Manuel du boîtier eniKma v.1.28

Composants **2**
Système **2**
Branchement **2**
Connexion **3**
Page d'accueil **3**

Menu général **3**
VPN 4
Filtre Web 6
Vidéo 7
Cloud 8
Webmail 9
Vocal 12
Configuration 13
Informations 15

Définitions **16**

Informations diverses **17**

Espace utilisateur **18**
Création des clés 18
Fonction vocale 18
Infos personnelles 19
Statistiques 19

Problèmes et solutions **20**

Développements en cours **24**

Boîtier eniKma

COMPOSANTS

Le boîtier eniKma est livré avec les pièces suivantes :

a) un boîtier électronique
b) un chargeur électrique
c) quatre pieds antidérapants
d) *un adaptateur USB/Ethernet (optionnel)*

SYSTEME

Système d'exploitation : ARMbian, Linux Debian 10 pour processeurs ARM.
Environnement logiciel : Apache2, MariaDB, PHP.

BRANCHEMENTS

Vous pouvez auparavant coller les 4 pieds antidérapants sous chacune des 4 vis situées sous la boîte.

a) Après déballage du matériel, reliez le boîtier eniKma à votre Box Internet à l'aide d'un câble Ethernet droit ordinaire (généralement fourni avec toutes les Box Internet).
→ *Attention : modèle LIVEBOX : reliez votre Livebox à l'adaptateur USB/Ethernet de votre boîtier eniKma, et non pas dans son port Ethernet comme indiqué ci-dessus*

En général une Box Internet dispose de 4 ports Ethernet RJ45 disponibles pour y brancher des ordinateurs ou autres périphériques.

b) Optionnel (modèle classique, non Livebox): si vous disposez d'un adaptateur USB/Ethernet, vous pourrez brancher directement votre ordinateur ou votre concentrateur réseau (hub) ou votre répartiteur réseau (switch) au boîtier eniKma sans passer par le WiFi. Dans ce cas, branchez-le maintenant à l'un des 3 ports USB. Puis branchez sur votre adaptateur votre ordinateur ou bien votre périphérique réseau (hub, switch, routeur, etc.).
Pour le modèle Livebox, il suffit d'inverser les ports : vous brancherez votre ordinateur ou hub ou switch dans le port Ethernet du boîtier eniKma et non pas l'adaptateur USB/Ethernet.

c) Branchez le cordon d'alimentation **toujours** en dernier lieu.

CONNEXION

Connectez-vous au réseau Wi-Fi nommé « eniKma-xxxx » où xxxx est une suite alphanumérique. Vous pourrez renommer plus tard ce réseau.
Le mot de passe par défaut est « enikmavpn ». Vous pourrez modifier plus tard ce mot de passe.

Si vous disposez de l'adaptateur optionnel USB/Ethernet, la connexion est immédiate et ne requiert pas de mot de passe.

ACCUEIL

Pour accéder à votre boîtier eniKma, ouvrez votre navigateur et saisissez l'adresse suivante :
http://192.168.75.1

Cliquez sur la boîte pour l'ouvrir. Saisissez votre identifiant et votre mot de passe. Par défaut, l'identifiant est « *admin* » et le mot de passe « *enikmavpn* ». **Nous vous conseillons de rapidement changer au moins le mot de passe** (voir *Configuration*).

MENU GENERAL

VPN
(OpenVPN)

Un réseau privé virtuel, (en anglais, VPN ou Virtual Private Network), est une solution technique permettant de créer un lien direct et sécurisé par chiffrement entre votre ordinateur et l'Internet. Votre navigation échappe donc entièrement à la surveillance de votre FAI, d'autant plus que vous aurez décidé des serveurs DNS que vous souhaitez utiliser (le boîtier eniKma utilise par défaut le projet libre OpenNIC).

Le VPN vous permet, si vous choisissez un serveur VPN étranger, de visualiser du contenu qui aurait été géographiquement bloqué.

Le VPN vous permet aussi de contourner la censure d'un pare-feu ou d'un proxy comme c'est souvent le cas dans les réseaux d'entreprise ou bien les Wi-Fi publics utilisant des listes noires dans lesquels peuvent se retrouver vos sites favoris (c'est le cas dans beaucoup de Mc Donald, quelques aéroports, etc.). Il permet aussi de contourner les censures nationales d'Etat.

Un bon VPN peut faire baisser légèrement le temps d'accès (c'est à dire la réactivité) de votre navigation mais n'entraîne pas nécessairement de baisse de débit. Au contraire, dans certains cas (par exemple l'accès à Youtube pour les utilisateurs Free) le débit est supérieur car le flux ne provient pas du site d'origine mais du serveur VPN.

Beaucoup de VPN commerciaux ralentissent la navigation Internet. A ce jour, ce n'est pas le cas des serveurs VPN eniKma.

A noter que plus le serveur VPN sera proche de vous géographiquement et moins la navigation sera impactée. Préférez les serveurs VPN français pour le quotidien.

VPN nomade : eniKma vous fournit un accès VPN nomade vous permettant aussi de bénéficier du VPN lors de vos déplacements, même si vous ne transportez pas le boîtier avec vous. Pour cela il vous suffit de créer des paires de clés nomades (pour chaque serveur VPN dans chaque pays) dans votre Espace utilisateur (*https://www.enikma.fr/connexion.php*) puis les télécharger (si vous avez oublié ou si vous n'avez jamais créé de mot de passe pour cet Espace, cliquez sur « *mot de passe oublié ?* »).

Les fichiers fournis sont au format .OVPN que vous pouvez utiliser tels quels avec le logiciel gratuit et Open Source appelé « OpenVPN Connect ». L'ensemble des fichiers .OVPN (un par serveur) est regroupé dans un seul fichier au format .TAR (ouvrable avec un simple programme de compression/décompression comme WinRar, par exemple). Décompressez l'ensemble des fichiers .OVPN dans le dossier de votre choix sur votre ordinateur.

◦ Pour ordinateur : nous vous conseillons le logiciel **gratuit** *OpenVPN Connect* téléchargeable à l'adresse suivante *https://openvpn.net/download-open-vpn/* au chapitre intitulé OPENVPN CLIENT / OPENVPN CONNECT.

Le programme "OpenVPNConnect" doit être en général lancé en mode administrateur (si nécessaire, par un clic droit sur l'icône, puis choisir d'exécuter en tant qu'administrateur sous Windows). Une fois installé vous n'avez plus qu'à importer (un simple glisser-déposer peut faire l'affaire) les fichiers .OVPN un à un en cliquant sur ADD à chaque fois.

Les utilisateurs de Linux Ubuntu (ou apparenté) trouveront une aide ici : *https://doc.ubuntu-fr.org/client_openvpn* . Ensuite, ils iront dans le menu des connexion VPN, onglet VPN, en laissant le type par défaut "Certificat TLS" et en lui fournissant les clés préalablement décompressées.

Une fois le logiciel installé, toute navigation échappe entièrement à la surveillance de votre Fournisseur téléphonique (en 4G) ou de votre Fournisseur d'Accès Internet (Box) ou fournisseur Wi-Fi (hôtel, aéroport, etc.).

◦ Téléphone portable : transférez tout d'abord les fichiers .OVPN dans un dossier de votre choix dans votre téléphone. Pour Android (Google Play) ou iPhone (Apple Store), cherchez l'application « OpenVPN Connect » puis installez-la. Une fois l'application ouverte, cliquez sur le menu en haut à gauche puis choisissez « *Import profile* » puis cliquez sur l'onglet « *File* ». Dirigez-vous ensuite dans le dossier contenant les fichiers .OVPN que vous venez de décompresser. Sélectionnez un des fichiers .OVPN en cliquant dessus, puis appuyez sur le bouton « *Import* ». Le profil est importé (« *Profile successfully imported* ») puis cliquez sur ADD en haut à gauche. Recommencez l'opération pour chaque serveur. Tous les serveurs importés mais non utilisés sont listés dans le menu (déroulable) nommé « *Disconnected* ».

Note 1 : pour des raisons techniques, votre connexion nomade utilise les serveurs DNS du service OpenDNS (Cisco) et non pas les serveurs DNS OpenNIC.

Note 2 : en mode nomade le statut du WiFi indique transitoirement « Erreur », cela est normal.

Note 3 : le mode VPN, en raison du chiffrement qui est gourmand en ressources processeur, entraînera une consommation électrique plus élevée de votre téléphone. Ceci est normal, mais surveillez votre batterie !

Cas particulier des réseaux WiFi gratuits des Fournisseurs d'Accès Internet (FreeWifi, etc.)

Pour vous connecter à ces réseaux nécessitant la saisie de codes personnels, il vous faut d'abord couper le VPN (dans le menu VPN) puis revenir dans le menu Configuration pour basculer en mode Nomade. Alors, vous choisirez le WiFi souhaité et ensuite, une fois connecté, vous pourrez réactiver votre VPN.

FILTRE WEB
(Privoxy)

Le filtre Web vous permet de faire filtrer en amont par le boîtier eniKma l'ensemble de votre navigation Internet avant même qu'elle n'atteigne votre ordinateur. Il utilise le principe du Proxy.

Suivant le niveau de filtrage choisi, le filtre Web pourra vous débarrasser des publicités, du contenu non-sécurisé, des cookies et autres traceurs. A noter qu'il peut aussi, dans un mode très restrictif, entraîner des difficultés à naviguer sur certains sites.

Le **VPN** masque votre adresse IP et cache votre navigation à votre fournisseur d'accès Internet. Le **filtre Web** rendra votre navigation plus sûre et encore plus anonyme en modifiant ou en masquant tout ou partie de votre empreinte numérique (suivant le niveau de protection).

Vous pouvez augmenter encore votre sécurité et votre anonymat en utilisant le browser TOR pour naviguer sur l'Internet.

Configuration

Pour utiliser le filtre Web, vous devez configurer votre navigateur pour qu'il utilise un "Proxy".

- Adresse du proxy : 192.168.75.1
- Port : 8118

Utilisateurs de pare-feu (firewall) : pensez à autoriser le port 8118.

Vous pouvez modifier rapidement le niveau de protection dans l'un des 3 modes prédéfinis disponibles : *Cautious* (protection de base), *Medium* (protection intermédiaire), *Advanced* (protection avancée).

Attention : plus la protection est élevée et plus grand est le risque que votre navigation rencontre des difficultés. Baissez le niveau en cas de problème (utilisateurs avancés : vous pouvez créer des exceptions site par site dans le fichier de configuration de *Privoxy* et vous pouvez configurer à l'infini le Filtre Web via sa page de configuration).

VIDEO
(ZoneMinder)

Le service Video de l'eniKma vous permet de placer une ou des caméras qui seront accessibles à tout moment via l'Internet, par ordinateur ou sur votre téléphone portable. Ce service fait l'objet actuellement de développements afin de faciliter son usage et l'intégration à l'interface eniKma.

L'adresse d'accès à vos caméras peut être modifiée à votre guise pour la protéger des spectateurs indésirables. Par défaut il s'agit du répertoire au nommage aléatoire « /zm-xxxxxx ». Vous pouvez modifier ce nom de répertoire.

La liste des caméras compatibles avec Zone Minder est plutôt longue et disponible par un lien dans votre interface. Par exemple, la caméra D-Link DCS-930L (ou 932L avec vision nocturne) fonctionne parfaitement bien pour un prix modique et une bonne disponibilité en magasin. Sa configuration est simple :

1. Branchez la caméra au réseau électrique et à votre ordinateur via un câble Ethernet.
2. Configurez votre carte réseau en 192.168.0.1 (sous-réseau : 255.255.255.0).
3. Accédez à votre caméra en tapant l'adresse 192.168.0.20 dans votre navigateur Internet. L'identifiant est « admin » et le mot de passe est vide (pas de mot de passe par défaut).
4. Dans le menu de la caméra, renseignez le SSID du réseau (le nom de votre réseau Wi-Fi eniKma), puis le mode de sécurité « WPA-PSK / WPA2-PSK » et enfin le mot de passe de votre réseau Wi-Fi (« Pre-Shared Key »). Sauvegardez le tout (« Save Settings »).
5. Votre caméra doit désormais être connectée au réseau Wi-Fi de votre eniKma. Vous pouvez le vérifier dans le menu *Informations* de votre administration. Débranchez le câble Ethernet et placez votre caméra à l'endroit de votre choix.

Dans votre interface eniKma vous trouverez un lien vers la configuration du système de surveillance (« Adresse locale : http://192.168.75.1/zm-xxxxxx »).

1. Ajoutez votre caméra (« Add New Monitor »)
2. Une petite fenêtre s'ouvre. Paramétrez comme ceci :

a) Onglet **General**

Name : le nom que vous souhaitez
Source Type : Remote

b) Onglet **Source**

Remote Host Name : admin:@<ADRESSE IP de la CAMERA>*
Remote Host Port : 80 (Default)
Remote Host Path : /image/jpeg.cgi
Capture Width (pixels) : 640
Capture Height (pixels) : 480

**Vous trouverez l'adresse IP de la caméra dans le menu* Informations *de l'interface eniKma*

CLOUD 

(NextCloud)

Le Cloud vous permet de partager des documents avec vous-même (sauvegarde et accès à distance de vos documents) ou bien avec des tiers (partage de documents).

Lors de la première utilisation vous devrez créer un compte d'administrateur en choisissant un « *Nom d'utilisateur* » et un « *Mot de passe* ».

Ne pas modifier le champ : « Répertoire des données ».

Ensuite vous devez saisir les informations relatives à la base de données :

- Utilisateur : *enikclouduser*
- Mot de passe : *enikldvpn*
- Nom de la Base de données : *nextcloud*
- Serveur : *localhost:3306*

Enfin, vous pouvez cliquer sur « *Terminer l'installation* ». Le processus de création peut prendre quelques minutes.

Ces informations ne sont pas modifiables par l'interface mais peuvent l'être en ligne de commande pour les utilisateurs très avancés. Cependant, la base de données n'étant accessible qu'en local, ces données peuvent être maintenues publiques sans aucune incidence, sous réserve que l'accès à votre boîtier eniKma ne soit pas compromis (par exemple si vous avez défini un mot de passe root et que celui-ci a été découvert).

Note : comme pour toute vos données en général, il est fortement conseillé de disposer d'une copie de sauvegarde des données partagées sur votre Cloud.

Remarques

Veillez à ne pas dépasser la capacité de la mémoire interne du boîtier (environ 4 Go) ou, le cas échéant, de votre support externe (carte SD ou disque dur).

La vélocité de votre Cloud dépend de celle de votre connexion Internet. Contrairement à la fibre, l'ADSL ayant un débit montant (upload) faible, cela impactera directement l'accès distant à vos fichiers.

WEBMAIL
(RoundCube)

Le Webmail vous permet d'accéder à vos courriels en n'utilisant pas l'interface de votre fournisseur mais en utilisant celle du boîtier eniKma.

Les courriels restent chez votre fournisseur et rien n'est stocké dans votre eniKma (hormis vos éventuels carnet d'adresse et liste de clés GPG/PGP). Dès lors vous pouvez continuer à utiliser conjointement l'interface de votre fournisseur si nécessaire.

Cependant, en utilisant ce Webmail vous bénéficiez d'une interface identique et personnalisable pour vos différentes adresses électroniques (*Gmail, Hotmail, Yahoo*). Mieux encore, vous pouvez envoyer et recevoir des messages chiffrés qui ne transiteront jamais en clair chez votre fournisseur.

Enfin, vous pouvez modifier l'adresse d'accès à votre Webmail afin de le protéger des personnes indésirables. Par défaut le répertoire est « /webmail-xxxxxx ». Nous vous conseillons de le modifier.

Le Webmail eniKma propose par défaut un paramétrage pré-configuré pour 7 fournisseurs d'adresses électroniques : Gmail, Hotmail, Yahoo, Free, Orange, Bouygues, SFR.

Gmail	ssl://imap.gmail.com:993
Hotmail	ssl://imap-mail.outlook.com:993
Yahoo	ssl://imap.mail.yahoo.com:993
Free	ssl://imap.free.fr:993
Orange	ssl://imap.orange.fr:993
Bouygues	ssl://imap.imap.bbox.fr:993
SFR	ssl://imap.sfr.fr:143

Vous pouvez ajouter, modifier ou supprimer des fournisseurs d'adresses électroniques grâce au tableau "Fournisseurs de mails". Seul un clic sur le bouton "Enregistrer les modifications" permet de mémoriser les modifications apportées.

Le protocole IMAP permet de lire vos mails à distance sans les télécharger ni les supprimer de leur stockage chez votre fournisseur.

Attention, le protocole IMAP est un protocole pour lire, modifier ou supprimer les mails et non pas pour les envoyer. Pour cela, consultez le manuel eniKma ou la question relative à l'envoi des mails dans la présente Foire Aux Questions.

Pour accéder à vos courriels, saisissez l'utilisateur (votre mail complet) et le mot de passe, en choisissant le bon fournisseur dans le menu déroulant.

Paramétrages

A paramétrer obligatoirement :

1. Dans « Paramètres », puis dans « Identités » modifiez le « Nom à afficher » par le nom tel que vous souhaitez que vos correspondants le voient.

2. Dans « Paramètres » puis « Identités », sous « Paramètres SMTP » :

a) décochez la case SMTP par défaut

b) Nom de l'hôte (choisissez selon votre fournisseur) :

- Gmail : tls://smtp.gmail.com
- Hotmail : tls://smtp.live.com
- Yahoo : tls://smtp.mail.yahoo.com
- Free : ssl://smtp.free.fr
- Orange : tls://smtp.orange.fr*
- Bouygues : tls://smtp.bbox.fr
- SFR : tls://smtp.sfr.fr

c) Port du serveur (choisissez selon votre fournisseur) :

- Gmail : 587
- Hotmail : 587
- Yahoo : 587
- Free : 465
- Orange : 465*
- Bouygues : 587
- SFR : 465

d) Nom d'utilisateur et mot de passe : votre mail complet et le mot de passe de votre mail.

** Information donnée à titre indicatif car le fournisseur Orange interdit par défaut d'utiliser son serveur SMTP si l'utilisateur n'est pas sur un réseau Orange.*

3. Cliquez sur « Paramètres », puis dans « Clés PGP », cliquez en haut sur l'icône « Importer » puis, si vous en disposez, importez les clés publiques de vos correspondants.

a) Si vous disposez d'une paire de clés (publique et privée), cliquez en haut sur l'icône « Importer » puis importez le fichier de votre paire de clés (publique **et** privée).

b) Si vous n'avez pas déjà une paire de clés, vous pouvez la créer dans le menu « Clés PGP » en cliquant sur l'icône **+** située en bas à côté de la molette. Pour plus de sécurité, choisissez 4096 bits ainsi qu'un mot de passe long (en général une *phrase de passe* longue et facile à retenir de type « *Noël au balcon, Pâques au tison* »).
Note : vous devez avoir modifié votre « Nom à afficher », voir point 1.
Attention : la génération de clés peut être long (quelques minutes). Patientez. Si problème, testez avec un autre navigateur.

4. Utilisateurs *Hotmail* : vous devez diriger la corbeille vers le dossier « Deleted » de Hotmail. Pour cela, une fois connecté à votre Webmail, cliquez sur « Paramètres » puis « Préférences » puis « Dossiers spéciaux ». En face de « Corbeille » choisissez dans le menu déroulant « Deleted ». Puis enregistrez vos modifications.

Nous vous conseillons par ailleurs les paramétrages suivants :

- Cliquez sur « Paramètres », puis dans « Préférences » cliquez sur « Affichage de la boîte de courriel » et cochez la case « Afficher le volet de visualisation ».

- Cliquez sur « Carnet d'adresses » puis cliquez sur l'icône « Importer » et importez votre carnet d'adresses au format CSV ou bien vCard que vous aurez exporté depuis votre messagerie actuelle.

Attention, si vous souhaitez écrire un mail chiffré PGP, préférez le format « Texte en clair » et non pas « HTML ». Cela vous interdira la mise en forme de votre texte, mais le chiffrement d'un texte brut par rapport à un texte HTML sera largement plus compatible. A vous de tester suivant vos correspondants.

Lorsque vous rédigez un mail, cliquez sur l'icône du cadenas puis cochez la case de ce que vous souhaitez faire :

- **Signer :** cela permet de prouver de façon certaine que vous êtes l'expéditeur du courriel car vous devrez saisir votre mot de passe (ou votre *phrase de passe* -cf ci-dessus) pour l'envoyer.
- **Chiffrer :** cela permet de chiffrer votre mail pour le rendre totalement illisible à toute personne sauf ceux dont vous aurez utiliser la clé publique pour leur écrire.
- **Joindre clé publique :** vous pouvez joindre à votre mail votre clé publique afin qu'un correspondant qui n'en dispose pas encore puisse vous écrire ensuite de façon chiffrée.

Les cases peuvent être cochées ou décochées par défaut. A vous de les paramétrer comme bon vous semble via les « Paramètres ».

Note de sécurité : le chiffrement se fait dans le boîtier eniKma. Cela assure une sécurité totale lors du transfert vers votre serveur de messagerie puis vers la messagerie de votre correspondant.
Notez que si vous utilisez du Wi-Fi pour vous connecter à votre boîtier eniKma, la distance parcourue jusqu'à votre boîtier sera sécurisée dans la limite de la sécurité du Wi-Fi (toutefois plutôt bonne).

Si vous utilisez votre Webmail à distance **sans** utiliser le VPN eniKma (ou un autre), alors le mail sera chiffré par la connexion HTTPS jusqu'à atteindre votre boîtier eniKma.
Pour chiffrer davantage vos communications même en déplacement (sur votre téléphone, à l'hôtel, l'aéroport, etc.), vous pouvez utilisez le VPN nomade offert avec votre boîtier. Ou bien vous déplacer avec votre boîtier eniKma (en mode *Station réceptrice*).

VOCAL
(Mumble)

Mumble est un outil de communication vocale vous permettant d'échanger à distance, avec une ou plusieurs personnes, par ordinateur (via l'application OpenSource *Mumble*) ou par téléphone (avec *Plumble*).

Vous pouvez communiquer par oral, un à un ou même en groupe, vous pouvez faire des salons où différentes personnes discutent entre elles (note : la création de salons ne peut se faire à ce jour que par le logiciel PC et non par l'application). Vous pouvez aussi communiquer par écrit via un *chat*.

Les communications sont entièrement chiffrées et, grâce au VPN, votre adresse IP n'est pas dévoilée à vos correspondants. Il s'agit donc d'une communication parfaitement sécurisée et sûre dont **vous** êtes le fournisseur de service avec votre boîtier eniKma, sans **aucun** intermédiaire (contrairement aux applications similaires : WhatsApp, Telegram, Skype, Signal, Silent, etc.).

Pour vous connecter à votre propre serveur Mumble, vous et vos correspondants devez simplement configurer votre client Mumble avec les informations indiquées sur votre interface eniKma.

Pour la première utilisation, modifiez le mot de passe par défaut. N'oubliez pas de redémarrer *Mumble* après chaque changement de mot de passe (bouton *Désactivé/Activé*).

CONFIGURATION

- Wi-Fi : deux modes existent, le mode *hotspot* et le mode *station réceptrice*.

Hotspot émetteur : dans ce mode l'eniKma est l'émetteur du Wi-Fi, permettant aux périphériques alentours de s'y connecter.

Station réceptrice : ce mode vous permet de vous déplacer avec votre boîtier en vous connectant à n'importe quel Wi-Fi public ou privé.
Utile en déplacement, ce mode *station réceptrice* permet l'utilisation complète de votre boîtier eniKma sans limite particulière.

Vous pouvez même le brancher à un port USB sous réserve que celui-ci fournisse un courant de 5V et 1A minimum (ce qui n'est en général pas le cas d'une sortie USB d'ordinateur – 0,5A).

Si vous ne souhaitez pas déplacer votre boîtier eniKma et plutôt le laisser chez vous ou à votre bureau, vous pourrez alors utiliser le VPN nomade lors de vos déplacements (cf. plus haut).
Note : le mode station réceptrice nécessite l'usage de l'adaptateur optionnel USB-Ethernet

- **Mode Activé** : le Wi-Fi est allumé, le planning n'est pas pris en compte.

- **Mode Désactivé** : le Wi-Fi est éteint, le planning n'est pas pris en compte.

- **Mode Planning** : en mode *Hotspot* vous pouvez planifier l'allumage ou l'extinction de votre Wi-Fi (en journée ou bien la nuit, etc.). La précision est au quart d'heure. Ensuite vous devez mettre votre Wi-Fi en mode *Planning* en cliquant sur le bouton « Planning » sinon le planning ne s'exécutera pas.

Dans la version actuelle du pilote de la carte Wi-Fi, chaque fois que le Wi-Fi doit s'activer (de façon automatique par le planning ou bien manuellement sur votre demande), le boîtier eniKma redémarre. Compter 1 à 2 minutes de rupture de service. Ce léger inconvénient est appelé à disparaître avec les mises à jour futures.

Note : au démarrage du boîtier, le Wi-Fi est nécessairement actif pendant quelques minutes. Cette sécurité permet d'accéder au menu même si, par erreur, vous avez coupé le Wi-Fi.

- DNS : serveurs de noms de domaine permettant de transformer un nom de domaine (ex. : google.com) en une adresse informatique (ex. : 66.249.64.0). Choisissez les serveurs DNS dont le temps d'accès est le plus bas. Vous pouvez aussi saisir les serveurs DNS de votre choix.
Les serveurs que propose le boîtier eniKma sont les serveurs DNS du projet libre OpenNIC.

- Accès « root » de mon boîtier eniKma : si vous souhaitez accéder à votre boîtier via une connexion SSH, vous devez définir un mot de passe pour l'utilisateur « root ». Nous déconseillons fortement la configuration d'un compte « root » si vous ne savez pas avec précision ce que vous faîtes.

- Accès à l'administration : nous vous conseillons de modifier votre mot de passe de temps en temps. Si vous souhaitez utiliser une adresse publique pour une connexion à distance (pour vous ou pour partager des documents (Cloud) ou discuter (Vocal) avec vos amis), vous devrez obligatoirement changer de mot de passe.

- <u>Adresse de l'administration</u> : nous vous conseillons de modifier le dossier (répertoire) d'accès à votre interface d'administration. Par défaut, il s'agit de « admin », ce qui est très courant. Il est donc conseillé de changer ce dossier, même faiblement, pour rendre encore plus complexe l'accès à votre administration.
Bien sûr si vous n'avez pas ouvert l'accès à distance, cela ne présente aucun intérêt.

- **<u>Connexion distante</u> :** si vous n'utilisez pas votre boîtier à distance (par exemple : Cloud, Webmail, Caméras, etc.) alors conservez la valeur par défaut (« Non »). Dans le cas contraire vous devez ouvrir l'accès à distant. Cet accès est limité aux applications utilisées et ne permet pas à une personne distante de prendre la main sur votre boîtier (sauf à avoir défini un accès « root » et vous être fait volé le mot de passe).

- **<u>Commandes système</u> :**

Ces commandes sont à utiliser en cas de problème et en général à la demande d'un technicien eniKma.

<u>Redémarrage du réseau</u> : redémarre la couche réseau du boîtier. Patienter quelques secondes.
<u>Vider le cache DNS</u> : vide la mémoire des résolutions DNS. Patienter quelques secondes.
<u>Redémarrage du boîtier</u> : redémarre totalement le boîtier. Patienter 1 à 2 minutes.
<u>Arrêt du boîtier</u> : extinction logicielle du boîtier. Patienter 1 minute environ. La lumière LED interne du boîtier ne s'éteint pas et reste verte.

INFORMATIONS

- <u>Etat des services</u> : l'ensemble des services fournis par l'eniKma sont listés ici. La petite lumière à LED est verte si le service est lancé et fonctionnel (actif). La légende indique la définition de chaque petite icône. Pensez à désactiver les services que vous n'utilisez pas afin de réserver le plus de ressources et de puissances aux services utilisés.

- <u>Machines connectées</u> : ce tableau recense l'ensemble des périphériques qui se sont connectés à votre eniKma dans les 24h, par câble ou par Wi-Fi. Si le voyant est vert, alors le périphérique est encore connecté au boîtier et accepte de répondre à la requête du boîtier eniKma (commande *ping*).

Note : si vous redémarrez votre boîtier eniKma, les informations -volatiles- disparaissent jusqu'à la prochaine demande de connexion des périphériques (appelée *demande de bail DHCP*).

- <u>Journaux systèmes</u> : chaque bouton fait apparaître le contenu de la commande ou du fichier demandé. Principalement pour les utilisateurs avancés.

- <u>Version</u> : affichage de la version de votre boîtier et d'une éventuelle mise à jour disponible, le cas échéant. Le tableau indique les différentes mises à jour, leur contenu, et la possibilité de l'installer.

DEFINITIONS

- **Compte client** : il s'agit du compte que vous avez créé pour commander votre boîtier et souscrire à l'abonnement.

- **Espace utilisateur** : il s'agit d'un espace situé sur le site *enikma.fr* vous permettant de configurer certains paramètres (voir chapitre "Espace utilisateur" ci-dessous).

- **Interface administration** : il s'agit de l'interface de votre boîtier auquel vous accédez en vous connectant sur celui-ci.
    - Vous pouvez vous y connecter directement depuis chez vous, c'est à dire n'importe quel périphérique qui navigue (ou naviguait, en cas de problème !) sur l'Internet grâce au boîtier eniKma (donc connecté au WiFi eniKma ou raccordé par câble via l'adptateur USB).
    - Vous pouvez aussi vous y connecter à distance, sous réserve que vous ayez ouvert l'accès à distance dans votre Interface d'administration et que vous ayez créé un sous-domaine dans votre Espace utilisateur.

INFORMATIONS DIVERSES

- Le boîtier eniKma dipose d'une mémoire interne (*eMMC*) de 8 Go contenant l'ensemble des fichiers nécessaires à son bon fonctionnement.

Utilisateurs avancés : peut être ajoutée, via le logement prévu à cet effet, une carte mémoire de type *micro SD* de la capacité de votre choix permettant d'accueillir les données de votre choix, en particulier pour l'outil **Cloud**. L'ajout du carte SD n'étant pas encore automatique gérée par l'interface, cette opération reste réservée aux utilisateurs avancés.

Mettre vos données sensibles (ou non) sur un carte mémoire externe vous permet aussi de pouvoir enlever cette carte *micro SD* et la remiser dans un lieu sécuriser voire même, dans l'urgence, la détruire, sans qu'il ne reste rien sur votre boîtier eniKma.

- Les utilisateurs qui ne souhaitent pas utiliser de Wi-Fi peuvent utiliser le boîtier eniKma par connexion filaire Ethernet. Pour cela il faut enficher l'adaptateur USB/Ethernet qu'eniKma propose en option ou que vous pouvez acheter sur Amazon (environ 10 euros).

- Pensez à désactiver le Wi-Fi dans votre interface si vous n'en avez pas besoin !

- Si vous souhaitez accélérer le démarrage et l'usage de votre boîtier eniKma, n'activez que les applications dont vous avez besoin.

- Débit théorique maximum du Wi-Fi : 150Mbits/s
- Débit théorique maximum de l'adaptateur Ethernet : 100Mbits/s

- Notre manuel utilise systématiquement le terme exact de « chiffrement » et ses dérivés, mais jamais « cryptage » ou ses dérivés. En effet seul le terme « décryptage » et ses dérivés possède une signification mais qui n'est pas la notre ici car les utilisateurs possèdent des clés pour déchiffrer (le décryptage consistant à retrouver un message originel alors qu'on ne possède pas la clé utilisée pour son chiffrement).

- Les noms de domaine sous la forme *xxxx.enikma.fr* bénéficient de la protection contre les attaques de la société CloudFlare® au même titre que le nom de domaine *enikma.fr* auxquels ils appartiennent. Les attaques DDOS seront repoussées et votre boîtier ne sera pas touché par une tentative d'effondrement par attaque massive.

Espace utilisateur

Votre Espace utilisateur est accessible via le site www.enikma.fr/connexion.php. Vous vous y connectez avec votre mail et le mot de passe que vous avez choisi lors de votre inscription.

INFOS PERSONNELLES

Vous pouvez ici modifier certaines données personnelles. Le port *Mumble* de la fonction Vocale ne peut être modifié ainsi que votre référence client.

STATISTIQUES

Vous trouverez ici quelques informations statistiques sur votre compte ainsi que la dernière heure précise où votre boîtier a été vu en ligne par les serveurs VPN.

Si vous avez ouvert votre accès distant (pour pouvoir accéder à certains services à distance, comme les mails ou la fonction Vocale, ou bien pour partager des documents avec vous-même ou d'autres personnes) une petite icône et un texte vous l'indiqueront.

TELECHARGEMENTS

- **Clés pour le Boîtier eniKma**

Ici vous créerez les paires de clés OpenPGP nécessaires au chiffrement de vos échanges sécurisés en VPN. Dans ce cas, il vous suffit de cliquer sur le bouton « Créer la paire de clés » afin de disposer d'une nouvelle paire que vous téléchargerez ensuite sur votre ordinateur. Enfin, vous vous connecterez sur l'interface de votre boîtier eniKma (http://192.168.75.1), vous dirigerez dans le menu VPN / Nouvelle paire de clés puis exporterez la paire précédemment téléchargée.

Pour rendre active la nouvelle paire de clés, vous patienterez 5 minutes puis changerez de serveur VPN.

- **Clés pour le VPN nomade**

Tout possesseur d'un boîtier eniKma bénéficie d'une connexion VPN nomade utilisable sans boîtier, quelque soit le périphérique utilisé : ordinateur, tablette, téléphone, etc. Très pratique en déplacement !

La création de la paire de clés OpenPGP se déroule comme indiqué précédemment avec le bouton « Créer la paire de clés ». Vous pourrez télécharger ensuite un fichier de type .tar qui sera lu par n'importe quel logiciel de compression (WinZip, WinRar, Jzip, 7zip, etc.). Vous y trouverez un fichier .ovpn pour chaque serveur VPN eniKma.

Pour utiliser ces fichiers il vous suffit d'installer le logiciel OpenSource nommé *OpenVPN* (https://openvpn.net) pour ordinateur ou *OpenVPN Connect* pour téléphone portable. Veillez à ne pas vous tromper de logiciel. Ensuite vous fournirez au logiciel les fichiers .ovpn de chaque serveur VPN (cf. mode d'emploi d'*OpenVPN*).

FONCTION VOCALE

La fonction vocale du boîtier eniKma permet de communiquer un-à-un ou bien à plusieurs de façon totalement sécurisée avec toute personne ayant installé les logiciels OpenSource Mumble (pour ordinateur) ou Plumble (pour téléphone). Vos correspondants n'ont pas besoin d'être utilisateur d'eniKma.

Le bon fonctionnement de la fonction Vocale nécessite que vous disposiez d'un sous-domaine (xxxx.enikma.mobi où xxxx est un préfixe que vous aurez choisi) et d'un numéro de port à 5 chiffres qui vous est attribué lorsque vous cliquerez sur « Activer ».

Vous créerez votre sous-domaine dans l'onglet INFOS PERSONNELLES. Une fois votre sous-domaine créé, vous pourrez activer votre fonction Vocale en cliquant sur le bouton qui apparaîtra.

PROBLEMES ET SOLUTIONS

Boîtier eniKma

• Je n'ai plus Internet sur mon ordinateur

Connectez vous sur l'interface de votre boîtier eniKma *(http://192.168.75.1)*. Si vous n'y arrivez pas, lisez les conseils plus bas relatif à ce problème spécifique.

Vérifiez toujours que la *Box* de votre Fournisseur d'Accès soit bien allumée et synchronisée.

a) Problème DNS

Dirigez-vous dans le menu *Configuration*, au chapitre DNS. Est-ce que les DNS sont actifs et opérationnels (icône) ? Dans le cas contraire, remplacez le DNS défectueux.
Si OpenNIC (fournisseur de DNS libres, gratuits et non surveillés) ne répondait plus, vous pouvez, de façon temporaire et dans l'urgence, utiliser le serveur DNS public de Google : « 8.8.8.8 ».

b) Problème serveur VPN

Dirigez-vous dans le menu VPN. Dans quel état se trouve le VPN ? S'il est en « Erreur », choisissez un autre VPN (ou désactivez le VPN, pour tester l'éventuel bon fonctionnement hors-VPN).

• Google me demande de remplir un captcha !

Un VPN partage des plages d'adresses IP entre un nombre élevé d'utilisateurs. Google étant très utilisé par ces utilisateurs, le moteur de recherche croit parfois que ce nombre élevé de requêtes est initié par des robots. Dès lors il se protège en provoquant des captchas qui sont des questions auxquels les robots ne peuvent pas répondre. Parfois il s'agit simplement de cocher une case, mais dans d'autres cas de nombreuses questions se succéderont. Patience !

Si cela survient sans cesse (et même parfois sans que répondre au captcha ne règle le problème, certaines mauvaises langues pensant que Google n'aime pas les VPN...), vous pouvez changer de serveur VPN. Vous pouvez aussi vous connecter sur votre compte Gmail et laisser l'onglet ouvert. Google vous reconnaîtra comme un utilisateur normal et enregistré et devrait faire rapidement disparaître les captchas.

• Je n'accède pas à l'interface de mon boîtier eniKma *(http://192.168.75.1)*

Tout d'abord êtes-vous bien connecté au Wi-Fi de l'eniKma (ou par câble Ethernet) et non pas au Wi-Fi de la Box de votre FAI, par exemple ?

Si vous êtes bien connecté au Wi-Fi de l'eniKma, alors la connexion semble avoir un problème. Débranchez le câble électrique puis vérifiez le bon branchement du câble Ethernet et des éventuels périphériques USB (par exemple : adaptateur Ethernet, etc.). Rebranchez le câble électrique.

=> Vérifiez toujours que la *Box* de votre Fournisseur d'Accès soit bien allumée et synchronisée **avant que de brancher électriquement** votre boîtier eniKma, sinon celui-ci échouera à dialoguer avec votre *Box*.

• Je n'accède pas à l'interface de mon boîtier eniKma via son adresse publique *(xxx.enikma.fr)*

Pour des raisons de sécurité, le boîtier eniKma n'est pas accessible par défaut depuis l'extérieur. Vous devez **explicitement** ouvrir la connexion distante pour que celui-ci soit accessible depuis l'Internet.
Pour cela vous devez d'abord modifier l'accès à l'administration de votre boîtier dans le menu *Configuration* afin que votre mot de passe ne soit pas le mot de passe « enikmavpn » fourni par défaut.
Ensuite, après le rechargement de la page (*F5* ou *Actualiser*), la section « *Connexion distante* » devient disponible, vous permettant de choisir l'option « *Oui* » permettant l'accès à distance par l'adresse que vous aurez choisie préalablement en vous connectant à votre Espace utilisateur sur www.enikma.fr.

• L'accès par l'extérieur de mon boîtier eniKma via son adresse publique *(xxx.enikma.fr)* **ne fonctionne plus.**

Lorsque vous changez de serveur VPN, l'ancien serveur que vous venez de quitter se met en « suspens » pendant une quinzaine de minutes. Si vous retournez sur ce serveur pendant ce court temps d'indisponibilité, vous pourrez naviguer sans problème sur l'Internet mais votre adresse publique ne fonctionnera plus (et donc vos applications nécessitant un accès depuis l'extérieur).

Si, par erreur, vous êtes revenus au serveur d'origine pendant ces 15 minutes, il vous suffit de choisir n'importe quel autre serveur VPN afin que tout rentre dans l'ordre.

• J'ai désactivé le Wi-Fi mais je n'ai aucun autre moyen de connexion que le Wi-Fi. Comment accéder à mon boîtier ?

Le boîtier eniKma a prévu cette situation en fournissant systématiquement quelques minutes de connexion Wi-Fi lors de tout redémarrage du boîtier, vous laissant le temps de modifier votre configuration.

• Je n'arrive pas à envoyer des mails avec le Webmail, bien que j'arrive à en recevoir.

Tout d'abord cela ne peut pas survenir tant que vous utilisez le Webmail de votre fournisseur de mail qui utilisera le port 80 commun à toute navigation Internet. En revanche, l'utilisation du Webmail présent dans le boîtier eniKma nécessite l'usage de ports distincts pour l'envoi (SMTP) et la réception (IMAP).

Quoiqu'il arrive, vous ne rencontrerez pas ce problème avec les messageries Gmail, Hotmail ou Yahoo. En revanche si vous utilisez l'adresse électronique fournie par votre Fournisseur d'accès Internet (FAI), il est possible que celui-ci vous oblige d'utiliser son propre réseau et non pas un VPN (c'est le cas d'*Orange*, par exemple). Nous ne saurions trop vous conseiller de quitter une messagerie qui vous imposerait cela. Vous pouvez garder votre FAI mais choisir une adresse électronique chez un fournisseur tiers (Gmail, Hotmail ou Yahoo, par exemple).

• Je veux expulser un utilisateur de mon application vocale Mumble

Si vous utilisez l'application mobile Plumble vous n'avez pas accès aux outils d'administration et vous ne pouvez donc pas expulser ou bannir un utilisateur. Cependant vous pouvez tout à fait

éteindre puis rallumer la fonction Vocale dans votre administration. Cela expulsera tous les utilisateurs. Avant de redémarrer la fonction Vocale, pensez à changer de mot de passe afin que l'intrus ne puisse pas revenir.

• Lorsque je me connecte sur mon interface via mon adresse publique « xxxx.enikma.fr » je suis parfois en *http://* et parfois en *https://*

Si vous vous connectez depuis chez vous, le boîtier eniKma détecte votre présence locale et reste en *http://* puisque le chiffrement n'aurait aucun intérêt. Si vous vous connectez à distance, le boîtier eniKma bascule immédiatement en *https://* afin de chiffrer la communication.

• Je veux redémarrer mon boîtier proprement mais je n'accède plus à mon administration.

Vous pouvez presser une fois le bouton « Reset » situé à côté de l'alimentation électrique, sur l'autre face (cerclé de rouge sur l'image).

Si ce redémarrage propre ne suffit pas, débranchez le câble électrique, patientez quelques secondes puis rebranchez.

Notez que ce bouton permet de démarrer le boîtier si celui-ci a été éteint de façon logicielle et que sa prise électrique est branchée.

• Le bouton « reset » du boîtier ne revient pas dans sa position initiale.

Il se peut que le bouton de la carte mère électronique ne soit pas exactement en face du loquet plastique. Dans ce cas le boîtier risque de ne jamais redémarrer. Pour faire revenir le bouton « reset », exercez une légère pression juste à côté de la prise d'alimentation électrique jusqu'à l'obtention du « clic » de retour du bouton.

• Mon accès distant pour un service (Webmail, par exemple) pointe sur un autre service (Vidéo, par exemple) !

Lorsque vous personnalisez l'adresse d'un dossier d'accès à un service, veillez à ne pas mettre une adresse que vous avez déjà utilisée pour un autre service !

• Autres problèmes

La plupart des problèmes que vous pourriez rencontrer ont déjà été soulevés et résolus. Rendez-vous sur :

- Le forum du Support technique sur le site www.enikma.fr ***(24h/24 et 7j/7)***
- La Foire Aux Questions (FAQ) sur le site www.enikma.fr
- Le dernier manuel en date sur le site www.enikma.fr

DEVELOPPEMENTS EN COURS

Le boîtier eniKma est un projet en constant développement. La plupart des développements sont le fruit du travail de notre équipe de Recherche & Développement, certains autres sont à l'initiative d'utilisateurs, ce que nous encourageons fortement, en particulier en collaboration avec nos équipes informatiques.

Toutes les nouvelles fonctionnalités logicielles sont fournies gratuitement aux utilisateurs par le biais des mises à jour. Celles-ci sont indiquées sur le fil d'actualité du site Web eniKma au fur et à mesure de leur survenue. Les nouvelles mises à jour sont indiquées aussi sur l'Interface d'administration du boîtier.