'émission d'email doit se faire à travers un SMTP valide et une adresse d'émission valide également.

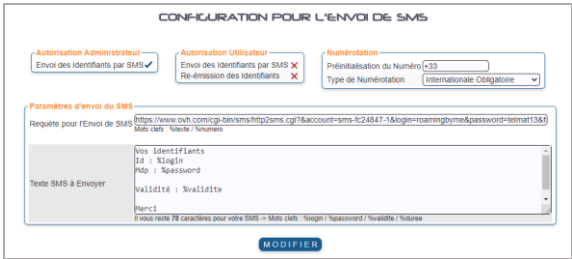
Si aucune adresse email n'est saisie, c'est celle définie dans la configuration générale qui sera utilisée.

Autorisation Administrateur / Envoi des identifiants par email : donne la possibilité à l'administrateur ou l'administrateur délégué d'envoyer l'identifiant par email.

Autorisation Utilisateur/Envoi des Identifiants par Mail : Autorise l'utilisateur à s'envoyer son identifiant suite à sa création via le portail utilisateur – Son adresse email doit être saisie dans les champs demandés

Autorisation Utilisateur/Réémission des Identifiants : Autorise l'utilisateur à s'envoyer son identifiant suite à sa création via le portail utilisateur – Son adresse email doit être saisie dans les champs demandés

Format HTML : Le mail envoyé est formaté en HTML. Permet de mettre des liens utilisables par l'utilisateur – Attention les mails dans ce format peuvent être bloqués par les antispams

	Pour utiliser cette fonction vous devez disposer d'un compte SMS chez un opérateur qui permet d'envoyer des SMS via une API SMS de type WEB. <u>Autorisation Administrateur/Envoi des Identifiants par SMS</u> : Permet l'envoi de l'identifiant par l'administrateur/administrateur délégué- Le numéro de portable doit être obligatoirement présent dans les champs à saisir. <u>Autorisation Utilisateur/Envoi des identifiants par SMS</u> : Permet l'envoi de l'identifiant par l'utilisateur via le portail d'authentification- Le numéro de portable doit être obligatoirement présent dans les champs à saisir. <u>Autorisation Utilisateur/Réémission des Identifiants</u> : Lors de la saisie du même numéro de portable, l'identifiant et mot de passe identiques à la création sont renvoyés. <u>Numérotation/Pré initialisation du Numéro</u> : Permet de préfixer le numéro de portable qui sera saisi- (ex 00, +33...) <u>Type de numérotation</u> : Trois choix possible • Libre : Saisie libre du numéro • International Obligatoire : Pré fixage du numéro en utilisant le paramétrage de Pré initialisation du numéro. • National uniquement : restreint la numérotation aux numéros portables uniquement. <u>Paramètres d'Envoi du SMS</u> : • Requête d'envoi du SMS : C'est l'URL d'émission du SMS vers l'opérateur- C'est ce dernier qui vous donne le lien de connexion à son API. En paramètre du SMS %texte : le libellé du SMS et %numero : le numéro de portable saisi pour la création du ticket • Texte SMS à Envoyer : Vous rédigez le texte qui sera émis (max 156 caractères) – les mots clés sont %login, %password, %validite, %duree.
---	---

9.5 Création d'identifiant par l'Administrateur par envoi de Mail et de SMS :

L'administrateur peut envoyer les identifiants qu'il crée par email ou par SMS. Dans les menus respectifs de configuration email et SMS la case Envoi de SMS ou de Mail par l'Administrateur doit être cochée.

	Dans le menu de création d'un nouvel utilisateur les boutons Envoi par MAIL, Envoi par SMS et Envoi par mail & SMS seront présents si les champs Adresse Email et Numéro de Portable sont présents dans les Champs affichés de la Configuration du Menu Administrateur. Il est possible de créer des utilisateurs par import de liste- Permet dans ce cas, en une seule opération, d'envoyer des identifiants à de multiples destinataires par email, SMS ou SMS et Email simultanément.
Configuration Administrateur	Création de l'utilisateur et envoi du mail

9.6 Configuration des Accès Réseaux Sociaux

L'authentification Réseaux Sociaux est une alternative possible pour la connexion internet sans la création directe d'un utilisateur à travers le portail captif.

La configuration est réalisée dans le menu de Mode d'Attribution des Identifiants.

MODE D'ATTRIBUTION DES IDENTIFIANTS

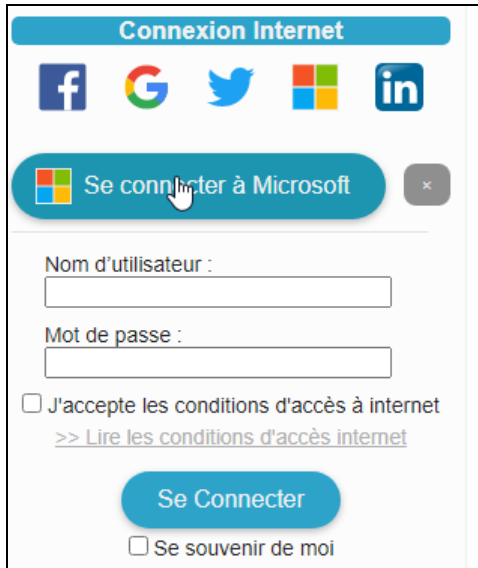
Mode de Déclaration d'un Nouvel Utilisateur		Authentification Externe	
Accès Libre	X	Facebook	✓
Accès Libre Avec Demande d'Information	X	Google+	✓
Par les Administrateurs Uniquement	X	Twitter	✓
Par l'utilisateur	✓	Microsoft	✓
Par l'utilisateur et Validation	X	Linkelin	✓
Par l'utilisateur avec retour par Email	X	AccessGuest	X
Par l'utilisateur avec retour par SMS	X		
Par l'utilisateur par envoi SMS avec retour par SMS	X		
Par l'utilisateur avec Paiement via Paypal	X		
Par l'utilisateur avec Paiement via Voxpay	X		
Connexion à un Front Office	X		

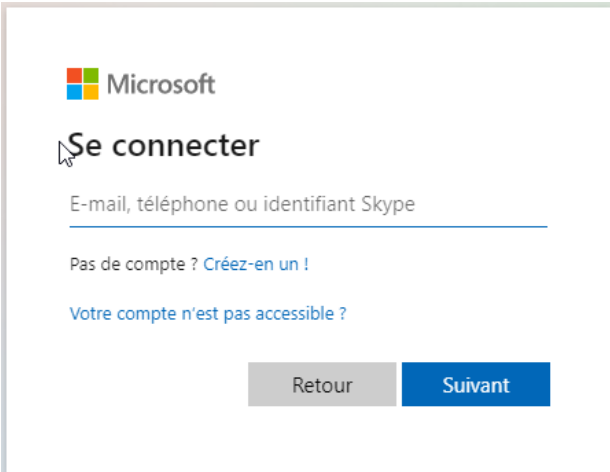
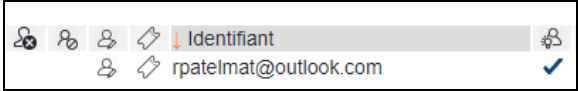
Suite à la sélection des réseaux sociaux désirés, vous pouvez paramétrer les applications pour chaque réseau social . Par défaut, l'**AccessLog-Evo/Pro** est configurée avec les applications de Telmat Industrie. Pour développer des nouvelles applications vous devez utiliser le mode Développeur de chaque réseau. Vous devez pour cela vous créer un compte développeur

Facebook, Google ...Puis référez-vous à chaque guide de développement mis à disposition par chaque réseau Social pour réaliser votre développement logiciel.

9.6.1 Connexion via le Portail

L'utilisateur clique sur l'icône réseau social qu'il désire utiliser

Choix du réseau social	Validation de la connexion
	

L'utilisateur est redirigé vers l'authentification du réseau Social choisi	Dans le cas d'une connexion, identifiant de connexion dépend du réseau social utilisé
	

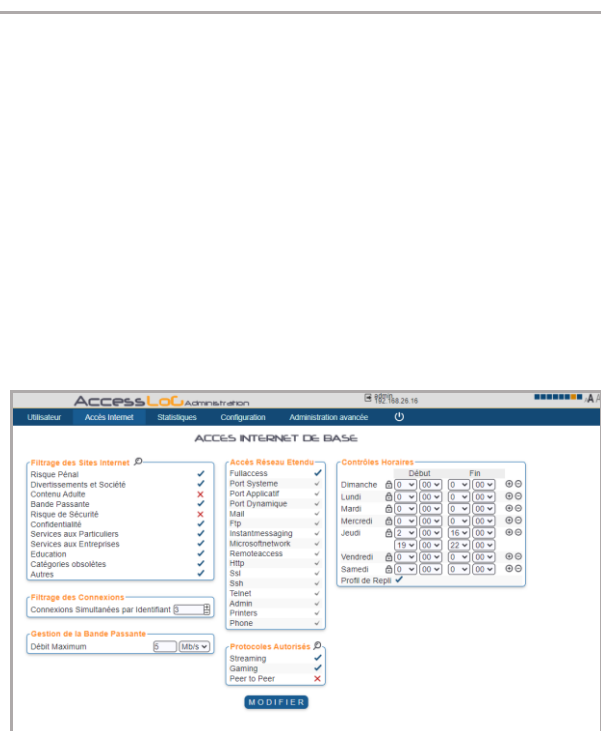
10 Profil Internet

Quel que soit le mode de connexion au portail utilisé ; authentifié, Web ou Log, vous pouvez utiliser les profils d'accès pour contrôler les connexions : Deux profils sont disponibles : **Base et Sécurisé**

Le profil de repli (contrôle parental ou horaire) est le profil Sécurisé

Le nombre d'identifiants par utilisateur se configure dans le profil de Base

Profil de Base :

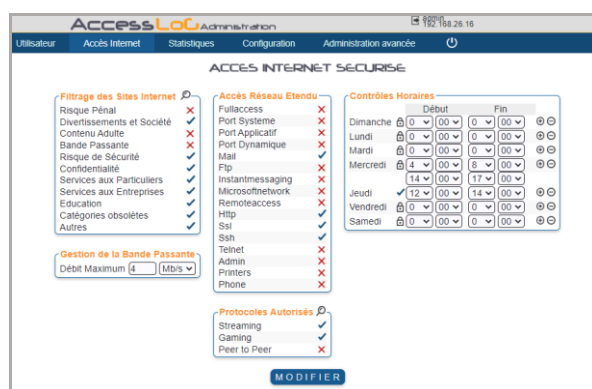


La configuration permet de restreindre

- ✓ Les ports de communication : Accès réseau étendu
- ✓ Le blocage par analyse de protocole : Protocole autorisé par détection automatique ; accès à la liste détaillée des protocoles en cliquant sur
- ✓ Gestion de la bande passante : Débit maxi alloué pour chaque utilisateur se connectant via ce profil
- ✓ Code Parental : Code pour la connexion via de profil. Cette option pour être présente doit être validée dans le panneau de Design du Portail Captif
- ✓ Connexion Simultanées par identifiant : Nombre autorisé de connexion de postes différents utilisant le même identifiant
- ✓ Filtrage des sites internet : c'est une option payante - si elle n'est pas souscrite le paramétrage n'est pas présent
- ✓ Contrôle horaire : Trois états sont possibles
 - ✓ : toujours autorisé
 - ✗ : toujours bloqué
 - : contrôle sur la plage horaire, basculement sur le profil de repli en dehors de la plage horaire

Suivant le **profil de repli** choisi

 - ✗ Blocage de l'accès
 - ✓ Basculement sur le profil sécurisé

Profil Sécurisé :

La configuration permet de restreindre

- ✓ Les ports de communication : Accès réseau étendu
- ✓ Le blocage par analyse de protocole : Protocole autorisé par détection automatique; accès à la liste détaillée des protocoles en cliquant sur
- ✓ Gestion de la bande passante : Débit maxi alloué pour chaque utilisateur se connectant via ce profil
- ✓ Code Parental : Code du code parental pour la connexion via de profil. Cette option pour être présente doit être validée dans le panneau de Design du Portail Captif
- ✓ Connexion Simultanées par identifiant : Nombre autorisé de connexion de poste différents utilisant le même identifiant
- ✓ Filtrage des sites internet : c'est une option payante - si elle n'est pas souscrite le paramétrage n'est pas présent
- ✓ Contrôle horaire : Trois états sont possibles
 - : toujours autorisé
 - : toujours bloqué
 - : blocage en dehors de la plage horaire.

Le profil **sécurisé** est mis en œuvre lorsque :

- ✓ L'utilisateur est créé avec ce profil
- ✓ Le code parental (lorsqu'il est demandé) n'est pas correctement saisi
- ✓ L'utilisateur est en dehors des plages horaires autorisées dans le profil de **base** et que le profil de repli est autorisé ()

Configuration complémentaire des profils :

1 Filtrage des Sites Internet ⓘ - Risque Pénal ✓ - Divertissements et Société ✓ - Contenu Adulte ✓ - Bande Passante ✓ - Risque de Sécurité ✓ - Confidentialité ✓ - Services aux Particuliers ✓ - Services aux Entreprises ✓ - Education ✓ - Catégories obsolètes ✓ - Autres ✓	Si cette option (Filtrage Par Catégories de Sites) est présente et active : Permet de sélectionner les catégories de sites interdits ou autorisés applicables aux utilisateurs liés au profil lors de la navigation. ✗ Interdiction d'accès ✓ Autorisation d'accès ⓘ Permet d'accéder à la configuration de la classification des sites interdits Cf chapitre Activation et filtrage Olféo pour la configuration.
2 Protocoles Autorisés - Streaming ✓ - Gaming ✓ - Peer to Peer ✗	Ce sont les droits d'accès mis en place automatiquement lors de la connexion des utilisateurs à internet après authentification. Pour ouvrir ou fermer les ports de communication cliquez sur ✓ ou ✗ <i>Fullaccess</i> équivaut à tous ports et protocoles
3 Gestion de la Bande Passante Débit Maximum 0 Mb/s ▼	Débit maximum autorisé pour chaque utilisateur connecté via le profil.

11 Contrôle Parental et Temps de maintien de la connexion au portail :

Ce code de connexion peut être demandé si vous désirez mettre en œuvre cette protection. Elle permet de faire la distinction entre une connexion authentifiée utilisant le profil de **base** et celle passant par le profil **sécurisé**.

Cette demande doit être active et visible lors de la connexion au portail

Elle est configurée dans l'onglet **Design du portail Captif** (doit être cochée) - Sinon les champs ne sont pas présents dans les menus.

Le paramétrage du code parental se fait :

Dans le profil de base	Dans l'onglet création d'un nouvel utilisateur

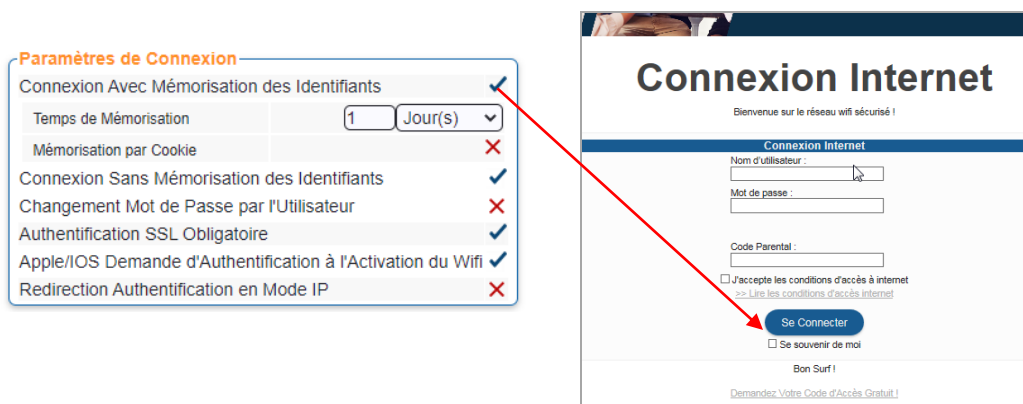
Temps de maintien de la connexion au portail :

En mode Sans fenêtre de présence vous pouvez spécifier le temps du maintien de la connexion après la dernière activité sur le poste. Suite à ce temps le poste est déconnecté et une demande d'identification est demandée suite à la reconnexion - le poste doit toujours être présent sur le réseau.

Reportez vous au chapitre Portail Captif pour plus de précision

12 Mémorisation des Identifiants

Il est possible de mémoriser les identifiants et mot de passe lors de la connexion de l'utilisateur à internet via le portail captif.



A sa première connexion l'utilisateur devra cliquer sur **SE CONNECTER Et se souvenir de moi**. Lors de toute connexion ultérieure avec le même poste, les champs d'identification seront pré-remplis. Le temps de mémorisation est paramétrable. A l'expiration, les champs d'identification seront vides. L'utilisateur devra s'authentifier. La mémorisation de l'identifiant correspond à l'association temporaire adresse MAC du poste et l'identifiant – Dans le cas d'adresse MAC dynamique il est possible de mémoriser par Cookie dans le navigateur.

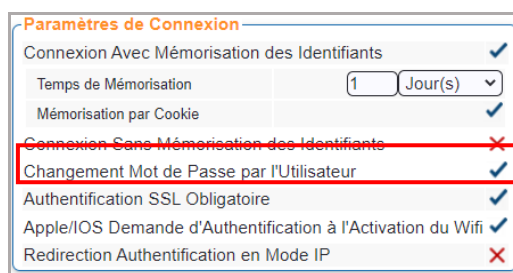
Si seule l'option **Connexion Avec Mémorisation de Identifiants** est cochée, il n'y aura que le bouton **Se connecter** affiché sur le portail. La mémorisation sera automatique.

13 Changement de mot de passe utilisateur par l'utilisateur :

En cochant cette option vous donnez la possibilité à l'utilisateur de changer son mot de passe via le portail.

Cette fonction n'est possible que pour des utilisateurs locaux. N'est pas fonctionnelle pour des utilisateurs déportés (Multibox).

Le mot de passe ne peut être changé qu'après connexion et identification de l'utilisateur au portail.



- ✓ L'option *Changement du mot de Passe Utilisateur* doit être cochée.
- ✓ L'utilisateur se connecte au portail avec son identifiant.

Suite à sa connexion l'utilisateur doit cliquer sur *Modification de Votre mot de Passe*.

Il doit alors saisir son mot de passe courant et saisir le nouveau mot de passe- **Ce nouveau mot de passe à une longueur minimale de 5 caractères alphanumériques.**

Suite à la saisie, il est redirigé vers le portail

Cette modification n'est possible que si la page du portail est affichée après connexion –Dans le cas sans fenêtre de présence et tant que le poste sera mémorisé (connexion avec mémorisation) la page de connexion ne sera pas visible.

14 Suppression du compte par l'utilisateur :

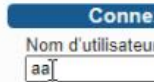
En cochant cette option vous donnez la possibilité à l'utilisateur de changer son mot de passe via le portail.

Cette fonction n'est possible que pour des utilisateurs locaux. N'est pas fonctionnelle pour des utilisateurs déportés (Multibox).

Le mot de passe ne peut être changé qu'après connexion et identification de l'utilisateur au portail.

Paramètres de Connexion	
Connexion Avec Mémorisation des Identifiants	✓
Temps de Mémorisation	1 Jour(s) ✓
Mémorisation par Cookie	✓
Connexion Sans Mémorisation des Identifiants	✗
Changement Mot de Passe par l'Utilisateur	✓
Authentification SSL Obligatoire	✓
Apple/iOS Demande d'Authentification à l'Activation du Wifi	✓
Redirection Authentification en Mode IP	✗

- ✓ L'option *Changement du mot de Passe Utilisateur* doit être cochée.
- ✓ L'utilisateur se connecte au portail avec son identifiant.



Connexion Internet

Nom d'utilisateur : aa

Mot de passe : ••

☒ J'accepte les conditions d'accès à internet
 >> [Lire les conditions d'accès internet](#)

Se Connecter

Suite à sa connexion l'utilisateur doit cliquer sur *Modification de Votre mot de Passe*.

Il aura la possibilité de changer son mot de passe ou de supprimer son compte en saisissant son mot de passe puis de Valider sa suppression

Modification de Votre Mot de Passe

Votre Mot de Passe

Votre Nouveau Mot de Passe

Votre Nouveau Mot de Passe

Valider

Suppression de votre Compte

Votre Mot de Passe

Suppression et Déconnexion

L'utilisateur est instantanément déconnecté et le compte supprimé.

```
01/Mar/2022:18:36:38 Base cc      disconnect [prof-mult] [192.168.0.100] [74:2f:68:56:b8:30] [vol/407850/73165] [con/0/0] [eth1/2/u]  
01/Mar/2022:18:36:37 Base cc      suppress  [adm+end_user] cc/cc [prof-mult] [prof-mult] [-|-|-|-|-|-|-|-|-|-] [1641976059] [145913200] [0] [A261-|-|-|]]  
01/Mar/2022:18:33:46 Base cc      connect   [prof-mult] [192.168.0.100] [74:2f:68:56:b8:30] [con/2/1] [eth1/2/u] [10mbit/10mbit/2] [0] [ASUS-N555] [Fr] [computer]  
01/Mar/2022:18:33:26 Base cc      disconnect [prof-mult] [192.168.0.100] [74:2f:68:56:b8:30] [con/2/1] [eth1/2/u] [10mbit/10mbit/2] [0] [ASUS-N555] [Fr] [computer]
```

Suite à la saisie, il est redirigé vers le portail

Cette modification n'est possible que si la page du portail est affichée après connexion – Dans le cas sans fenêtre de présence et tant que le poste sera mémorisé (connexion avec mémorisation) la page de connexion ne sera pas visible.

15 Accès sans Authentification

15.1 Postes sans Authentification :

Ce menu permet de définir les postes ayant besoin d'un accès Internet via le portail en mode authentifié de se connecter sans aucune authentification. Dans ce cas il faut fournir son adresse IP ou son adresse Mac ou sa classe. Les accès sont contrôlés par rapport au profil associé : **Base ou Sécurisé**

La classe d'adresses MAC se définit par la syntaxe suivante *9c:b7:0d:6f:* ou *9c:b7:0d:6f*

La classe d'adresses IP n'est pas disponible.

Le nombre maximum d'adresse IP ou Mac pouvant être saisi est de 256.

Au-delà du temps de maintien de la connexion sans Activité le poste sera déconnecté du portail. Si ce temps est paramétré à 0, le/les postes ne sont plus déconnectés.

15.2 Réseaux sans Authentification :

Les interfaces en mode **Enregistreur de site web** ou **Enregistreur de Log** doivent être associées à un des deux profils (**Base ou Sécurisé**). Le basculement de profil **Base** en profil **Sécurisé** se fait automatiquement en fonction de la plage horaire. Une relance du DNS peut s'avérer nécessaire (Configuration générale/Services Réseaux/Proxy DNS à relancer)

Interface	Service DHCP	IP Début	IP Fin	Accès	Enregistreur	DNS	SMTP	ZeroConf	Demande SMS
Wan									
Lan1		192.168.0.10	192.168.0.250	Libre	URL			-	-
Lan2		192.168.2.10	192.168.2.250	Libre	Log			-	-
Lan3		192.168.3.10	192.168.3.250	Authentifié	URL			-	-

Pour ajouter des indications sur les postes ou le réseau sans authentification, il est possible de rajouter des commentaires dans les cases adjacentes.

16 Déclaration d'un nouvel identifiant par l'Administrateur

Concerne tous les modes de création, car l'administrateur a toujours la possibilité de créer un utilisateur.

16.1 Choix des informations à saisir

AccessLog Administration admin 192.168.26.14

Utilisateur Accès Internet Statistiques Configuration Administration avancée

CONFIGURATION DU MENU ADMINISTRATEUR : « NOUVEAU »

Champs Disponibles

- Identifiant
- Mot de Passe
- Número de pièce d'identité
- Número de Chambre
- Entreprise
- Service
- Adresse
- Contact Local
- Número de Téléphone
- Número de Portable
- Adresse Email
- Nationalité
- Accord Enregistrement Données
- Accord Exploitation Commerciale
- Nombre de Nuit d'accès Internet
- Plage Horaire d'accès Internet
- Jours d'accès Internet
- Jours et Heures d'accès Internet
- Temps Maximum d'Inactivité
- Accès Internet Pré-définis
- Nombre d'Heure d'accès Internet
- Plage d'accès Internet
- Volume Téléchargé Autorisé
- Nombre d'identifiant
- Plage d'identifiant

Informations Pour la Demande d'Identifiant

Position	Champs	Actif	Obligatoire/Détail
1	Nom	✓	✗
2	Prénom	✓	✗
3	Profil d'accès	✓	✗
4	Nombre de Jour d'accès Internet	✓	✗

Paramètres de Création

- Format Identifiant: 4 Chiffres Aléatoires
- Format Mot de Passe: 4 Chiffres Aléatoires
- Identifiant Permanent: Affiché ✓
- Activation à la 1^{re} Connexion: Affiché ✗
- Conservation des Tickets: 4 Chiffres Aléatoires

Sélection des champs souhaités

- 4 Chiffres Aléatoires
- 6 Chiffres Aléatoires
- 8 Chiffres Aléatoires
- 10 Chiffres Aléatoires
- 4 Caractères Aléatoires
- 6 Caractères Aléatoires
- 4 Syllabes Aléatoires
- 5 Syllabes Aléatoires
- Nom
- Prénom
- Identifiant
- Mot de Passe
- Profil d'accès
- Número de pièce d'identité
- Número de Chambre

MODIFIER

16.2 Personnalisation du Ticket Utilisateur

Suite à la création de l'utilisateur un ticket de création est généré, il est personnalisable

AccessLog Administration admin 192.168.26.25

Utilisateur Accès Internet Statistiques Configuration Administration avancée

DESIGN DU TICKET UTILISATEUR

Logo en Haut de Ticket

Texte d'Accueil

Paramètres d'identification

Texte Explicatif

Logo de Bas de Ticket

Paramètres Généraux du Ticket

Couleur du Texte par défaut: #222222 Taille du Texte par défaut: 12

Fond de Page: #FFFFFF

Mise en Page du Ticket

Format du Ticket: ☐ HTML ☒ PDF

Taille du Ticket: Largeur: 100 mm Longueur: 60 mm

Taille des Marges: ☐ Avec Sélection ☐ Sans Sélection

Impression d'un Cadre: ☒ Non ☐ Oui

Plusieurs Ticket par Page: ☒ Non ☐ Oui

Mise en Page sur Deux Colonnes: ☒ Non ☐ Oui

MODIFIER

La présence des champs dans le ticket final est paramétrable en cliquant sur  pour la suppression (passe en ) ou  pour la présence (passe en ) et de positionner les informations 



Il est possible d'ajouter ou de supprimer des lignes complémentaires dans les champs.

Texte d'Accueil points to the main title area.

Texte identifiant points to the 'Vos Parametres de Connexion' header.

Texte Mot de Passe points to the 'Votre mot de passe' field.

Période Validité points to the 'Validité' field.

Zone « Titre » points to the main title 'Votre Connexion Internet'.

Texte Explicatif points to the footer text 'Ce ticket contient vos informations de connexion.'

Vos Parametres de Connexion	
Votre Identifiant	mon_login1
Votre mot de passe	mon_mot_de_passe1
Validité	26/02/2013 08:00 -> 27/02/2013 20:00

Exemple de Ticket

16.2.1.1 QR-Code Connexion Wifi



La configuration du contenu du QRCode est réalisée en cliquant sur l'icône . Ne contient que le paramétrage Wifi et par l'identifiant (QR-Code connexion Internet)

SSID : C'est SSID du WIFI disponible dans votre réseau (1 seul)

Protection/Clé : Si le Wifi est protégé par code, sélectionnez le type de clé – Pour un Wifi « ouvert », sélectionnez *Pas de mot de Passe*.

Mot de Passe : saisir le code WEP/WAP/WAP2, sinon laisser le champ vide dans le cas de *Pas de Mot de Passe*.

Réseau Caché : Si le réseau est non visible

QR-CODE CONNEXION WIFI

Paramètres du Réseau Wifi

SSID: DAP-2360AP

Protection/Clé: WAP/WAP2

Mot de Passe: moncode

Réseau Caché: 

Paramètres du QR Code

Niveau de Correction: Bon

Définition/Pixel: 3

Taille d'Affichage: 70%

VALIDER

Niveau de Correction et définition pixel : définit la qualité du QRcode

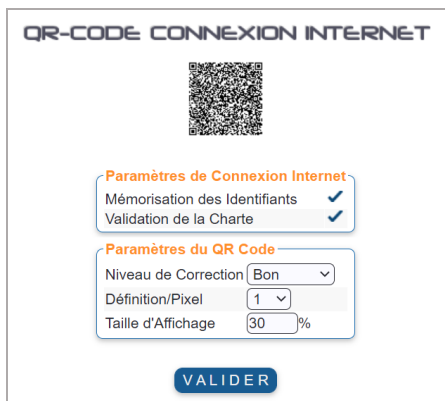
Taille d'affichage : Ratio en pourcentage de l'affichage du code dans le ticket

Bouton VALIDER : Permet d'enregistrer et de pré-visualiser le résultat.

16.2.1.2 QR-Code Connexion Internet :

La configuration du contenu du QRCode est réalisée en cliquant sur l'icône 
Contient l'identifiant généré lors de la création du ticket

Paramètre de connexion Internet : Permet de réaliser lors de la connexion les opérations de mémorisation de la connexion et de forcer la validation de la charte d'utilisation d'internet.



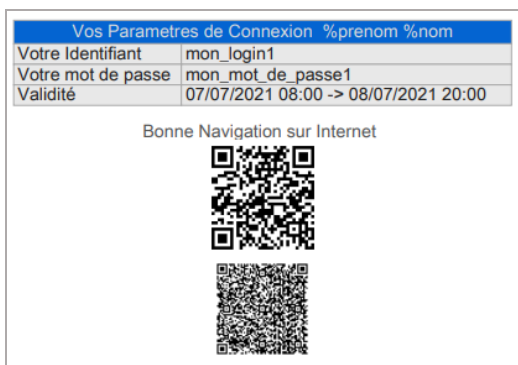
Niveau de Correction et définition pixel : défini la qualité du QRcode

Taille d'affichage : Ratio en pourcentage de l'affichage du code dans le ticket

Bouton VALIDER : Permet d'enregistrer et de pré-visualiser le résultat.

16.2.1.3 Utilisation du QR-Code :

Un scanner de QR-Code doit être utilisé pour les déchiffrer - Tous les lecteurs de QR-code ne donnent pas la possibilité de rediriger automatiquement sur la connexion, mais affiche simplement les informations à utiliser pour se connecter (comme les réseau Wifi disponibles pour la sélection).



Vos Parametres de Connexion %prenom %nom	
Votre Identifiant	mon_login1
Votre mot de passe	mon_mot_de_passe1
Validité	07/07/2021 08:00 -> 08/07/2021 20:00

Bonne Navigation sur Internet

16.3 Création d'un utilisateur

La création de l'utilisateur se fait en fonction du mode de déclaration choisi.

Dans le cas où l'administrateur crée les identifiants, les champs paramétrés sont à remplir ;

L'administrateur a toujours la possibilité de créer un identifiant

L'identifiant et le mot de passe peuvent être générés aléatoirement si ces deux champs sont laissés blancs au moment de la création.

16.4 Visualisation des utilisateurs/postes connectés

Les utilisateurs créés par l'administrateur ou par l'utilisateur, ainsi que ceux connectés sont affichés en temps réels (cliquer sur )

Identifiant	Profil d'accès	Numéro de Portable	Adresse Email	Fin d'Autorisation	Volume	Temps	ID
aa	Base	-	-	07/12/2020 14:03	10.3Ko	1:05m	A341
egr1	Base	0679973198	egr1@telmat.fr	25/07/2021 09:27	-	-	A346
jms2	Sécurisé	0679973127	reneapathenay@sposte.fr	25/07/2021 09:27	-	-	A347
rpa	Sécurisé	0679973197	rpa@telmat.fr	25/07/2021 09:27	119.9Ko	9:05m	A348

Si plusieurs utilisateurs sont connectés avec le même identifiant :

Identifiant	Temps	Volume Recu	Volume Envoyé	Débit en Réception	Débit en Emission
rpa	2m03s	1.2M	262.2K	0.0K/s	0.0K/s
rpa	14s	133.9K	14.8K	0.0K/s	0.0K/s

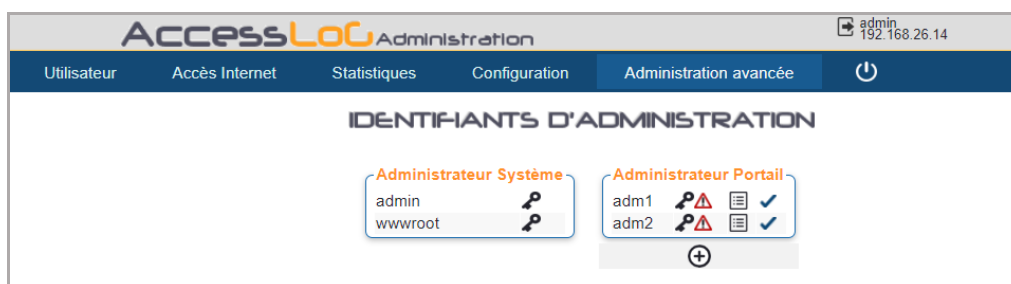
Si l'Administrateur est autorisé à envoyer les identifiants pas email et SMS (menu configuration Envoi Mail et SMS)

Et les champs email et SMS correctement renseignés l'administrateur peut envoyer les informations de connexion en cliquant sur les icônes désirées



17 Création d'Administrateurs Délégués et modification mot de passe administrateur

Permet de créer un administrateur qui n'aura accès qu'aux menus de gestion des utilisateurs. Saisir le nouvel utilisateur associé à son mot de passe, puis VALIDER



Dans le menu Administrateur du Portail cliquer sur et saisir les champs nécessaires.

L'administrateur créé est affiché , pour le supprimer, cliquer sur et répondre à la question de suppression demandée. Pour modifier le mot de passe cliquer sur .

L'Isolation de l'Administration (case cochée), permet en cas de création de plusieurs administrateurs délégués d'isoler la création et la connexion des utilisateurs créés par un administrateur délégué particulier. Par exemple, le sous administrateur A ne pourra voir et accéder aux utilisateurs créés par le sous Administrateur B et inversement. Pour Modifier cliquer sur .

La connexion se fait de la même manière que l'administrateur de l'AccessLog-Evo/Pro. Les menus sont restreints.

18 Personnalisation du Portail Captif

18.1 Design du Portail Captif avec Assistant

Correspond à la mire d'accès affichée lorsque l'utilisateur désire se connecter à internet.
Les champs à saisir pour la création de l'identifiant sont fonction de la configuration de la saisie utilisateur.

The screenshot shows the 'DESIGN DU PORTAIL CAPTIF' configuration page. It is divided into several sections for customizing the captive portal's appearance and functionality. Annotations with yellow boxes and arrows highlight specific features:

- Logo:** A section for uploading a logo, with a note: "Logo en haut de Page".
- Paramètres Généraux de la Page:** General page settings including title, default text color, font size, and background color.
- Titre:** Title settings for the portal.
- Zone d'identification:** Identification area settings, including text color, font, and fields for username, password, and information.
- Protection Parental:** Parental protection settings, including a parental code.
- Texte d'Accueil:** Welcome text and color settings.
- Lien Multi-Langue:** Multi-language link settings, including language selection and link text.
- Demande d'Identifiant:** Username request settings, including text and link color.
- Conditions Générales d'Utilisation:** Terms and conditions settings, including acceptance text and link.
- Bouton de Validation:** Validation button settings, including text, button color, and active button color.
- Texte Explicatif:** Explanatory text settings.
- Redirection:** Redirection settings for local and external sites.

Additional annotations include:

- Prévisualisation du portail:** A preview icon in the top right corner.
- Choix des langues pour la configuration:** A language selection dropdown menu.
- Choix de langue affiché sur le portail de connexion:** A language selection dropdown menu for the login portal.
- Affichage de la demande d'identifiant sur la même page:** A checkbox to display the username request on the same page.
- Charte d'utilisation Internet:** A checkbox to display the Internet usage charter, with a note: "Affichage optionnel - Texte modifiable - Disponible en plusieurs langues".
- Demande de code parental:** A checkbox to request a parental code.

Exemple de Portail Captif

Conditions Générales d'Utilisation :

L'Administrateur valide  ou pas  l'obligation d'acceptation des conditions d'accès Internet.

L'acceptation des conditions générales d'utilisation peut être demandée :

- Soit sur Accès libre.
- Soit sur Authentification.
- Soit sur Demande d'identifiant.

Conditions Générales d'Utilisation

Sur Accès Libre	Sur Authentification	Sur Demande d'Identifiant
Accès au Règlement	>> Lire les conditions d'accès internet	
Acceptation du Règlement	J'accepte les conditions d'accès à internet	

L'acceptation des conditions peut être demandée :

- Soit dans le portail captif ✓.

L'utilisateur doit accepter les conditions pour accès à internet

- Soit après authentification dans une nouvelle page dans laquelle s'affiche le règlement

[illegible]

L'utilisateur doit Accepter les conditions pour continuer la connexion.

Dans la configuration  le paramétrage d'affichage des conditions  est nécessaire.

ACCESSLOG Administration

CONDITIONS D'UTILISATION

Conditions Générales d'Utilisation

Taille Checkbox

Affichage du Règlement d'Utilisation Fois

MODIF

- A Chaque Connexion
- A Chaque Connexion**
- A Chaque Modification de Règlement
- Par Heure
- Par Jour
- Par Semaine
- Par Mois
- Par An

Attention : dans le cas « **Sur demande d'identifiant** », le règlement s'affichera à chaque fois, car un nouvel utilisateur sera créé.

Le "nombre de Fois" d'affichage doit être fixé au minimum à 1.

Choix portail:

RESTAURATION D'UN DESIGN PORTAIL CAPTIF

Choisissez une Sauvegarde de Design

RESTAURATION / Accueil

Plusieurs designs de portail captif sont disponibles.

Pour choisir celui qui vous convient, cliquez sur

(partie supérieure droite du menu).

Il est possible de restaurer un design précédemment sauvegardé (même version)

Hopital1

Hopital2

Hopital3

HopitalF1

HopitalF2

HopitalF3

Commerce1

Commerce2

Commerce3

Redirection sur Page ou Site spécifique

Avant pour après authentification via le portail, il est possible de rediriger l'utilisateur vers une page Web pré chargée ou vers un site Web déterminé.

Redirection				
Avant Authentification	Vers une page locale	✗	Vers un site Web	✗ 
Après Authentification	Vers une page locale	✗	Vers un site Web	✗ 

Pour éviter tout blocage le site web doit être ajouté dans les Sites en Libres Accès

SITE EN LIBRE ACCES SANS AUTHENTIFICATION

Liste des Sites en Libre Accès Sans Authentification

collection.wifi4eu.ec.europa

www.caf.fr

www.gitabox.fr

www.radio-en-ligne.fr

www.telmat.fr

Champs du portail Captif:

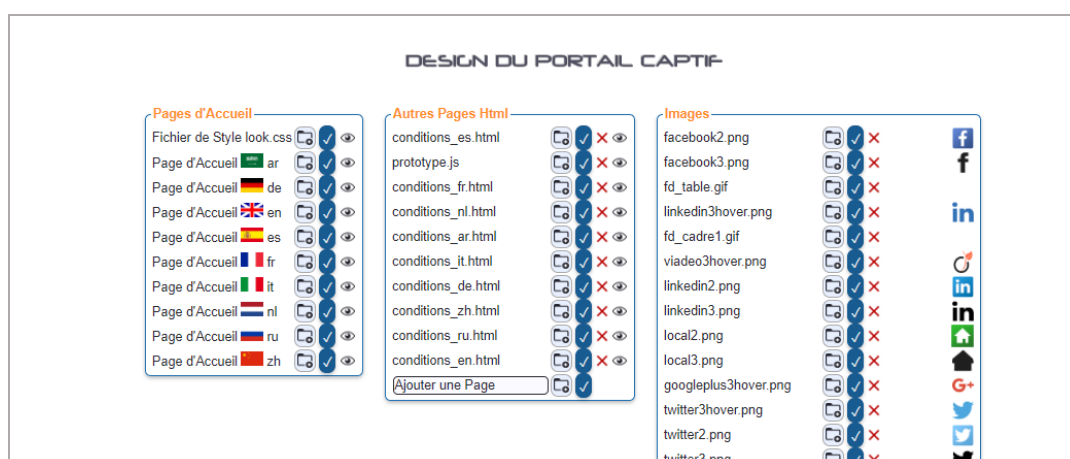
L'ajout de langue est possible à travers le menu : **Veuillez contacter le Support Technique TelmatWeb pour cette opération.**

**18.2 Design du Portail Captif en mode Expert**

Pour passer dans ce mode il faut cliquer sur **Mode Design Expert**. Dès que le portail est dans ce mode, l'administrateur a la possibilité de modifier et de télécharger de nouvelles images, d'ajouter des pages html et de modifier le look et le comportement de la page d'accueil.

Ce mode nécessite la connaissance du langage html et PHP. Telmat Industrie ne fait pas de support sur les codes développés par les utilisateurs.

Avant de rentrer dans ce mode il faudra avoir défini le mode de fonctionnement du portail. Toute modification ultérieure ne sera alors plus prise en compte.



18.3 Demande d'identifiant utilisateur

Un utilisateur peut créer ses propres identifiants dans les modes suivants :

Mode de Déclaration d'un Nouvel Utilisateur	
Accès Libre	X
Accès Libre Avec Demande d'Information	X
Par les Administrateurs Uniquement	X
Par l'utilisateur	✓
Par l'utilisateur et Validation	X
Par l'utilisateur avec retour par Email	X
Par l'utilisateur avec retour par SMS	X
Par l'utilisateur par envoi SMS avec retour par SMS	X
Par l'utilisateur avec Paiement via Paypal	X
Par l'utilisateur avec Paiement via Voxpay	X
Connexion à un Front Office	X

- ▶ Par l'utilisateur
- ▶ Par l'utilisateur et validation par l'administrateur
- ▶ Par l'utilisateur avec retour par email
- ▶ Par l'utilisateur avec retour pas SMS
- ▶ Par l'utilisateur par envoi de SMS avec retour par SMS
- ▶ Par l'utilisateur avec paiement via Paypal
- ▶ Par l'utilisateur avec paiement via Voxpay/Monético

Le Mode **Accès Libre** et **Accès libre Avec demande d'information** permet à l'utilisateur de se connecter via le portail en cliquant sur le bouton de validation. Il n'a pas d'identifiant à saisir.

Dans le mode **Accès libre Avec demande d'information** les champs demandés peuvent être obligatoires. Ceux-ci sont configurés via les champs de création d'un utilisateur.

18.4 Champs de configuration pour la création d'un utilisateur

Champs Disponibles	
① Nom	X
① Prénom	X
① Identifiant	X
🔒 Mot de Passe	X
👤 Profil d'accès	X
① Numéro de pièce d'identité	X
① Numéro de Chambre	X
① Entreprise	X
① Service	X
① Adresse	X
① Contact Local	X
① Numéro de Téléphone	X
📱 Numéro de Portable	X
✉ Adresse Email	X
① Nationalité	X
① Accord Enregistrement Données	X
① Accord Exploitation Commerciale	X
📅 Nombre de Jour d'accès Internet	X
📅 Nombre de Nuit d'accès Internet	X
📅 Plage Horaire d'accès Internet	X
📅 Temps Maximum d'Inactivité	X
📅 ⌚ Accès Internet Prédéfinis	X
⌚ Nombre d'Heure d'accès Internet	X
⌚ Plage d'accès Internet	X
⬇ Volume Téléchargé Autorisé	X
🛡 Protection par Code Secret	X
🛡 Protection par Captcha	X

① les champs sont informatifs et n'ont pas d'implication sur la gestion des utilisateurs

🔒 Ces champs liés à l'identifiant et au mot de passe peuvent être sélectionnés pour saisie ou alors configurés pour la génération automatique (Paramètres de création)

Les divers paramètres de temps sont sélectionnés en fonction du mode de décompte de connexion choisie.

📅 Paramètre du type validité

⌚ Paramètre du type temps d'utilisation

👤 Paramètre de type compteur d'identifiants

📱✉ Paramètre de type communication. Permet l'émission des paramètres vers un téléphone portable ou une adresse email

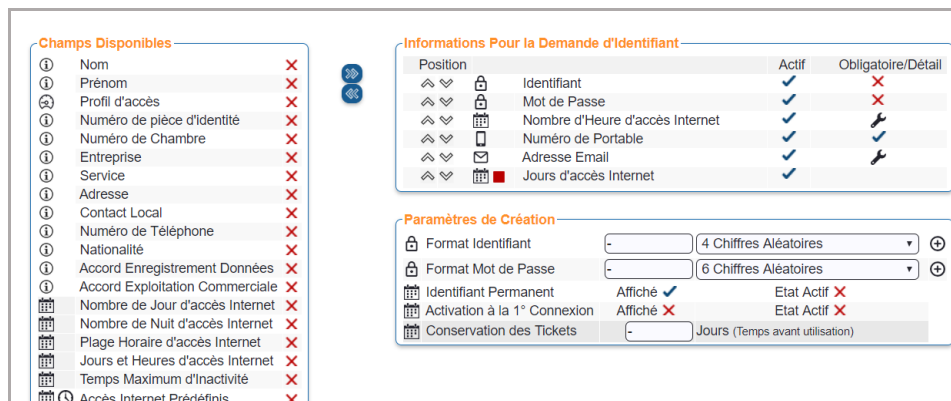
⬇ configuration des limites de téléchargement.

■ : Information d'incompatibilité de champ sélectionné. Les temps du ticket alloués seront erronés.

Les champs sont configurables dans ***'Ecran de saisie Administrateur et 'Ecran de saisie Utilisateur.***

Certains champs peuvent être présents ou non en fonction de l'écran de saisie et du *choix information cachée* dans le menu de l'option -

En cliquant sur  la fenêtre de paramétrage de la restriction s'ouvre.
Le/les champs non remplis lors de la création alors qu'ils sont obligatoires empêchera la création de l'utilisateur.



Champs Disponibles

- Nom
- Prénom
- Profil d'accès
- Numéro de pièce d'identité
- Numéro de Chambre
- Entreprise
- Service
- Adresse
- Contact Local
- Numéro de Téléphone
- Nationalité
- Accord Enregistrement Données
- Accord Exploitation Commerciale
- Nombre de Jour d'accès Internet
- Nombre de Nuit d'accès Internet
- Plage Horaire d'accès Internet
- Jours et Heures d'accès Internet
- Temps Maximum d'inactivité
- Accès Internet Prédéfinis

Informations Pour la Demande d'Identifiant

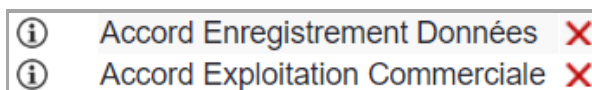
Position	Identifiant	Actif	Obligatoire/Détail
1	Identifiant	✓	✗
2	Mot de Passe	✓	✗
3	Nombre d'Heure d'accès Internet	✓	✓
4	Numéro de Portable	✓	✓
5	Adresse Email	✓	✓
6	Jours d'accès Internet	✓	✓

Paramètres de Création

- Format Identifiant: 4 Chiffres Aléatoires
- Format Mot de Passe: 6 Chiffres Aléatoires
- Identifiant Permanent: Affiché ✓, Etat Actif ✗
- Activation à la 1^{re} Connexion: Affiché ✗, Etat Actif ✗
- Conservation des Tickets: Jours (Temps avant utilisation)

Le système surveille constamment les connexions des utilisateurs et des postes. En cas de dépassement l'utilisateur est déconnecté du portail.

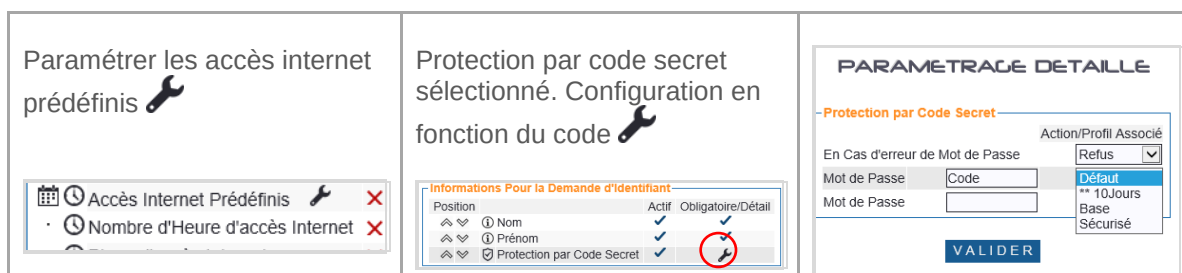
RGDP 2018 : Deux champs spécifiques sont disponibles pour répondre à la RGPD 2018. Ces deux champs sont à valider par l'utilisateur ou l'administrateur au moment de la création de l'identifiant.



La valeur de saisie de ces champs (y ou n) est exploitable dans les Traces de Gestion des Utilisateurs. Ces valeurs sont récupérées dans les champs "réponses1" et "réponses2" via l'export périodique des traces. (Administration avancée/Trace/Gestion des Utilisateurs).

Création utilisateur en fonction du code secret :

- ✓ Cette fonction permet de créer l'utilisateur en fonction du code secret. Ces restrictions sont définies dans *Accès internet prédéfinis*, Menu « Utilisateur / Ecran de saisie Utilisateur »



Paramétrer les accès internet prédéfinis

- Accès Internet Prédéfinis
- Nombre d'Heure d'accès Internet

Protection par code secret sélectionné. Configuration en fonction du code

PARAMETRAGE DETAILLE

Protection par Code Secret

Action/Profil Associé: Refus

En Cas d'erreur de Mot de Passe: Code

Mot de Passe: 10 Jours

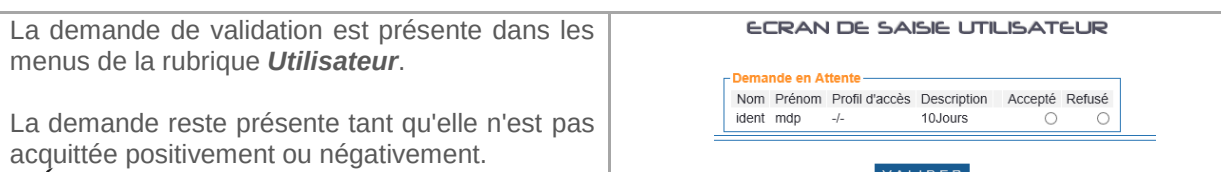
Mot de Passe: Base Sécurisée

VALIDER

Création par l'utilisateur avec Validation :

Dans ce mode, l'administrateur ou l'administrateur délégué validera ou refusera la création de l'utilisateur.

L'utilisateur remplit les champs demandés sur le portail, puis sa demande est envoyée à l'administrateur. Deux modes sont possibles pour créer ou pas l'administrateur.



La demande de validation est présente dans les menus de la rubrique *Utilisateur*.

La demande reste présente tant qu'elle n'est pas acquittée positivement ou négativement.

ECRAN DE SAISIE UTILISATEUR

Demande en Attente

Nom	Prénom	Profil d'accès	Description	Accepté	Refusé
ident	mdp	-/-	10Jours	☐	☐

VALIDER

Par email : L'avertissement est envoyé à l'adresse email paramétrée dans *Avertissement par Mail*.

L'avertissement est envoyé à l'adresse email paramétrée dans *Avertissement par Mail*.

Il y a possibilité d'accepter ou de refuser la création. **Ceci n'est fonctionnel que si la messagerie de l'administrateur est dans le réseau local**

Vous avez une Demande d'Identifiant

Emis le : 04/04/2017 à 10:12:41

Informations Transmises	
Nom	lenom
Prénom	leprenom

Il est possible d'utiliser le mode de parrainage pour la réception du mail – Le mail d'avertissement dans ce cas est envoyé à l'adresse mail saisie dans l'option contact local (qu'il faut avoir sélectionné) . Il y a possibilité d'accepter ou de refuser la création. **Ceci n'est fonctionnel que si la messagerie de l'utilisateur est dans le réseau local**

19 Administration Cloud :

19.1 Introduction :

Le portail d'Administration Centralisé Telmat vous permet de configurer le portail de présentation avant authentification d'un utilisateur sur le Portail Captif.

- Cette fonctionnalité n'est disponible que pour les machines ayant une Release Système minimum N° TAL_20191001
- Ce portail paramétré sur l'administration centralisée Telmat peut être associé à un ou plusieurs équipements portails captifs distants AccessLog
- La configuration de ce portail permet de définir une page d'accueil, d'afficher des textes défilants et des blocs de fonctions (Calendrier, logos, flux RSS, Fichiers, Vidéos...)
- L'utilisateur désirant se connecter à internet à travers le Portail Captif de l'AccessLog sera redirigé automatiquement vers ce portail spécifique avant son authentification.

L'accès à cette fonction se réalise en plusieurs étapes.

1. Création d'un compte sur l'Administration Centralisé Telmat (*admin.accessbox.fr*)
2. Association de ou des machines par rapport à ce compte
3. Paramétrage du portail centralisé
4. Paramétrage du design portail captif des machines distantes
5. Vérification bon fonctionnement

Pour la configuration complète du portail reportez-vous à la documentation spécifique de configuration du portail que vous pouvez télécharger à l'adresse suivante

<http://www.telmatweb.com/doc/data/documents/administration-centralisee.pdf>



19.2 Création d'un compte :

Pour créer un compte deux informations sont nécessaires

- ✓ Le Numéro de série de l'Appareil (unique par appareil)
- ✓ Le code Cloud de l'Appareil (unique par appareil)

Ces deux informations sont accessibles à travers l'interface d'administration de votre machine en se connectant en Administrateur puis en cliquant sur l'icone ?



Dans la fenêtre d'information sont affichés le numéro de Machine et le code Cloud

Numéro de Série :	0507V99997
Version Logicielle :	AccessLog 6.0
Licence :	100 Utilisateurs
Garantie Matérielle :	Retour Usine 20/04/2023
Release :	TAL64_20230501 25/05/2025
Filtrage URL Olfeo :	Actif 10/06/2024
Clé d'accès / Administration Cloud	MDAzMDE4MEI4ODZC
Langue :	FR ▼
Aide en ligne :	On ▼
Timeout Administration :	Inactif ▼ mn

Connectez-vous sur le portail d'admin centralisé <https://admin.accessbox.fr>

Attention : Ces informations sont uniques et liées entre elles.

Cliquer sur **CREER UN COMPTE**

- ✓ Vous ne pouvez utiliser plusieurs fois le numéro de série et le code Cloud avec le même administrateur.
- ✓ Vous ne pouvez pas utiliser un code cloud non associé à la machine.



Dans le cas d'information erronée, un retour négatif est affiché



Suite à la saisie des informations demandées, la réponse positive du serveur vous permet d'associer la machine au compte d'administration que vous désirez créer.

Vous devez saisir une adresse email qui sera par la suite votre de compte de connexion à l'administration Cloud



Un mail d'association est envoyé à l'adresse email que vous avez déclaré



Se connecter au compte de messagerie pour finaliser l'association



CONSOLE D'ADMINISTRATION

TELMAT

CRÉER UN COMPTE

APPAREIL TROUVÉ :
FORM-TAB3

MAIL ENVOYÉ À TELMAT@WANADOO.FR.
VEUILLEZ SUIVRE LA PROCÉDURE DEPUIS LE MAIL DE DEMANDE DE CONFIRMATION.

RETOUR À L'ACCUEIL

L'étape finale consiste à créer l'association en cliquant sur le lien [confirmer l'association](#). Vous serez redirigé vers une nouvelle fenêtre



TELMAT

Votre compte sur admin.accessbox.fr

Pour confirmer l'association de l'appareil à votre compte, cliquez sur le lien ci-dessous :
[confirmer l'association](#)

Console d'administration Telmat : admin.accessbox.fr

Lors de cette étape de confirmation, vous devez saisir le mot de passe que vous utiliserez ultérieurement pour vous connecter.



VOTRE MOT DE PASSE (MIN 4 CAR.)

Votre mot de passe

DÉFINIR

Ainsi que quelques informations d'identités liées à ce compte



APPAREIL ASSOCIÉ :
TELMAT
(Sérial : FORM-TAB3)

VOTRE COMPTE

VOTRE PRÉNOM : Rene

VOTRE NOM : wanadoo

VOTRE SOCIÉTÉ : Telmat Industrie

ADRESSE SOCIÉTÉ : 6 rue de l'industrie

CODE POSTAL : 68360

VILLE : Soultz

VALIDER

Lorsque toutes les étapes ont été effectuées avec succès, vous pouvez vous connecter à l'Administration Cloud

APPAREIL ASSOCIÉ :
TELMAT
 (Sérial : FORM-TAB3)

VOS INFORMATIONS DE VOTRE COMPTE ONT ÉTÉ ENREGISTRÉES AVEC SUCCÈS.

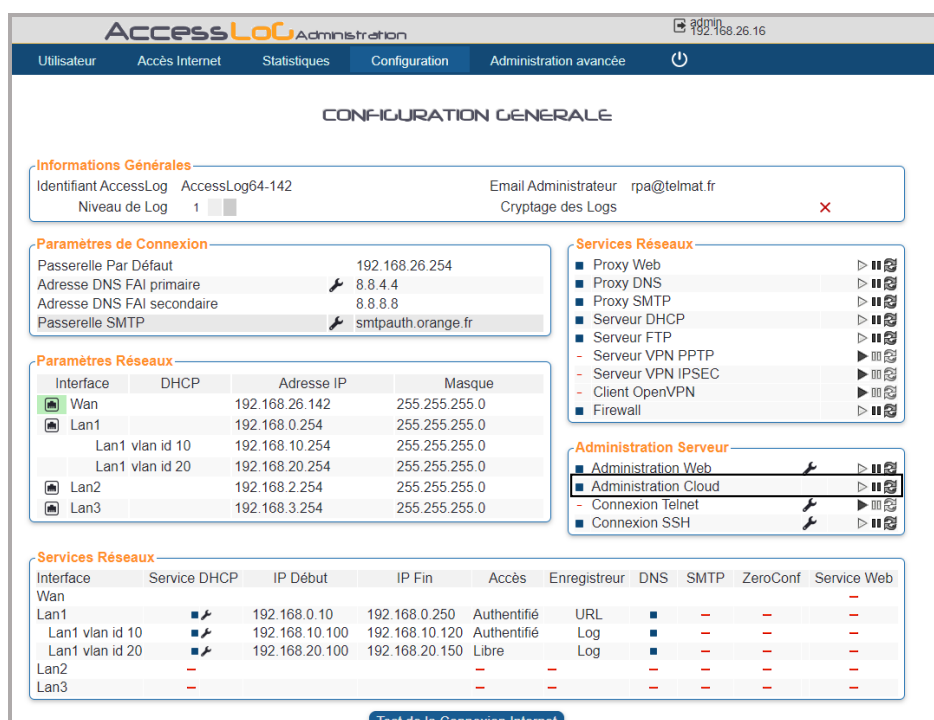
SE CONNECTER

19.3 Synchronisation des machines rattachées :

Le paramétrage que vous réalisez à sur le serveur d'Administration Cloud doit être synchronisé sur la machine associée à votre compte.

Pour que cette synchronisation soit opérationnelle, il faut que le service d'Administration Cloud soit démarré et fonctionnel sur l'appareil distant.

- Démarrez le service 
- Vérifiez son bon fonctionnement
 - ✓ machine connectée mais aucun administrateur connecté  ,
 - ✓ machine connectée, un administrateur est connecté  ,
 - ✓ machine déconnectée, le service ne peut atteindre le serveur Cloud 
- Relance du service 



AccessLog Administration 192.168.26.16

Utilisateur Accès Internet Statistiques Configuration Administration avancée

CONFIGURATION GÉNÉRALE

Informations Générales

Identifiant AccessLog AccessLog64-142 Email Administrateur rpa@telmat.fr
 Niveau de Log 1 Cryptage des Logs

Paramètres de Connexion

Passerelle Par Défaut 192.168.26.254
 Adresse DNS FAI primaire 8.8.4.4
 Adresse DNS FAI secondaire 8.8.8.8
 Passerelle SMTP smtpauth.orange.fr

Paramètres Réseaux

Interface	DHCP	Adresse IP	Masque
Wan		192.168.26.142	255.255.255.0
Lan1		192.168.0.254	255.255.255.0
Lan1 vlan id 10		192.168.10.254	255.255.255.0
Lan1 vlan id 20		192.168.20.254	255.255.255.0
Lan2		192.168.2.254	255.255.255.0
Lan3		192.168.3.254	255.255.255.0

Services Réseaux

- Proxy Web
- Proxy DNS
- Proxy SMTP
- Serveur DHCP
- Serveur FTP
- Serveur VPN PPTP
- Serveur VPN IPSEC
- Client OpenVPN
- Firewall

Administration Serveur

- Administration Web
- Administration Cloud
- Connexion Telnet
- Connexion SSH

Services Réseaux

Interface	Service DHCP	IP Début	IP Fin	Accès	Enregistreur	DNS	SMTP	ZeroConf	Service Web
Wan									
Lan1		192.168.0.10	192.168.0.250	Authentifié	URL				
Lan1 vlan id 10		192.168.10.100	192.168.10.120	Authentifié	Log				
Lan1 vlan id 20		192.168.20.100	192.168.20.150	Libre	Log				
Lan2									
Lan3									

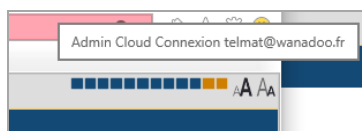
Test de la Connexion Internet

Le service Connexion SSH doit être démarré (démarré par défaut).

Administration Serveur

- Administration Web
- Administration Cloud
- Connexion Telnet
- Connexion SSH

Lorsque la machine est connectée au serveur central, le voyant orange associé clignote, l'administrateur connecté est affiché



Si le voyant est fixe orange, La connexion est en cours d'établissement

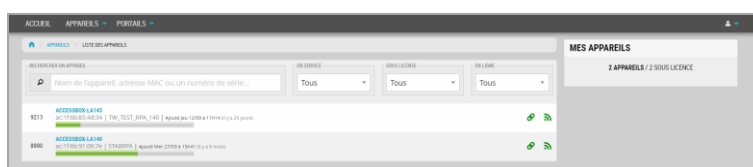
Une surveillance du service est opérée cycliquement (2 minutes). Une phase de reconnexion est lancée si le tunnel n'est pas connecté. Vous pouvez

- ✓ Attendre la relance du service
- ✓ Relancer à travers le menu d'administration

Si c'est la première connexion et que celle-ci ne s'effectue pas, vérifier qu'aucun équipement en amont ne bloque le port de connexion (22).

19.4 Liste des machines associées au compte :

Lors de votre inscription la première machine est associée à votre compte
Dans la liste des appareils vous visualisez les appareils rattachés



19.5 Configuration Redirection portail avant authentification :

Pour afficher la page de redirection sur le portail avant authentification, le **Design du Portail Captif** doit être préalablement configuré.



Accédez à la configuration de Redirection Avant Authentification

Redirection			
Avant Authentification	Vers une page locale ✓	Vers un site Web ✗	🔧
Après Authentification	Vers une page locale ✗	Vers un site Web ✗	🔧

- Cocher : Avant authentification
 - Editer la configuration de redirection
- Vers une page locale ✓

Configurer la Fréquence de Redirection Uniquement

REDIRECTION AVANT AUTHENTIFICATION

Redirection Avant Authentification

Fréquence de Redirection: 1 Fois [A Chaque Connexion]

Page Web à Importer:

Import Périodique: ✗

MODIFIER

Import de Fichier

Selectionnez le ou les Fichiers 📁 html ✓

Il n'y a pas d'import périodique car la synchronisation est réalisée à partir du serveur centralisé

La prévisualisation de la page portail est possible en cliquant sur  dans le bloc Fichiers Importés.

L'entrée *annonces.htm* doit être présente. Il est réinstallé à chaque synchronisation du portail



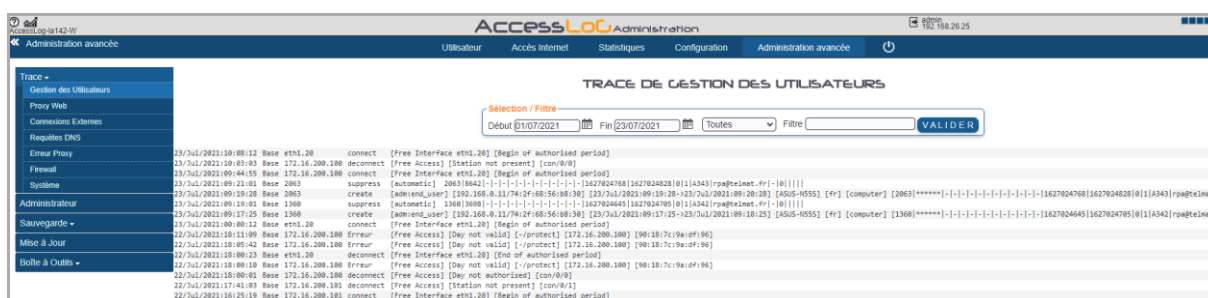
20 Les Traces enregistrées par AccessLog-Evo/Pro

Les traces sont enregistrées et stockées dans l'**AccessLog-Evo/Pro**. Toutes les nuits une rotation des traces permet un archivage et une conservation sur une durée de 12 mois.

20.1 Traces d'Accès

Les différentes traces d'activité sont accessibles dans les trois menus suivants :

- ✓ Gestion utilisateurs
- ✓ Proxy Web : Trace de connexion port http mode Authentifié et Enregistreur de site Web
- ✓ Connexion Externes – Traces hors port http et toute trace dans le mode enregistreur de logs
- ✓ Les mots de passe utilisateurs sont cachés « ***** » - Rééditer le ticket pour récupérer le mot de passe.



Les traces enregistrées par l'**AccessLog-Evo/Pro** peuvent être sauvegardées manuellement ou stockées quotidiennement sur une unité de sauvegarde externe.

20.2 La Sauvegarde des Traces d'Accès

SAUVEGARDE DES LOGS

Sauvegarde sur :

☒ Serveur FTP
☐ Serveur de Fichier
☐ Serveur Rsync
☐ Disque Amovible USB

Adresse/Nom du serveur distant

Port

Protocole ☒ ftp ☐ sftp

Login de connexion distant

Mot de passe distant

SAUVEGARDE DES LOGS SUR VOTRE POSTE D'ADMINISTRATION

SAUVEGARDE SUR VOTRE POSTE D'ADMINISTRATION / 192.168.26.135

La sélection du media permet d'avoir accès à la configuration du système de sauvegardes.

Le bouton **TEST** permet de vérifier si la connexion réseau vers le serveur de sauvegarde est possible ou si le media est présent et reconnu.

20.3 Externalisation périodique des traces

Dans ce mode le serveur de stockage est déporté sur le réseau (internet ou local). La sauvegarde se fait quotidiennement. Les traces peuvent être conservées localement ou bien supprimées.

The screenshot shows the 'EXTERNALISATION DES LOGS' configuration page. The sidebar on the left contains the following menu items: Trace, Administrateur, Sauvegarde, Sauvegarde de la configuration, Sauvegarde des Logs, Externalisation des Logs (highlighted), Gestion des Logs, Mise à Jour, and Boîte à Outils. The main area is titled 'EXTERNALISATION DES LOGS' and contains two sections: 'Sauvegarde sur :' and 'Configuration'. The 'Sauvegarde sur :' section has a table with the following items: Sauvegarde Inactive (X), Serveur FTP (X), Serveur de Fichiers (checkmark), Serveur Rayonic (X), and Disque Amovible USB (X). The 'Configuration' section has a table with the following items: Nom de partage (accesslog), Adresse/Port du serveur distant (127.0.0.1), Login de connexion distant (utilisateur), Mot de passe distant (motdepasse), Compte Rendu par Email (checkmark), and Purge des Logs Après Transfert (checkmark). At the bottom of the configuration section are two buttons: 'ENREGISTRER' and 'TEST'.

EXTERNALISATION DES LOGS	
Sauvegarde sur :	
Sauvegarde Inactive	X
Serveur FTP	X
Serveur de Fichiers	✓
Serveur Rayonic	X
Disque Amovible USB	X
Configuration	
Nom de partage	accesslog
Adresse/Port du serveur distant	127.0.0.1
Login de connexion distant	utilisateur
Mot de passe distant	motdepasse
Compte Rendu par Email	✓
Purge des Logs Après Transfert	✓

ENREGISTRER TEST

Pour un disque amovible USB, assurez-vous que ce dernier soit formaté en FAT32

21 Réseaux privés virtuels (V.P.N.)

21.1 Introduction

Le réseau privé virtuel (VPN) est construit autour de l'exploitation des réseaux publics. Pour l'utilisateur tout se passe comme s'il disposait d'un véritable réseau privé. Pour simuler une connexion point à point sur le réseau public, nous avons recours au tunneling, qui consiste à créer des conduits virtuels sur les liens des Opérateurs. Ces trajets supportés par les infrastructures partagées, imposent des contraintes de sécurité telles que :

L'authentification de l'émetteur et du récepteur

- Le contrôle des droits
- La confidentialité des données
- L'intégrité des données

Toutes ces conditions imposent la mise en œuvre d'un éventail de technologies de chiffrement, fondées sur des clés et des algorithmes de codage.

De base, l'**AccessLog** dispose de plusieurs possibilités pour mettre en place le VPN :

- ✓ Le VPN pour Poste distant, utilisant le standard de cryptage PPTP, et permettant de relier des postes de travail nomades à un site central. PPTP (Point to Point Tunneling Protocol) de Microsoft, est un protocole de niveau 2, le "tunnel" de communication est établi depuis un poste nomade (de type Windows) vers un site central équipé d'un **AccessLog**.
- ✓ Le VPN L2TP est une combinaison entre le PPTP et IPSec. Le protocole L2TP repose sur la sécurité IPSEC, en mode Transport pour le chiffrement.
- ✓ Le client VPN OpenVPN qui permet de créer des tunnels Lan-to-Lan avec un site central serveur **AccessBox**

21.2 Accès au menu de configuration

Les onglets VPN PPTP, PPTP/L2TP vous permettent d'accéder à la configuration des comptes PPTP / L2TP.

The screenshot shows the 'AccessLog Administration' web interface. The top navigation bar includes 'Utilisateur', 'Accès Internet', 'Statistiques', 'Configuration', and 'Administration avancée'. The main content area is titled 'COMPTES VPN PPTP/L2TP'. Below the title, there is a 'Sélection' dropdown menu with 'rpa' selected. A 'Paramètres de Connexion' section contains a 'Connexion Active' status with a red 'X' icon, and three input fields for 'Login de connexion distant', 'Password', and 'Adresse IP distante propre à ce login'. At the bottom of this section are two buttons: 'MODIFIER' (disabled) and 'MODIFIER' (active).

21.3 VPN pour poste de travail distant (PPTP)

21.3.1 Démarrage du service :

AccessLog Administration 192.168.26.16

Utilisateur Accès Internet Statistiques Configuration Administration avancée

CONFIGURATION GÉNÉRALE

Informations Générales

Identifiant AccessLog AccessLog64-142 Email Administrateur rpa@telmat.fr
Niveau de Log 1 Cryptage des Logs

Paramètres de Connexion

Passerelle Par Défaut 192.168.26.254
Adresse DNS FAI primaire 8.8.4.4
Adresse DNS FAI secondaire 8.8.8.8
Passerelle SMTP smtpauth.orange.fr

Paramètres Réseaux

Interface	DHCP	Adresse IP	Masque
Wan		192.168.26.142	255.255.255.0
Lan1		192.168.0.254	255.255.255.0
Lan1 vlan id 10		192.168.10.254	255.255.255.0
Lan1 vlan id 20		192.168.20.254	255.255.255.0
Lan2		192.168.2.254	255.255.255.0
Lan3		192.168.3.254	255.255.255.0

Services Réseaux

- Proxy Web
- Proxy DNS
- Proxy SMTP
- Serveur DHCP
- Serveur FTP
- Serveur VPN PPTP
- Serveur VPN IPSEC
- Client OpenVPN
- Firewall

Administration Serveur

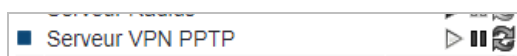
- Administration Web
- Administration Cloud
- Connexion Telnet
- Connexion SSH

Services Réseaux

Interface	Service DHCP	IP Début	IP Fin	Accès	Enregistreur	DNS	SMTP	ZeroConf	Service Web
Wan									
Lan1		192.168.0.10	192.168.0.250	Authentifié	URL				
Lan1 vlan id 10		192.168.10.100	192.168.10.120	Authentifié	Log				
Lan1 vlan id 20		192.168.20.100	192.168.20.150	Libre	Log				
Lan2									
Lan3									

[Test de la Connexion Internet](#)

Démarrer le service en cliquant sur ►



Pour arrêter le service cliquez sur ||, pour le redémarrer/recharger cliquez sur ↺

21.3.2 Configuration du serveur VPN PPTP

La configuration du serveur PPTP s'effectue en deux étapes,

- Création d'un utilisateur
- Configuration des adresses distribuées suite à la connexion.

21.3.2.1 Création du compte :

Vous devez sélectionner un login existant pour réaliser cette opération

Les opérations de configuration sont :

- Choix d'un login existant
- Remplacement du login et mot de passe par les nouveaux paramètres
- Saisie d'une adresse IP spécifique pour une distribution statique ou laisser "-" pour une distribution dynamique par le serveur PPTP

Login de connexion distant : Indiquez le login de connexion autorisant la connexion du poste distant sur le site central.

Password : Indiquez le *mot de passe* de connexion autorisant la connexion sur le site central

Adresse IP distante propre à ce login : le paramétrage de ce champ en spécifiant une adresse IP force le serveur à distribuer cette adresse IP au client suite à la réussite de la connexion. C'est cette adresse IP qui circulera sur votre réseau interne. Il faut alors paramétrer les équipements internes pour le routage de celle-ci. Si le champ est laissé par défaut "-", le serveur distribuera une des adresses contenue dans la plage d'adresses spécifiées (onglet pptp/configuration).

21.3.2.2 Configuration du VPN PPTP

Le serveur pptp distribue des adresses IP suite à la connexion authentifiée. Les adresses IP locales et distantes sont à définir dans la partie VPN PPTP. Ces adresses doivent être différentes des adresses locales de la machine sous peine de ne pas router correctement les paquets.

La configuration permet soit une distribution d'adresse par rapport à un pool de distribution soit à une adresse IP unique. La distribution unique ne permettra la connexion d'un seul poste.

Afin de résoudre les requêtes DNS du poste, vous pouvez renseigner l'adresse du serveur DNS. Elle sera distribuée lors de la connexion

21.3.2.3 Arrêt / redémarrage du service

L'état du service est donné par la couleur du point.

- Signifie que le service est actif mais qu'il ne fonctionne pas correctement,
- Le service est arrêté,
- Le service est démarré et fonctionne correctement.

Pour arrêter le service il faut cliquer sur , pour le démarrer sur  et le relancer sur .



Le firewall doit autoriser le poste nomade connecté en PPTP à se connecter vers le réseau interne. Pour cela, les règles liées au VPN PPTP sont à définir.

Après le démarrage du service, il faut affecter un nom de Zone à la nouvelle entrée qui s'est rajoutée dans l'onglet des Zones.

21.3.2.4 Création des règles de Firewall :

Suite au démarrage du service pptp une nouvelle entrée s'ajoute dans les zones du firewall permanent. Cette interface s'appelle pptp+. Le paramétrage consiste à affecter une zone de firewall à cette interface.

CONFIGURATION DES INTERFACES RESEAU

Interface	Zone	broadcast	dhcp	roustestop	norfc1918	routefilter	routeback	blacklist
eth0	eth0	×	×	×	×	×	✓	✓
eth1	eth1	×	×	×	×	×	✓	×
eth2	eth2	×	×	×	×	×	✓	×
eth3	eth3	×	×	×	×	×	✓	×
eth1 vian 10	eth1v10	×	×	×	×	×	×	×
eth1 vian 20	eth1v20	×	×	×	×	×	×	×
eth1 vian 30	eth1v30	×	×	×	×	×	×	×
pptp+	pptp	×	×	×	×	×	×	×

RESET ENREGISTRER

La zone pptp (prédéfinie) est usuellement affectée à l'interface pptp+

AccessLog Administration

Utilisateur Accès Internet Statistiques Configuration Administration avancée

FIREWALL: REGLES PAR DEF-AUT

Règles générales

Sources	Destinations	Règles	Niveau de trace
fw	eth0	ACCEPT	
fw	eth1	ACCEPT	
fw	eth2	ACCEPT	
fw	eth3	ACCEPT	
eth1	fw	ACCEPT	
eth2	fw	ACCEPT	
eth3	fw	ACCEPT	
pptp	fw	ACCEPT	
eth1	pptp	ACCEPT	
pptp	eth1	ACCEPT	
fw	pptp	ACCEPT	
gw	fw	ACCEPT	
fw	gw	ACCEPT	
gw	eth1	ACCEPT	
eth1	gw	ACCEPT	
eth0	all	DROP	INFO
all	all	REJECT	INFO

RESET ENREGISTRER

La configuration du firewall permet de créer les autorisations entre cette nouvelle Zone et celles existantes.

En générale quatre règles doivent être rajoutées pour une connexion PPTP et le réseau local. Cependant, si vous désirez autoriser une connexion PPTP à aller vers d'autres Zones, il faudra créer autant de règles bidirectionnelles.

Les règles doivent autoriser le flux de la zone pptp vers les zones désirées.

↑ ↓	pptp	eth1	ACCEPT	
↑ ↓	eth1	pptp	ACCEPT	

Le port pour la connexion est en TCP le numéro 1723. Ce port est prédéfini dans les groupes de Firewall SRV_VPN et SRV_PPTP.

SRV_NAGIOS	9999	↺ ↻
SRV_VPN	500,4500,1701,1723	↺ ↻

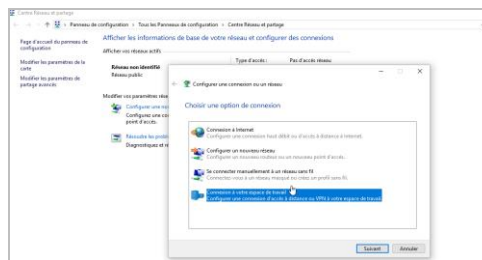
Ensuite vous créez la Règle de firewall intégrant le **TCP/1723** et le protocole VPN PPTP qui est le **GRE**

FIREWALL RÈGLES SPECIFIQUES POUR LA ZONE eth0 (Source)							
				Destination eth0			
Source eth0	Source	Destination	Règles	Protocole	Port	Commentaires	Edition
✓	eth0	eth1	REDIRECT	TCP	3389	ASSISTANCE TELMAT	[?]
✓	eth0	fw	ACCEPT	TCP	*SRV_ALL	ADMINISTRATION	[?]
✓	eth0	fw	ACCEPT	TCP	*SRV_HTTP	WEB	[?]
✓	eth0	fw	ACCEPT	TCP	*SRV_VPN		[?]
✓	eth0	fw	ACCEPT	UDP	*SRV_VPN		[?]
✓	eth0	fw	ACCEPT	GRE			[?]
✓	eth0	fw	ACCEPT	TCP	*SRV_HTTPS		[?]

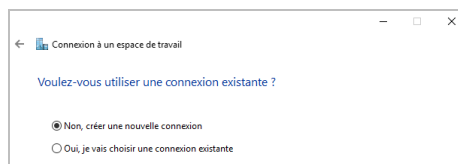
21.3.3 Configuration Client PPTP :

Le client PPTP est disponible sous Windows® Seven, 8, Win10

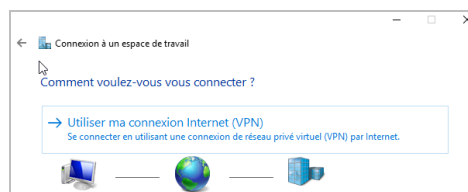
Exemple de configuration sous Windows 10



Vous devez créer une connexion *réseau privé via internet* à partir de l'assistant de connexion réseau
Vous suivez les instructions en cliquant sur *suivant*



Etape suivante



Etape suivante

← Connexion à un espace de travail

Entrez l'adresse Internet à laquelle vous souhaitez vous connecter

Votre administrateur réseau peut vous fournir cette adresse.

Adresse Internet : 212.103.26.250

Nom de la destination : PPTP TW64 VPN

☐ Utiliser une carte à puce

☒ Mémoriser mes informations d'identification

☐ Autoriser d'autres personnes à utiliser cette connexion
Cette option permet à toute personne disposant d'un accès à cet ordinateur d'utiliser cette connexion.

Ouvrir les propriétés liées au tunnel créé

Propriétés de PPTP TW64 VPN Général Options Sécurité Gestion de réseau Partage Type de réseau VPN : Protocole PPTP (Point to Point Tunneling Protocol) Chiffrement des données : Aucun chiffrement autorisé (le serveur se déconnectera si le ch...) Authentification ☐ Utiliser le protocole EAP (Extensible Authentication Protocol) ☒ Autoriser ces protocoles ☐ Mot de passe non chiffré (PAP) ☐ Protocole CHAP (Challenge Handshake Authentication Protocol) ☒ Protocole Microsoft CHAP Version 2 (MS-CHAP v2) ☐ Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine) OK Annuler	* Protocole PPTP * Aucun Chiffrement * MSchap V2
---	--

L'adresse de destination correspondant à l'IP publique de votre l'**AccessLog**, puis vous terminez la configuration.

En cliquant sur l'icône de connexion distante que vous venez de créer, à l'invite d'authentification vous saisissez le login et le mot de passe que vous avez configuré dans le serveur PPTP de l'**AccessLog**.

Au lancement de la connexion le Login/Mot de passe sera demandé Sécurité Windows Se connecter dark OK Annuler	La connexion réalisée PPTP TW64 VPN Connecté Déconnecter
---	--

21.3.4 Connexion en cours :

La visualisation de/des connexions en cours permet d'avoir le login, les adresses IP de connexion, le type de compression.

ETAT DES CONNEXIONS VPN PPTP/L2TP						
Connexion PPTP/L2TP En Cours						
Login	Début de Connexion	Connexion	Adresse IP locale attribuée	Adresse IP distante attribuée	Volume Reçu	Volume Emis
rpa	May 22 17:30:08	ppp0	192.168.0.240	192.168.132.128	8.8 KiB	140.0 b

La connexion réalisée, les informations doivent transiter vers le réseau local distant. Si ce n'est pas le cas, la configuration firewall doit être vérifiée ou le poste distant sur lequel on désire se connecter n'est pas correctement configuré.

```

Sélection Invite de commandes
Microsoft Windows [version 10.0.17134.472]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\TELMATWEB>ping 192.168.0.100

Envoi d'une requête 'Ping' 192.168.0.100 avec 32 octets de données :
Réponse de 192.168.0.100 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.100 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.100 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.0.100 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 192.168.0.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms
  
```

21.3.5 Prise en compte des modifications :

La prise en compte des modifications n'est pas dynamique. Le rechargement se fait en cliquant sur .

21.4 VPN L2TP / IPSEC :

La fonctionnalité VPN PPTP/L2TP n'est disponible que sur système **AccessLog** à partir de la Release système **TAL_20200730**.

Pour accéder aux informations de votre système cliquez sur l'icône  (en haut à gauche dans le menu d'administration)

21.4.1 Configuration du service et création du compte PPTP/L2TP :

21.4.1.1 Configuration du Service :

La configuration du Service se fait par le menu

- Configuration/ VPN PPTP/L2TP/Configuration
 - Permet la configuration des adresses IP qui seront utilisées par le service lors de la connexion du client.
 - Adresse IP locale attribuée : C'est l'adresse utilisée par le service s'exécutant sur la machine. Cette adresse d'écoute est unique
 - Plage d'Adresses IP distantes attribuées : Pool d'adresses disponibles pour la distribution. Il doit y en avoir autant que de postes susceptibles de se connecter :

La syntaxe est "AddIpDepart-AddIpFin"

- Serveur DNS et Server Wins sont les adresses distribuées au moment de la connexion

AccessLog Administration (admin 192.168.26.14)

Utilisateur | Accès Internet | Statistiques | **Configuration** | Administration avancée

CONFIGURATION VPN PPTP/L2TP

VPN PPTP	VPN L2TP
Plage d'Adresses IP locales attribuées: 192.168.0.240-250	Adresse IP locale attribuée: 10.10.10.1
Plage d'Adresses IP distantes attribuées: 192.168.132.128-138	Plage d'Adresses IP distantes attribuées: 10.10.10.30-10.10.100
Serveur DNS:	Serveur DNS: 8.8.4.4
Serveur WINS:	Serveur WINS:

MODIFIER

21.4.1.2 Création du compte :

La création du compte se fait par le menu

- Configuration générale/VPN PPTP/L2TP/compte

COMPTES VPN PPTP/L2TP

Sélection: dark

Paramètres de Connexion

Connexion Active: ☒

Login de connexion distant: dark

Password: vador

Adresse IP distante propre à ce login: -

MODIFIER MODIFIER

- Sélectionner un compte existant
- Cocher Connexion Active
- Saisir le login et le mot de passe
- Optionnel : Saisir une adresse IP propre à ce login. Laisser le "-" pour l'attribution par le système
- Choisir l'action d'AJOUTER et dans le menu déroulant et cliquer sur MODIFIER

COMPTES VPN PPTP/L2TP

Sélection: dark

Paramètres de Connexion

Connexion Active: ☒

Login de connexion distant: dark

Password: vador

Adresse IP distante propre à ce login: -

MODIFIER MODIFIER

MODIFIER
AJOUTER
SUPPRIMER

21.4.1.3 Relance du Service PPTP/L2TP

Le voyant d'état du service ainsi que les actions possibles sont localisé dans la partie supérieure droite du menu



L'état du service est symbolisé par l'aspect du voyant :

L'état du service est donné par la couleur du point.

- Signifie que le service est actif mais qu'il ne fonctionne pas correctement,
- Le service est arrêté,
- Le service est démarré et fonctionne correctement.

21.4.2 Configuration du service IPSEC pour L2TP :

Le protocole L2TP s'appuie pour le cryptage sur l'IPSEC

La configuration de l'IPSEC pour le L2TP s'effectue en deux étapes.

- Le paramétrage du circuit VPN local
- La clé partagée secrète associée.

21.4.2.1 Paramétrage du circuit VPN L2TP local :

- Configuration/VPN PPTP/L2TP/Configuration Locale

La configuration du VPN IPSEC L2TP s'effectue en paramétrant la Configuration Locale et la Configuration locale L2TP.

Configuration Locale : Définit le paramétrage de configuration général de l'IPSEC au moment du démarrage.

- Left Adresse IP WAN locale : Adresse IP sur laquelle l'IPSEC est en écoute. %defaultroute
- LeftNexthop Nexthop Local : Adresse IP du routeur de sortie. C'est la route par défaut du système. %defaultroute permet d'hériter de l'adresse IP de la route par défaut.
- Left Identifiant local : Identifiant utilisé lors de l'authentification
- Type de clé : Méthode d'authentification entre les deux machines. A choisir entre Clé partagée secrète SECRET, et Clé RSA.

Configuration locale L2TP : description commune à toutes les connexions L2TP

- Leftid Identifiant local : Identifiant pour l'authentification. Uniquement adresse IP.%defaultroute reprend l'adresse IP de la route par défaut.
- Classes Réseau autorisées : contient les classes réseau autorisées pour le client distant
- Les classes prédéfinies correspondent aux adresses autorisées dans les réseaux privés. Sont définis dans les RFC1918 pour IPV4 et RFC5156, RFC4291, RFC3587 pour IPV6

A la fin du paramétrage cliquer sur ENREGISTRER.

Désactivation du Test D'Entrée n'est à utiliser : Laisser activé, c'est un contrôle sur les adresses IP sources qui doivent être dans les classes réseaux privées

NAT Traversal : Permet de configurer l'encapsulation des trames ESP dans le cas où il a un routeur qui fait de la translation d'adresse en amont

21.4.2.2 Paramétrage des clés partagées Secrètes :

Dans le cas du L2TP le circuit IPSEC doit accepter en identifiant distant n'importe quelle adresse IP du poste distant. Le champ *Adresse IP distante ou identifiant* doit être paramétré à **%any**.

Toutes les connexions L2TP et IPSEC en mode itinérant devront utiliser la même clé.

Menu concerné :

- Configuration/VPN IPSEC / Clés Partagées Secrètes

Suite à la configuration ENREGISTRER la configuration.

21.4.2.3 Relance du Service VPN IPSEC

Le voyant d'état du service ainsi que les actions possibles sont localisé dans la partie supérieure droite du menu

L'état du service est symbolisé par l'aspect du voyant :

- Signifie que le service est actif mais qu'il ne fonctionne pas correctement,
- Le service est arrêté,
- Le service est démarré et fonctionne correctement.

Les Actions possibles :

- Démarrage du service
- Arrêt du service
- Relance du service , une fenêtre affichant tous les circuits IPSEC et le circuit L2TP s'ouvre. Il est alors possible de relancer tous les circuits ou uniquement ceux choisis.

21.4.2.4 Configuration Firewall :

Le firewall est par défaut non configuré pour accepter les connexions VPN.

Celui-ci doit être configuré pour accepter l'échange des données.

Service	Protocoles	Ports
VPN IPSEC	UDP	500,4500
VPN PPTP	TCP	1723
VPN PPTP	GRE	
VPN PPTP/L2TP	UDP	1701
VPN OpenVPN	UDP/TCP	1194 (peut être modifié)

Lorsque les tunnels sont établis le firewall doit être configuré en fonction des échanges à donner à l'intérieur du tunnel.

Les zones firewall réservées sont

Type Tunnel	Zone Firewall
IPSEC	gw
PPTP/L2TP	ppp+
OpenVpn	ovpn

Les règles générales pour établir une connexion VPN L2TP sont les suivantes :

Sources	Destinations	Règles	Niveau de trace
fw	eth0	ACCEPT	
fw	eth1	ACCEPT	
fw	eth2	ACCEPT	
fw	eth3	ACCEPT	
eth1	fw	ACCEPT	
eth2	fw	ACCEPT	
eth3	fw	ACCEPT	
pptp	fw	ACCEPT	
eth1	pptp	ACCEPT	
pptp	eth1	ACCEPT	
fw	pptp	ACCEPT	
gw	fw	ACCEPT	
fw	gw	ACCEPT	
gw	eth1	ACCEPT	
eth1	gw	ACCEPT	
eth0	all	DROP	INFO
all	all	REJECT	INFO

RESET ENREGISTRER

Ces règles doivent permettre le dialogue avec le réseau local (eth1 dans ce cas) et le service VPN (zone fw).

21.4.3 Visualisation des connexions en cours :

Les connexions en cours sont visibles dans le menu

- Configuration/VPN PPTP/L2TP/ Etat des connexions

Login	Début de Connexion	Connexion	Adresse IP locale attribuée	Adresse IP distante attribuée	Volume Reçu	Volume Emis
rpa	May 22 17:30:08	ppp0	192.168.0.240	192.168.132.128	8.8 KiB	140.0 b

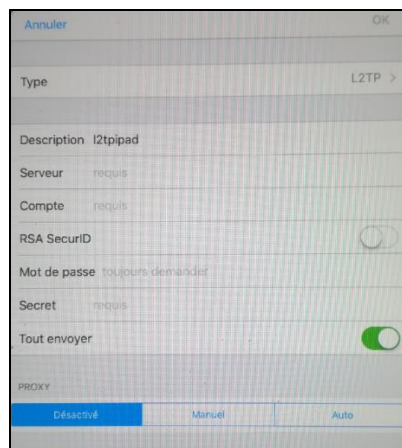
21.4.4 Configuration Client de Connexion :

21.4.4.1 Configuration Client IPAD™ :

L'appareil doit être connecté au réseau WIFI.

Menu Réglage, toucher l'icône VPN

Choisir : Ajouter une connexion VPN



Type : Choisir dans la liste L2TP. Le menu s'affiche en conséquence

Description : Nom de la connexion que vous choisissez

Serveur : Adresse IP ou nom du serveur distant

Compte : Compte de la connexion (VPN PPTP/L2TP)

RSA SecurID : ne pas activer

Mot de passe : Mot de passe de l'utilisateur défini lors de la création du compte VPN PPTP/L2TP

Secret : Clé partagée secrète définie dans le VPN IPSEC.

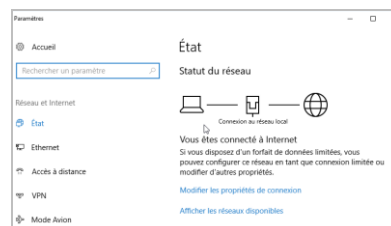
Lancer la connexion. L'utilisateur connecté est visible dans le menu Etat des connexions VPN PPTP/L2TP

21.4.4.2 Configuration client Microsoft Windows™ :

La configuration présentée est sous Windows10

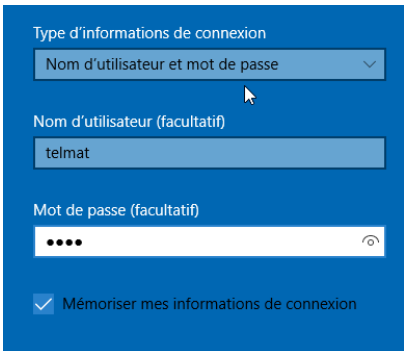
Le Poste doit être connecté au réseau

➤ Menu Paramètres réseau et internet

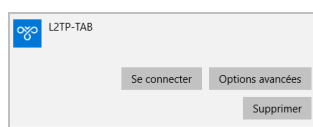


- Cliquer sur VPN et Ajouter une Connexion VPN

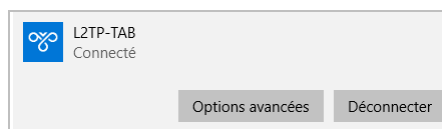
	<u>Fournisseur VPN</u> : choisie Windows (intégré) <u>Nom de la connexion</u> : saisir un nom évocateur <u>Nom ou adresse IP du serveur VPN</u> : peut-être un nom ou une adresse IP <u>Type de réseau</u> : Choisir L2TP avec clé pré-chargée <u>Clé pré-partagée</u> : saisie la clé saisie dans le menu <i>clé partagée secrète</i> de l'AccessLog
---	---

	<u>Type d'informations de connexion</u> : choisir dans la liste <i>Nom d'utilisateur et mot de passe</i>. <u>Nom d'utilisateur</u> : Nom déclaré dans le menu VPN PPTP/L2TP <u>Mot de passe</u> : Mot de passe déclaré dans le menu VPN PPTP/L2TP
--	--

Après avoir ENREGISTRER la configuration, le nom de la connexion s'affiche
La connexion est prête pour être lancée : Se connecter



La connexion réalisée,



Dans les traces de connexions L2TP/IPSEC

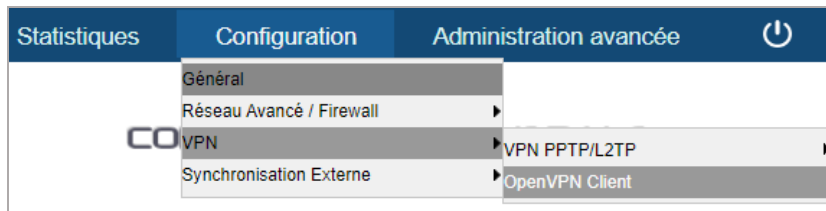

```

-----
Profile: xl2tp
-----
000 "xl2tp": 192.168.26.140:17/1701---192.168.26.254...%any:17/%any; unrouted; eroute owner: #0
000 "xl2tp": myip=unset; hisip=unset;
000 "xl2tp": ike_life: 28800s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 3
000 "xl2tp": policy: PSK+ENCRYPT+IKEv2ALLOW+SAREFTRACK+rKOD; prio: 32,32; interface: eth0;
000 "xl2tp": dpd: action:clear; delay:10; timeout:20;
000 "xl2tp": newest ISAKMP SA: #0; newest IPsec SA: #0;
000 "xl2tp"[2]: 192.168.26.140:17/1701---192.168.26.254...192.168.26.22:17/1701; erouted; eroute owner: #4
000 "xl2tp"[2]: myip=unset; hisip=unset;
000 "xl2tp"[2]: ike_life: 28800s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 3
000 "xl2tp"[2]: policy: PSK+ENCRYPT+IKEv2ALLOW+SAREFTRACK+rKOD; prio: 32,32; interface: eth0;
000 "xl2tp"[2]: dpd: action:clear; delay:10; timeout:20;
000 "xl2tp"[2]: newest ISAKMP SA: #3; newest IPsec SA: #4;
000 "xl2tp"[2]: IKE algorithm newest: AES_CBC_256-SHA1-MODP2048
++++++
Tunnel: xl2tp
++++++
000 #4: "xl2tp"[2] 192.168.26.22:500 STATE_QUICK_R2 (IPsec SA established); EVENT_SA_REPLACE in 3208s; newest IPSEC; eroute owner; isakmp#3; idle; import: not set
000 #4: "xl2tp"[2] 192.168.26.22 esp.707cb17e@192.168.26.22 esp.fc9ed405@192.168.26.140 ref=0 rethim=4294901761
000 #3: "xl2tp"[2] 192.168.26.22:500 STATE_MAIN_R3 (sent MR3, ISAKMP SA established); EVENT_SA_REPLACE in 28408s; newest ISAKMP; nodpd; idle; import: not set

```

21.5 Client OpenVpn :

L'AccessLog permet une interconnexion type LAN-to-LAN par l'utilisation du client OPENVPN vers un site centralisé Accesslog disposant du serveur OPENVPN

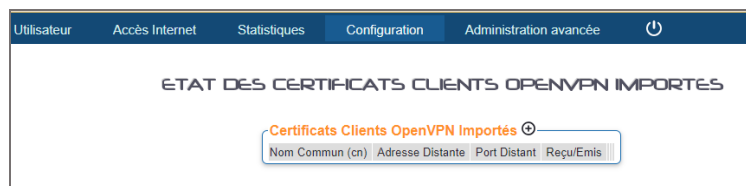


Les étapes pour configurer la partie clientes sont les suivantes :

21.5.1.1 Injection du certificat :

Vous devez disposer d'un certificat OpenVpn généré sur le serveur OpenVpn (Cf chapitre OpenVpn Serveur).

Il doit être importé via le menu d'importation des certificats clients



Cliquer sur l'icone  pour accéder au menu d'importation



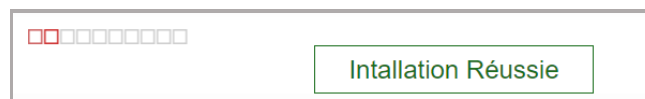
Sélectionner le certificat à importer en cliquant sur 



Puis cliquer sur **AJOUTER**.

Renseignez les informations nécessaires lors de l'importation

Importation réussie



En version Client le service n'est pas démarré - lancer l'exécution du service et de la connexion avec le certificat désiré.



Lorsque le service est correctement démarré les voyants passent en bleue.



21.5.1.2 Configuration du Firewall :

Les règles de firewall sont à paramétrer

- Pour la communication du client / serveur du côté Wan : Port et protocole paramétrés dans le serveur OPENVPN.



- Pour la communication des réseaux VPN entre eux
Cela dépend de l'interface locale et si la communication est autorisée vers les services locaux (zone fw) :

^ v	eth1	ovpn	ACCEPT	
^ v	ovpn	eth1	ACCEPT	
^ v	ovpn	fw	ACCEPT	
^ v	fw	ovpn	ACCEPT	

Lors d'une connexion par portail captif il est impératif de rajouter la classe d'adresse IP distante (vers le serveur) dans *Site en Libre Accès Sans Authentication*. Dans cet exemple, la classe 192.168.148.0/24 est le réseau distant accédé côté serveur.

SITE EN LIBRE ACCÈS SANS AUTHENTIFICATION

Liste des Sites en Libre Accès Sans Authentication

192.168.148.0/24					
------------------	--	--	--	--	--

Etat du circuit établi :

- Côté client

Certificats Clients OpenVPN Importés

Nom Commun (cn)	Adresse Distante	Port Distant	Reçu/Emis
Cert Res17	192.168.26.148	1194	28840/29332

- Côté serveur

CERTIFICATS CLIENTS OPENVPN GÉNÉRÉS

Sélection Le cert Central

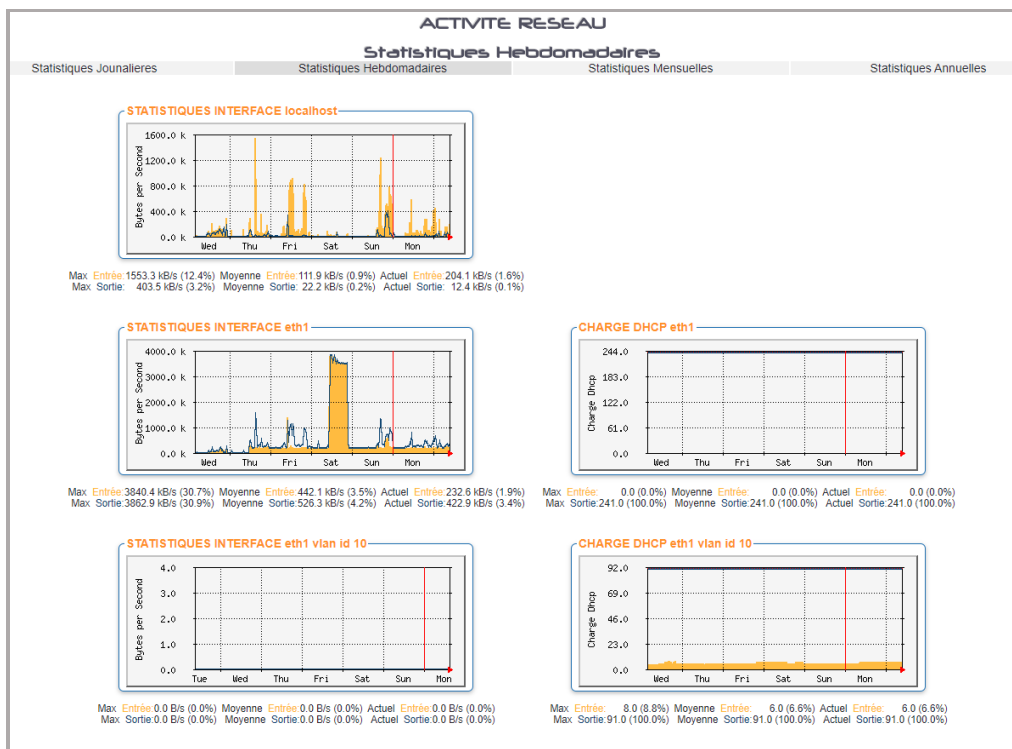
Nom Commun (cn)	Adresse Distante	Adresse Locale	Reçu/Emis	Connecté	Certificat Serveur	Route	Valable jusqu'à			
Cert Mag Central					Le cert Central	192.168.148.0/255.255.255.0	9/Feb/2024 17:22:31 GMT	ovpn	igtz	
Cert Res17	192.168.26.17	10.8.0.54	29660/29168	03/Mar/2023 15:59:42	Le cert Central	192.168.17.0/255.255.255.0	18/Mar/2023 14:44:01 GMT	ovpn	igtz	
cert warrior2					Le cert Central	-	4/Feb/2023 14:31:25 GMT	ovpn	igtz	

22 Statistiques

Plusieurs types de statistiques sont disponibles sur **AccessLog**.

22.1 Activités Réseau :

Retrace l'activité de chaque interface réseau ainsi que la charge du service DHCP lié. Elles sont enregistrées sur une durée de maximum une année.



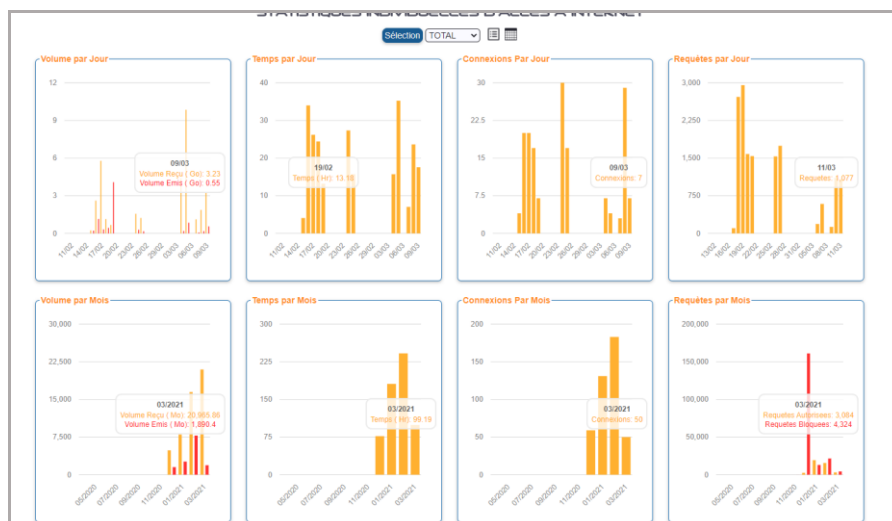
22.2 Accès Internet :

Le tableau affiche les consommations volume/temps des utilisateurs ou des postes. Cela dépend des modes de connexions ayant été paramétrés sur la machine

Légende : Accès Internet il y a moins de 10 s 1 mn 5 mn 30 mn

	Accès du 09/03			Cumul par Mois			Maxi par Mois			Cumul par An			Maxi par An		
	Volume	Temps	Connexion	Volume	Temps	Connexion	Volume	Temps	Connexion	Volume	Temps	Connexion	Volume	Temps	Connexion
TOTAL	3.2G	17h34m	7	37.1G	244h05m	165	9.9G	35h14m	30	49.1G	598h43m	423	20.5G	241h44m	183
wopijidi	1.5G	1h26m	1	1.5G	1h26m	1	1.5G	1h26m	1	1.5G	1h26m	1	1.5G	1h26m	1
jumasiki	868.8M	8h32m	1	1.3G	9h01m	2	868.8M	8h32m	1	1.3G	9h01m	2	1.3G	9h01m	2
fineruxa	830.9M	4h58m	2	830.9M	4h58m	2	830.9M	4h58m	2	830.9M	4h58m	2	830.9M	4h58m	2
hajeqalu	37.2M	49m14s	1	116.6M	49m14s	1	116.6M	49m14s	1	116.6M	49m14s	1	116.6M	49m14s	1
wigyhesi	-	-	-	85.4M	28m35s	1	85.4M	28m35s	1	85.4M	28m35s	1	85.4M	28m35s	1
nadogihia	3.1M	1h17m	1	25.6M	1h17m	1	25.6M	1h17m	1	25.6M	1h17m	1	25.6M	1h17m	1
pydawowi	9.0M	1h53m	273	9.0M	1h53m	273	9.0M	1h53m	273	9.0M	1h53m	273	9.0M	1h53m	273
bunudogu	4.4M	30m16s	1	4.4M	30m16s	1	4.4M	30m16s	1	4.4M	30m16s	1	4.4M	30m16s	1
xacuzybo	43.3K	14m18s	57	43.3K	14m18s	57	43.3K	14m18s	57	43.3K	14m18s	57	43.3K	14m18s	57
sopogyha	21.2K	40m01s	56	21.2K	40m01s	56	21.2K	40m01s	56	21.2K	40m01s	56	21.2K	40m01s	56
vuhudify	19.3K	8m03s	23	19.3K	8m03s	23	19.3K	8m03s	23	19.3K	8m03s	23	19.3K	8m03s	23

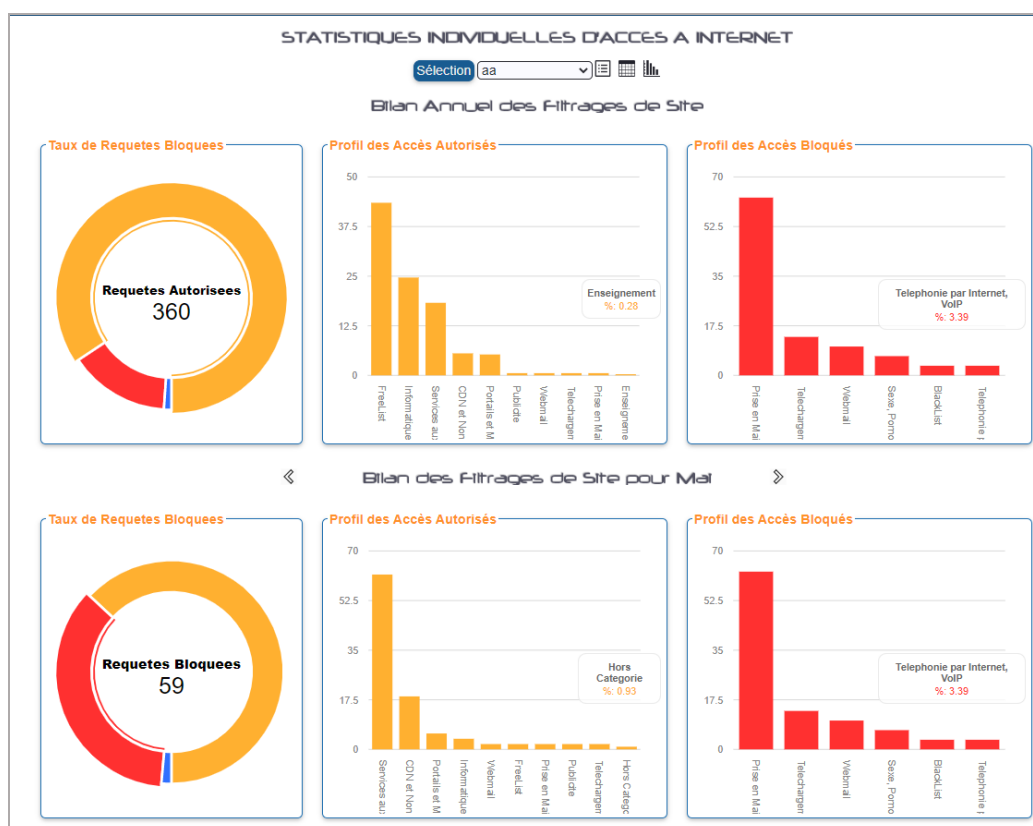
L'affichage est du type barre-graphe – Ne donne pas d'indication sur les sites accédés.



Si le module filtrage par catégorie de sites est présent, des statistiques complémentaires sont disponibles

Légende : Accès Internet il y a moins de 10 s 1 mn 5 mn 30 mn

	Accès du 31/05			Cumul par Mois			Maxi par Mois			Cumul par An			Maxi par An		
	Volume	Temps	Connexion	Volume	Temps	Connexion	Volume	Temps	Connexion	Volume	Temps	Connexion	Volume	Temps	Connexion
TOTAL	-	-	-	136.2M	2h27m	14	136.2M	2h27m	14	217.5M	6h52m	25	136.2M	3h35m	14
cc	-	-	-	130.3M	2h22m	8	130.3M	2h22m	8	130.3M	2h22m	8	130.3M	2h22m	8
aa	-	-	-	4.7M	4m58s	3	4.7M	4m58s	3	15.8M	55m07s	9	7.6M	28m11s	5

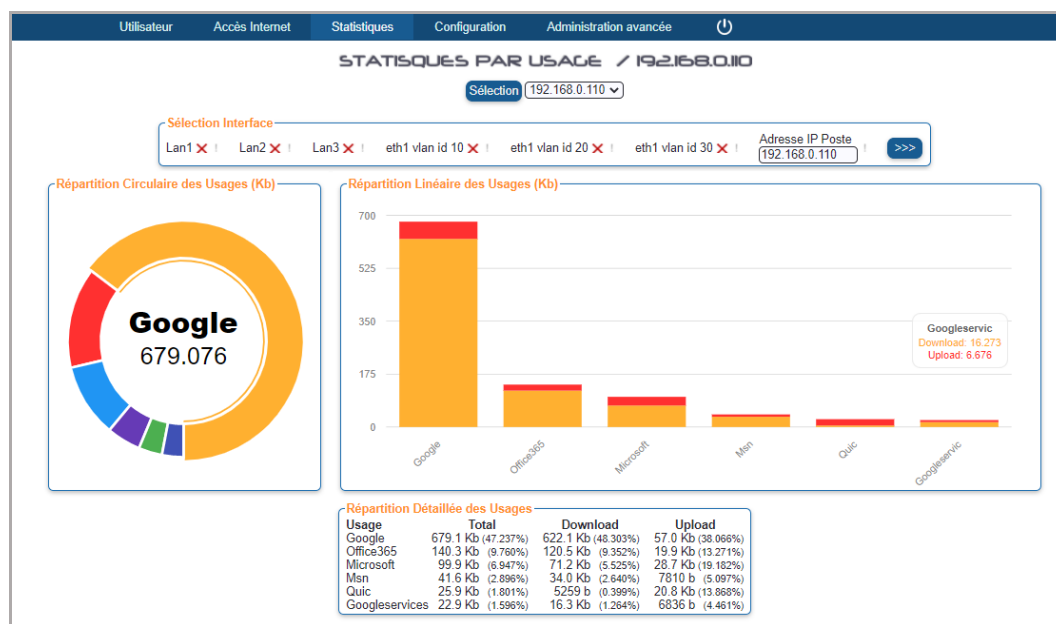


22.3 Statistiques par usage :

Des statistiques par usage peuvent être calculées puis affichées.

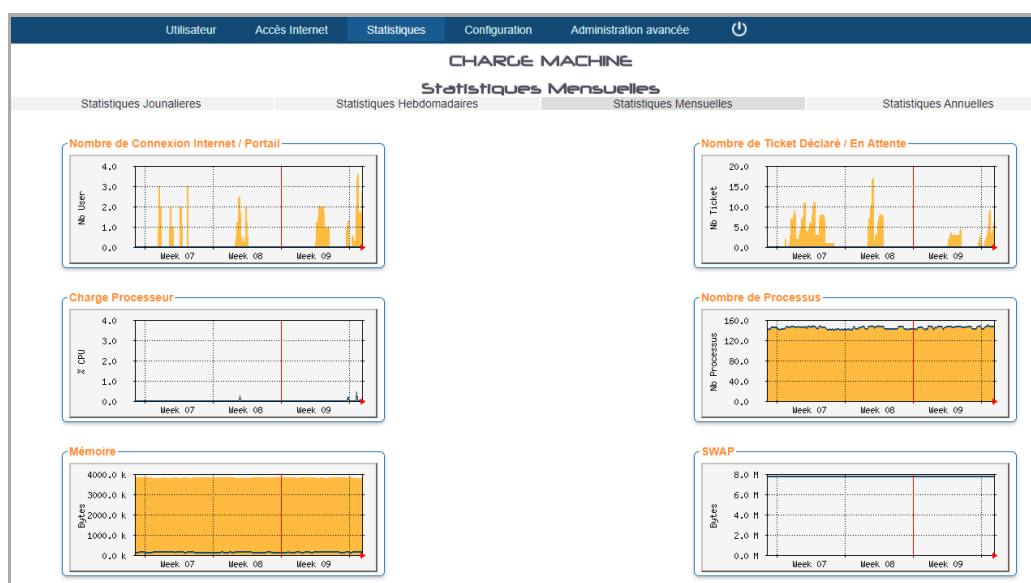
Attention, ces statistiques sont volatiles, elles sont remises à zéro lors d'un rechargement de configuration, redémarrage de la machine

L'enregistrement peut se faire sur une interface entière ou alors par adresses IP.



22.4 Charge machine :

Statistiques enregistrées jusqu'à un an, retrace la charge mémoire, disque, processeur, connexions



23 Administration avancée

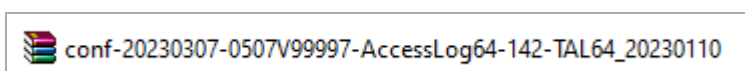
23.1 Sauvegarde/Restauration de la configuration

Permet de réaliser la sauvegarde/duplication de la configuration système de l'AccessLog-Evo/Pro.



- ✓ La sauvegarde de la configuration contient le paramétrage complet de votre machine et l'enregistre sur le poste de travail administrateur.
- ✓ La duplication de configuration permet de reporter une configuration existante sur une nouvelle machine.
- ✓ Nom de la sauvegarde : en cliquant sur  vous accédez au menu de configuration du nom de la sauvegarde.

Le choix des champs se fait à travers les menus déroulants présents.



23.2 Restauration de la configuration USINE

- ▶ La restauration de la configuration usine permet de remettre une machine en configuration d'origine, sans effacer les traces enregistrées.
- ▶ Vous pouvez restaurer une configuration usine par le biais d'une clé USB. La clé USB doit avoir une seule partition et contenir un fichier vide nommé **forcereinit** (aucune extension), forcereinit.txt. La clé insérée dans la prise USB, il faut redémarrer la machine.

23.3 Mise à jour logicielle

Les mises à jour **AccessLog-Evo/Pro** sont automatiques.



Lorsque le voyant de mise à jour est orange, cela signifie qu'une mise à jour du système est nécessaire.

Lorsque le voyant de mise à jour est orange et clignote cela signifie qu'une mise à jour est en cours.

Ne pas éteindre la machine, pendant la phase de mise à jour.

23.4 Saisie Licence :

Pour bénéficier des dernières évolutions logicielles et maintenir la garantie matérielle de votre **AccessLog Evo/Pro** à jour, les

- ✓ Mises à jour logicielles
- ✓ Extension de Garantie
- ✓ Renouvellement option logicielle

Sont à souscrire annuellement. Le numéro de licence qui vous est retourné suite à votre commande doit être saisi dans le menu : **Administration Avancée/Mise à jour**

Numero de Série de votre Equipement : 0507V99997	
Date de fin d'abonnement des mises à jour Systeme :	25/05/2025
Date de fin d'abonnement du Filtrage des Sites Internet Dynamique :	11/05/2024
Date de fin de garantie matérielle constructeur (RU) :	20/04/2023
Ajout d'une Extension de Licence, Code :	
Valider	

- ✓ Veiller à saisir cette licence avant la date d'expiration inscrite sur le document
- ✓ Veiller à saisir une licence compatible avec la configuration de votre équipement

24 Activation Licence Olféo, Filtrage :

Le filtrage par catégorie de sites de l'AccessLog utilise les bases de données filtrage de l'éditeur Olféo.

Ces catégories sont classées par thème et configurable dans les profils Base et Sécurisé.

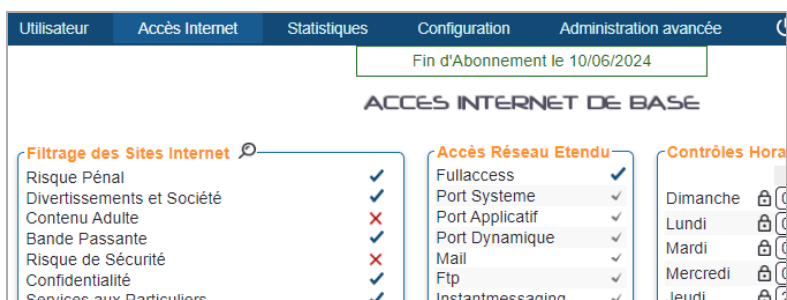
Plusieurs cas se présente pour l'activation de la licence

24.1 Souscription nouvelle licence Olféo :

- ✓ L'option Filtrage Olféo doit être Active
- ✓ La machine doit être connectée à internet
- ✓ La machine doit être à l'heure

Pour activer la clé cliquer sur le bouton **ACTIVER VOTRE CLE** dans le menu *Accès Internet/Accès internet de Base*

Suite à l'activation la date de fin d'abonnement s'affiche

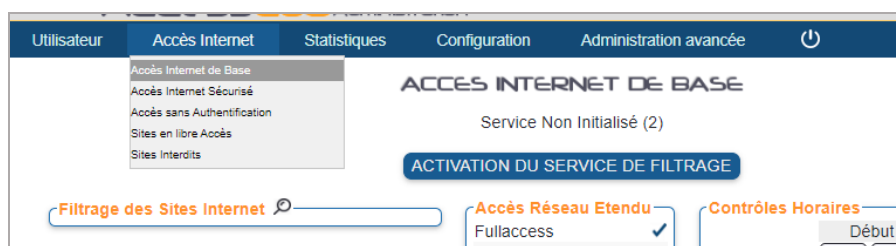


24.2 Restauration configuration utilisateur et usine :

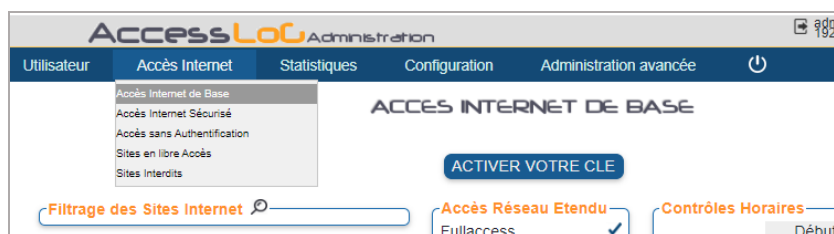
La clé doit être réactivée lors de la **Duplication d'une configuration** ainsi que lors de la **Restauration de la Configuration Usine**.

Ceci se fait en deux étapes :

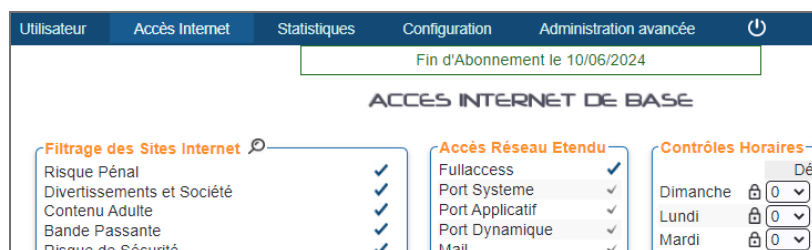
- ✓ Activation du Service de Filtrage : Cliquer sur le bouton dans le profil base ou sécurisé



Activation de la clé : Suite à l'activation du filtrage vous devez activer la Clé



La synchro **réussie** affiche la date de fin d'abonnement



24.3 Filtrage :

Le filtrage par catégorie se configure via les profils : Base ou Sécurisé

Pour accéder à la liste complète cliquer sur

FILTRE PAR CATEGORIE DE SITE / Base

Risque Pénal ✓ Alcool et Tabac Condamnés par la Loi Française Atteinte Physique et Morale Contrefaçon Drogue (UT1) Hacking (UT1) Immigration clandestine et Travail illégal Jeux d'Argent Condamnés par la Loi Française Jeux de Hasard (UT1) Matériel Dangereux (UT1) Musique, Films, Logiciels Piratés Peer to Peer Pornographie Condamnée par la Loi Française Promotion et Vente de Drogue Racisme, Discrimination, Révisionnisme Terrorisme, Incitation à la Violence, Explosifs Tricheur (UT1) Vente d'Armes Condamnée par la Loi Française Vente de Médicaments Condamnée par la Loi Française Warex (UT1)	Diversissements et Société ✓ Arts et Culture Astrologie (UT1) Cinéma Commerce en Ligne Clébrité (UT1) Humour Informatique et Technologies Jeux (UT1) Jeux Vidéo, Jeux en Ligne Jeux, Jouets Loisirs, Hobbies, Passions Mode, Beauté, Bien-Être, Décoration Médias, Actualités Météo Organisations Politiques et Sociales People Photographie, Bases de Données d'images Religions Non Traditionnelles, Occultes, Sectes Religions Traditionnelles Sexe (UT1) Shopping (UT1) Sorties, Soirées, Concerts Sports Sujets de Société Tourisme, Hôtels, Restaurants Téléphone Mobile (UT1) Téléphone Mobile, Logos, Sonneries Volures, Mécaniques	Contenu Adulte ✗ Adulte (UT1) Adulte Mince (UT1) Agresseur (UT1) Alcool et Tabac Armes, Chasse, Equipement de Sécurité Contenu Agressif, de Mauvais Goût Education Sexuelle (UT1) Jeux d'Argent, Micro Paiement, Loteries Lingerie, Maillots de Bain Nuauté Rencontres Rencontres (UT1) Sexe, Pornographie Sexualité	Bande Passante ✓ Audio et Vidéo Audio-vidéo (UT1) Hébergement de Fichiers (UT1) Navigation Réamplifiée Prise en Main à Distance, Outils de Collabor Publicité (UT1) Radio (UT1) Serveurs de Statistiques Sites de Partage de Vidéo Stockage de Données en Ligne Téléchargement de Fichiers Téléphone par Internet, VoIP Télévision, Radio
Risque de Sécurité ✗ Caches Domaines Parkés Phishing (UT1) Proxies, Redirecteurs Redirector (UT1) Redirector Strong (UT1) Redirector Strong (UT1) Réducteurs d'URL Virus, Spywares, Phishing, Codes Malicieux	Confidentialité ✓ Blog Blog (UT1) Chat Forum, Wiki Forums (UT1) Hébergement de Sites, FAI Pages Personnelles Réseaux Sociaux Webmail Webmail (UT1)	Services aux Particuliers ✓ Banques, Assurances, Caisses Emploi, Recrutement Financier (UT1) Immobilier Investissement, Bourse, Placement Petites Annonces Portails et Moteurs de Recherche Généralist Santé Services aux Particuliers	Services aux Entreprises ✓ Administrations Comités d'Entreprises Communication d'Entreprise Droit Social Droit, Fiscalité Forum, Wiki Professionnels Guides, Plans, Etat des Routes Marketingware (UT1) Nettoyage (UT1) Services aux Entreprises Site Interne Traducteurs
Education ✓ Enfance Priorité Temporaire Sciences, Recherches	Catégories obsolètes ✓ Envoi de Textos et MMS Priorité Temporaire Réaffecté (UT1)	Autres ✓ CDN et Non Définissable IP Non Classée Site Indisponible Site à Accès Restreint URL Non Classé	

MODIFIER RESET

TEST

Pour vérifier dans quelle catégorie est référencée le site utilisez le champ **TEST**
 La catégorie résultat (si elle existe) est colorée

Pages Personnelles Réseaux Sociaux Webmail Webmail (UT1)	Petites Annonces Portails et Moteurs de Recherche Généralist Santé Services aux Particuliers	Guides, Plans, Etat des Routes Marketingware (UT1) Nettoyage (UT1) Services aux Entreprises Site Interne Traducteurs
Catégories obsolètes ✓ Envoi de Textos et MMS Priorité Temporaire Réaffecté (UT1)	Autres ✓ CDN et Non Définissable IP Non Classée Site Indisponible Site à Accès Restreint URL Non Classé	

MODIFIER RESET

www.telmat.fr TEST Temps d'accès Mini : 0.304 ms
 Temps d'accès Maxi : 3.509 ms

Il est possible de déplacer une catégorie d'un thème vers un autre. Par exemple d'un thème interdit ✗ vers une thème autorisé ✓.

Ce déplacement se fait par un *Glisser et Déposer (Drag and Drop)*
 Sélectionner l'élément avec votre souris et sans relâcher le bouton de celle-ci, déplacer celle-ci vers le thème choisi. Puis cliquer sur **MODIFIER**

FILTRE PAR CATEGORIE DE SITE / Base

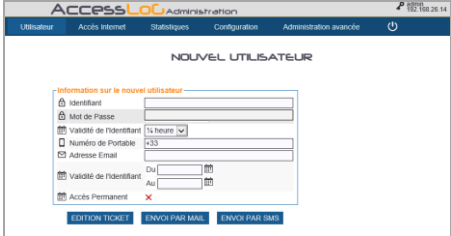
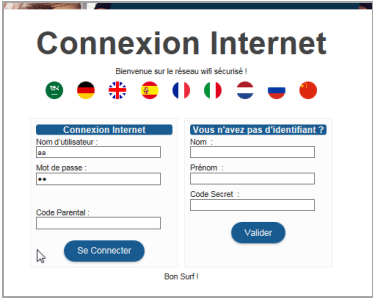
Divertissements et Société ✓ Arts et Culture Astrologie (UT1) Cinéma Commerce en Ligne Célébrité (UT1) Humour Informatique et Technologies Jeux (UT1) Jeux Vidéo, Jeux en Ligne Jeux, Jouets Loisirs, Hobbies, Passions Mode, Beauté, Bien-Etre, Décoration Météo Organisations Politiques et Sociales People Médias, Actualités Photographie, Bases de Données d'Images Religions Non Traditionnelles, Occultes, Sect Religions Traditionnelles Secte (UT1) Shopping (UT1) Sorties, Soirées, Concerts Sports Sujets de Société Tourisme, Hôtels, Restaurants Téléphone Mobile (UT1) Téléphonie Mobile, Logos, Sonneries Voitures, Mécaniques	Contenu Adulte ✗ Adulte (UT1) Adulte Mixte (UT1) Agressif (UT1) Alcool et Tabac Armes, Chasse, Equipement de Sécurité Contenu Agressif, de Mauvais Goût Education Sexuelle (UT1) Jeux d'Argent, Micro Paiement, Loteries Lingerie, Maillots de Bains Nudité Rencontres (UT1) Sexe, Pornographie Sexualité	Bande Passante ✓ Audio et Vidéo Audio-vidéo (UT1) Hébergement de Fichiers (UT1) Navigation Rémunérée Prise en Main à Distance, Outils de Collabor Publicité Publicité (UT1) Radio (UT1) Serveurs de Statistiques Sites de Partage de Vidéo Stockage de Données en Ligne Téléchargement de Fichiers Téléphonie par Internet, VoIP Télévision, Radio
Confidentialité ✓ Blog Blog (UT1) Chat Forum, Wiki Forums (UT1) Hébergement de Sites, FAI Pages Personnelles Réseaux Sociaux Webmail Webmail (UT1)	Services aux Particuliers ✓ Banques, Assurances, Caisses Emploi, Recrutement Enchères en Ligne Financier (UT1) Immobilier Investissement, Bourse, Placement Petites Annonces Portails et Moteurs de Recherche Généralist Santé Services aux Particuliers	Services aux Entreprises ✓ Administrations Comités d'Entreprises Communication d'Entreprise Droit Social Droit, Fiscalité Forum, Wiki Professionnels Guides, Plans, Etat des Routes Marketingware (UT1) Nettoyage (UT1) Site Interne Traducteurs

Services aux Entreprises

Pour replacer les catégories déplacées dans leurs thèmes originaux cliquer sur **RESET**

Annexe 1 : Vérification du bon fonctionnement du Portail Captif

La bonne configuration de votre **AccessLog-Evo/Pro**, sera vérifiée par l'accès à Internet d'un utilisateur.

	▶ Depuis l'interface d'administration, déclarez un nouvel utilisateur.
	▶ Depuis un poste utilisateur connecté au réseau local, tentez un accès à un site internet. ▶ Vous devez obtenir la fenêtre d'authentification de l'AccessLog-Evo/Pro ▶ Le Bouton de mémorisation de la connexion est présent si l'option mémorisation des identifiants est présent
	▶ Entrez votre identifiant ▶ Entrez votre mot de passe ▶ Puis cliquez sur VALIDER ▶ En cas d'échec un message est affiché à l'écran. Les traces permettent aussi de déterminer la raison du refus.
	▶ Lorsque la connexion est réalisée, la fenêtre de Connexion Autorisée s'ouvre. Celle-ci doit être maintenue pendant toute la période de la connexion. ▶ La fenêtre de Connexion Autorisée vous signale que vous êtes correctement authentifié
	▶ La cohérence des connexions se fait par vérification des différentes traces d'accès : ✓ Gestion utilisateurs ✓ Proxy Web ✓ Connexion Externes

Annexe 2 : Supervision des fonctions

Le processus de supervision intégré à l'**AccessLog-Evo/Pro** permet de voir si un service est actif ou en phase de synchronisation.



L'état de chaque service est visualisable par un voyant de couleur.



:Le service est démarré et s'exécute normalement.



: Le service est démarré, mais n'a pas pris en compte les dernières modifications de configuration.



: Le service s'est arrêté de manière inattendue.

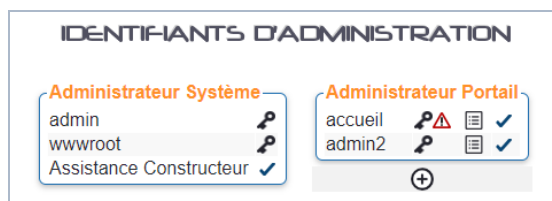
En cas de surcharge processeur ou de remplissage de la Flash disque et du spool de messagerie un voyant d'information clignote. Un email est envoyé à l'adresse configurée dans le menu de configuration générale.

L'alerte peut être acquittée après avoir appuyé sur l'icône  puis sur EFFACER.



Annexe 3 : Gestion des mots de passe des Administrateurs

Deux types d'Administrateurs : Administrateur du portail, ou un ou plusieurs administrateurs délégués



Assistance Constructeur :

Lorsque vous cochez l'option Assistance Constructeur dans le menu Identifiants d'Administration, vous autorisez Le Support de Telmat Industrie à se connecter sur l'Administration de votre équipement en utilisant un mode de connexion sécurisé et cela, sans que vous ayez besoin de communiquer le mot de passe Administrateur – Cette connexion ne peut se faire que si la console d'Administration est accessible (Cloud, ouverture de port ...) et que cette option est validée

La gestion des mots de passe permet de définir :

- La durée de validité.
- Le nombre de fois que le même mot de passe peut être utilisé.
- Le nombre de tentatives de connexion autorisée.
- La temporisation après échec de connexion (pas d'accès à l'administration page blanche)

Modification du mot de passe Admin :

Vous accéder au menu de modification du mot de passe en cliquant sur 
Le mot de passe à saisir est limité à 256 caractères alpha-numériques

Réinitialisation du mot de passe Admin :

En cas d'échec de saisie, le mécanisme de contrôle s'active : affichage d'une barre de défilement d'attente (par défaut 10mn).



A la fin de la temporisation après Echec de la connexion, la mire s'affiche
Pour réinitialiser le compte admin (uniquement) cliquer sur mot de passe oublié

Deux méthodes sont possibles :

- Par l'adresse email de l'administrateur → nécessité de son fonctionnement et d'y avoir accès
- Par le code Cloud (unique pour chaque machine) → nécessite qu'il soit récupéré au préalable

Le mot de passe à saisir est limité à 256 caractères alpha-numériques

Contactez le support par téléphone ou email pour des informations plus détaillées

Annexe 4 : Compléments de configuration et documentation détaillée

La présente documentation d'installation **AccessLog Evo**

<https://www.accesslog.fr/documents/install-accesslog.pdf>

- ▶ La mise en œuvre de certaines fonctionnalités est décrite également dans la documentation détaillée.
- ▶ Vous pouvez également contacter le L'assistance technique par téléphone ou email.

Du lundi au vendredi (sauf jours fériés) de 9h00 à 12h00 et de 14h00 à 17h30 (vendredi 16h30).

Fax.: 03 89 62 13 31
Tel.: 03 67 35 08 30
support@telmatweb.com