



Guide d'Installation

Version 7.2

Date : Mars 2025

Classification : Non classifié

Rédacteur : Team IKare

Bienvenue.....	3
1. Installation.....	3
1.1 Prérequis matériel	3
1.1.1 Licence monosonde.....	4
1.1.2 Licence multisondes	4
1.2 Prérequis d'installation	4
1.3 Installation du système d'exploitation à partir de l'image ISO.....	6
1.4 Installation de la solution IKare	17
1.4.1 Prérequis de paquets Debian	17
1.4.2 Lancement de l'installation IKare	18
2. Glossaire	29

Bienvenue

Ce guide vous accompagne dans l'installation de votre logiciel IKare.

IKare est un outil qui automatise la mise en place des meilleures pratiques de sécurité et du management des vulnérabilités.

1. Installation

1.1 Prérequis matériel

IKare peut être installé sur une ressource physique ou virtuelle.

Dans le cas d'une installation virtuelle, il convient donc de vérifier que votre CPU supporte la technologie de virtualisation et que celle-ci soit bien active sur votre système.

L'installation d'IKare a été validée sur les plateformes de virtualisation et versions suivantes :

- VMWareESXetFusion (ESXversion 6.7 et +, VMversion 14 et +), plus d'informations <https://www.vmware.com/>
- Hyper-V (version 10 et +), plus d'informations <https://docs.microsoft.com/> (menu virtualisation)
- Virtualbox (version 5.2.34_Ubuntu r133883 et +), plus d'informations <https://www.virtualbox.org/>
- KVM(version 2.11.1 et +), plus d'informations <https://www.linux-kvm.org/>

Les pré-requis matériels divergent en cas de licence multisondes, en cas de doute, veuillez vous rapprocher de votre interlocuteur Itrust

1.1.1 Licence monosonde

Dans le cas d'une licence monosonde (un seul IKare Master), les prérequis matériels sont les suivants pour la machine IKare :

- 4 processeurs d'architecture 64 bits
- 4 giga octets de RAM (8 giga octets sont recommandés au-dessus de 100 machines supervisées)
- Un disque dur de 64 giga octets

1.1.2 Licence multisondes

Dans le cas d'une licence multisondes (un IKare Master et plusieurs sondes externes), les prérequis minimaux pour une sonde externe sont ceux-ci :

Pour l'IKare Master :

- 4 processeurs d'architecture 64 bits
- 4 giga octets de RAM (8 giga octets sont recommandés au-dessus de 100 machines supervisées)
- Un disque dur de 64 giga octets

Pour une sonde externe IKare :

- 4 processeurs d'architecture 64 bits (4 processeurs sont recommandés)
- 4 giga octets de RAM (4 giga octets sont recommandés au-dessus de 100 machines supervisées)
- Un disque dur de 64 giga octets

1.2 Prérequis d'installation

Des paramètres réseau sont nécessaires pour effectuer la configuration lors de l'installation :

- **IP, Mask, Gateway** : il est recommandé de mettre en place des IP, Mask, Gateway fixes de la machine IKare
- **Proxy Web sortant** : il est nécessaire de connaître la configuration du Proxy Web sortant avec ou sans identifiant (login/pwd si utilisé)

Une connexion internet vers notre serveur **license.itrust.fr sur le port 443**. Cela est nécessaire pour enregistrer votre clé de licence, bénéficier des mises à jour et utiliser IKare de manière optimale.

L'installation de la solution IKare s'effectue en deux étapes :

(1) Installation du système d'exploitation hébergeant la solution IKare. L'installation du système d'exploitation peut être réalisée :

- directement par le client (machine virtuelle, ressource cloud...) en respectant les prérequis décrits ci-dessous (Cf. paragraphe 1.4.1 Prérequis de paquets Debian). Dans ce cas, vous pouvez directement accéder au paragraphe 2.4 Installation de la solution IKare
- À partir d'un ISO Debian téléchargeable sur notre serveur de licences (<http://license.itrust.fr/ikare/ikare-latest.iso>) et incluant les prérequis système nécessaires à l'installation de la solution IKare. (Cf. le paragraphe 1.3 Installation du système d'exploitation à partir de l'image ISO pour la description des étapes d'installation du système Debian)

(2) Installation de la solution IKare : l'installation de la solution IKare est décrite dans le paragraphe 1.4 Installation de la solution IKare

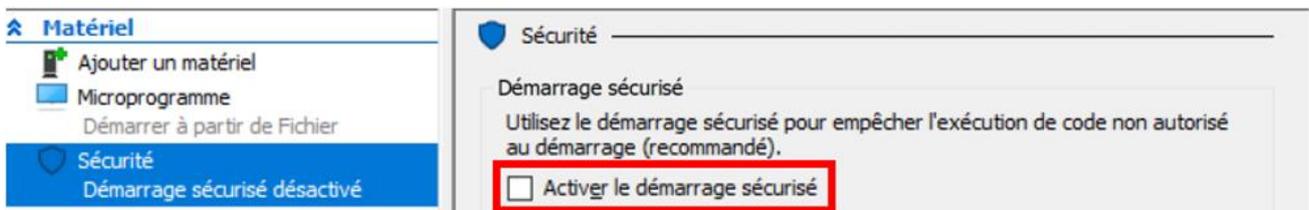
1.3 Installation du système d'exploitation à partir de l'image ISO

L'image ISO est l'image du CD d'installation du système d'exploitation Debian 11 (Bullseye) nécessaire au déploiement des services IKare.

⚠ Important : L'installation de l'ISO Debian va supprimer toutes les données pré-existantes sur le disque sans demande de confirmation.

i Note 1 : Dans le cas d'un environnement VMWare ESX, il est recommandé d'uploader l'image ISO dans la banque de données (ce qui nécessite des droits privilégiés).

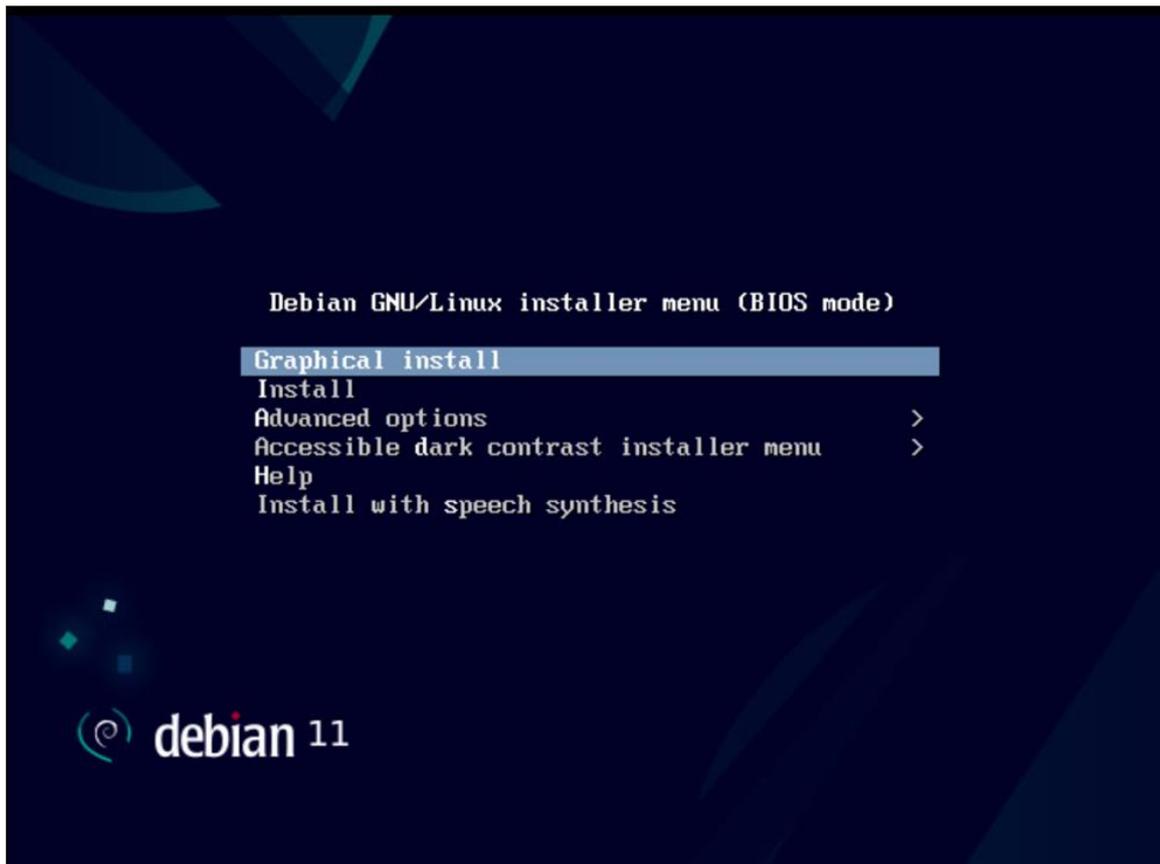
i Note 2 : Dans le cas d'un environnement Hyper-V, il est possible de choisir le mode de VM de type "Génération 2". Si vous n'arrivez pas à démarrer votre machine virtuelle, vous pouvez désactiver l'option de démarrage sécurisé (décocher l'option **Activer le démarrage sécurisé** dans le menu de configuration **Sécurité**)



Une fois la machine virtuelle créée avec les prérequis précédents, il suffit de démarrer la machine sur l'image ISO contenant le programme d'installation du système d'exploitation Debian.

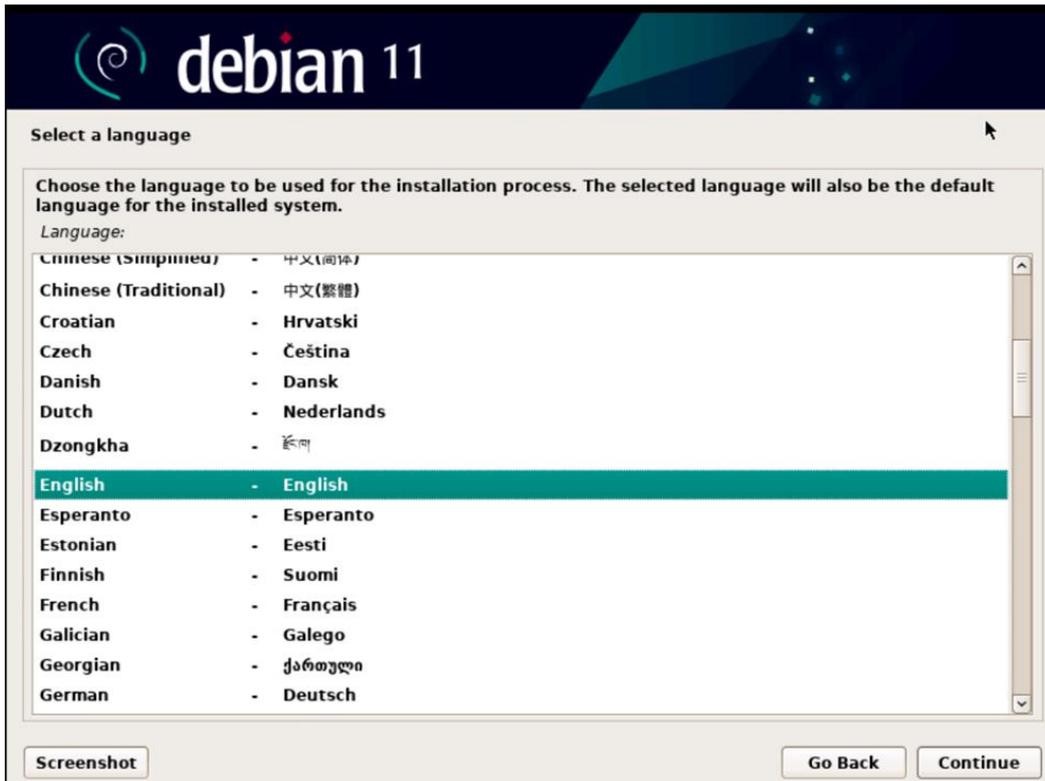
En premier lieu, vous devrez choisir le type d'installation pour la machine Debian. Les flèches haut et bas permettent de naviguer dans la liste des choix possibles. Vous devez sélectionner le mode **Graphical install**.

Une fois cette option sélectionnée, appuyez sur continuer.

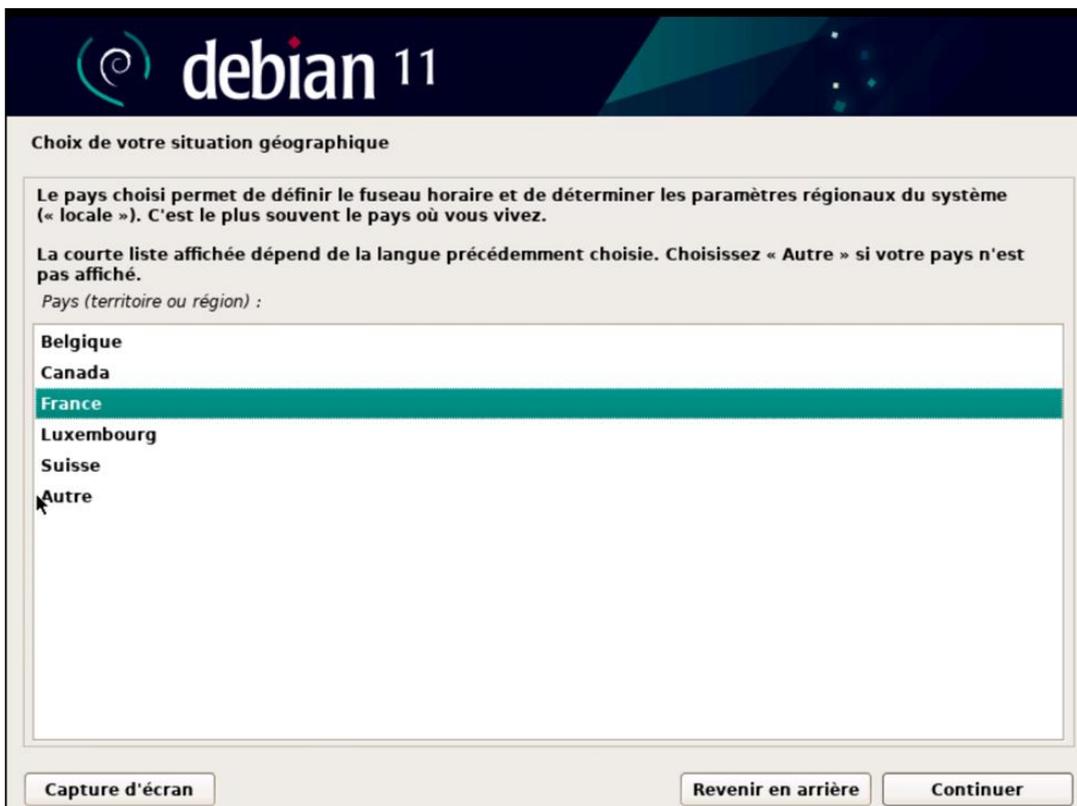


Vous devrez ensuite choisir la langue d'installation. Les flèches haut et bas permettent de naviguer dans la liste de langues possibles.

Une fois la langue choisie, appuyez sur continuer.



De la même façon, choisissez la zone géographique puis appuyez sur continuer.



Ainsi que la configuration du clavier puis appuyez sur entrée.

Configurer le clavier*Disposition de clavier à utiliser :*

Danois
Néerlandais
Dvorak
Dzongkha
Espéranto
Estonien
Éthiopien
Finnois
Français
Géorgien
Allemand
Grec
Gujarati
Gourmoukhi
Hébreu
Hindi
Hongrois

Capture d'écran

Revenir en arrière

Continuer

Si votre machine n'est pas connectée au réseau internet ou si la configuration réseau (DHCP par exemple) échoue, la fenêtre suivante s'affichera pour vous indiquer l'échec de configuration automatique du réseau. Appuyez sur continuer pour accéder à la fonction de configuration manuelle du réseau.

Configurer le réseau



La configuration automatique a échoué

Le protocole DHCP n'est probablement pas utilisé sur le réseau. Il est également possible que le serveur DHCP soit lent ou que certains équipements réseau ne fonctionnent pas correctement.

Capture d'écran

Continuer

L'écran suivant vous permet de réessayer la configuration automatique du réseau ou de configurer manuellement la configuration du réseau.

Configurer le réseau

Vous pouvez maintenant réessayer la configuration automatique du réseau, - cela peut réussir si le serveur DHCP met du temps à répondre -, ou bien vous pouvez configurer vous-même le réseau. Certains serveurs DHCP demandent qu'un hôte DHCP soit donné par le client, vous pouvez l'indiquer avant de réessayer la configuration automatique.

Méthode pour la configuration du réseau :

Réessayer la configuration automatique du réseau

Réessayer la configuration automatique avec un nom d'hôte DHCP

Configurer vous-même le réseau

Ne pas configurer le réseau maintenant

Capture d'écran

Revenir en arrière

Continuer

Les écrans suivants vous permettent de configurer la machine IKare sur le réseau :

- Choix du nom de la machine (valeur par défaut **ikare-scanner**), appuyez sur continuer.

Configurer le réseau

Veillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

Capture d'écran

Revenir en arrière

Continuer

- Choix du domaine de la machine (valeur vide par défaut), appuyez sur continuer.

Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

Domaine :

Capture d'écran

Revenir en arrière

Continuer

L'installation des éléments de base du système Debian démarre.

Les deux écrans suivants concernent la configuration de la sélection d'un miroir Debian. Vous pouvez laisser les valeurs présélectionnées et appuyez sur continuer sur les 2 écrans.

Puis

Configurer l'outil de gestion des paquets

Veillez choisir un miroir de l'archive Debian. Vous devriez utiliser un miroir situé dans votre pays ou votre région si vous ne savez pas quel miroir possède la meilleure connexion Internet avec vous.

Généralement, deb.debian.org est un choix pertinent.

Miroir de l'archive Debian :

- ftp.fr.debian.org
- debian.proxad.net
- deb-mir1.naitways.net
- murol.dc.univ-lorraine.fr
- ftp.u-picardie.fr
- ftp.u-strasbg.fr
- deb.debian.org**
- debian-archive.trafficmanager.net
- ftp.ec-m.fr
- mirror.plusserver.com
- debian.mirror.ate.info
- debian.univ-tlse2.fr
- ftp.rezopole.net
- debian.univ-reims.fr

Capture d'écran

Revenir en arrière

Continuer

Ensuite, l'écran suivant vous permet de configurer une adresse proxy (authentifiée ou non) pour que la machine virtuelle en cours d'installation puisse communiquer avec l'extérieur du réseau. Si vous n'avez pas de configuration proxy, laissez le champ de saisie vide et appuyez sur continuer.

Configurer l'outil de gestion des paquets

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

Les paramètres du mandataire doivent être indiqués avec la forme normalisée « http://[[utilisateur]:[mot-de-passe]@]hôte[:port]/ ».

Mandataire HTTP (laisser vide si aucun) :

Capture d'écran

Revenir en arrière

Continuer

Pour finir, le menu de configuration du gestionnaire de démarrage apparaît. Il faut sélectionner la partition (Ex : /dev/sda) avec les flèches et ne pas sélectionner l'option **Choix manuel du périphérique**. Appuyez sur continuer.

Installer le programme de démarrage GRUB

Le système nouvellement installé doit pouvoir être démarré. Cette opération consiste à installer le programme de démarrage GRUB sur un périphérique de démarrage. La méthode habituelle pour cela est de l'installer sur le disque principal (partition UEFI ou secteur d'amorçage). Vous pouvez, si vous le souhaitez, l'installer ailleurs sur un autre disque, une autre partition, ou même sur un support amovible.

Périphérique où sera installé le programme de démarrage :

Choix manuel du périphérique

/dev/sda

Capture d'écran

Revenir en arrière

Continuer

A ce stade, le paramétrage basique de la machine virtuelle est terminé. Le processus va poursuivre l'installation du système (étapes de plusieurs minutes).

Une fois l'installation du système d'exploitation Debian terminée, la fenêtre de login apparaît.

```
Debian GNU/Linux 11 ikare-scanner tty1
ikare-scanner login: _
```

Vous disposez d'un compte d'installation de la solution IKare.

Le compte d'installation IKare est "**ikareinstall**", le mot de passe par défaut est "**se[o@ph3Cees**". C'est avec ce compte que vous allez effectuer l'installation des services IKare.

⚠ Important : Il s'agit d'un compte uniquement utilisable pour l'installation de la solution IKare. Il ne sera plus utilisable une fois IKare installé.

L'installation de la solution IKare est décrite au paragraphe **1.4.2 Lancement de l'installation IKare**

1.4 Installation de la solution IKare

1.4.1 Prérequis de paquets Debian

Le système d'exploitation nécessaire pour l'installation et l'utilisation de notre solution IKare est Debian 11 (bullseye) minimaliste ayant les paquets suivants installés :

- gnupg ou gnupg2
- sudo
- ca-certificates
- curl
- openssh-server
- dialog
- jq

Un compte d'installation **ikareinstall** sudoer est nécessaire pour lancer l'installation de la solution IKare et doit disposer d'un répertoire de connexion pointant sur le chemin suivant : /home/ikareinstall.

1.4.2 Lancement de l'installation IKare

Connectez-vous sur la machine IKare avec le compte **ikareinstall** pour lancer les commandes d'installation suivantes :

- Si le système d'exploitation a été installé à partir de l'image ISO de notre kit d'installation :

```
cd /home/ikareinstall
sudo ./ikare_install.sh 2>&1 | tee ikare-install.log
```

- Si le système d'exploitation a été installé directement par le client sans utiliser l'ISO ITrust :

```
cd /home/ikareinstall
```

```
curl https://license.itrust.fr/ikare/ikare_install.sh -o ikare_install.sh && chmod +x
ikare_install.sh sudo ./ikare_install.sh 2>&1 | tee ikare-install.log
```

Au lancement du script d'installation, une question vous est posée pour savoir si vous souhaitez installer un IKare Master (choix **m**) ou une sonde IKare (choix **p**).

```
Do you want to install a master (m) or a probe (p) ? [m/p] (default: m)
```

Après avoir saisi votre choix, validez votre choix avec le bouton "Entrée".

L'installation des différents paquets et services, ainsi que la synchronisation de la base de vulnérabilité peut prendre plusieurs minutes (voire dizaines de minutes en fonction du flux réseau disponible entre la machine et le serveur de licences ITrust).

Une fois l'installation terminée, la machine va redémarrer.

Une fois la machine redémarrée, si vous êtes sur la console de votre hyperviseur, l'invite de commande suivant apparaît pour vous permettre de vous connecter à l'écran d'administration SSH d'IKare

```
IKARE by INFLUX
6.0.0                an Innovative Solution

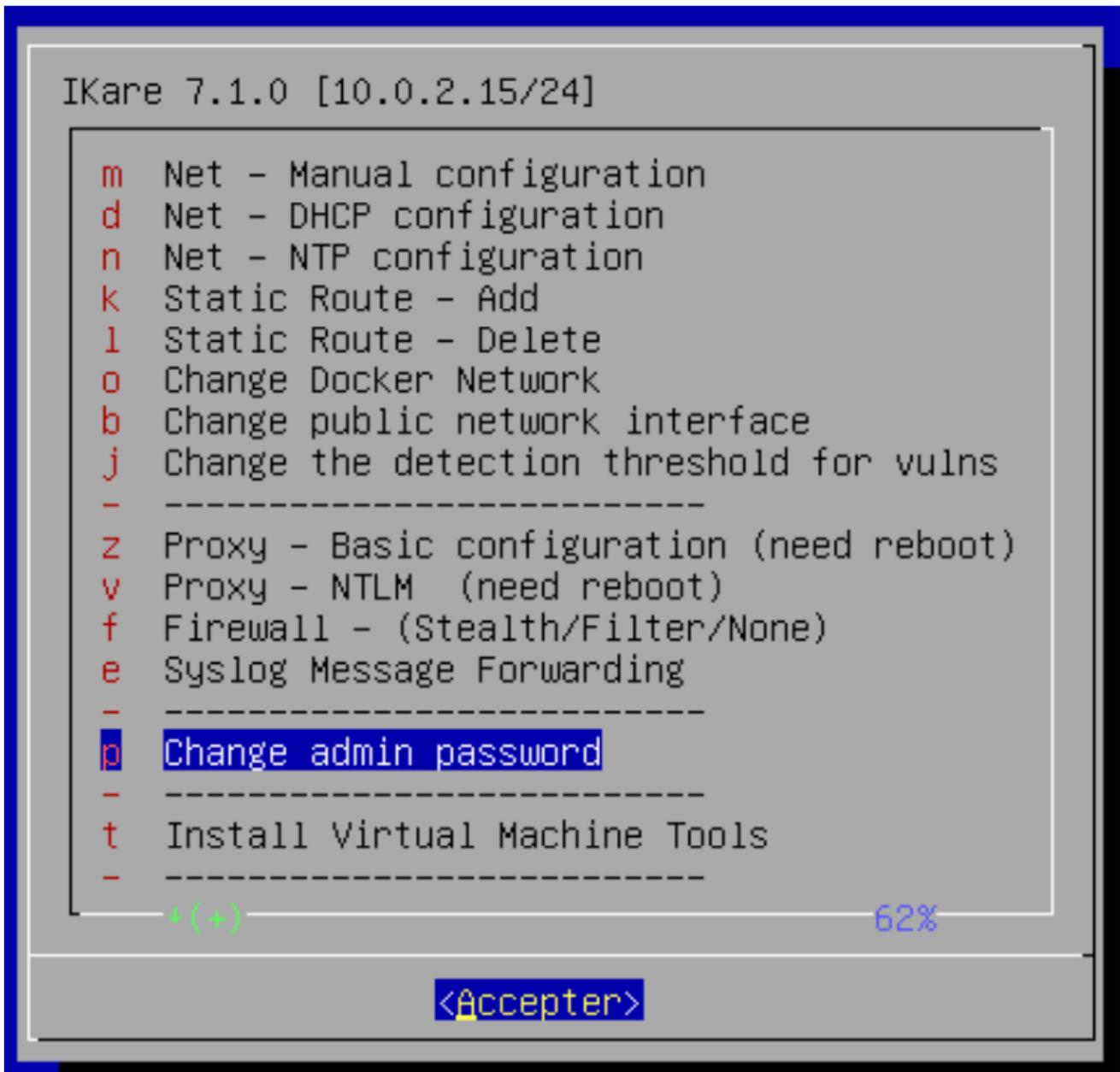
Access the graphical web interface at https://10.31.30.24
or the administration console through ssh admin@10.31.30.24

ikare-scanner login:
```

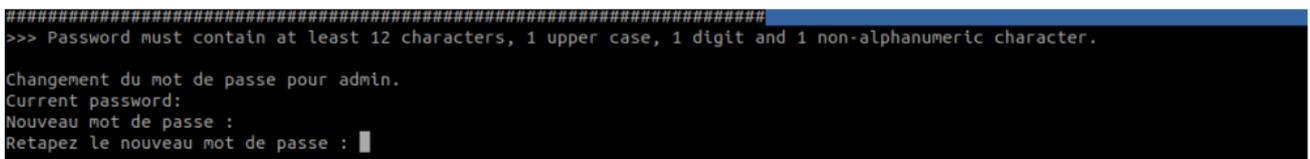
Le compte d'administration de la machine est "**admin**", le mot de passe par défaut est "**IkareCh4ng3!**".

Une fois loggé en tant qu'admin, vous arrivez sur le menu admin ssh. Votre adresse IP apparaît en haut et, après l'installation complète, vous pourrez vous connecter par la suite avec votre navigateur à l'interface web avec l'adresse <https://votreadresseIP/> A cette adresse, le compte d'utilisation par défaut de l'interface web est "**admin**", le mot de passe par défaut est "**admin**". Il vous sera demandé de modifier ce mot de passe, à la première connexion.

Il convient, avant tout, de modifier votre mot de passe du compte "admin" de la machine. Aussi, déplacez-vous sur le menu p (**Change admin password**) à l'aide des flèches de votre clavier et appuyez sur la touche "Entrée".



En bas du menu, s'affiche successivement les trois étapes du changement du mot de passe.



Appuyez sur “Entrée” après avoir tapé chaque mot de passe. Lorsque le troisième est validé, vous revenez sur le menu admin.

Il faut maintenant procéder à l’enregistrement de votre licence. Aussi, déplacez-vous sur le menu l (**Ikare license register**) à l’aide des flèches de votre clavier et appuyez sur “Entrée”.

IKare 7.0.2 [10.31.30.161/24]

```
m Net - Manual configuration
d Net - DHCP configuration
n Net - NTP configuration
k Static Route - Add
l Static Route - Delete
o Change Docker Network
b Change public network interface
j Change the detection threshold for vulns
- -----
z Proxy - Basic configuration (need reboot)
v Proxy - NTLM (need reboot)
f Firewall - (Stealth/Filter/None)
e Syslog Message Forwarding
- -----
p Change admin password
- -----
t Install Virtual Machine Tools
- -----
i Import certificates
- -----
c Test Network Connectivity
I Ikare license register
g Generate diagnostic logs file
s Change IKare update mode
u Check and Run upgrades
r Reboot
h Shutdown
- -----
↓(+)
```

96%

<Accepter>

Entrez votre numéro de licence Ikare puis validez en appuyant sur “Entrée”.

```
----- Press "ctrl + c" to exit -----
#####
>>> Register your license number

Write your license number:
59c923f54f2545a095165a23163d4c88
#####
>>> Please verify your license before continuing

59c923f54f2545a095165a23163d4c88
Is this correct? (y/n):
y
License data:
* usage: 3
* was_valid: False
* consultant: False
* company: Mika
* secret: U91A652IJTKM2699
* ips: 142
* token: 59c923f54f2545a095165a23163d4c88
* expiration: 2021-06-01 00:00:00+02:00
* demo: False
* duration: 365
* sondes: 3
* validation: 2020-06-02 11:31:47.635404+02:00
* id: 2712
License register ended.
If we have any problems, please contact Ikare support.
You can now upgrade to Ikare premium solution using right entry in the menu.
Please hit RETURN to continue...
-
```

La procédure va vous demander de confirmer que le numéro est correct en tapant y et en appuyant sur "Entrée". Si vous observez les données de licence, votre licence est donc bien enregistrée. Tapez "Entrée" pour revenir au menu.

Il faut maintenant procéder au test de connectivité. Aussi, déplacez-vous sur le menu C (**Test Network Connectivity**) à l'aide des flèches de votre clavier et appuyez sur "Entrée".

Menu C - Test Network Connectivity : test de connexion au serveur de licence

IKare 7.0.2 [10.31.30.161/24]

↑(-)

- v Proxy - NTLM (need reboot)
- f Firewall - (Stealth/Filter/None)
- e Syslog Message Forwarding
- -----
- p Change admin password
- -----
- t Install Virtual Machine Tools
- -----
- i Import certificates
- -----
- c** **Test Network Connectivity**
- I Ikare license register
- g Generate diagnostic logs file
- s Change IKare update mode
- u Check and Run upgrades
- r Reboot
- h Shutdown
- -----

↓(+)

96%

<Accepter>

Le programme va dérouler quelques tests réseaux permettant de valider le bon paramétrage réseau de votre machine et les accès aux servers Ikare. Pour sortir du test et revenir au menu, tapez les touches "Ctrl" et "C" sur votre clavier.

```

Your Network Interface:
IFACE lo 127.0.0.1 loopback
IFACE ens192 10.31.30.24 ether
IFACE br 203.0.133.254 ether
IFACE docker0 172.17.0.1 ether

Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref      Use Iface
0.0.0.0          10.31.30.254   0.0.0.0          UG    0      0      0 ens192
10.31.30.0       0.0.0.0         255.255.255.0    U    0      0      0 ens192
172.17.0.0       0.0.0.0         255.255.0.0      U    0      0      0 docker0
203.0.133.0      0.0.0.0         255.255.255.0    U    0      0      0 br-2003aca6caff

OK: Default Route Detected
PING 10.31.30.254 (10.31.30.254) 56(84) bytes of data.
64 bytes from 10.31.30.254: icmp_seq=1 ttl=255 time=2.01 ms
64 bytes from 10.31.30.254: icmp_seq=2 ttl=255 time=0.347 ms
64 bytes from 10.31.30.254: icmp_seq=3 ttl=255 time=0.270 ms

--- 10.31.30.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 35ms
rtt min/avg/max/mdev = 0.270/0.874/2.005/0.800 ms
OK: Gateway @10.31.30.254 Ping Successful
OK: DNS Settings Detected
PING 10.31.10.10 (10.31.10.10) 56(84) bytes of data.
64 bytes from 10.31.10.10: icmp_seq=1 ttl=63 time=0.571 ms
64 bytes from 10.31.10.10: icmp_seq=2 ttl=63 time=2.00 ms
64 bytes from 10.31.10.10: icmp_seq=3 ttl=63 time=3.10 ms

--- 10.31.10.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 21ms
rtt min/avg/max/mdev = 0.571/1.888/3.097/1.034 ms
OK: DNS @10.31.10.10 Ping Successful
PING license.itrust.fr (163.172.62.226) 56(84) bytes of data.
64 bytes from license.itrust.fr (163.172.62.226): icmp_seq=1 ttl=52 time=14.2 ms
64 bytes from license.itrust.fr (163.172.62.226): icmp_seq=2 ttl=52 time=13.0 ms
64 bytes from license.itrust.fr (163.172.62.226): icmp_seq=3 ttl=52 time=21.2 ms

--- license.itrust.fr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 13.001/16.133/21.213/3.625 ms
OK: license.itrust.fr Ping Successful
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
OK: Connect license.itrust.fr Successful
OK: Connectivity Test run SUCCESSFULLY

You can run a traceroute to the IP or Hostname of your choice (CTRL-C to break)::

```

Pour la sécurité de Ikare, il est fourni des certificats SSL par défaut. Vous avez néanmoins la possibilité de changer ces certificats et y installer les vôtres. Déplacez-vous sur le menu i (**Import certificates**) à l'aide des flèches de votre clavier et appuyez sur "Entrée".

IKare 7.0.2 [10.31.30.161/24]

↑(-)

```
z Proxy - Basic configuration (need reboot)
v Proxy - NTLM (need reboot)
f Firewall - (Stealth/Filter/None)
e Syslog Message Forwarding
- -----
p Change admin password
- -----
t Install Virtual Machine Tools
- -----
t Import certificates
- -----
c Test Network Connectivity
I Ikare license register
g Generate diagnostic logs file
s Change IKare update mode
u Check and Run upgrades
r Reboot
h Shutdown
```

↓(+)

93%

<Accepter>

L'écran suivant permet soit :

- d'afficher les certificats déjà importés (choix 2, 3 ou 4)
- d'importer des nouveaux certificats (choix 1)
- de restaurer les certificats par défaut d'IKare (choix 5).

```
-----  
-- Press "ctrl + c" to exit --  
-----  
  
#####  
>>> Import SSL certificates  
  
1 - Import certificates  
2 - Show imported certificate file  
3 - Show imported key file  
4 - Show imported ca file  
5 - Restore default certificates  
Your choice (1, 2, 3, 4 or 5):
```

Si vous souhaitez importer vos propres certificats, vous devez générer vos certificats SSL avec une clé d'encryptage (clé RSA 4096 bits conseillé, au format PEM) et définir dans le certificat les informations suivantes pour la machine IKare :

- Country
- State
- Organization
- FQDN
- Mail address
- Subject Name incluant la machine IKare (wildcard sur un domaine de votre organisation ou le nom DNS de la machine IKare ou son IP lorsqu'elle est fixe).

Lors de l'importation de vos certificats dans IKare, vous devez appliquer les règles suivantes :

- Import du certificat : insérez le contenu base64 du certificat
 - Il doit commencer par la chaîne : -----BEGIN CERTIFICATE-----
 - Et se terminer par la chaîne -----END CERTIFICATE-----
- Import de la clé privée : insérez le contenu base64 de la clé privée
 - Elle doit commencer par la chaîne : -----BEGIN RSA PRIVATE KEY-----
 - Et se terminer par la chaîne -----END RSA PRIVATE KEY-----
- Import du certificat de l'autorité de certification (CA) : vous devez importer l'ensemble de la chaîne de certification (il faut éventuellement importer tous les certificats intermédiaires jusqu'au certificat racine du CA. Dans le cas où le certificat CA contient une chaîne de certification, insérez les certificats dans l'ordre du premier certificat intermédiaire et terminez par le certificat racine) :
 - Chaque certificat ajouté doit commencer par la chaîne : -----BEGIN CERTIFICATE-----
 - Et se terminer par la chaîne -----END CERTIFICATE-----

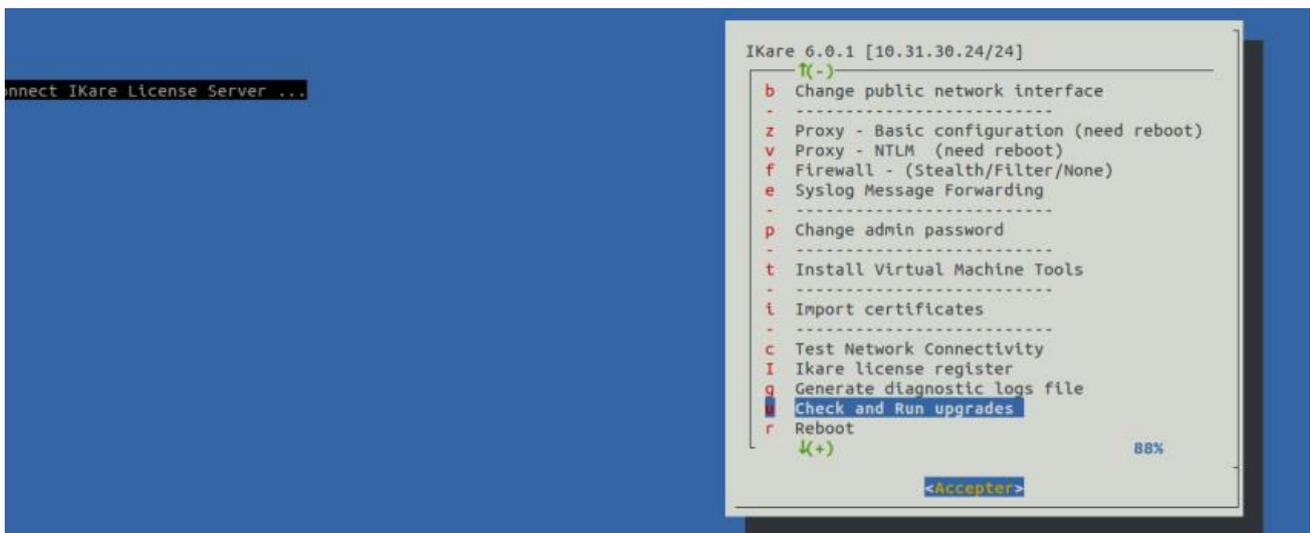
i Note : Pour vérifier si votre certificat CA est un certificat intermédiaire ou un racine, vous pouvez exécuter la commande :

```
` openssl x509 -text -noout -in `
```

Si le CN de la partie “**Issuer**” et “**Subject**” sont identiques, il s’agit d’un certificat racine. Sinon, il s’agit d’un certificat intermédiaire, il est donc nécessaire d’ajouter également le certificat CA ayant comme partie “Subject” la valeur de la partie “Issuer” du certificat intermédiaire (et ainsi de suite pour atteindre le certificat racine). Vous pouvez vous procurer ce certificat racine auprès de l’autorité ayant délivré le certificat pour votre organisation.

sos En cas de problème lors de cette configuration, le support ITrust peut vous aider dans le déploiement de vos propres certificats.

Pour finir, il faut maintenant procéder au test de vérification de mise à jour. Aussi, déplacez-vous sur le menu u (**Check and Run upgrades**) à l’aide des flèches de votre clavier et appuyez sur “Entrée”.



Voilà, votre installation est terminée, vous pouvez maintenant accéder à votre logiciel avec votre navigateur en interface web avec l’adresse <https://votreadresseIP/>. Le compte d’utilisation par défaut de l’interface web est “**admin**”, le mot de passe par défaut est “**admin**”. Lors de votre première connexion, il vous sera demandé de modifier ce mot de passe par défaut et de renseigner votre mot de passe personnalisé.



Dans le cas où l'interface web ne répondrait pas (ex. erreur HTTP 502) :

502 Bad Gateway

nginx

Veuillez effectuer un dernier Reboot (menu r) pour relancer le service web.

```
IKare 7.0.2 [10.31.30.161/24]
↑(-)
f Firewall - (Stealth/Filter/None)
e Syslog Message Forwarding
- -----
p Change admin password
- -----
t Install Virtual Machine Tools
- -----
i Import certificates
- -----
c Test Network Connectivity
I Ikare license register
g Generate diagnostic logs file
s Change IKare update mode
u Check and Run upgrades
r Reboot
h Shutdown
- -----
Q Quit Menu

100%

<Accepter>
```

i Nous vous invitons à suivre le [guide d'administration](#) pour découvrir le fonctionnement du logiciel et de son paramétrage.

2. Glossaire

- Scan: Fait de balayer un ensemble de paramètres et de données.
- Asset: Equipement ou ressource informatique.
- Probe: Sonde
- Grades: Notes ou évaluations