Gît@Box

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

Sommaire

Modèles disponibles de Cit@Box

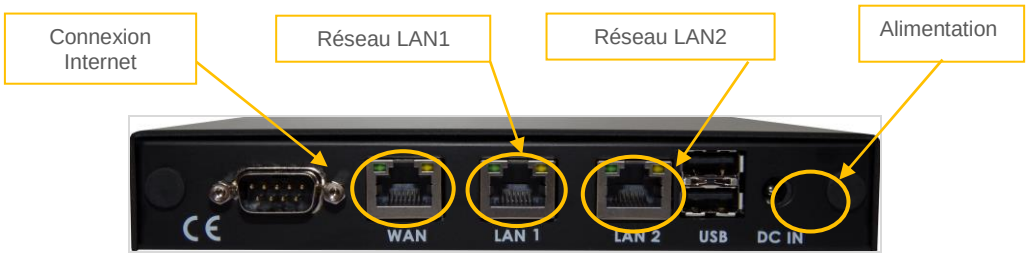
Cit@Box avec WIFI Intégré

Cit@Box

1 Contenu de votre package Cit@Box

Cit@Box	
Bloc Alimentation	
1 Câbles Réseaux RJ45 longueur 2 mètres	
4 Antennes : modèle Wifi intégré	

2 Connexion de la Git@Box au réseau



- Pour une Git@Box Wifi visser les quatre antennes fournies, ne pas utiliser de pince.

- Connecter l'Alimentation, le câble réseau WAN (réseau internet), LAN1 et LAN2 (réseaux locaux).

- Le système démarre automatiquement à la mise sous tension Le temps de démarrage est d'environ 1mn 30 (3 mn pour la Git@Box Wifi) et se termine par 3 bips.

3 Principe de fonctionnement

3.1 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, La Git@box agira en fonction du paramétrage du portail. Quatre modes sont ainsi disponibles sur la machine.

Authentifié Web / Log	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 *Code Parental et des horaires. En mode* ***Authentifié Web*** Les traces sont conservées dans *connexions externes et traces proxy* En mode ***Authentifié Log*** les traces sont conservées dans *connexions externes.*
Libre / URL	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 *connexions externes et traces proxy*
Libre /Log	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 *connexions externes.*

3.2 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 code 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 Base***

4 Accès à l'interface de configuration

L'accès à l'administration se fait à travers un navigateur internet
Le lien d'accès à l'interface d'administration par la connexion **LAN1** est

- **https://192.168.0.254:99**

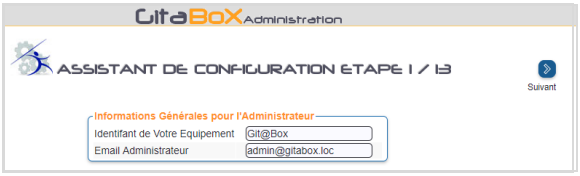
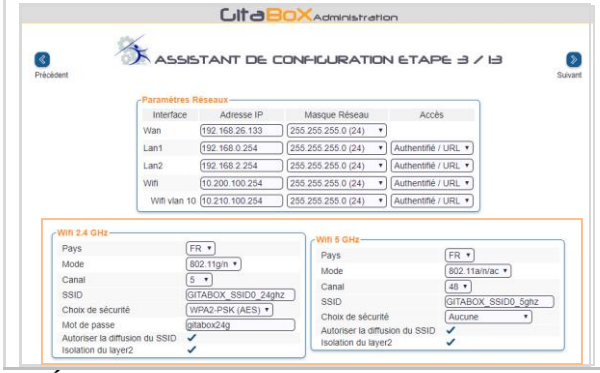
Identifiant à saisir dans la mire d'authentification- **Nous vous recommandons de modifier le mot de passe rapidement**

- Nom d'utilisateur : **admin**
- Mot de passe : **webctrl**
- Pour paramétrer la Git@Box par l'assistant de configuration cliquer sur  . Reportez-vous au chapitre *Assistant de Configuration* pour plus d'information.

- Accéder au menu de configuration via l'onglet correspondant.

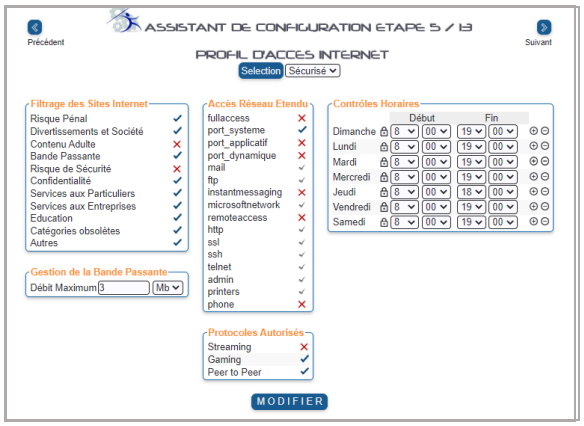
5 Assistant de Configuration Portail

Pour démarrer l'assistant cliquer sur l'icône . Vous ne pouvez pas abandonner l'assistant en cours de configuration vous devez aller au bout, puis cliquer sur redémarrage. Pour passer au tableau suivant cliquer sur pour revenir en arrière

	Quatre choix sont possibles. Cliquer sur le bouton voulu : 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, etc… L'email Administrateur est l'adresse qui recevra les mails d'alerte du système. Cette adresse doit être valide pour un bon fonctionnement de votre équipement. ***Ne pas laisser la configuration usine*** !
	Paramétrage de la passerelle par défaut, DNS primaire et secondaire, privilégier ceux de votre FAI Pour l'émission de messages, la configuration d'une passerelle SMTP valide est requise
	Adresse IP et masque de l'interface WAN (coté internet) et des interfaces LAN Sélection du mode de fonctionnement de l'accès internet. Configuration WIFI* de chaque fréquence. Reportez-vous au chapitre configuration WIFI dans la présente documentation

Configuration du dhcp du coté réseau interne : LAN1 ou LAN2.

Le paramétrage des VLAN se fait dans l'onglet de configuration général (hors assistant)

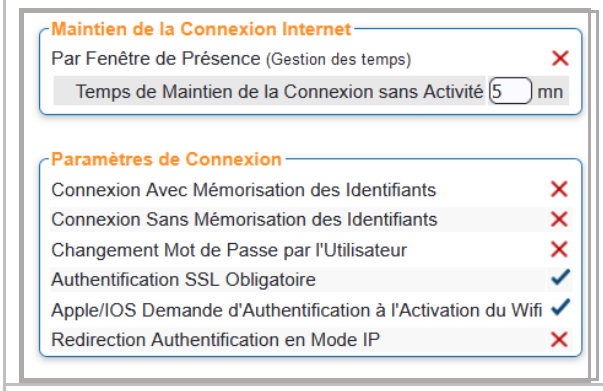


Configuration des deux profils existants : ***Base et Sécurisé.***

- ✓ 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 protocoles en fonction du service utilisé – Le système reconnait 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***

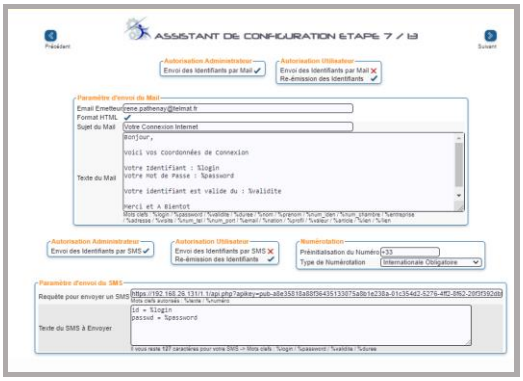
L'administrateur choisit le mode de création des identifiants. Pour le détail des options, reportez-vous au paragraphe de configuration des accès internet.
Le mode maintien de la connexion au portail est valide pour tous les utilisateurs.

- ✓ **Par Fenêtre de Présence** : conseillé pour une gestion des temps de connexion précise.
- ✓ **Sans fenêtre de présence** : paramétrage du temps maintien de la connexion sans activité.
- ✓ **Avec ou Sans Mémorisation des identifiants** : Permet à l'utilisateur de ne pas ressaisir ses identifiants
- ✓ **Changement du mot de passe Utilisateur** : Autorisation donnée à l'utilisateur de modifier son mot de passe à travers le portail (5 caractères mini) et de supprimer son compte via la connexion portail.
- ✓ **Authentification SSL obligatoire**, permet une authentification sécurisée
- ✓ **IOS** : Pour les systèmes Apple, ouverture automatique de la demande d'authentification à la connexion au réseau Wifi.



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 Mémorisation des identifiants : Mémorisation de la connexion adresse MAC et IP avec l'identifiant
- ✓ Authentification SSL obligatoire



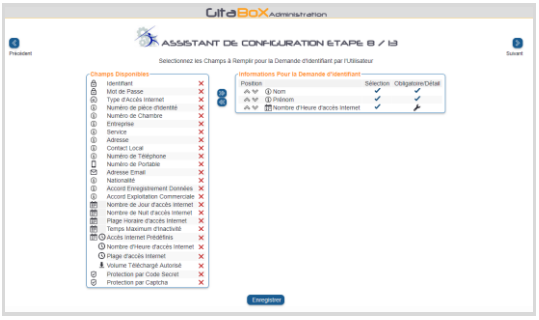
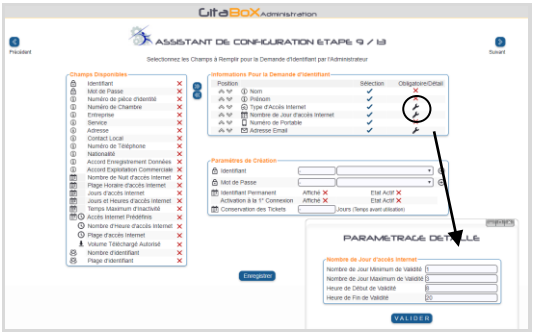
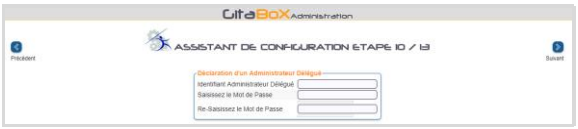
Menu présent si mode attribution par email et/ou SMS validés

<u>Envoi Mail/SMS par l'administrateur :</u>
L'Administrateur/ Administrateur délégué peut envoyer les identifiants

<u>Envoi Mail/SMS par l'utilisateur :</u> L'utilisateur peut envoyer ses identifiants par email ou SMS (ces fonctions doivent être démarrées et paramétrées).

<u>Réémission d'identifiant</u> : permet à l'utilisateur connecté au portail de se réémettre son identifiant : même adresse email ou même numéro de téléphone utilisé lors de la création.

Paramétrage des informations d'émission email et/ou SMS

	Ces informations sont demandées lors d'une demande de création d'un identifiant par le futur utilisateur dans le portail captif. 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. Une protection complémentaire par code (Captcha) est possible
	Ces informations sont demandées lors d'une demande de création d'un identifiant par l'administrateur ou l'administrateur délégué. Les champs cochés et paramétrés sont ceux qui s'affichent lors de la création de l'identifiant. Pour accéder au paramétrage spécifique de certains champs cliquer sur 🔧
	Ce menu permet de créer un administrateur délégué. Il a un accès limité à la gestion des identifiants à travers l'interface d'administration.
	Configuration des restrictions de connexions à l'administration de la machine. Elles peuvent être restreintes 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 modifiée dans la page de configuration du portail.
	Dès que vous cliquez sur le bouton, la machine redémarre pour la prise en compte des modifications. Attendre environ 1mn30 (3 mn Cit@Box Wifi) par la suite au redémarrage.

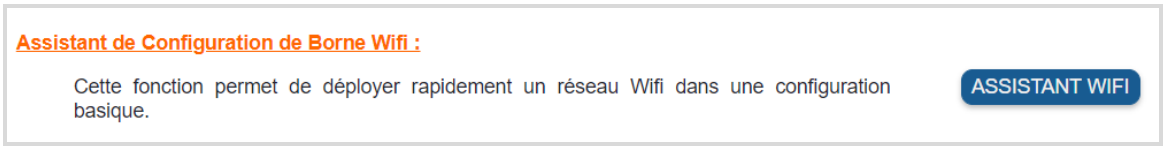
L'assistant de configuration ne crée pas les utilisateurs – Pour cela, se reporter au chapitre sur la création des utilisateurs.

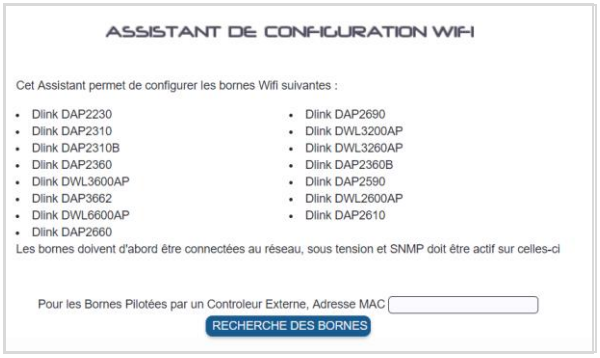
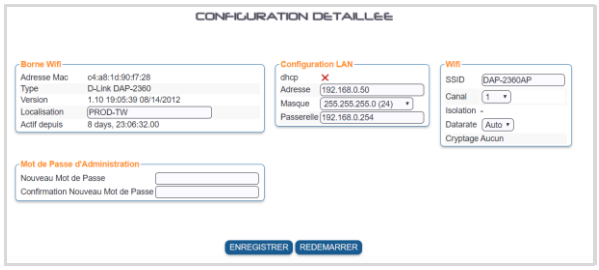
6 Assistant de Configuration WIFI :

A travers l'assistant de configuration, il est possible configurer

- Des Bornes Wifi DLINK (pré-paramétrées usine)
- L'accès direct de bornes sur un contrôleur WIFI externe

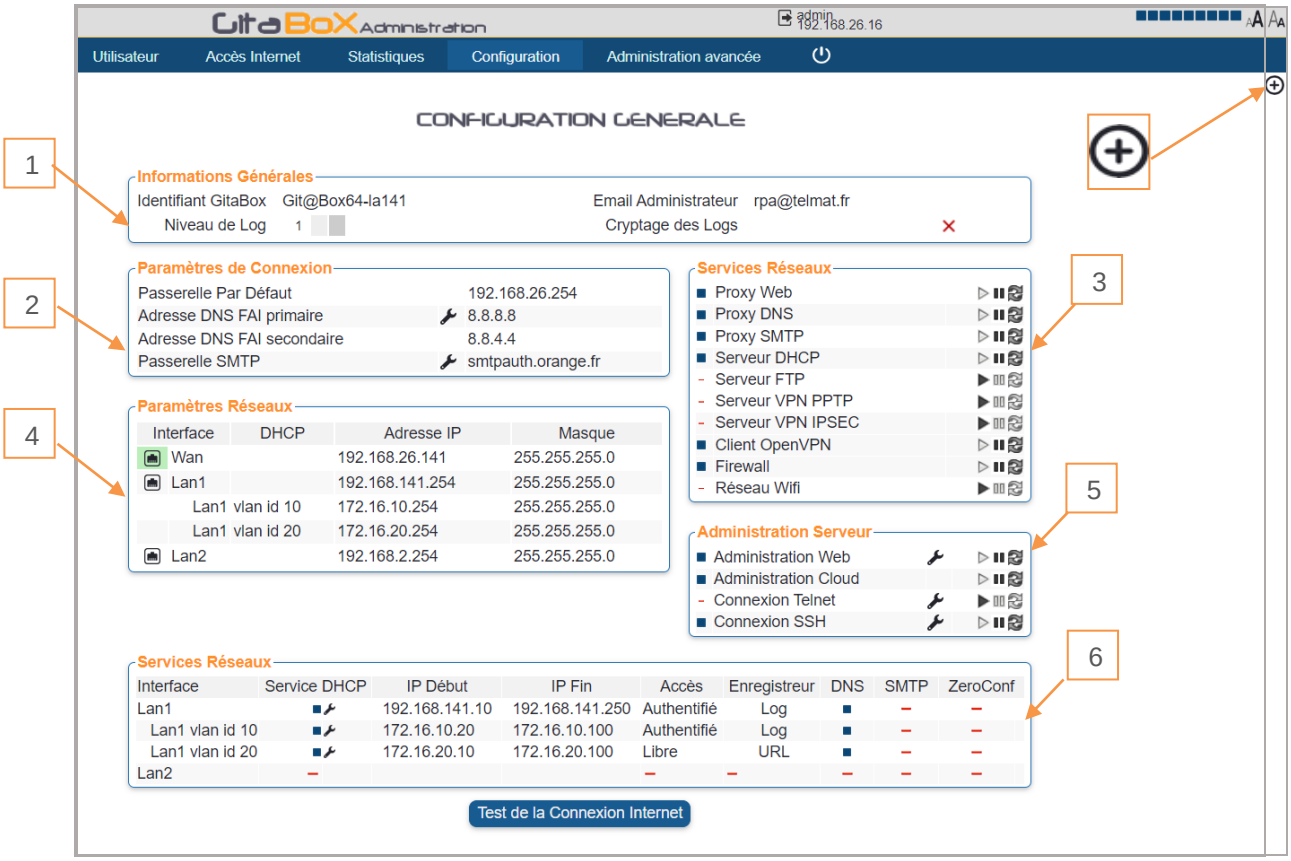
L'assistant vous guide au long de la configuration



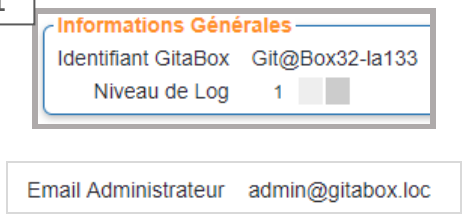
Configuration des bornes DLINK	Configuration bornes sur contrôleur WIFI Externe
	
	

7 Configuration Réseau Générale

- ✓ Menu « *Configuration* / *Générale* » La configuration du Wifi et du service Wifi est uniquement présent sur la modèle Git@Box WIFI.
- ✓ Les interfaces électriquement connectées sont détectées par un affichage coloré



1



Identifiant Git@Box : nom unique attribué à cette machine. Utilisé dans le sujet d'un email envoyé à l'administrateur

Email Administrateur : Adresse mail qui recevra les mails d'alerte du système. Cette adresse doit être valide pour un bon fonctionnement de votre équipement.
Ne pas laisser la configuration usine !

2

Passerelle par Défaut : Adresse IP et interface réseau du routeur connecté à la Git@Box.

Adresses DNS : Adresses IP des Serveurs de Nom (DNS) de votre FAI.
Pour ajouter des noms de machines dans le DNS local, cliquer sur au niveau DNS primaire

Passerelle SMTP : Nom ou adresse IP de la passerelle de messagerie du FAI (configuration obligatoire).
Cliquez sur pour configurer le mode authentifié

Limitation du nombre d'emails emails sur une période:
Cette limite est fixé par poste

3

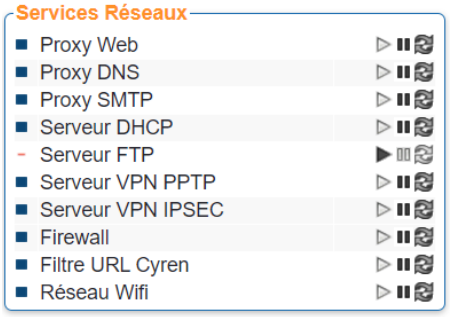
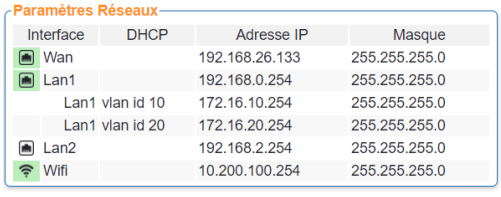


Tableau de pilotage des services.

Ne pas modifier les services en cours d'exécution.

: Démarrage, Arrêt, Rechargement du service local

4



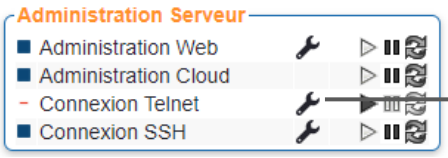
DHCP : Mise en DHCP client de l'interface. **Attention**, l'interface attend une adresse IP distribuée par un système.

Adresses IP et Masque : Adresse IP fixe et masque réseau de l'interface. Configurer les interfaces Wan et Lan.

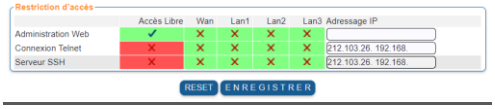
VLAN ID : C'est l'identifiant du VLAN associé à l'interface

WIFI : assistant de configuration cliquer sur

5



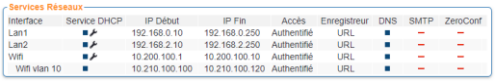
En cliquant sur cette icône vous accédez à la configuration des restrictions d'accès. Le firewall est automatiquement réglé et relancé après ACTIVATION de la configuration.



▷ ⏸ : Démarrage, Arrêt, Rechargement du service local

Administration Cloud : Se reporter au chapitre ***Administration Cloud***

6



Service DHCP : Démarrage du service DHCP sur l'interface cochée. Déclaration de la plage d'adresses IP distribuées – l'association adresse IP adresse MAC est possible .

Portail Captif : activation de la fonction sur cette interface – les modes sont disponibles : Accès Authentifié – Enregistreur de Site Web – Enregistreur de Log

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

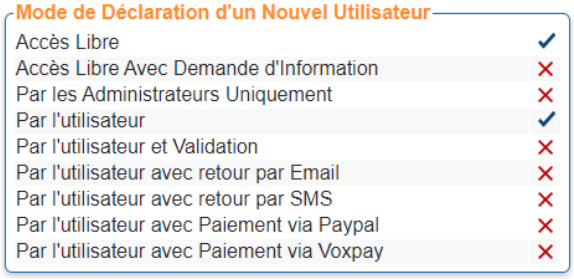
Case SMTP : Autorisation de relayage des requêtes SMTP vers la passerelle smtp du FAI sur cette interface.

8 Configuration des Accès Internet :

8.1 Mode d'attribution des Identifiants :

- Dans les modes avec SMS et email, les champs d'adresse email et/ou numéro de portable sont obligatoires dans le formulaire de demande d'identifiant.
- Il est possible d'utiliser simultanément les modes retour par SMS et par Email.
- Il est possible d'utiliser simultanément le mode d'Accès Libre avec ou sans information et un autre mode.

Menu « *Utilisateur / Configuration des interfaces / Mode d'attribution des identifiants* »



Accès Libre : L'utilisateur accède à Internet en validant la connexion sans authentification.

Accès Libre avec demande d'information : L'utilisateur devra remplir les champs demandés lors de la demande de connexion au portail.

Par les Administrateurs Uniquement : Seuls les administrateurs définis sont autorisés à créer un nouvel utilisateur.

Par l'utilisateur : A la première connexion sur le portail, l'utilisateur doit saisir les informations demandées pour obtenir ses identifiants.

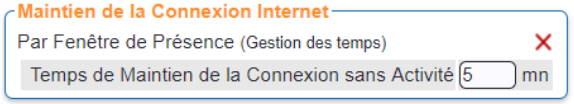
Par l'utilisateur et validation : A la première connexion l'utilisateur doit saisir les informations demandées. La demande est alors en attente de validation par l'Administrateur. Suite à l'acceptation, les identifiants sont affichés sur le navigateur client.

Par l'utilisateur avec retour par Email : A la première connexion, l'utilisateur doit saisir les informations demandées. Le temps d'accès pour l'accès à sa messagerie est paramétrable.

Par l'utilisateur avec retour par SMS : A la première connexion, l'utilisateur doit saisir les informations demandées. Ses identifiants de connexion sont envoyés par SMS. L'administrateur doit souscrire un abonnement auprès d'un fournisseur de SMS.

Par l'Utilisateur avec Paiement via Paypal : Permet l'achat de ticket via l'application de paiement Paypal. Paiement par compte Paypal ou Carte Bancaire (Affichage 2 boutons) – Redirection vers le site Paypal. L'identifiant créé est affiché sur la page du portail – Il doit être conservé par l'utilisateur

Par l'utilisateur avec Paiement via VoxPay/Monético : 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. La configuration Monético se fait à partir de l'environnement Voxpay en cliquant sur ⚙.

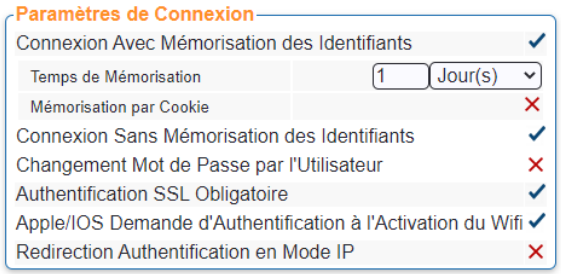


Le choix applicable à tous les utilisateurs en mode authentifié permet de définir le maintien de la connexion

Par la fenêtre de présence : 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)

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 un demande d'identification est demandée suite à la reconnexion.

Sans fenêtre de présence et mémorisation des identifiants: 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. L'utilisateur n'aura plus à s'authentifié pendant toute la durée des identifiants ou s'il change de poste et se connecte avec les mêmes identifiants.



Connexion Avec ou Sans Mémorisation 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 mémorisées par rapport au poste. Ceux-ci seront automatiquement affichés dans le portail à toute nouvelle détection de connexion (avec fenêtre de présence)

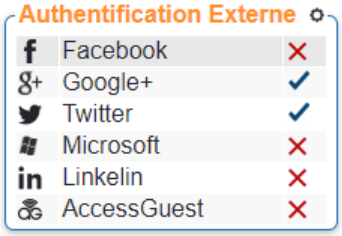
Changement du Mot de passe par l'Utilisateur : Permet suite à sa connexion au portail de modifier son mot de passe.

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

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

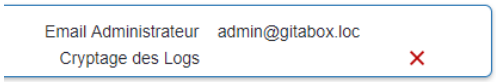
Redirection Authentification IP : L'accès au portail se fait par son adresse IP. Pas de résolution DNS effectuée lors de la connexion



L'utilisateur devra cliquer sur l'icône correspondant au réseau social qu'il désire utiliser avant de saisir l'identifiant du réseau social concerné.
Les réseaux sociaux concernés sont :

- ✓ : utilisation du compte Facebook ® de l'utilisateur
- ✓ : utilisation du compte Twitter ® de l'utilisateur
- ✓ : utilisation du compte Google+ ® de l'utilisateur
- ✓ : utilisation du compte Linkelin ® de l'utilisateur
- ✓ : utilisation du compte MicroSoft ® de l'utilisateur
- ✓ : Configuration **AccessGuest**

Cryptage des logs : Permet de crypter les logs contenant les informations de connexions internet des utilisateurs ; Cette opération se fait à travers une clé générée directement à partir du menu. Cette clé est unique.
Il est impératif de conserver celle-ci dans un endroit sûr. Elle est nécessaire pour la lecture des logs archivés. **En cas de perte de la clé, le déchiffrage est impossible.**



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

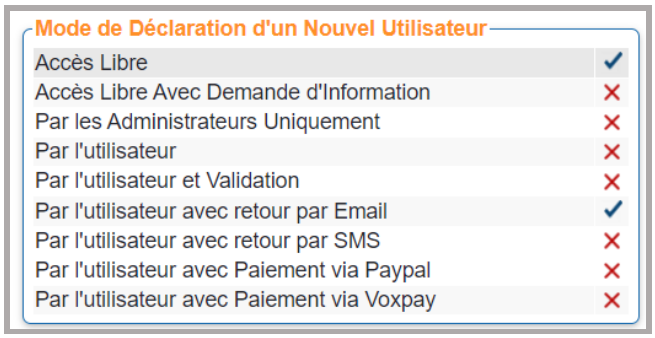
8.2 Mode Accès libre avec ou sans Demande d'Information :

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

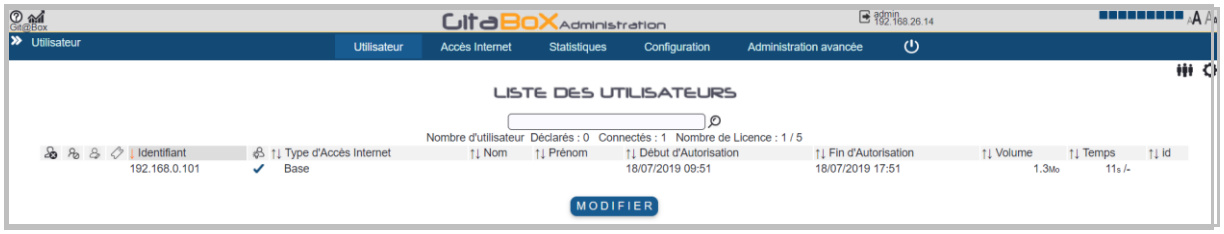
Paramétrage du mode

Le mode de déclaration doit être paramétré en conséquence.



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.



Paramétrage des limites :

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

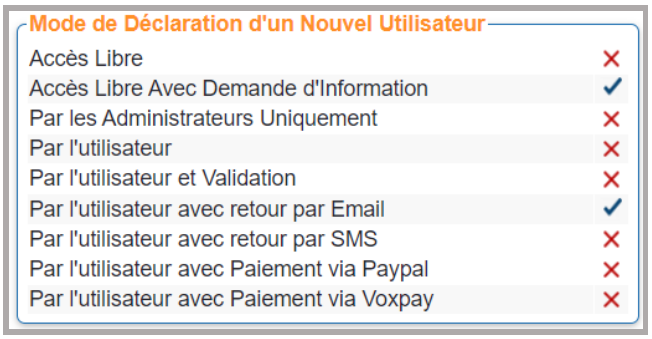
Période de Supervision : Durée de mémorisation du compteur et du temps de connexion par poste ; Remis à zéro après chaque fin de période.

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.

Accès Libre Avec demande d'Information :

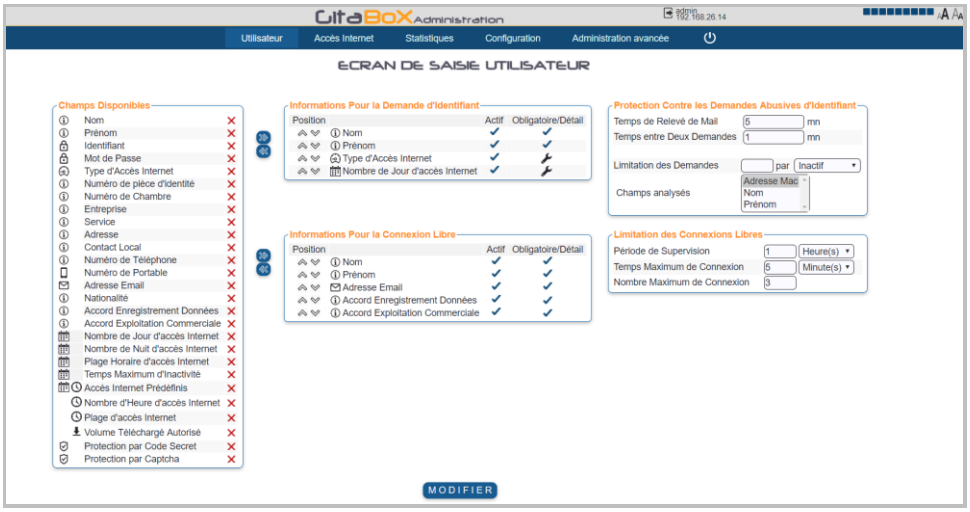
Le mode de déclaration doit être paramétré en conséquence.



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

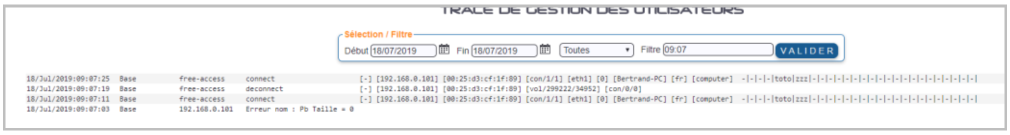
Paramétrage des champs :

Les champs à remplir correspondent à ceux demandés dans la configuration de l'écran de saisie utilisateur.
Ce sont les champs infos ⓘ mail, téléphone paramétrés dans le champs affichés.



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

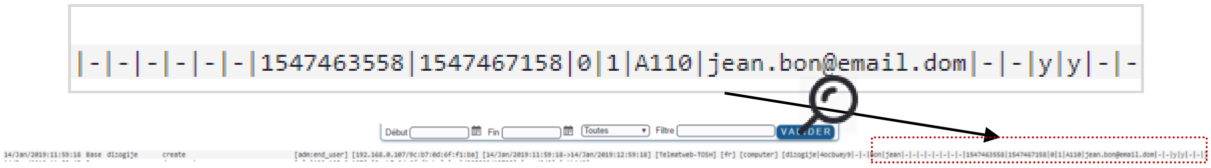
La raison de l'échec est consignée dans les traces de Gestion de Utilisateurs.



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

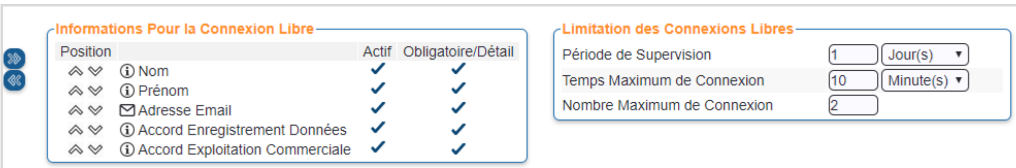
Dans la fenêtre de connexion, l'utilisateur doit cliquer sur le bouton **SE CONNECTER**.
Les connexions en cours sont affichées dans liste d'utilisateur. Seule l'adresse IP du poste est affichée.

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



Paramétrage des limites :

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



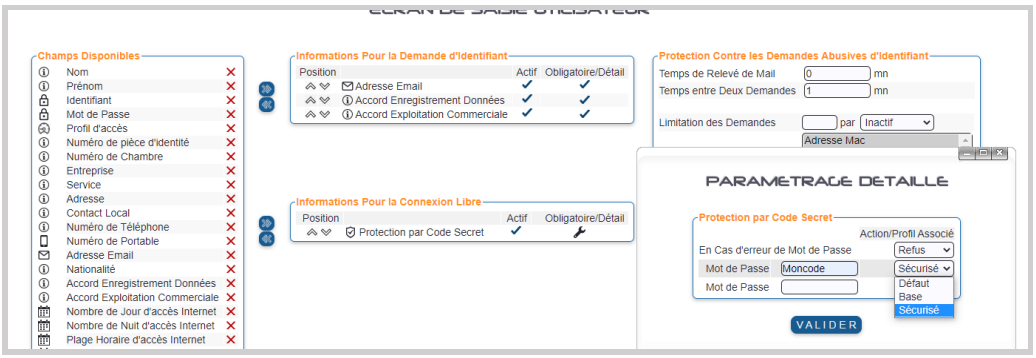
Période de Supervision : Durée de mémorisation du compteur et du temps de connexion par poste ; Remis à zéro après chaque fin de période.

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

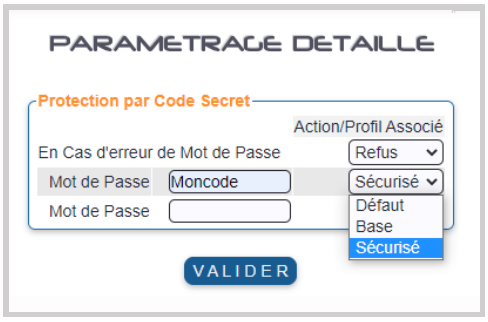
Nombre Maximum de connexions : Nombre maximum de connexions possibles pendant le temps maximum de connexion alloué.

8.2.1 Mode accès libre avec code d'accès

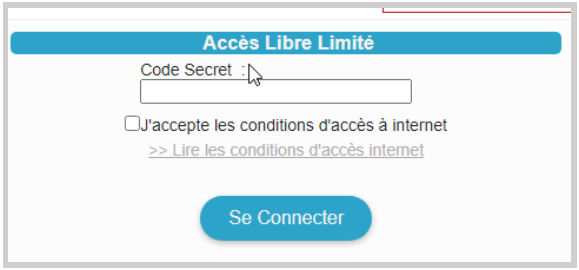
Ce mode de configuration permet de demander un code d'accès lors de la connexion en mode libre
Permet en fonction du code d'affecter un profil à l'utilisateur/poste qui se connecte
C'est une protection qui permet de mettre en place un contrôle sur les connexions sans avoir à créer d'utilisateur.
Il faut être en mode ***Accès libre avec demande d'information*** pour utiliser cette fonction



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

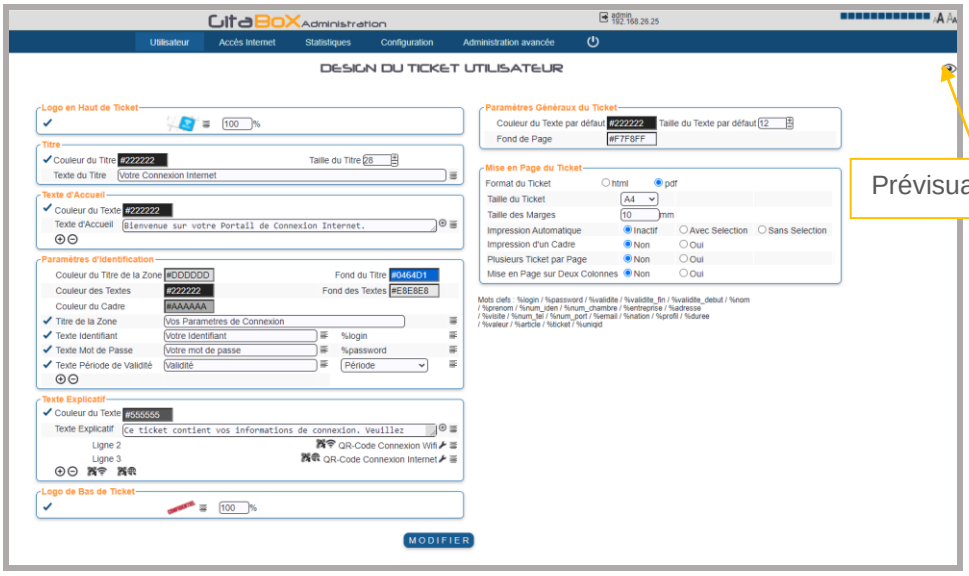


Paramétrer le code et affecter le profil.
Toute erreur de saisie de code par l'utilisateur refuse la connexion



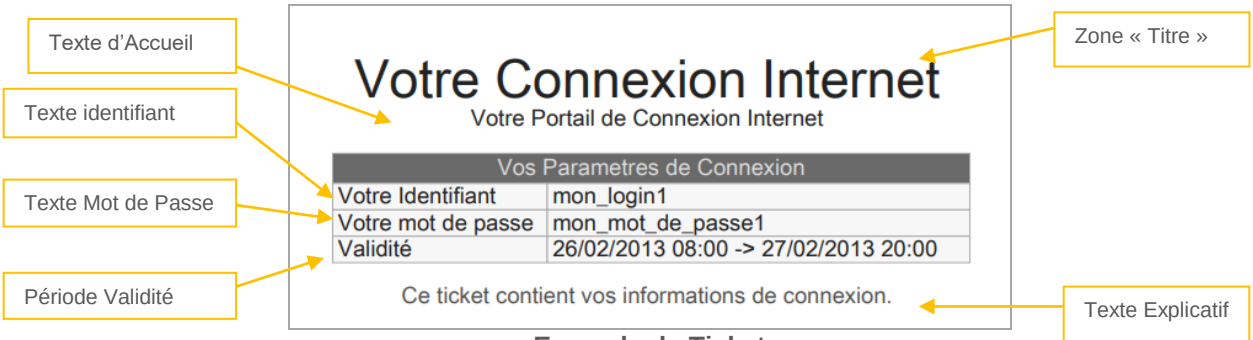
8.3 Personnalisation du Ticket Utilisateur

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



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.



Exemple de Ticket

8.3.1.1 QR-Code Connexion Wifi :

La configuration du contenu du QR Code 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 vide dans le cas de *Pas de Mot de Passe*.

Réseau Caché : Si le réseau est non visible

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.

8.3.1.2 QR-Code Connexion Internet :

La configuration du contenu du QR Code 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.

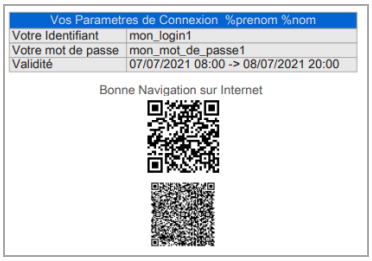
Niveau de Correction et définition pixel : défini la qualité du QRcode

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.

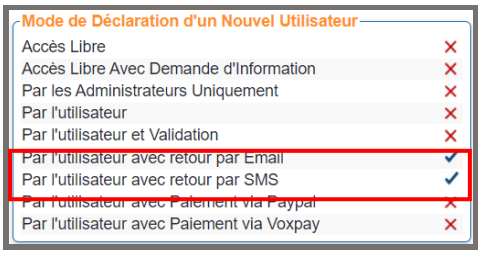
8.3.1.3 Utilisation du QR-Code :

Un scanner de QR-Code doit être utilisé pour les déchiffrer - Tous les lecteurs 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).



8.4 Configuration Emission de Mail / SMS :

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



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.

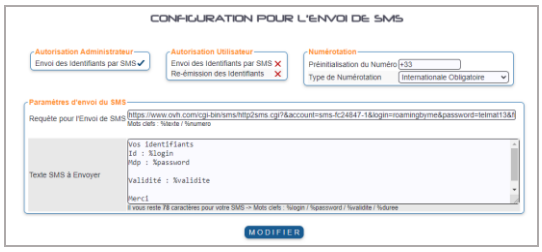
Si aucune adresse email n'est saisie, c'est celle définie dans la configuration générale qui sera utilisée.

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 saisi 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 anti spams



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.

Autorisation Administrateur/Envoi des Identifiants par SMS : Permet l'envoi de l'identifiant par l'administrateur/administrateur délégué- Le numéro de portable doit être obligatoirement présent dans les champs à saisir.

Autorisation Utilisateur/Envoi des identifiants par SMS : 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.

Autorisation Utilisateur/Réémission des Identifiants : Lors de la saisie du même numéro de portable, l'identifiant et mot de passe identiques à la création sont renvoyés.

Numérotation/Pré initialisation du Numéro : Permet de préfixé le numéro de portable qui sera saisi- (ex 00, +33…)

Type de numérotation : 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.

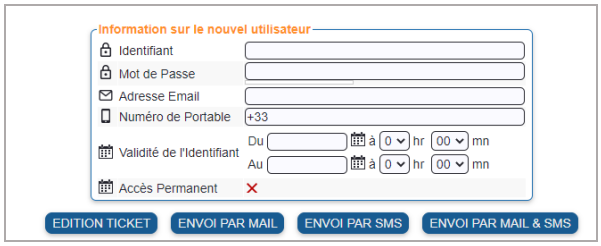
Paramètres d'Envoi du SMS :

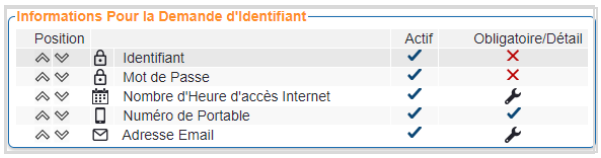
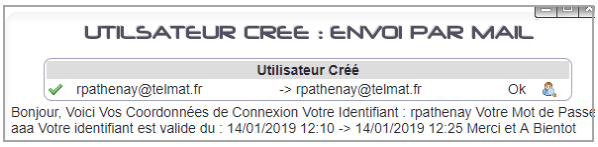
- Requête d'envoi du SMS : C'est l'URL d'émission du SMS vers l'opérateur- C'est ce dernier qui vois donne le lien de connexion à son API. En paramètre du SMS %texte : le libellé du SMS et %numero : le numéro de portable saisi pour la création du ticket

- Texte SMS à Envoyer : Vous rédigez le texte qui sera émis (max 156 caractères) – les mots clés sont %login, %password, %validite, %duree.

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

L'administrateur peut envoyer les identifiants qu'il créée par email ou par SMS. Dans les menus respectifs de configuration email et SMS la cas Envoi de SMS ou de Mail par l'Administrateur doit être cochée. La création par liste contenant une adresse email et/ou numéro de portable permet une création des utilisateurs en mode rafale par création et émission simultanée des identifiants.

<table>
<tr>
<td> 
</td>
<td>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.

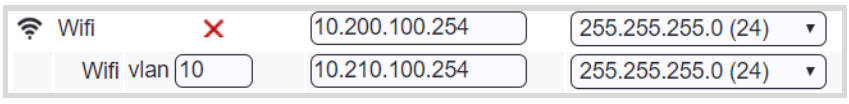
Il est possible de créer des utilisateurs par import de liste- Permet dans ce cas, en une seule opération, d'envoyer des identifiants à de multiples destinataires par email, SMS ou SMS et Email simultanément.</td>
</tr>
<tr>
<td>Configuration Administrateur
 
</td>
<td>Création de l'utilisateur et envoi du mail
 
</td>
</tr>
</table>

9 Configuration WIFI (modèle Git@box Wifi uniquement) :

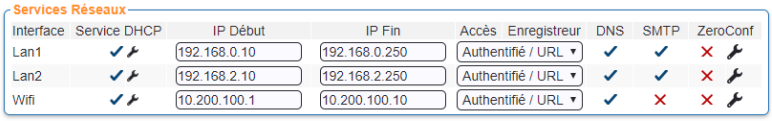
Wifi double bandes de fréquences : 2,4Ghz et 5GHz. La configuration de chaque bande est individuelle.

1) La première étape est la configuration réseau

- Menu « Configuration/Configuration Générale »
  - Paramétrage de l'adresse IP de l'interface



  - Paramétrage du DCHP et mode de fonctionnement du portail de l'interface



2) La seconde étape est le paramétrage du WIFI

- Menu « Configuration/Configuration Générale »
  Pour accéder au paramétrage du WIFI cliquer sur .

Dans ce menu vous configurez les paramètres généraux de fonctionnement du WIFI (Pays, mode, canal ...) le SSID (identifiant du réseau sans fil), le mode de sécurité : WEP, WPA ou aucun et le mot de passe associé pour la clé WEP et WPA.

9.1 Paramétrage Interface WIFI 2,4GHz et 5GHz :

La bande WIFI est à sélectionner dans le menu

Le paramétrage du Pays est important car il défini les restrictions de paramétrage lié au pays (fréquences et canaux). **Il est de la responsabilité de l'installateur de correctement le configurer.**

9.1.1 Paramétrage généraux :

Paramètres	Valeurs/limites	Description
Pays	Choisir dans la liste	Liste des pays disponibles dans la configuration
Mode	802.11g 802.11g/n	Choix du protocole
Canal	1 à 11	Choisir un canal libre sur votre lieu d'installation.
Largeur	20/40 MHz	Largeur canal 20 Mhz pour le 802.11g, Largeur canal 20/40 Mhz pour le 802.11n
Intervalle des beacons	Valeur en ms	Intervalle de temps en ms d'émission des trames
Fragment Limit	-1 non actif	Taille maximale des paquets émis Laisser à -1
RTS Limite	-1 non actif 0...65535	Taille d'un paquet en octets à partir de laquelle l'émetteur demande la "prise de parole" unique
Intervalle DTIM	Valeur en ms	Intervalle d'émission entre deux trames DTIM - Réveille des équipements en mode économies d'énergie
Nb limite connexions	Valeur maxi : 2007	Nombre maximum de machines /ID permis
Activer le WMM	Cocher pour activer	Priorise les flux multimédia (WME)
Activer le SGI	Cocher pour activer	Permet de réduire les intervalles de transmission afin d'augmenter la vitesse de transfert

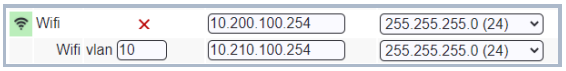
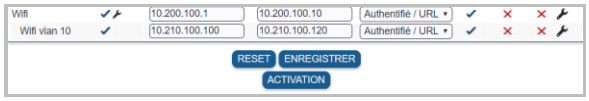
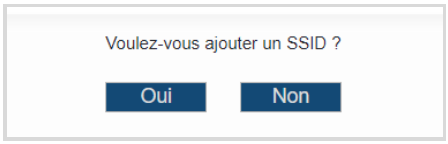
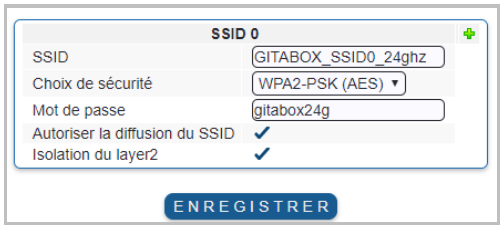
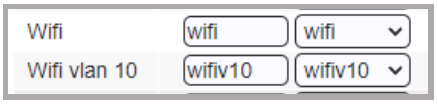
9.1.2 Paramétrage SSID :

Permet de définir le nom du SSID, le choix de la sécurité (mot de passe associé).

Paramètre	Valeurs/limites	Description
SSID	Nom du SSID associé/diffusé	Nom évocateur du SSID.
Choix de Sécurité	Aucune WPA-PSK (TKIP) WPA2-PSK (AES) WPA&WPA2	Mode à choisir parmi la liste
Mot de Passe	Alphanumérique	Clé à saisir dans le champ
Autorisation de la diffusion du SSID	Cocher pour activer	Rend SSID visible sur le réseau WIFI
Isolation du layer L2	Cocher pour activer	Permet d'isoler les postes entre eux.

9.1.3 Ajout d'un SSID

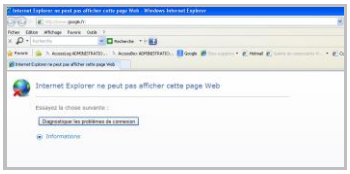
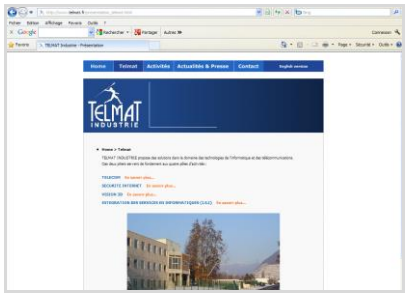
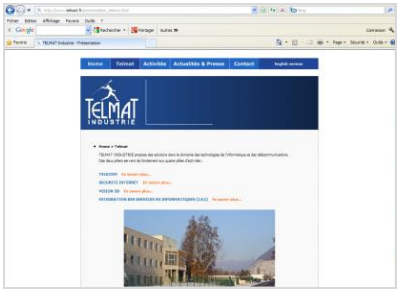
L'ajout de SSID est réalisé en deux étapes :
Dans le menu de configuration générale : Création VLAN, (adresse, dhcp et mode d'accès portail)
Dans le menu dédié au Wifi : Création du SSID avec affection VLAN associé.

Passage en mode modification dans la configuration générale	
Paramétrage du VLAN puis ENREGISTRER	
Paramétrage du DHCP et mode d'accès puis ENREGISTRER et ACTIVATION	
Edition WIFI et ajout du SSID  Paramétrage du SSID associé puis ENREGISTRER	
Pour naviguer entre les différents SSIDs	
Les zones de firewall ainsi que ses règles doivent être définies dans le Firewall.	

10 Accès au Portail

10.1 Mode d'accès au portail

- Menu « Configuration / Générale »

Inactif : Ce n'est pas un mode de fonctionnement – Aucun Accès Internet n'est possible.	
Accès Authentifié (URL ou Log) : Lors d'une tentative d'accès internet avec un navigateur, une page d'authentification s'affiche. L'accès internet ne pourra se faire qu'après authentification. Les conditions et contrôle d'accès internet de l'utilisateur sont définis dans le profil qui lui est associé (Base ou Sécurisé). Les traces de connexions sont consignées dans le menu ***Administration avancée/traces/Proxy Web et*** dans le menu ***Administration avancée /traces /Connexions externes***	
Libre (URL ou Log) : Aucune authentification n'est demandée à l'utilisateur lors de sa connexion à internet. Les contrôles d'accès internet sont définis par le profil associé (Base ou Sécurisé) qui est associé à l'interface réseau dans le menu ***Accès Internet / Accès Sans Authentification***. Les traces de connexions sont consignées dans le menu ***Administration avancée/traces/Proxy Web et*** dans le menu ***Administration avancée /traces /Connexions externes***	
Libre Log : Aucune authentification n'est demandée à l'utilisateur lors de sa connexion à internet. Les contrôles d'accès internet sont définis par le profil associé (Base ou Sécurisé) qui est associé à l'interface réseau dans le menu ***Accès Internet / Accès Sans Authentification***. Les traces de connexions sont consignées dans le menu ***Administration avancée /traces /Connexions externes***	

10.1.1 Mémorisation des Identifiants

La mémorisation des identifiants (identifiant, mot de passe, poste) sont paramétrés dans

- Menu « Utilisateurs/Configuration des Interfaces/Mode d'attribution des identifiants »

A sa première connexion, l'utilisateur devra cliquer sur ***SE CONNECTER et se souvenir de moi***.
Le temps de mémorisation est paramétrable.
Il est possible de ne cocher que l'entrée Connexion Avec Mémorisation – dans ce cas, En cliquant sur le bouton de connexion la mémorisation sera faite (pas d'affichage de *Se Souvenir de moi*)

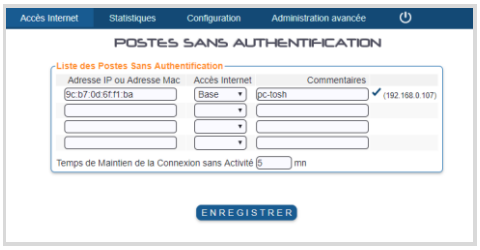
10.2 Accès sans Authentification :

La classe d'adresses MAC se définie par la syntaxe suivante *9c:b7:0d:6f:* (classe mac) ou *9c:b7:0d:6f:4c:89*

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

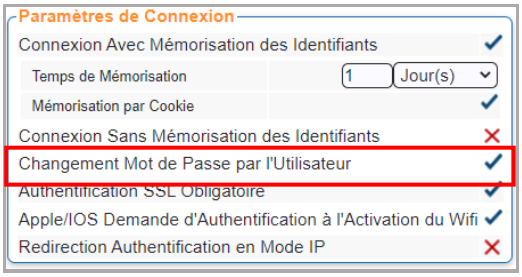
Le nombre maximum d'adresse IP ou Mac pouvant être saisi est de 256. A chaque poste connecté à travers cette méthode, une licence est décomptée du pool total

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 seront plus déconnectés.

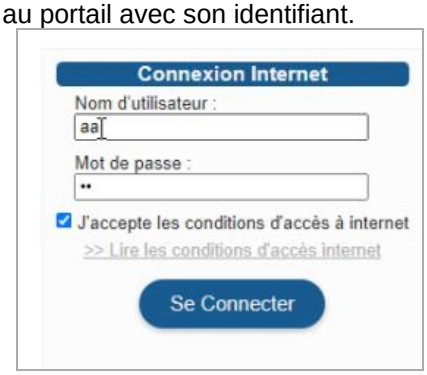


11 Changement de mot de passe utilisateur par l'utilisateur :

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 (Mutlibox).
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*.

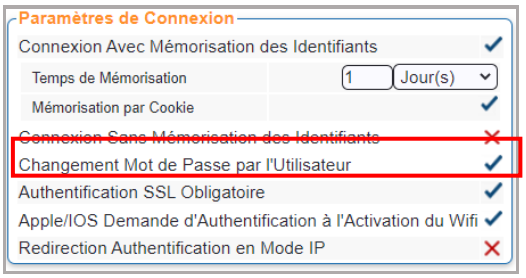
Il doit alors saisir son mot de passe courant et saisir le nouveau mot de passe- **Ce nouveau mot de passe à une longueur minimale de 5 caractères alphanumériques.**

Suite à la saisie, il est redirigé vers le portail

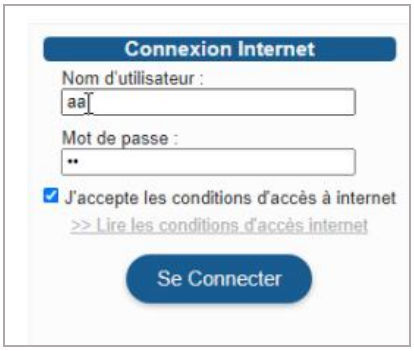
Cette modification n'est possible que si la page du portail est affichée après connexion –Dans le cas sans fenêtre de présence et tant que le poste sera mémorisé (connexion avec mémorisation) la page de connexion ne sera pas visible.

12 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.



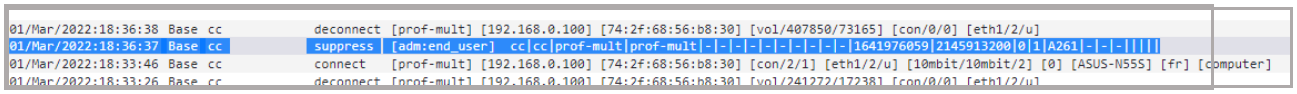
- ✓ L'option *Changement du mot de Passe Utilisateur* doit être cochée.
- ✓ L'utilisateur se connecte au portail avec son identifiant.



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

Il 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

L'utilisateur est instantanément déconnecté et le compte supprimé.



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.

13 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.

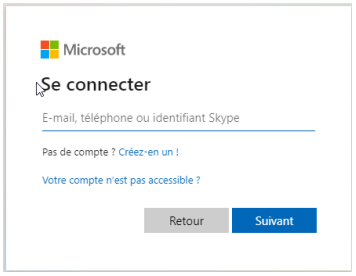
Suite à la sélection des réseaux sociaux désirés, vous pouvez paramétrer les applications pour chaque réseau social ⚙. Par défaut, la Cit@Box est configurée avec les applications de Telmat Industrie. Pour développer des nouvelles applications vous devez utiliser le mode Développeur de chaque réseau. 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.

13.1 Connexion via le Portail

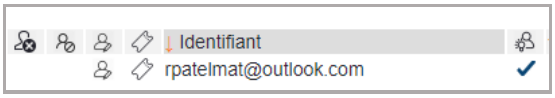
L'utilisateur clique sur l'icône réseau social qu'il désire utiliser

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 l'identifiant de connexion dépend du réseau social utilisé.

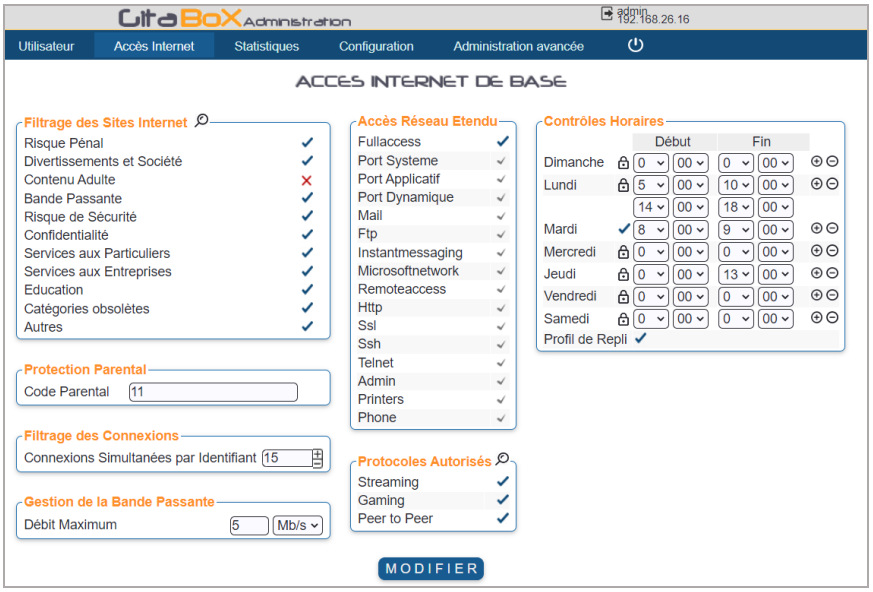


Ce n'est pas le cas de tous les réseaux sociaux.

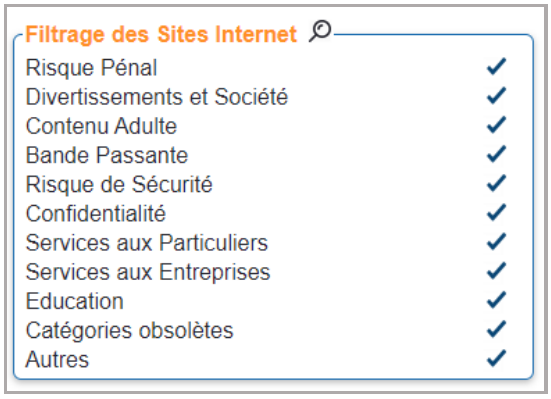
14 Configuration des profils d'accès Internet

Deux profils sont disponibles sur la **Git@Box**. Le profil ***Base*** et le profil ***Sécurisé***:

- ✓ Menu « *Accès Internet /Accès Internet de Base* »
- ✓ Menu « *Accès Internet /Accès Internet de Sécurisé* »



Le *profil de repli* est ***le profil sécurisé***



- ✓ Filtrage des sites internet : Présent si l'option Filtrage Dynamique est souscrite.

Permet de sélectionner les Thèmes 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 Clé / Filtrage*** pour la configuration.

- ✓ Les ports de communication : Accès réseau étendu.
- ✓ Le blocage par analyse de protocole : Protocole autorisé par détection automatique.
- ✓ Gestion de la bande passante : Débit maxi alloué pour chaque utilisateur se connectant via ce profil.
- ✓ Code Parental : Code pour la connexion via ce profil. 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.
- ✓ 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
    - ✗ blocage de l'accès
    - ✓ basculement sur le profil sécurisé

    Plusieurs plages sont configurables pour la même journée ⊕ et ⊖

Le profil sécurisé est mis en œuvre lorsque :

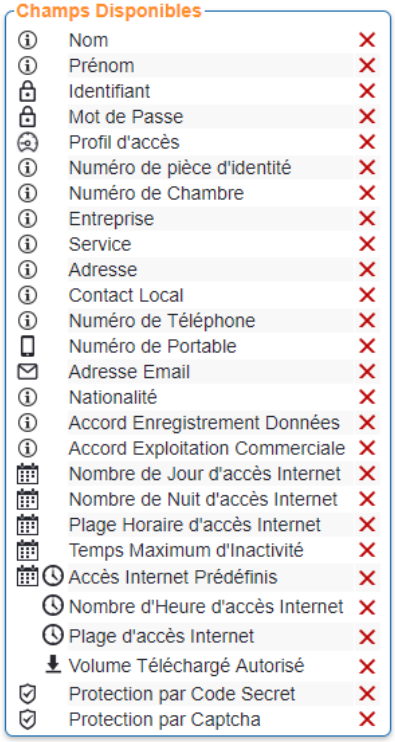
- ✓ l'utilisateur est créé avec ce profil.
- ✓ le code parental (lorsqu'il est demandé) n'est pas correctement saisi lors de l'authentification au portail.
- ✓ l'utilisateur est en dehors des plages horaires autorisées dans le profil de base et que le profil de repli est autorisé (✔).

15 Configuration des champs pour la création d'identifiant

La création d'un identifiant peut nécessiter des informations (nom, prénom …) et une durée ou volume autorisé suite à la connexion.

Pour l'administrateur le
- Menu « *Utilisateur / Ecran de saisie Administrateur* »

Pour l'utilisateur (affiché sur le portail)
- Menu « *Utilisateur / Ecran de saisie Utilisateur* »



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

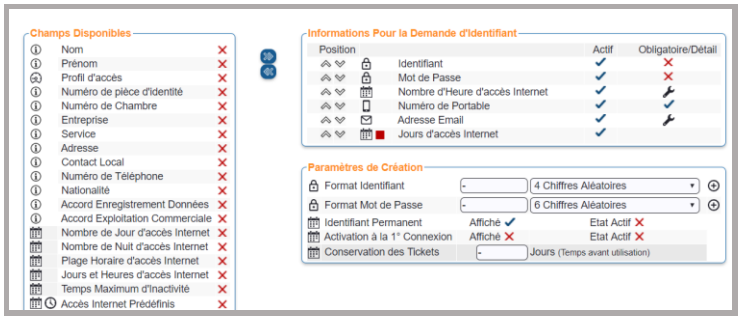
Paramètre de type communication. Permet l'émission des paramètres vers un téléphone portable ou une adresse email

configuration des limites de téléchargement.

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

Les champs sont configurables dans ***l'Ecran de saisie Administrateur et l'Ecran de saisie Utilisateur.***
Certains champs peuvent être présents ou non en fonction de l'écran de saisie

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.



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

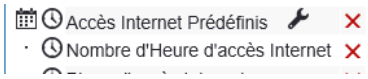
RGDP 2018 : Deux champs spécifiques sont disponibles pour répondre à la RGPD 2018. Ces deux champs sont à valider par l'utilisateur ou l'administrateur au moment de la création de l'identifiant.

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).

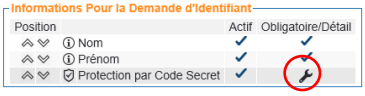
Création utilisateur en fonction du code secret :

- 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



Protection par code secret sélectionné. Configuration en fonction du code

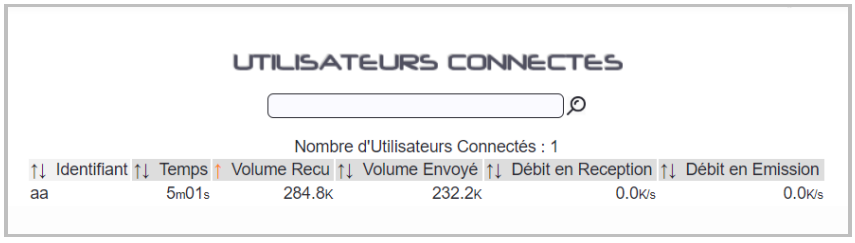


15.1 Visualisation des utilisateurs

Les utilisateurs créés sont affichés dans la liste des utilisateurs actifs.

- Menu « Utilisateur / Utilisateurs Actifs »

Les connexions en temps réel sont visualisées en cliquant sur



16 Configuration et utilisation *AccessGuest*

16.1 Description

L'utilisation d'***AccessGuest*** *par Telmat* permet après installation de l'application sur son smartphone ou tablette fonctionnant sous Android ou IOS, de se connecter de façon automatique aux points d'accès Wifi des établissements visités, en fonction du voyage préparé au préalable.
Les fonctionnalités intégrées dans l'application sont les suivantes :

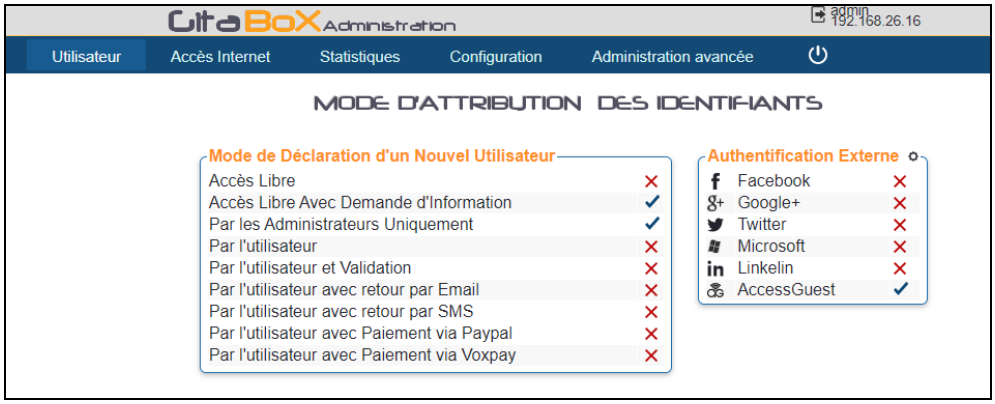
– La connexion automatique aux réseaux Wifi à l'arrivée dans les établissements réservés – La connexion automatique à Internet sans aucune saisie d'information
– La Liste des différentes réservations effectuées – La possibilité de gérer un voyage comportant plusieurs étapes
– La connexion directe avec le GPS de votre smartphone pour rejoindre l'établissement réservé
– Le partage de cette facilité de connexion avec vos amis
– L'invitation de vos amis à utiliser ***AccessGuest*** – Inscription par mail.

Les fonctionnalités intégrées dans la Cit@box sont les suivantes :

– Déclaration de l'hôtel
– Création des Séjours par l'administrateur ou l'utilisateur suivant le mode de création
– Suppression automatique des séjours échus
  Les données séjours sont répliquées automatiquement et régulièrement sur le serveur central ***Accessguest***.

16.2 Configuration Option *AccessGuest*

La fonction ***AccessGuest*** s'active dans *Authentification Externe* en cochant l'option ✔
Pour l'accès au paramétrage de l'hôtel cliquer sur ⚙



La mise en fonction de l'accessguest valide l'enregistrement des séjours sur le serveur centralisé Accessguest d'un utilisateur créé par l'Administrateur ou l'Utilisateur par le portail sur la Cit@box

Le champ obligatoire pour la création d'un séjour est l'adresse email, la même que celle de l'utilisateur ayant créé sont compte Accessguest par l'application.
Si le champ adresse email n'est pas configuré et/ou saisi lors de la création du ticket, il n'y aura pas de création de séjour sur le serveur centralisé et l'utilisateur ne pourra pas utiliser son application Accessguest de son Smartphone/Tablette – Il pourra cependant se connecter en utilisant le ticket généré par l'hôtelier.

16.3 Configuration de l'hôtel :

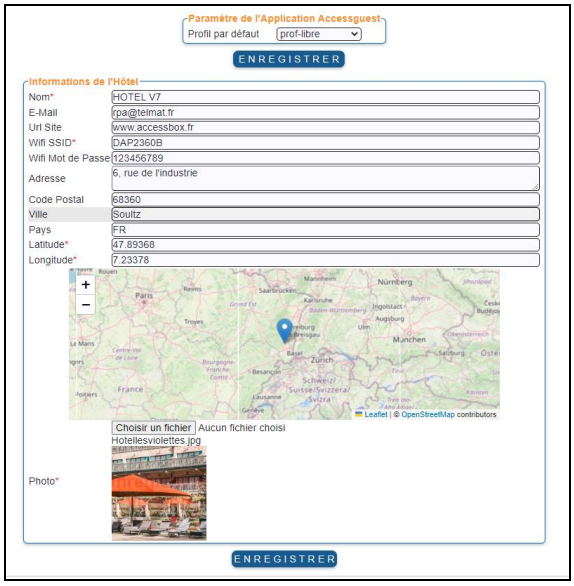
Pour l'accès au paramétrage de l'hôtel cliquer sur ⚙ puis onglet ***AccessGuest***

Les champs contenant le symbole * sont obligatoires

Nom* :	Obligatoire,	Nom du lieu de séjour qui sera affiché dans l'application
E-Mail :	Option,	Adresse email du lieu de séjour
Url Site :	Option,	Url du site Web du lieu de séjour
Wifi SSID * :	Obligatoire,	SSID du Wifi accessible par les clients
Wifi Mot de Passe :	Option,	Clé Wifi si elle est définie sur les bornes
Adresse :	Option,	Adresse du lieu de séjour
Code Postal :	Option,	Code postal du lieu de séjour
Ville :	Option,	Localité du lieu de séjour
Pays :	Option,	Pays du lieu de séjour
Latitude* :	Obligatoire	Coordonée GPS latitude du lieu de séjour
Longitude* :	Obligatoire	Coordonée GPS longitude du lieu de séjour
Photo* :	Obligatoire	Image/Photo du lieu de séjour, format jpg, gif … limiter la taille à moins de 1Mo pour des raisons de performance sur l'application mobile

Pour les coordonnées GPS vous pouvez utiliser la carte en positionnant le point de manière la plus précise

Cliquer sur ENREGISTRER au bas du formulaire valider la saisie des informations

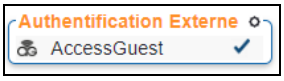


Le champ profil par défaut est réservé aux connexions ***AccessGuest*** dont les séjours sont directement créés sur le serveur ***AccessGuest*** centralisé et non sur la Cit@box (non disponible dans la version TAHX_20240901)

16.4 Configuration et Création de séjours :

La création d'un séjour peut se faire soit par l'Administrateur/Administrateur Délégué soit par l'utilisateur en fonction du mode de Déclaration d'un Nouvel Utilisateur sélectionné.

Sur Git@box, un administrateur à toujours la possibilité de créer un utilisateur/séjour – Pour ce faire, l'Authentification ***AccessGuest*** doit-être validée et l'hôtel configuré.Le menu diffère en fonction du mode choisi.

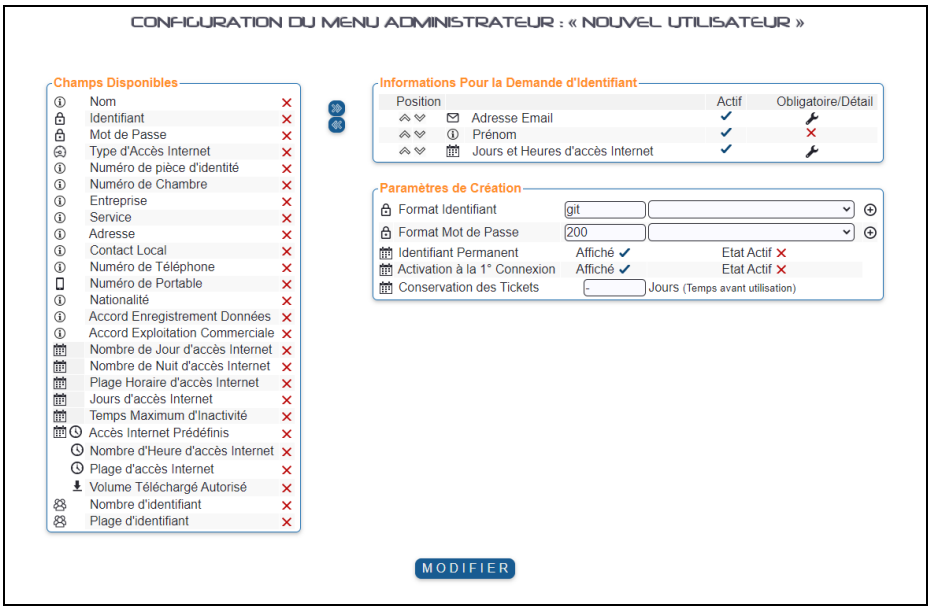


Le compte AccessGuest des utilisateurs est basé sur l'adresse email de l'enregistrement lors de la création du compte. Par convention, tout utilisateur créé avec en paramètre l'adresse email enregistré dans les Utilisateurs Actifs aura un séjours qui sera créé sur le serveur centralisé.

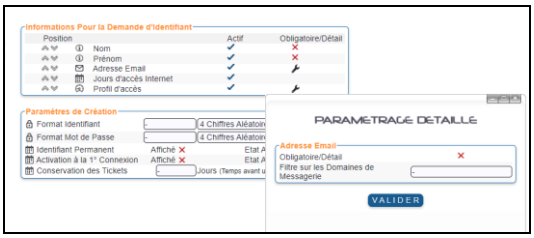
Note : Dans le mode **AccessGuest**, un séjour est créé lors de la création de l'utilisateur avec saisie de l'adresse email.

16.4.1 Création d'un séjour par l'Administrateur/Administrateur délégué

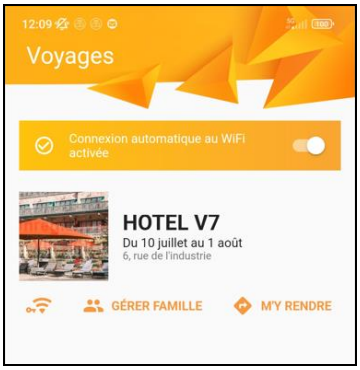
La configuration des champs de saisis de l'administrateur sont à configurer par le menu *Ecran de Saisie Administrateur*.
Pour créer un utilisateur et son séjour, l'adresse email doit être demandée à minima



La configuration des autres champs ; information, durée, profil … se fait comme un utilisateur qui n'est pas **AccessGuest** – Reportez-vous aux chapitres création utilisateur pour la configuration détaillées des champs.
Il est toujours possible de créer un utilisateur non **AccessGuest**, en paramétrant l'adresse email en non obligatoire.Le ticket créé ne sera pas reporté comme séjour sur le serveur centralisé.



Lorsque l'utilisateur/séjour est créé sur la Cit@box il est visible dans l'application smartphone sur le compte de l'utilisateur **AccessGuest**.L'adresse email utilisée pour lacréation du séjour doit être la même que celle du compte **AccessGuest** de l'utilisateur(client).

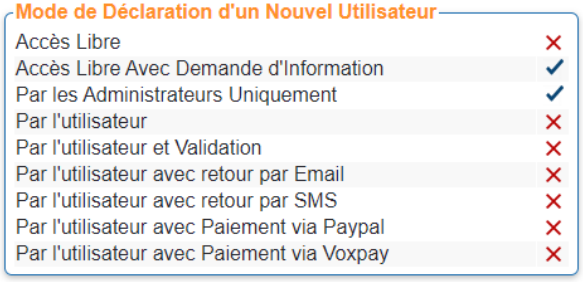


L'utilisateur sera connecté automatiquement au Wifi dès sont arrivé sur place via les coordonnées GPS.

	3254	✓	-		rene.pathenay@telmat.fr	10/07/2024 00:00	01/08/2024 00:00	-	- /-	A689

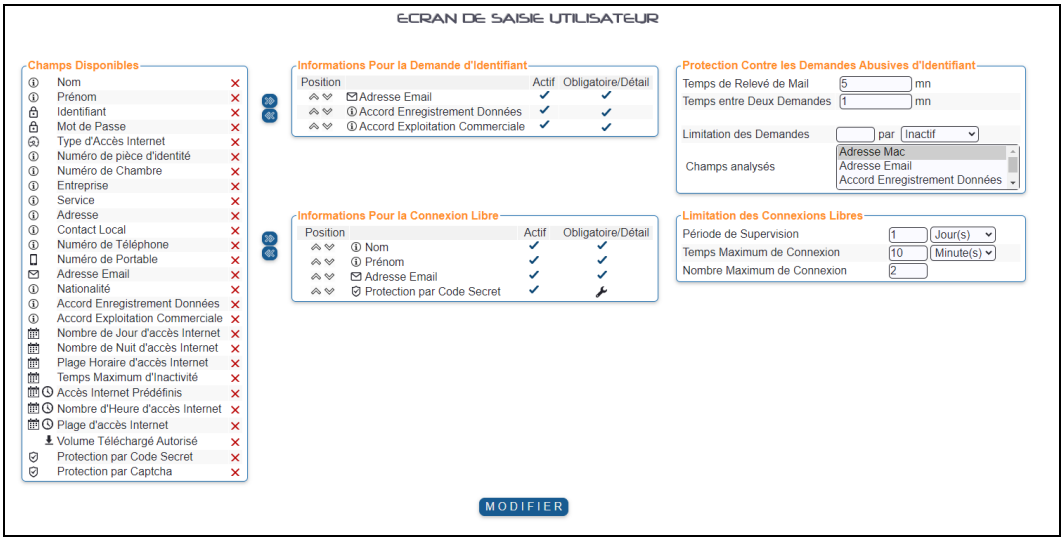
16.4.1.1 Création d'un séjour par L'utilisateur

Différents modes de création d'un nouvel utilsateurs sont disponibles sur la Cit@box.
Certains d'entre eux permettent de créer un séjour suite à la demande de l'utilisateur par le portail captif
Le champ nécessaire pour la création du séjour par l'utilisateur est ***l'adresse email***. Elle doit correspondre à celle du compte **AccessGuest** de l'utilisateur. Pour certains mode le séjour n'est pas créé même si l'adresse email est saisie (Non dans la colonne Création Séjour)



Mode de création	Création séjour
Accès Libre	Non
Accès Libre Avec Demande d'Information	Non
Par les Administrateurs Uniquement	Oui
Par l'utilisateur	Oui
Par l'utilisateur et Validation	Oui
Par l'utilisateur avec retour par Email	Oui
Par l'utilisateur avec retour par SMS	Non
Par l'utilisateur par envoi SMS avec retour par SMS	Non
Par l'utilisateur avec Paiement via Paypal	Oui
Par l'utilisateur avec Paiement via Voxpay	Oui

Les champs sont à configurer dans l'écran de saisie utilisateur



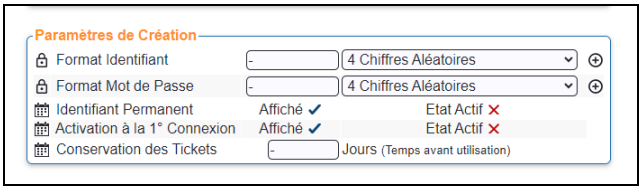
Reportez-vous aux chapitre de création des utilisateurs pour le détail des champs. La durée de validité est configurée via cette même interface.
Suite à cette création, le séjour sera créé sur le serveur **AccessGuest** et visible dans les séjours de l'application smartphone/tablette.

16.4.1.2 Option de création des utilisateurs :

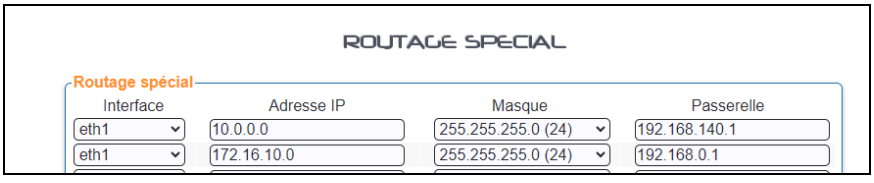
Les option et configuration suivantes ne sont pas compatibles avec l'application AccessGuest version TAHX_20240901

- **Activation à la première connexion**
- **Connexion à partir d'un sous-réseau distant**

Activation à la prémière connexion
Paramétrable dans les paramètres de Création



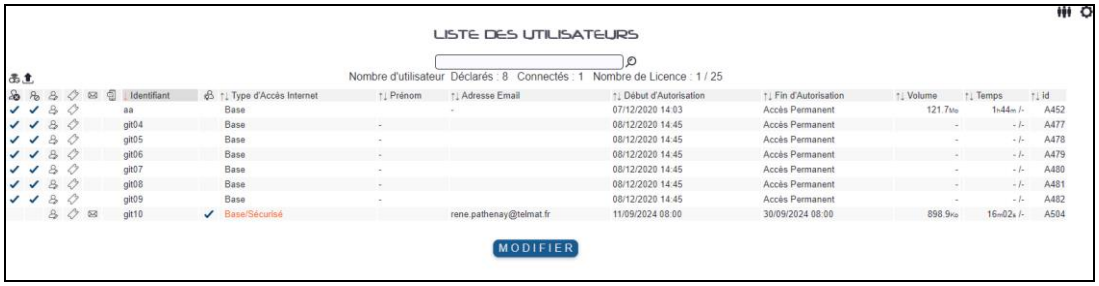
Sous réseau



16.5 Utilisateurs actifs :

Les utilisateurs sont visualisés dans l'onglet *Utilisateurs Actifs*.
Lorsque l'option **AccessGuest** est configurée et fonctionnelle, un bouton de synchronisation manuelle vers le serveur central de séjour est présent . Permet de resynchroniser la liste manuellement

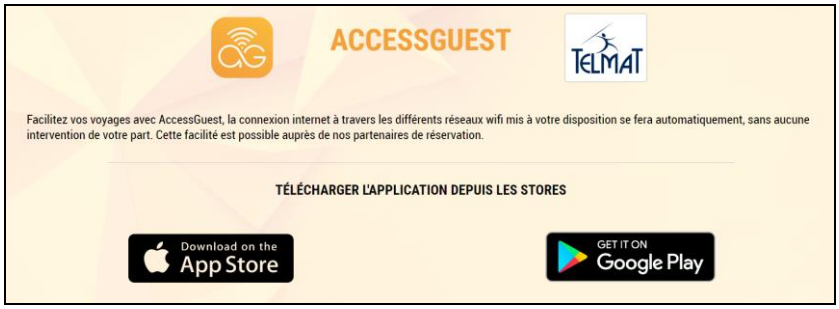
Cette liste est périodiquement synchronisée vers le serveur – Toutes les deux minutes actuellement
Dans le mode **AccessGuest** seules les utilisateurs ayant le champ *adresse email* rempli sont synchronisés sous forme de séjour sur le serveur



16.6 Application AccessGuest :

L'application **AccessGuest** pour smartphone/IPad est disponible dans les stores respectifs pour la version Android et IOS

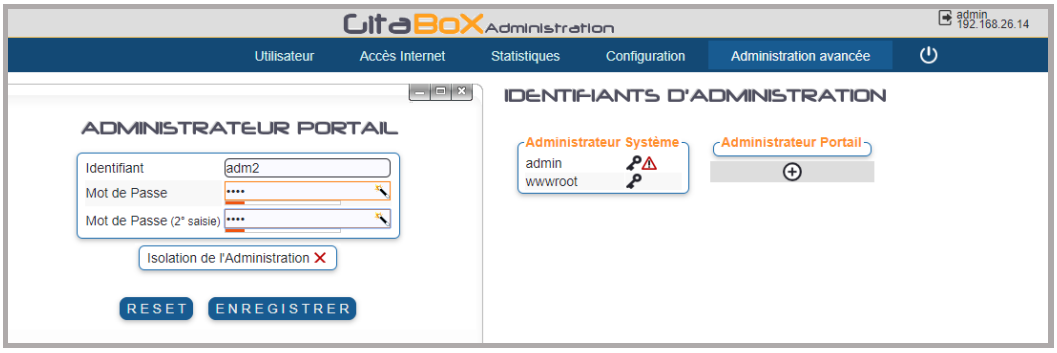
https://accessguest.fr/



Les informations liées à la configuration et utilisation du produit sont disponibles via l'onglet Assistance sur le site Accessguest.fr

17 Création d'Administrateurs Délégués

- Menu « Administration avancée / Administrateur »



Cliquer sur ⊕ de Administrateur Portail pour ajouter le compte

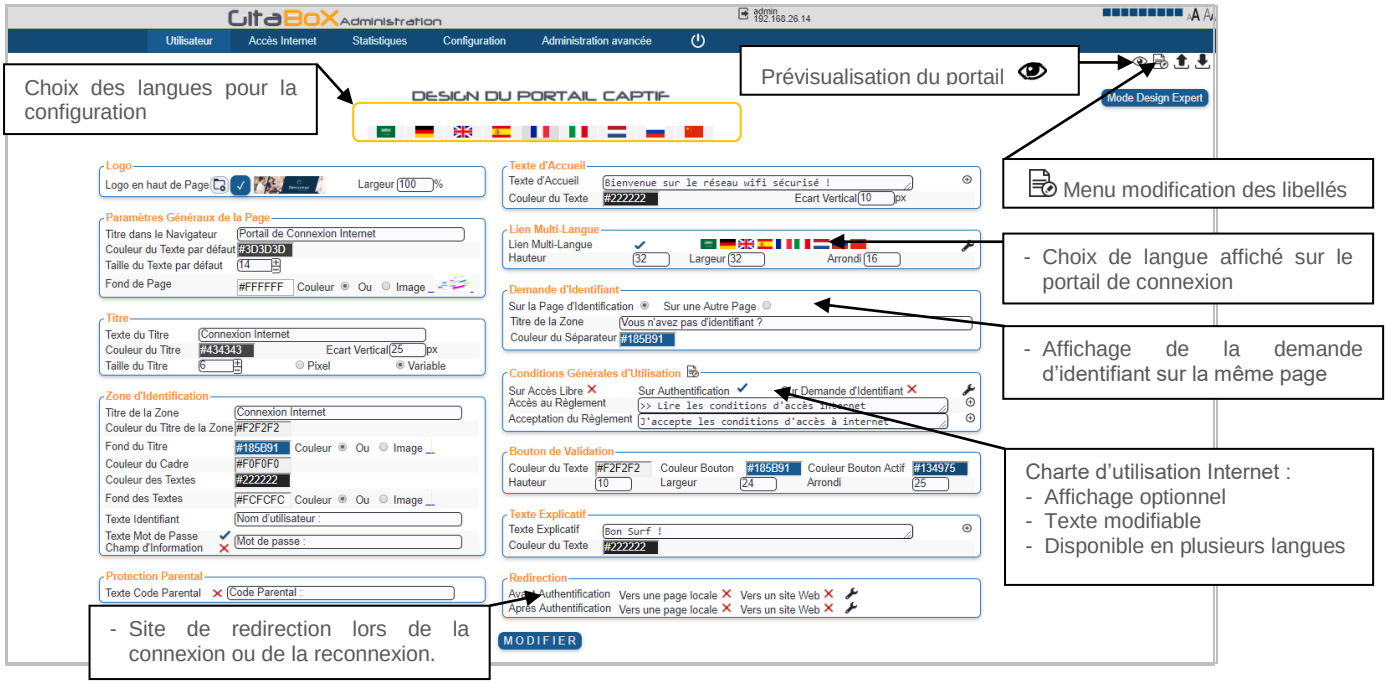
L' *Isolation de l'Administration (case cochée)*, permet, en cas de création de plusieurs administrateurs délégués, d'isoler la création et la connexion des utilisateurs créés par un administrateur délégué particulier. Dans ce cas, chaque administrateur n'a pas de « vue » et d'accès aux données des autres administrateurs. L'administrateur « admin » conserve tous les droits et accès.

18 Personnalisation du Portail Captif

- Menu « Utilisateur / Design du portail Captif »

Certaines options ne sont paramétrables que par ce menu

- Identification de l'utilisateur sur le portail sans mot de passe
- Mise en fonction du code parental
- Affichage sur la même page de la demande de création de l'identifiant et de l'authentification



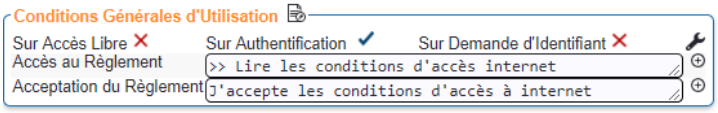
18.1 Conditions Générales d'Utilisation :

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.



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

18.2 Modification des libellés :

Cette fonction n'est disponible que dans le Design en mode Assistant. Pour y accéder cliquer sur l'icône (en haut à droite dans le menu 👁 ⬆ ⬇). Pour un champ identique, la modification du libellé doit être réalisé dans chaque langue.

Certains libellés ont une portée immédiate, pour d'autres, il faut cliquer sur Enregistrer dans le menu "Mode d'attribution des identifiants" ou "Ecran de saisie Utilisateur".

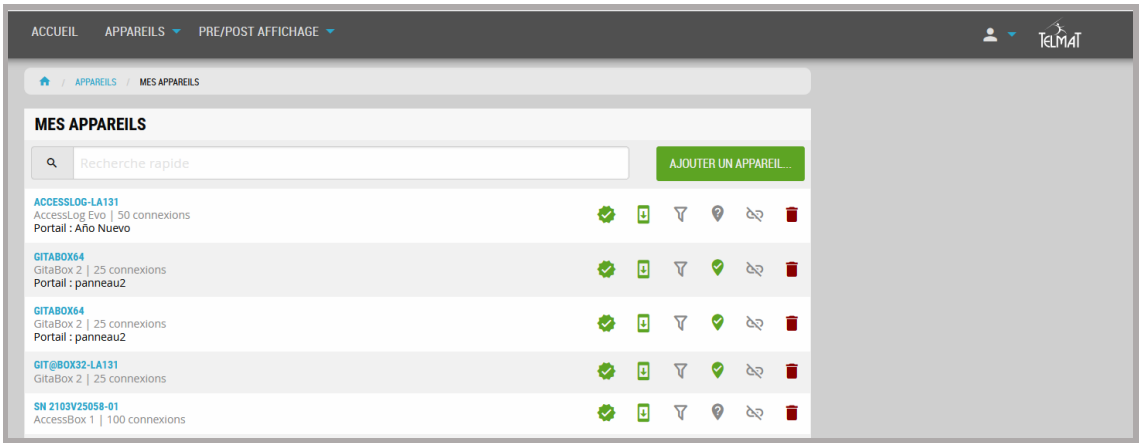
19 Administration par CLOUD ADMIN:

CLOUD ADMIN de Telmat vous permet d'administrer à distance vos machines individuellement ou par groupe, de configurer le portail de présentation avant authentification d'un utilisateur sur le Portail Captif, de visualiser d'état des abonnements et leurs localisations géographiques.

- Cette fonctionnalité n'est disponible que pour les machines ayant une Release Système minimum N° TAH_20211001
- Le CLOUD ADMIN vous permet d'associer plusieurs machines à un compte.
- D'accéder à vos machines à distance.
- De configurer une page d'accueil du portail en utilisant des blocs de fonction (Calendrier, logos, flux RSS, Fichiers, Vidéos...)
- De vérifier l'état des abonnements de vos machines.

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. Création des groupes éventuellement



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

https://www.telmatweb.com/doc/data/documents/administration-centralisee.pdf

20 Réseaux privés virtuels (V.P.N.)

20.1 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

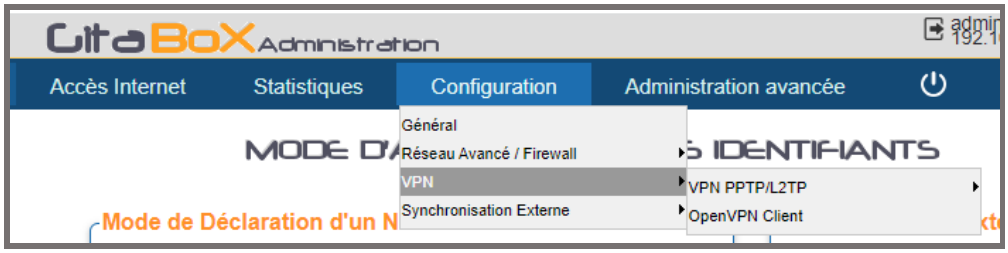
Toutes ces conditions imposent la mise en œuvre d'un éventail de technologies de chiffrement, fondées sur des clés et des algorithmes de codage.

De base, la Git@box 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 Git@box.
- 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 VPN pour réseau distant ou itinérant OpenVpn. La Git@box ne dispose que du client permettant de réaliser une interconnexion LanToLan.

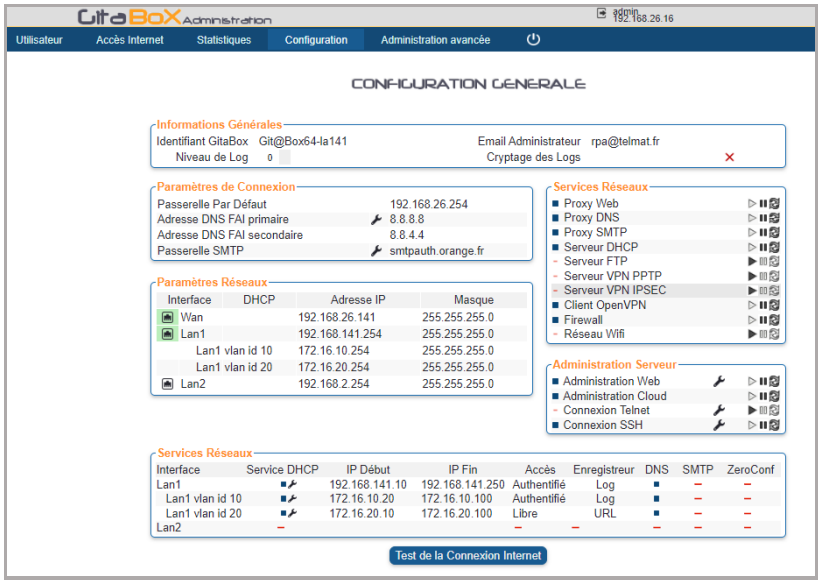
20.2 Accès au menu de configuration

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



20.3 VPN pour poste de travail distant (PPTP)

20.3.1 Démarrage du service :



Démarrer le service en cliquant sur ▶

Pour arrêter le service cliquez sur ⏸, pour le redémarrer/recharger cliquez sur 🔄

20.3.2 Configuration du serveur VPN PPTP

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

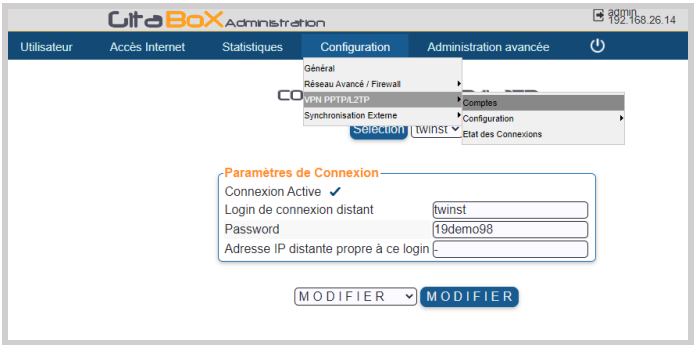
- Création d'un utilisateur
- Configuration des adresses distribuées suite à la connexion.

20.3.2.1 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

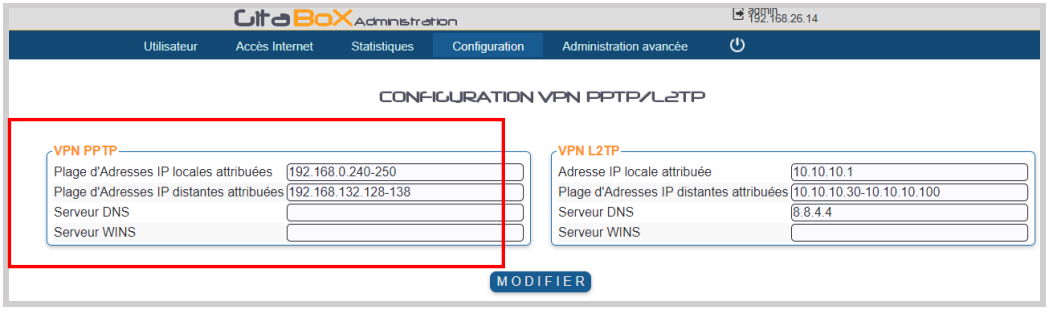
Adresse IP distante propre à ce login : le paramétrage de ce champ en spécifiant une adresse IP force le serveur à distribuer cette adresse IP au client suite à la réussite de la connexion. C'est cette adresse IP qui circulera sur votre réseau interne. Il faut alors paramétrer les équipements internes 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).

20.3.2.2 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



20.3.2.3 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.

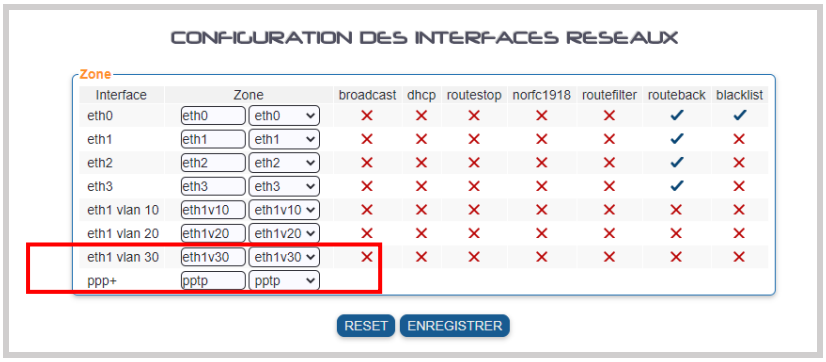
Pour arrêter le service il faut cliquer sur , pour le démarrer sur et le relancer sur .

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.

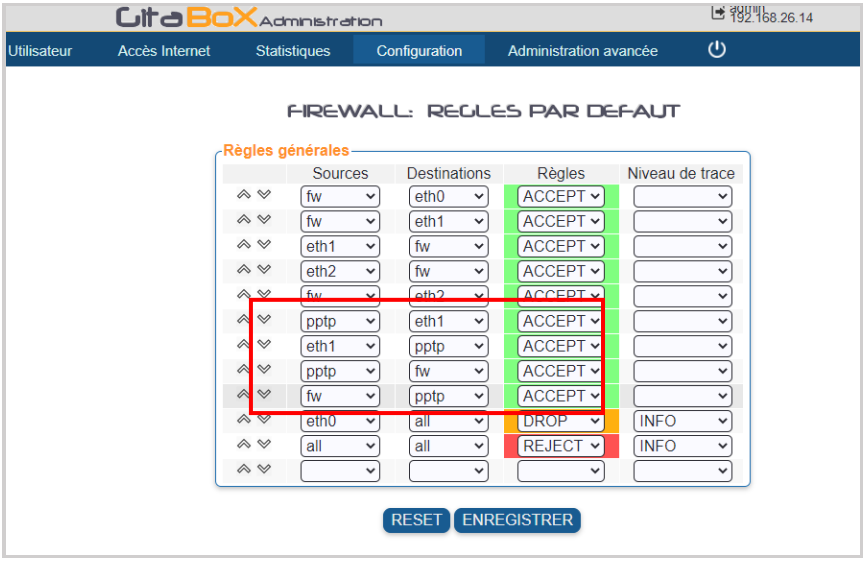
Après le démarrage du service, il faut affecter un nom de Zone à la nouvelle entrée qui s'est rajoutée dans l'onglet des Zones.

20.3.2.4 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 ppp+, Le paramétrage consiste à affecter une zone de firewall à cette interface. (*Firewall Permanent / Zone*)



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

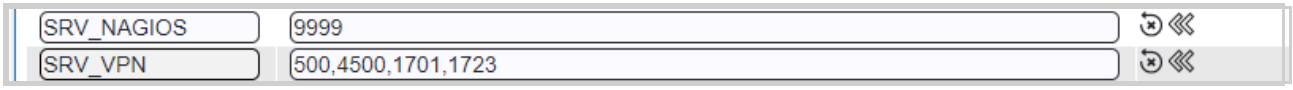


La configuration du firewall permet de créer les autorisations entre cette nouvelle Zone et celles existantes.

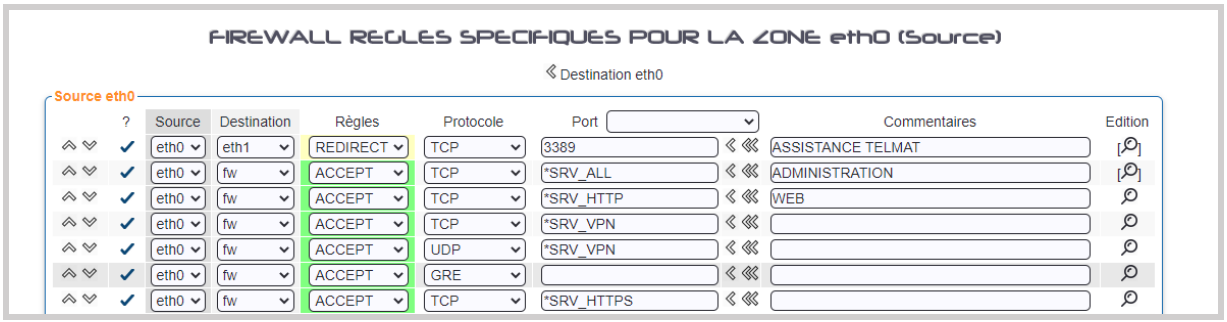
En générale quatre règles doivent être rajoutées pour une connexion PPTP et le réseau local. Cependant, si vous désirez autoriser une connexion PPTP à aller vers d'autres Zones, il faudra créer autant de règles bidirectionnelles.

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

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.



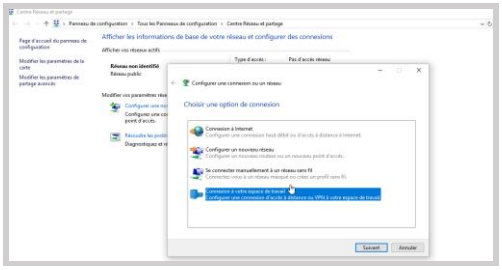
Ensuite vous créez la Règle de firewall intégrant le **TCP/1723** et le protocole VPN PPTP qui est le **GRE**



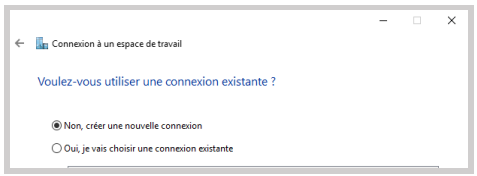
20.3.3 Configuration Client PPTP :

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

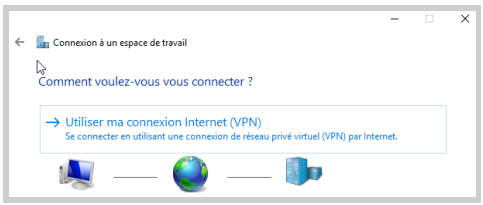
Exemple de configuration sous Windows 10



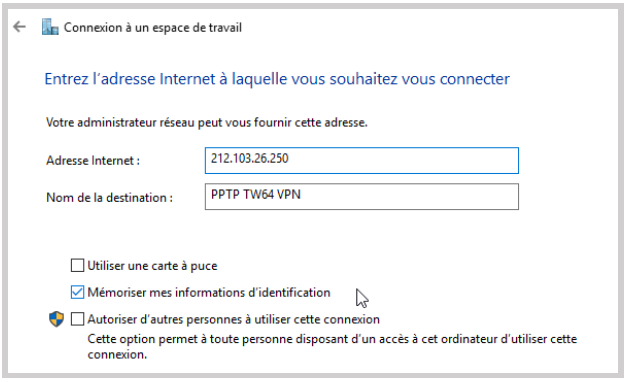
Vous devez créer une connexion *réseau privé via internet* à partir de *l'assistant de connexion réseau*
Vous suivez les instructions en cliquant sur *suivant*



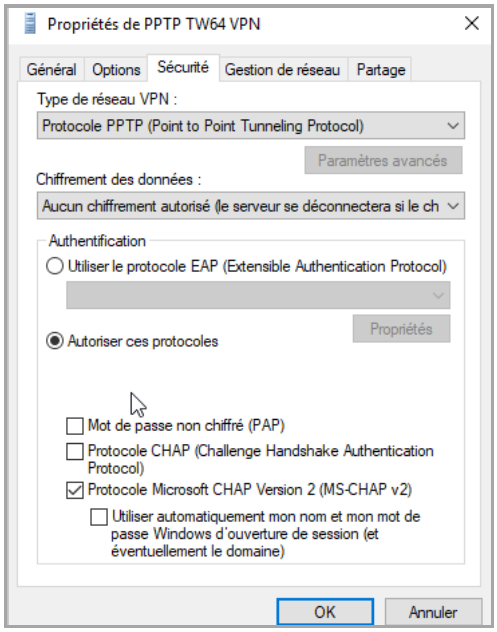
Etape suivante



Etape suivante



Ouvrir les propriétés liées au tunnel créé



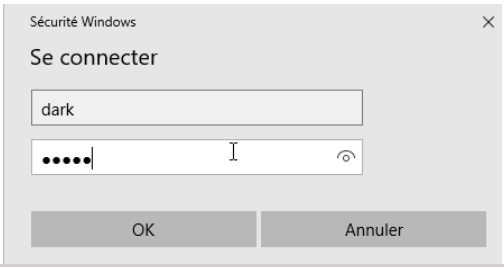
* Protocole PPTP

* Aucun Chiffrement

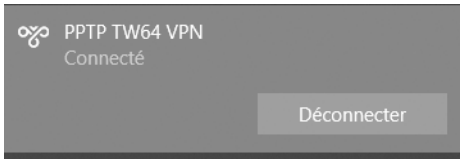
* MSchap V2

L'adresse de destination correspondant à l'IP publique de votre **Cit@box,** 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 avec configuré dans le serveur PPTP de la **Cit@box.**

Au lancement de la connexion le Login/Mot de passe sera demandé

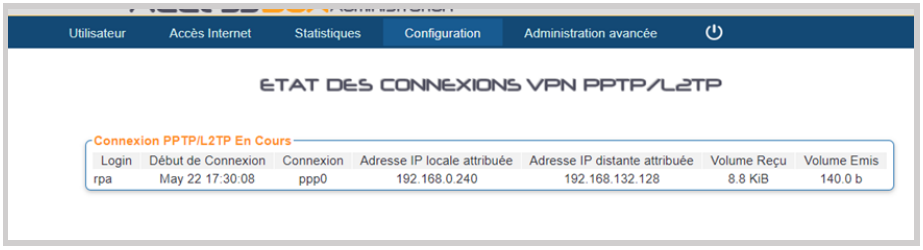


La connexion réalisée

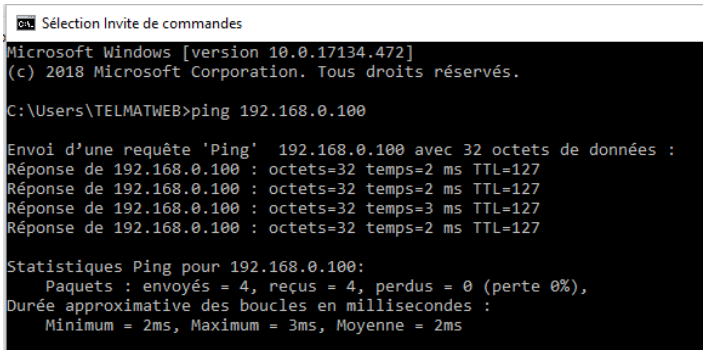


20.3.4 Connexion en cours:

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



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.



20.3.5 Prise en compte des modifications :

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

20.4 VPN L2TP / IPSEC :

La fonctionnalité VPN PPTP/L2TP n'est disponible que sur système Cit@box 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)

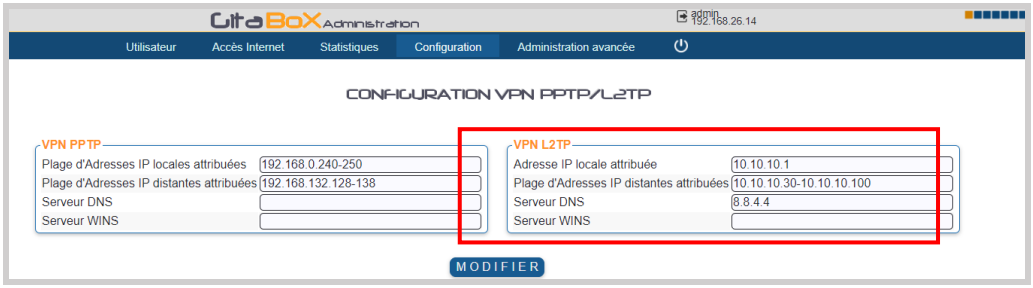
20.4.1 Configuration du service et création du compte PPTP/L2TP :

20.4.1.1 Configuration du Service :

La configuration du Service se fait par le menu

- Configuration/ VPN PPTP/L2TP/Configuration

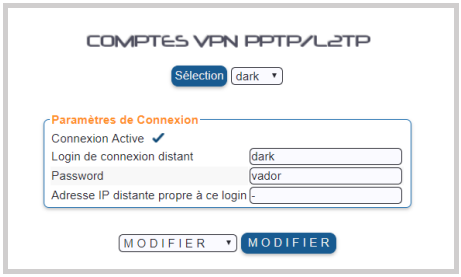
- Permet la configuration des adresses IP qui seront utilisées pas le service lors de la connexion du client.
- Adresse IP locale attribuée : C'est l'adresse utilisée par le service s'exécutant sur la machine. Cette adresse d'écoute est unique
- Plage d'Adresses IP distantes attribuées : Pool d'adresses 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



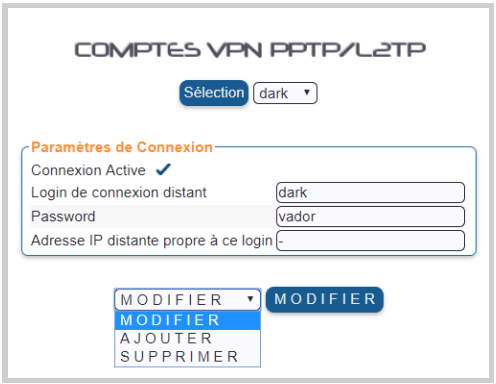
20.4.1.2 Création du compte:

La création du compte se fait par le menu

- Configuration générale/VPN PPTP/L2TP/compte



- 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



20.4.1.3 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.

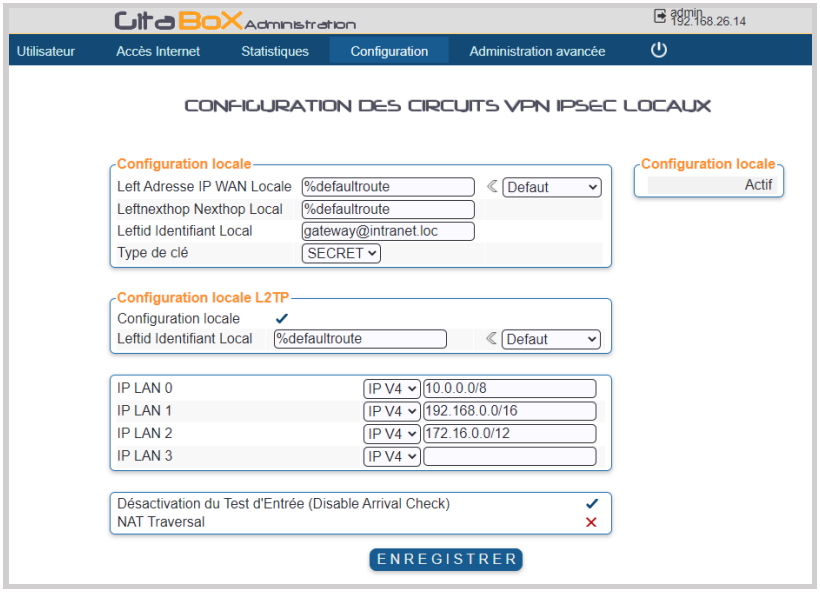
20.4.2 Configuration du service IPSEC pour L2TP :

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.

20.4.2.1 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 : Défini 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 se 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 : Laisser activer, c'est un contrôle sur les adresses IP sources qui doivent êtres 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

20.4.2.2 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.

20.4.2.3 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.

20.4.2.4 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.

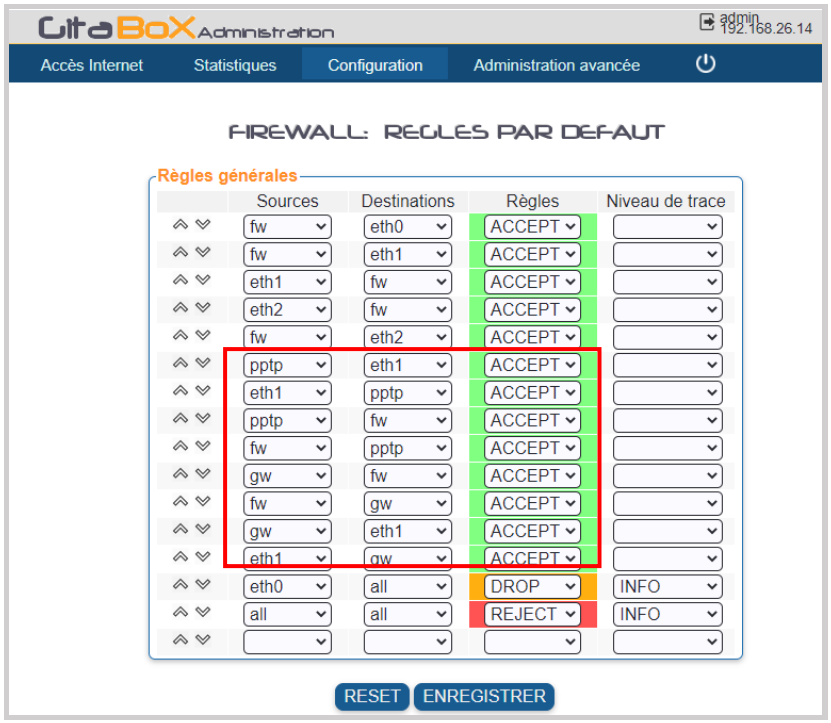
Service	Protocoles	Ports
VPN IPSEC	UDP	500,4500
VPN PPTP	TCP	1723
VPN PPTP	GRE	
VPN PPTP/L2TP	UDP	1701
VPN OpenVPN	UDP/TCP	1194 (peut être modifié)

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 :

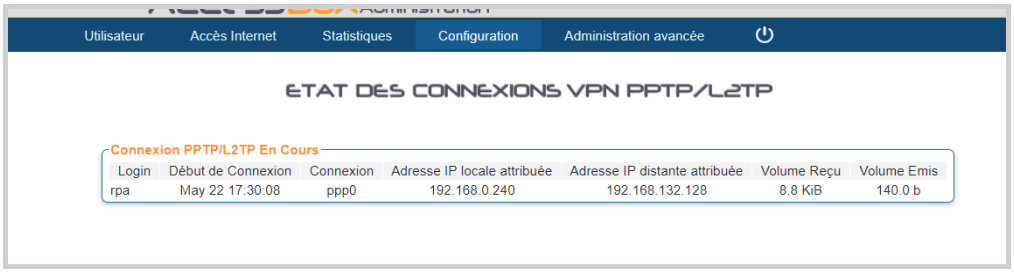


Ces règles doivent permettre le dialogue avec le réseau local (eth1 dans ce cas) et le service VPN (zone fw).

20.4.3 Visualisation des connexions en cours :

Les connexions en cours sont visibles dans le menu

- Configuration/VPN PPTP/L2TP/ Etat des connexions

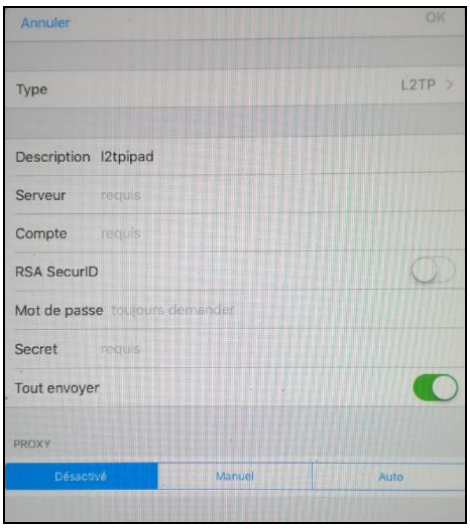


20.4.4 Configuration Client de Connexion :

20.4.4.1 Configuration Client IPAD™ :

L'appareil doit être connecté au réseau WIFI.

Menu Réglage, toucher l'cône 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 PPT/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

20.4.4.2 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

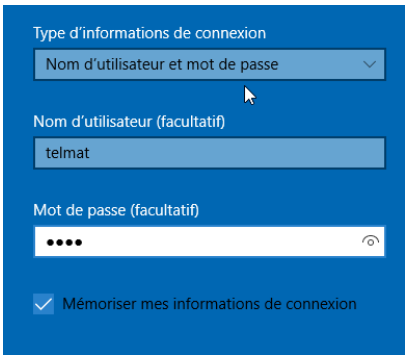
Fournisseur VPN : choisie Windows (intégré)

Nom de la connexion : saisir un nom évocateur

Nom ou adresse IP du serveur VPN : peut être un nom ou une adresse IP

Type de réseau : Choisir L2TP avec clé pré-chargée

Clé pré-partagée : saisie la clé saisie dans le menu *clé partagée secrète* de la Cit@box



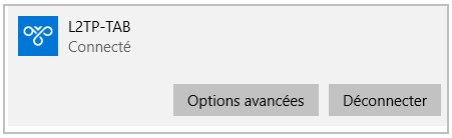
Type d'informations de connexion : choisir dans la liste *Nom d'utilisateur et mot de passe.*

Nom d'utilisateur :
Nom déclaré dans le menu VPN PPTP/L2TP

Mot de passe :
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 prêtre pour être lancée : Se connecter

La connexion réalisée,

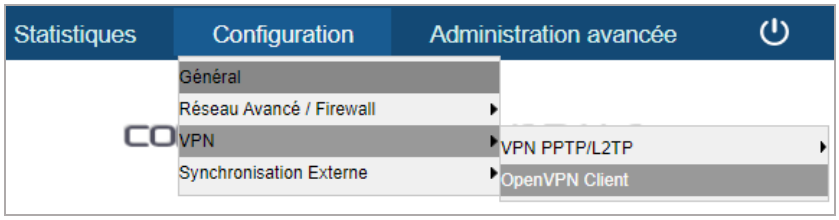


Dans les traces de connexions L2TP/IPSEC

```
-------
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 refhim=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
```

20.5 Client OpenVpn :

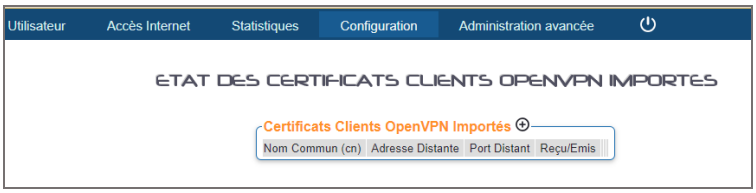
La CitaBox permet une interconnexion type LAN-to-LAN par l'utilisation du client OPENVPN vers un site centralisé CitaBox disposant du serveur OpenVpn



Les étapes pour configurer la partie cliente sont les suivantes :

20.5.1.1 Injection du certificat :

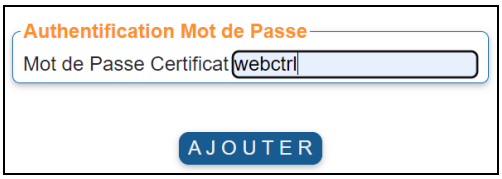
Vous devez disposer d'un certificat OpenVpn généré sur le serveur OpenVpn (Cf chapitre OpenVpn Serveur de la documentation AccessBox).
Il doit être injecté via le menu d'importation des certificats clients



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

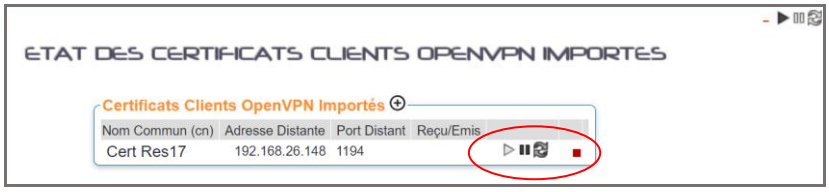
Sélectionner le certificat à importer en cliquant sur 

Puis cliquer sur AJOUTER.
Renseignez les informationssi nécessaire lors de l'importation



Importation réussie

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

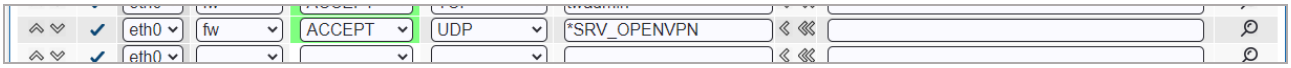


Lorsque le service est correctement démarré les voyants passent en bleue.

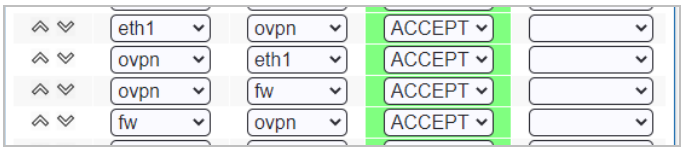
20.5.1.2 Configuration du Firewall :

Les règles de firewall sont à paramétrer

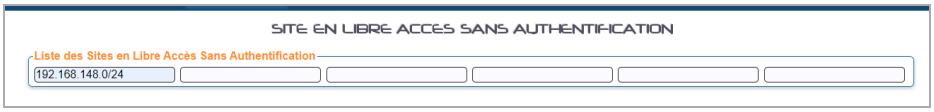
- Pour la communication du client / serveur du coté Wan : Port et protocole paramétrés dans le serveur OpenVpn.



- 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) :



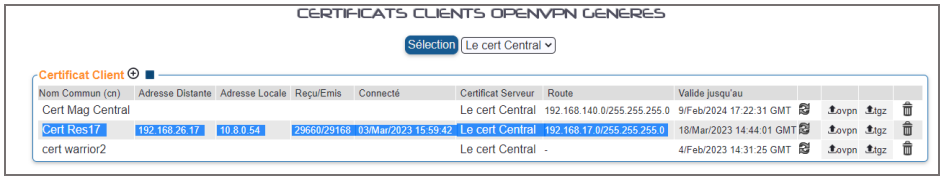
Lors d'un connexion par portail captif avec authentification, pour éviter la déconnexion du tunnel OpenVpn, il est impératif de rajouter la classe d'adresse IP distante (vers le serveur) dans *Site en Libre Accès Sans Authentication*. Dans cet exemple, la classe 192.168.148.0/24 est le réseau distant accedé coté serveur.



Etat du circuit établi :

- Côté client

- Côté serveur

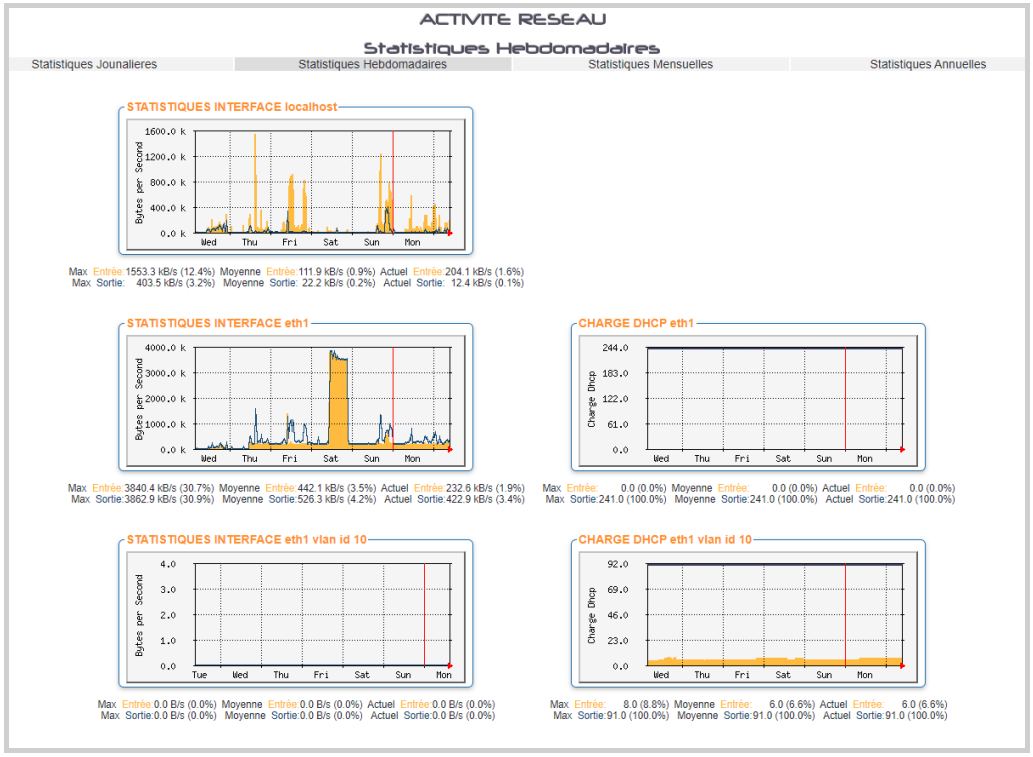


21 Statistiques

Plusieurs types de statistiques sont disponibles sur Cit@Box.

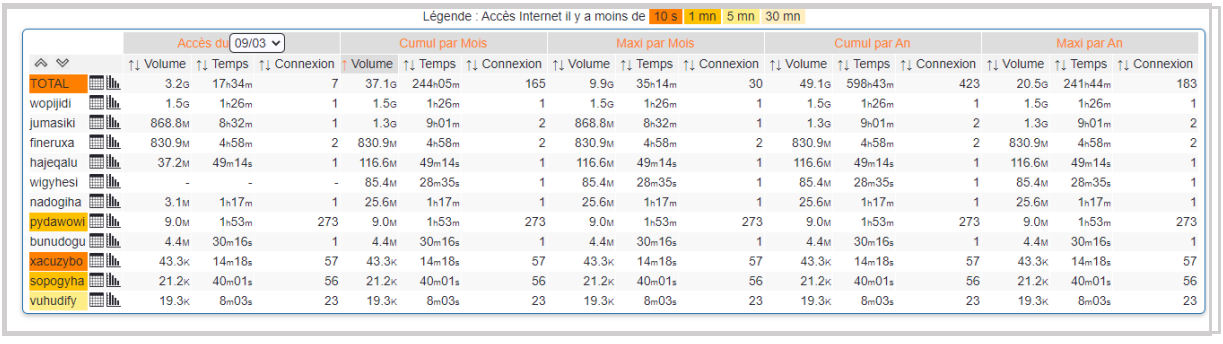
21.1 Activités Réseau :

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.



21.2 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

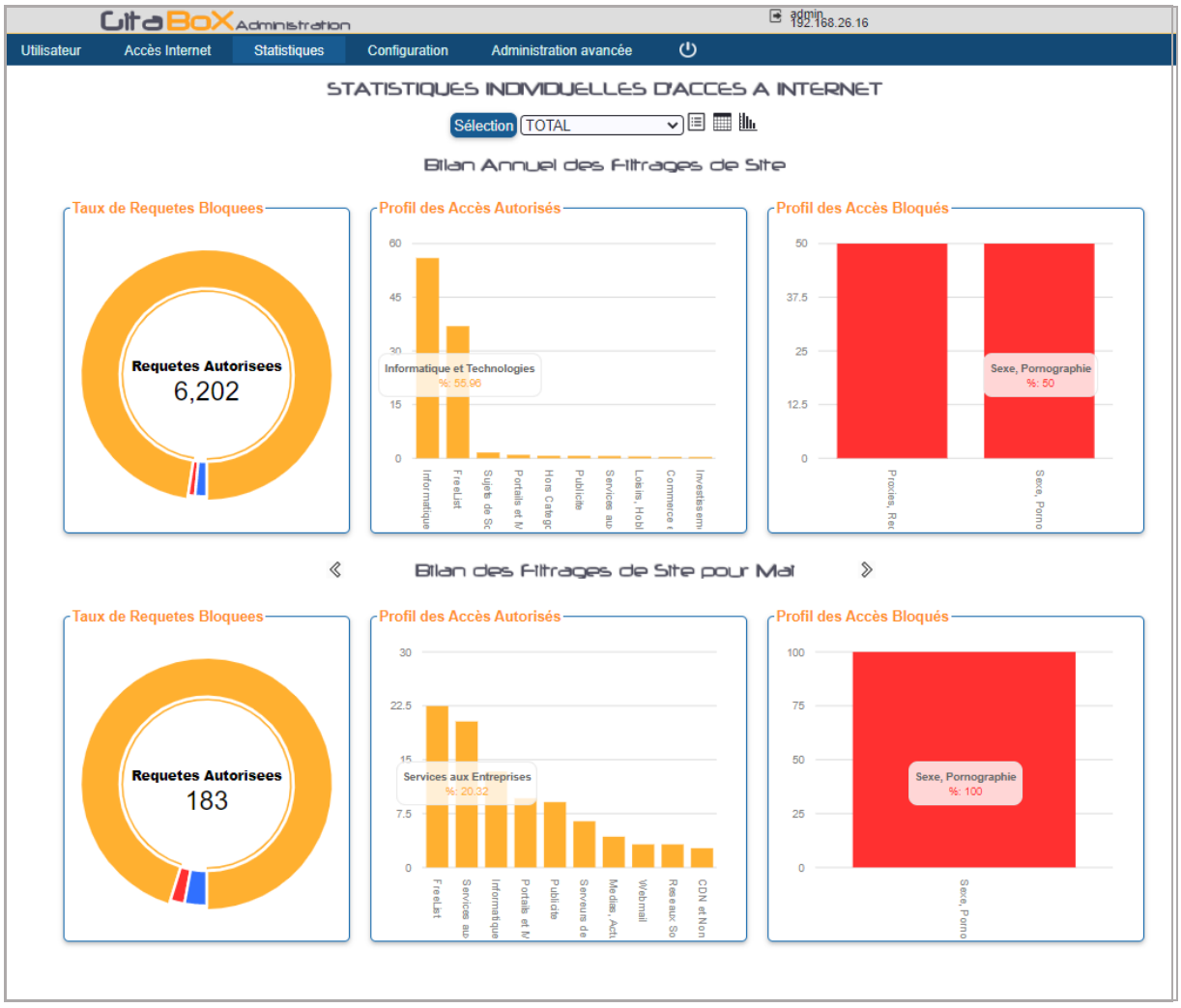


Légende : Accès Internet il y a moins de 10 s 1 mn 5 mn 30 mn

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
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
nadogiha	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.

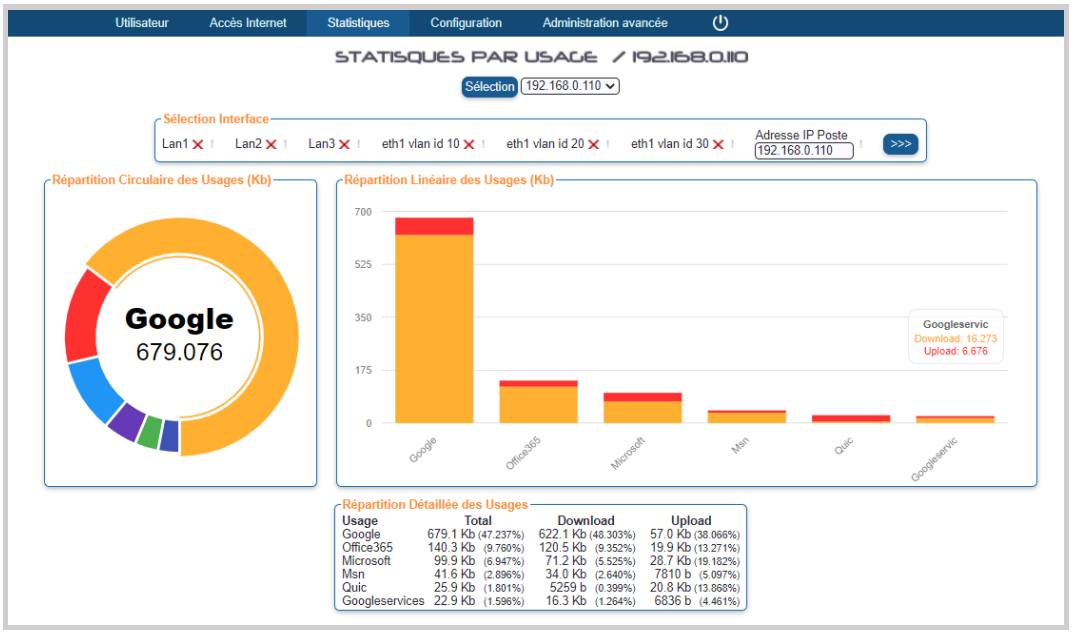


21.3 Statistiques par usage :

Des statistiques par usage peuvent être calculées puis affichées.

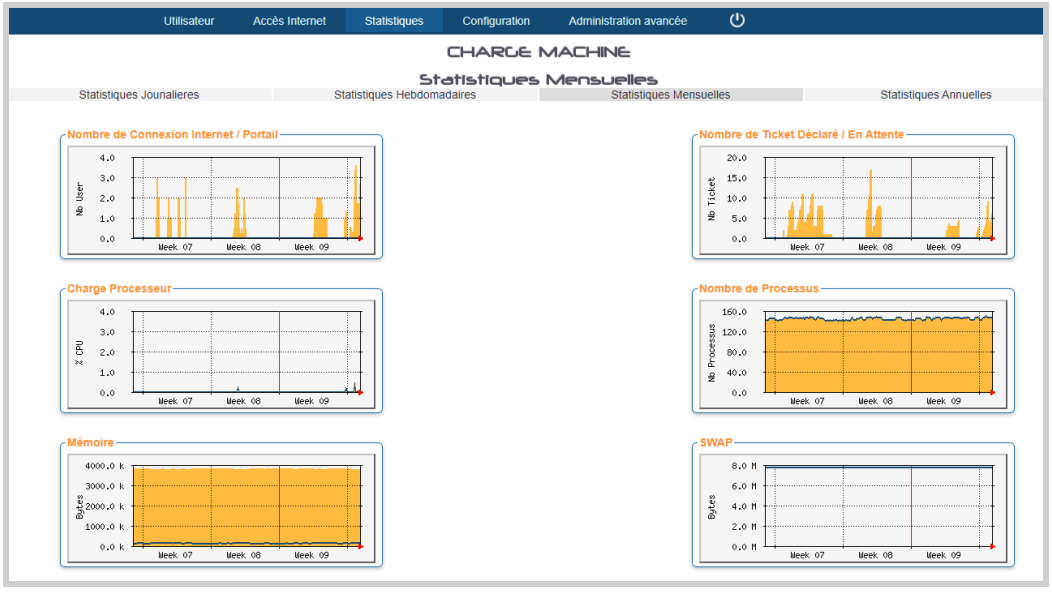
Attention, ces statistiques sont volatiles, elles sont remises à zéro lors d'un rechargement de configuration, redémarrage de la machine – Elles sont également consommatrices de ressources – A utiliser avec précaution

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



21.4 Charge machine :

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



22 Les Traces enregistrées par la Git@Box

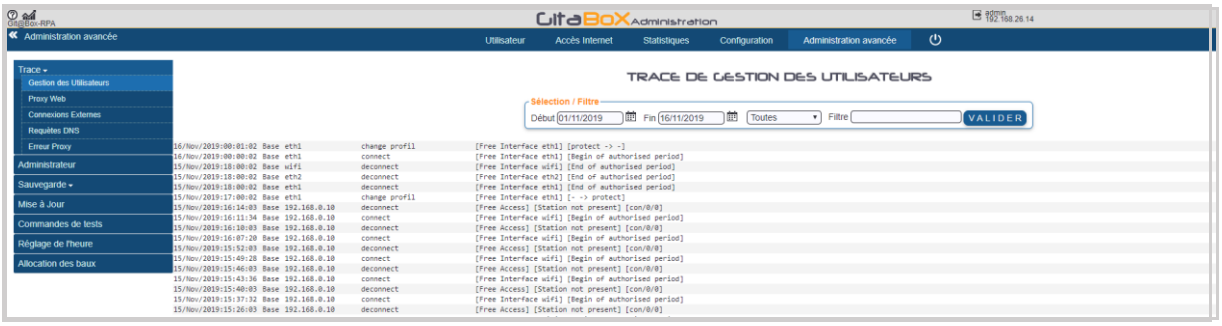
Les traces sont enregistrées et stockées dans la Git@box. Toutes les nuits une rotation des traces permet un archivage et une conservation sur une durée de 12 mois.

Lors de la création et ou connexion des utilisateurs au portail, les mots de passes ne sont pas affichés en clair dans les logs

22.1 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
- Requêtes DNS



Les traces enregistrées par la Git@box peuvent être sauvegardées manuellement ou stockées quotidiennement sur une unité de sauvegarde externe.

22.2 La Sauvegarde des Traces d'Accès

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.

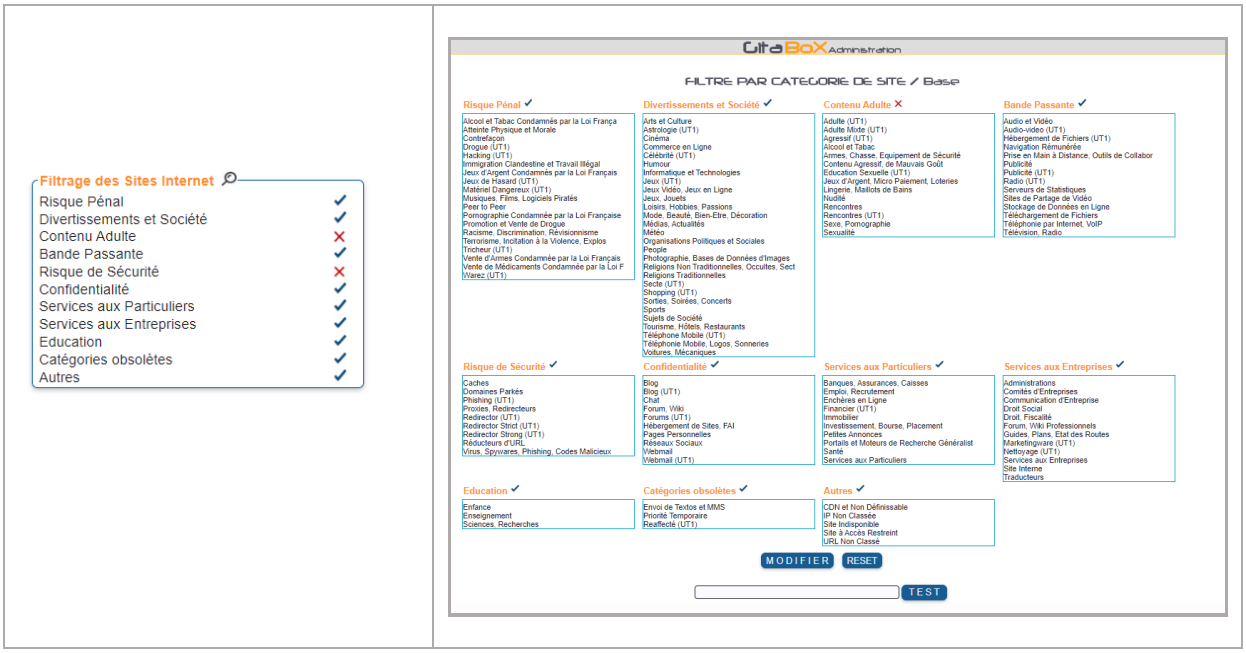
22.3 Externalisation périodique des traces

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.

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

23 Activation Licence Olféo, Filtrage :

Le filtrage par catégorie de sites de la Cit@box utilise les bases de données filtrage de l'éditeur Olféo.
Ces catégories sont classées par thème et configurable dans les profils Base et Sécurisé.

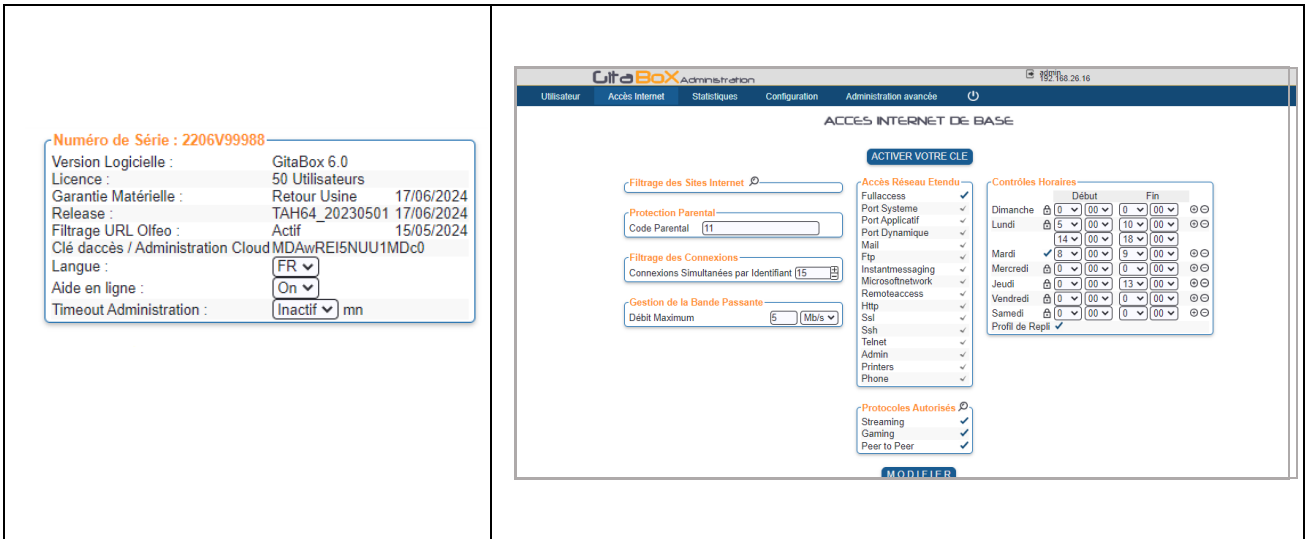


Plusieurs cas se présente pour l'activation de la licence

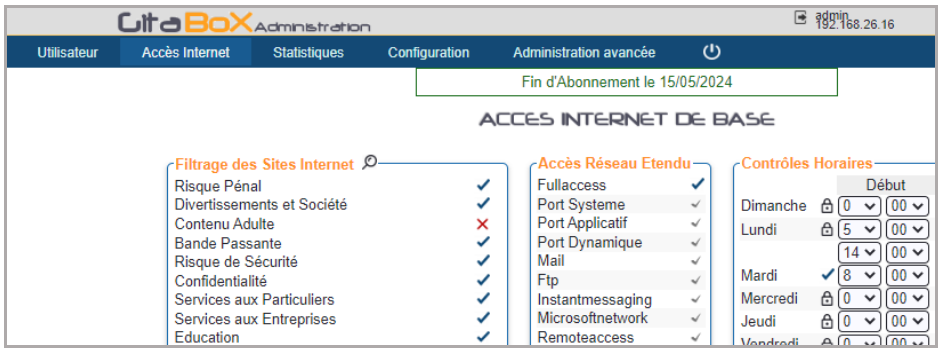
23.1 Souscription nouvelle licence Olféo :

- ✓ 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

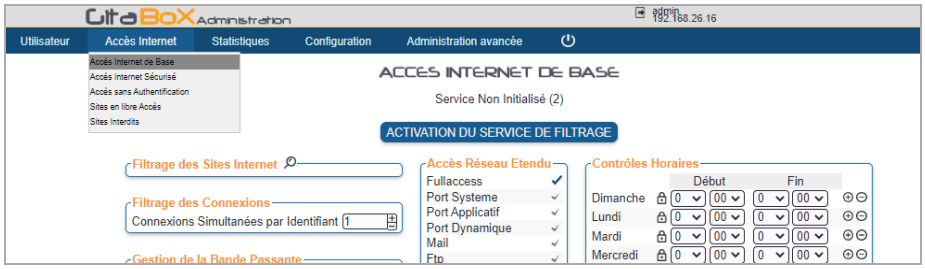


23.2 Restauration configuration utilisateur et usine :

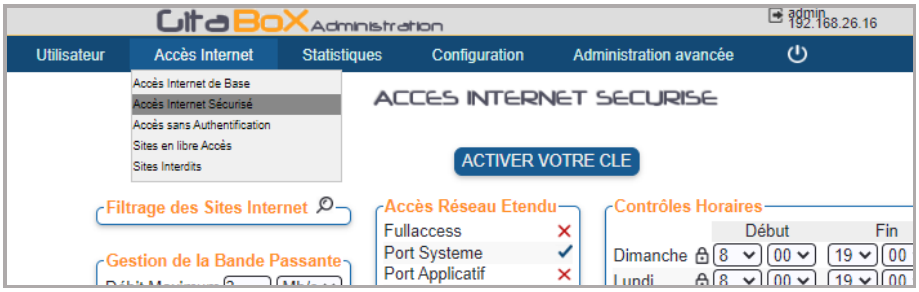
La clé doit être réactivée lors de la **Duplication d'une configuration** ainsi que lors de la **Restauration de la Configuration Usine**.

Ceci se fait en deux étapes :

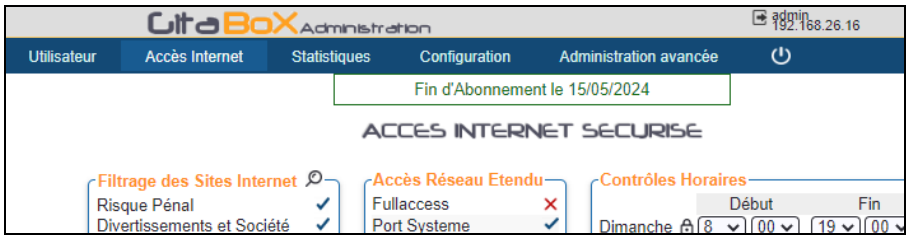
- ✓ Activation du Service de Filtrage : Cliquer sur le bouton dans le profil base ou sécurisé



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

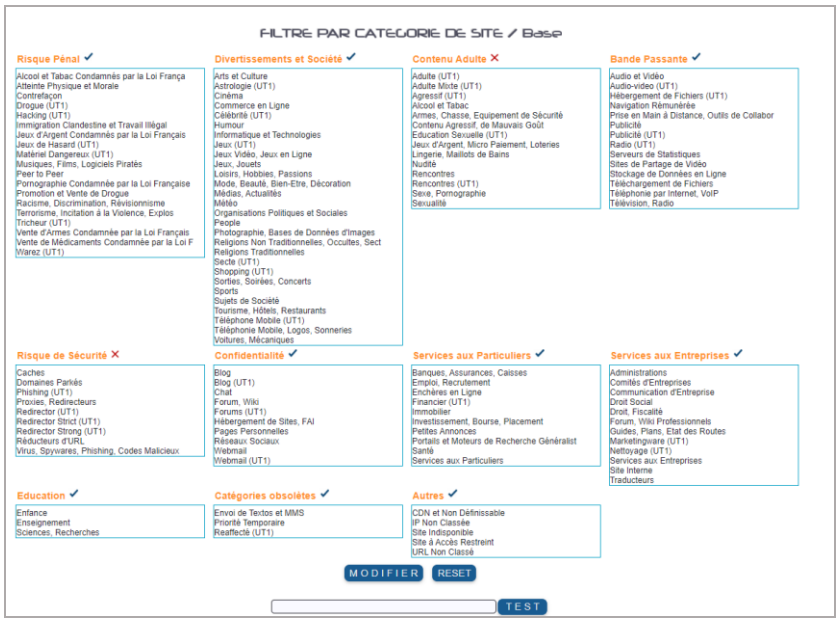


La synchro **réussie** affiche la date de fin d'abonnement

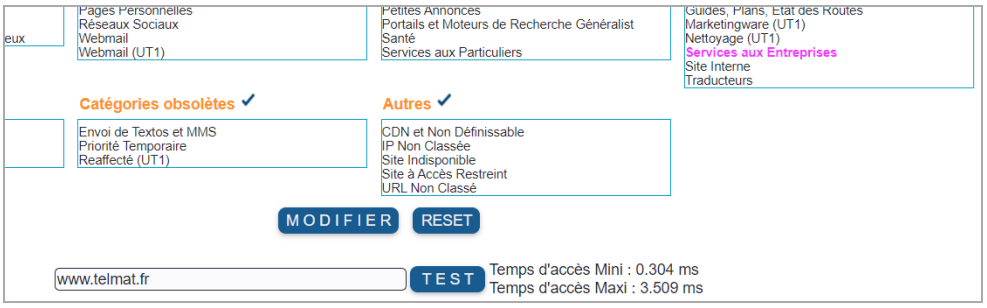


23.3 Filtrage :

Le filtrage par catégorie se configure via les profils : Base ou Sécurisé
Pour accéder à la liste complète cliquer sur

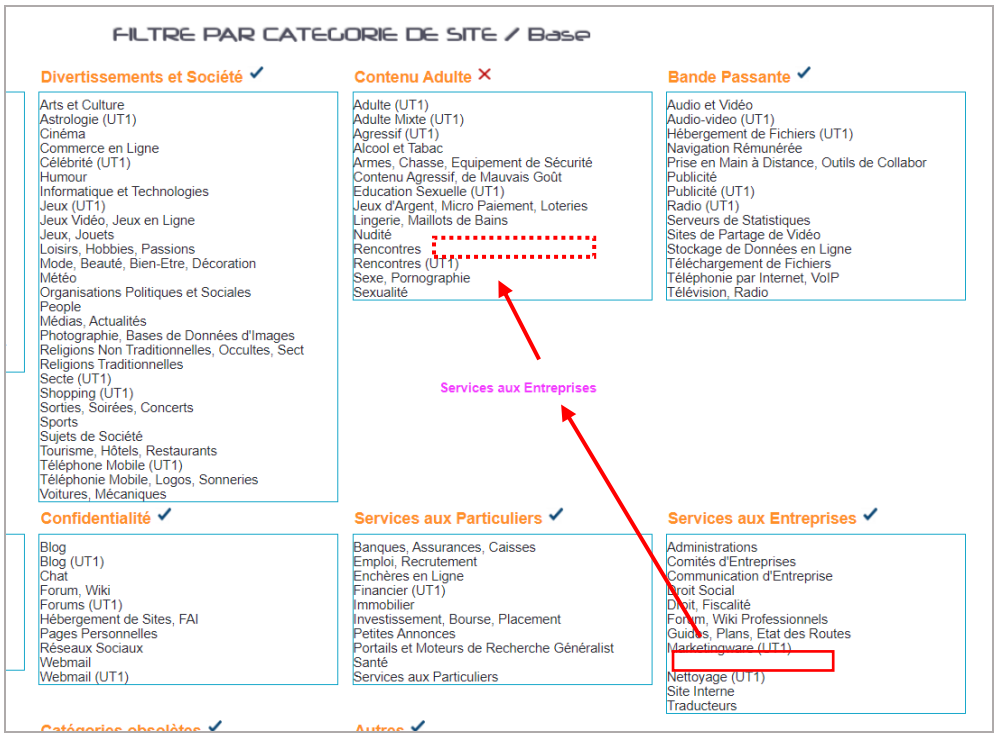


Pour vérifier dans quelle catégorie est référencée le site utilisez le champ *TEST*
La catégorie résultat (si elle existe) est colorée



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 relacher le bouton de celle-ci, déplacer celle-ci vers le thème choisi. Puis cliquer sur MODIFIER



Pour replacer les catégoriés déplacées dans leurs thèmes originaux cliquer sur RESET

24 Administration avancée

24.1 Sauvegarde/Restauration de la configuration

Permet de réaliser la sauvegarde/duplication de la configuration système de la Git@Box. La Restauration/Duplication d'une configuration n'est possible que sur le même type de machine ayant la même release système.

- Menu « Administration avancée / Sauvegarde/ Sauvegarde de la Configuration »

- 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 ou la même machine.

24.2 Restauration de la configuration 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*** (sans extension, ou txt). La clé insérée dans la prise USB, il faut redémarrer la machine.

24.3 Mise à jour logicielle

Les mises à jour Git@Box sont automatiques par défaut. Il est possible également de la faire manuellement, dans ce cas, il faut clique sur le bouton de mise à jour dans le menu.

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

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

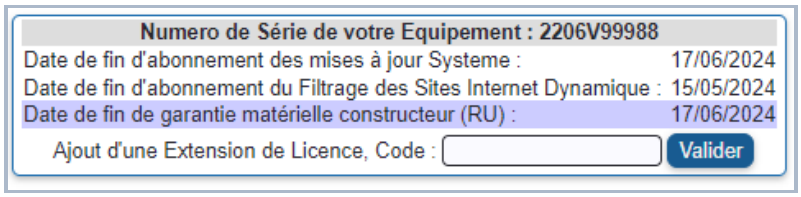
Ne pas éteindre la machine, pendant la phase de mise à jour.

24.4 Saisie Licence :

Pour bénéficier des dernières évolutions logicielles et maintenir la garantie matérielle de votre Cit@Box 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 saisie dans le menu : *Administration Avancée/Mise à jour*



- ✓ 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

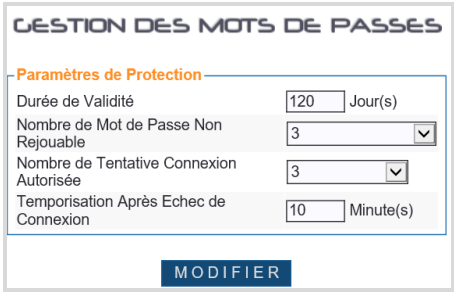
24.5 Gestion des mots de passe des Administrateurs :

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

25 Compléments de configuration

- **Contacter l'Assistance**
  Du lundi au vendredi (sauf jours fériés) de 9h00 à 12h00 et de 14h00 à 17h30 (vendredi 16h30)
  - 🖷 : 03 89 62 13 31
  - ☎: 03 67 35 08 30 (appel non surtaxé)
  - ✉ support@telmatweb.com

- La documentation de configuration de la Git@box est téléchargeable à l'adresse suivante :

  https://www.gitabox.fr/documents/install-gitabox.pdf