MediData

Annexe technique MediData Appliance (français)

La notice ci-après présuppose des connaissances au niveau réseau et système d'exploitation. Veuillez consulter votre interlocuteur pour le logiciel de votre cabinet ou le spécialiste responsable du système de réseau (si existant).

Historique des modifications

Version rév.	Description de la modification	Date de modification	Auteur
0.1	Première version de la documentation	Jul 20, 2021	Manuel Gebistorf (gem)
1.0	Publication	Sep 7, 2021	Manuel Gebistorf (gem)
1.1	Description plage IP 172.x.x.x complétée	Sep 8, 2021	Manuel Gebistorf (gem)

Contenu:

MediData

Conditions préalables

La MediData Appliance doit être allumée et connectée à Internet.

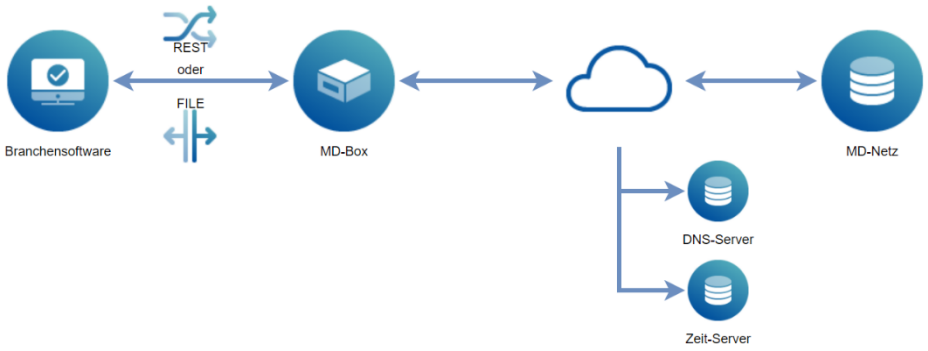
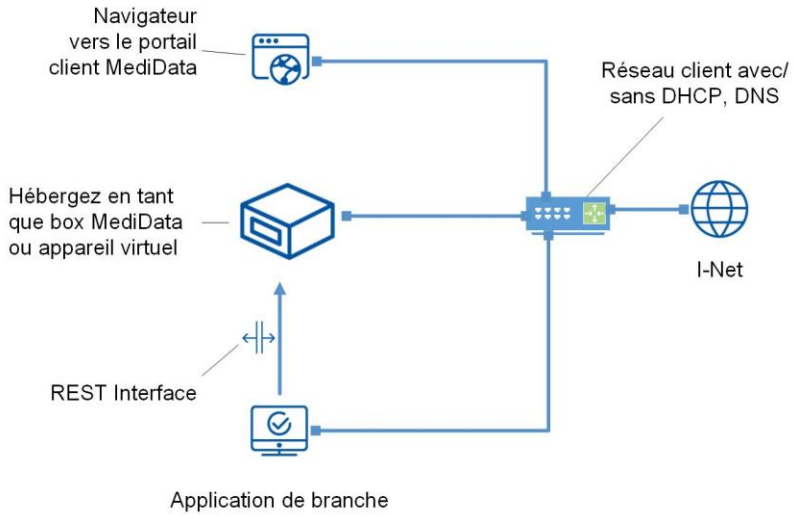


Schéma du réseau client



Joignabilité

Les adresses suivantes sont accessibles par l'intermédiaire des ports mentionnés. Veillez à ce que les ports du réseau soient libres:

Système productif

MediData

Objectif	Port	Objet
sshmdclient.medidata.ch	TCP 9022	Lien de gestion avec MediData (SSH)
wsr.medidata.ch	TCP 443	Lien de gestion avec MediData (SSL)
Tous*	UDP 123	Synchronisation temporelle
Prescrit par le DHCP Client	UDP 53	Résolution du nom

*Pour la synchronisation temporelle, CentOS utilise l'infrastructure de réseau proposée par le projet https://www.ntppool.org/de/.

Système ACC

Objectif	Port	Objet
sshmdclient-acc.medidata.ch	TCP 9022	Lien de gestion avec MediData (SSH)
wsr-acc.medidata.ch	TCP 443	Lien de gestion avec MediData (SSL)
Tous*	UDP 123	Synchronisation temporelle
Prescrit par le DHCP Client	UDP 53	Résolution du nom

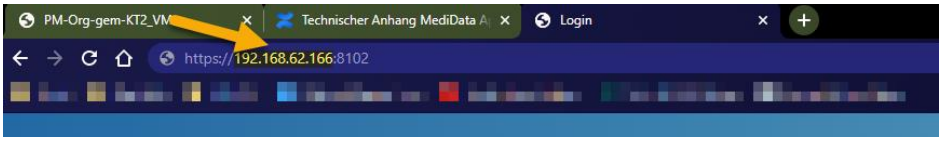
*Pour la synchronisation temporelle, CentOS utilise l'infrastructure de réseau proposée par le projet https://www.ntppool.org/de/.

Page d'accueil de la configuration

Il existe une page d'accueil sécurisée pour l'ensemble de la configuration de la MediData Appliance.

→ La MediData Appliance doit être allumée. Si la MediData Appliance est éteinte, allumez-la et attendez qu'elle ait démarré.

→ Entrez l'URL suivante dans la barre d'adresse de votre navigateur Internet.

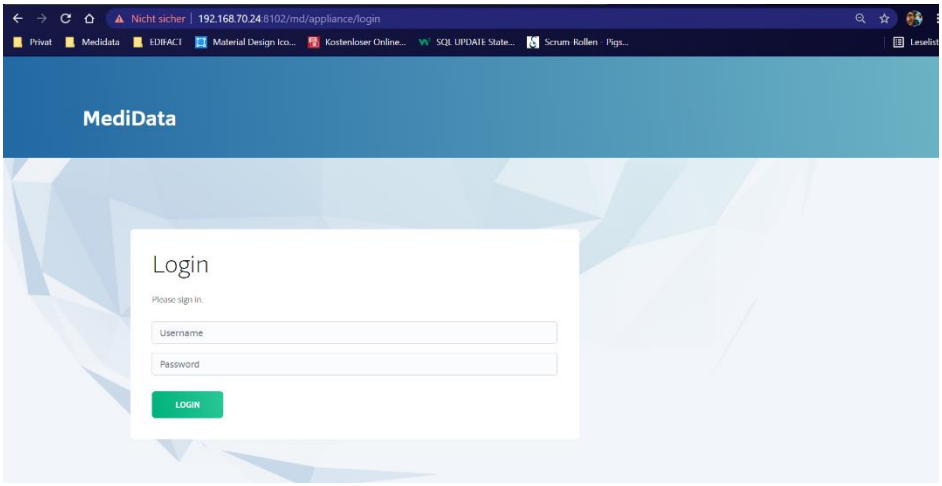


Notez que la partie marquée en jaune peut varier. L'URL entrée ici n'est qu'un exemple. Vous trouverez l'adresse IP correcte à entrer sur le portail clients p. ex.

Réseau sans DHCP

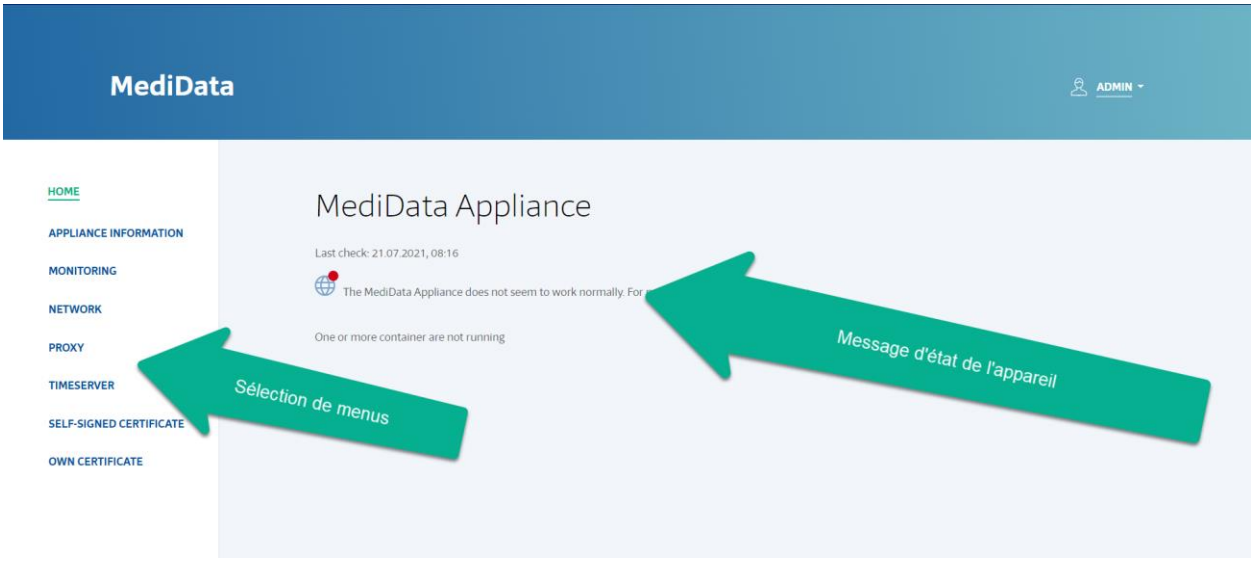
Si la MediData Appliance se trouve au sein d'un réseau qui ne soutient pas DHCP, aucune adresse IP ne sera attribuée. Si tel est le cas, vous pouvez joindre l'Appliance en passant par l'adresse IP **169.254.99.198**.

→ Ensuite, vous pouvez vous connecter à la Management UI par la fenêtre de login. L'Appliance est fournie avec: Username = admin, Password = admin.



Après connexion, vous arriverez sur la page 'Home' de la Management UI

MediData



Messages d’état

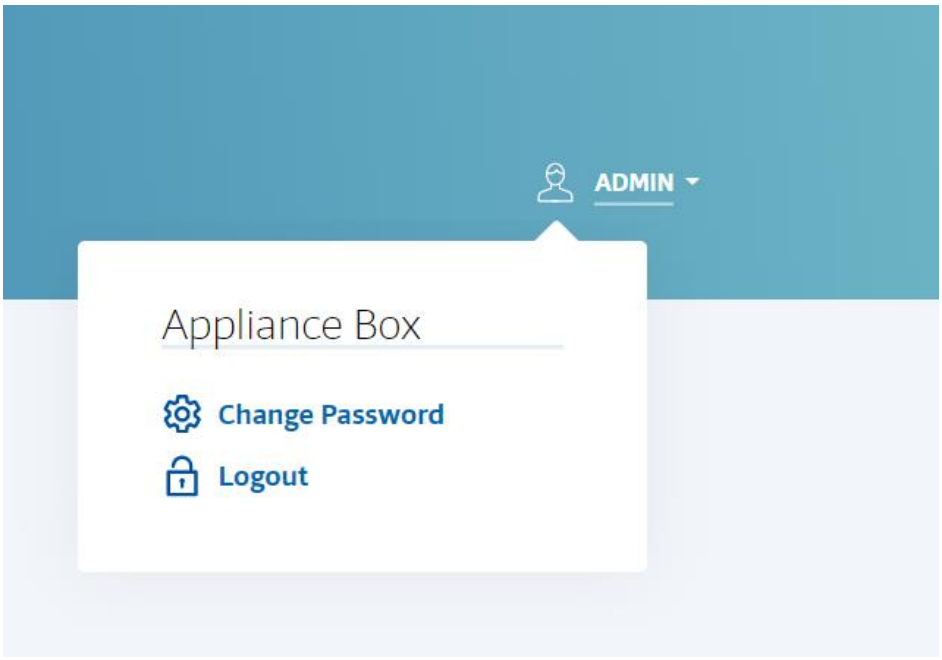
Les messages d’état sont consultés selon un intervalle de temps défini et apparaissent dans le menu 'Home'.

- Last Check: horodatage de la dernière base de données
- Statut: il existe deux statuts;
  - vert → tout est OK
  - rouge → il y a des problèmes au niveau de l’Appliance qui pourraient perturber la transmission des données. Le problème s’affiche sous forme de texte.

Paramètres de l’utilisateur

En cliquant sur le bouton 'Admin', vous pouvez modifier le mot de passe de la Management UI ou vous déconnecter.

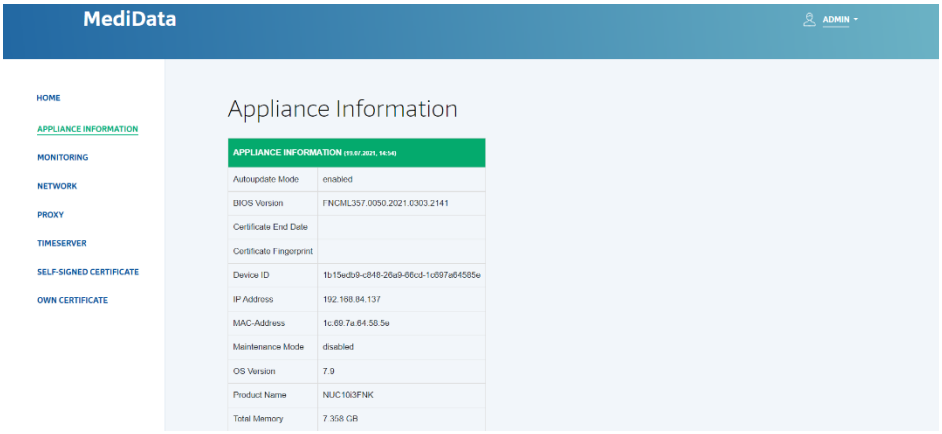
MediData



MediData

Informations sur l'Appliance

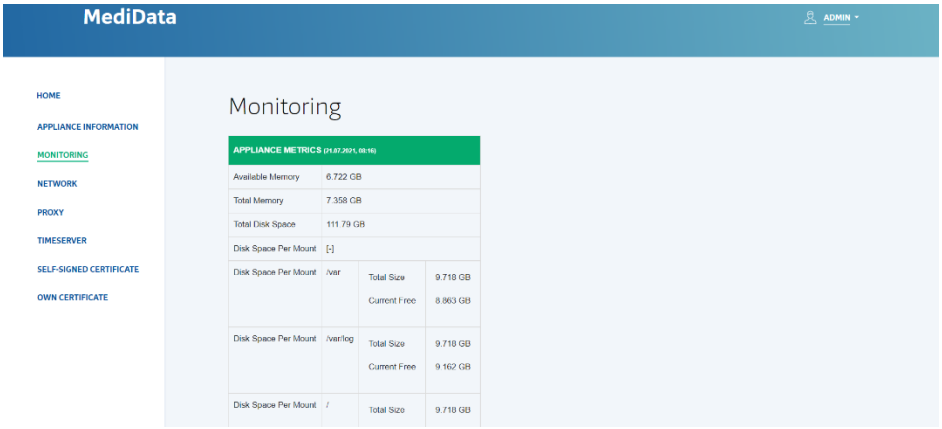
Ce menu affiche des informations (essentiellement statiques) sur l'Appliance.



Ces informations peuvent aussi être consultées sur l'interface REST.

Métriques de l'Appliance (monitoring)

Ce menu contient des métriques sur l'Appliance (informations dynamiques comme la mémoire utilisée).

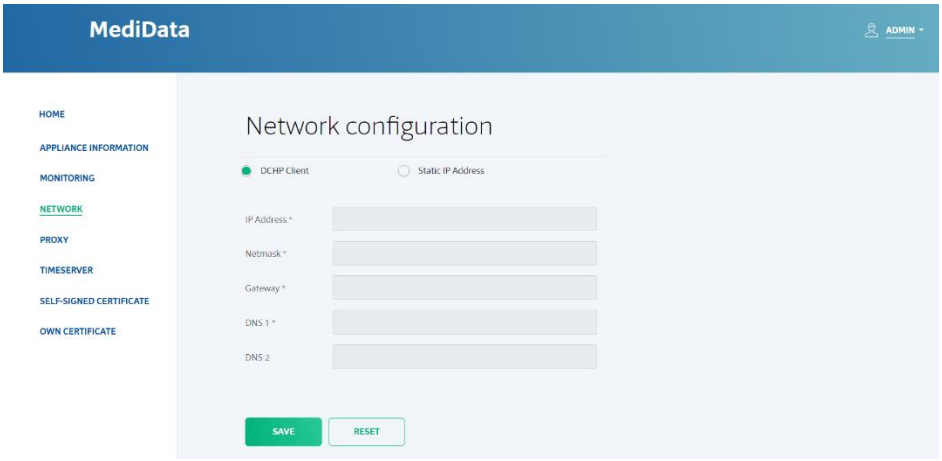


Ces informations peuvent aussi être consultées sur l'interface REST.

MediData

Configuration réseau

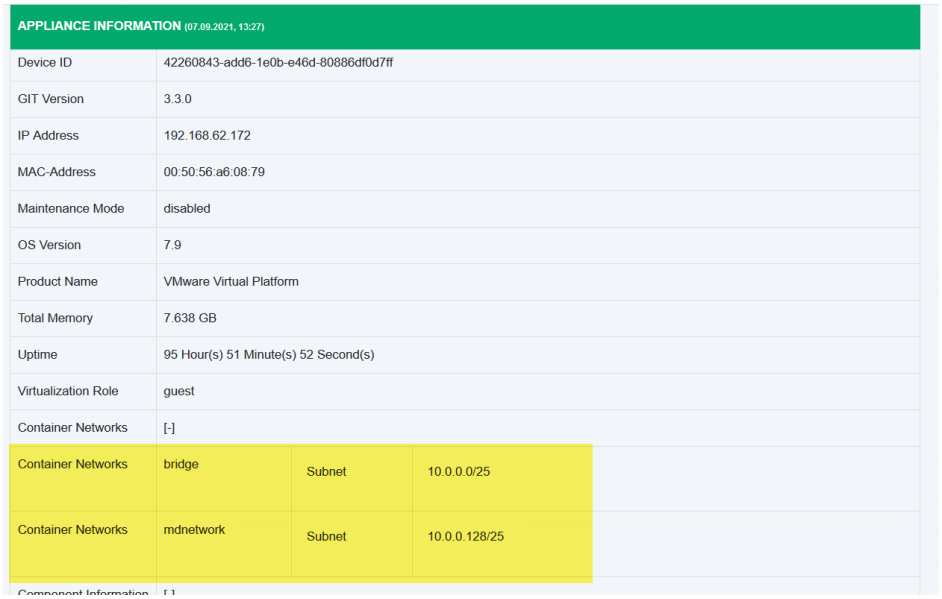
L’adresse IP de l’Appliance peut être paramétrée de DHCP à Fixe dans le menu 'Configuration réseau'.



Les champs suivis d’un * doivent être complétés.

Réseau docker interne

La plage d’adresses IP 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) est réservée à l’usage interne. Si le réseau côté client est configuré dans cette plage, l’Appliance le détectera lors d’un redémarrage et basculera le réseau interne sur la plage 10.0.0.0/8. La plage d’adresses utilisée pour le secteur interne est consultable sur la Management UI sous 'Appliance Information'.

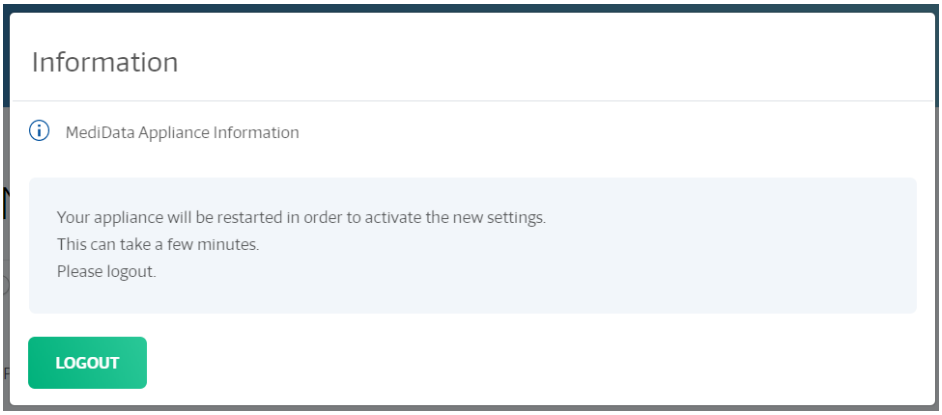


APPLIANCE INFORMATION (07.09.2021, 13:27)			
Device ID	42260843-add6-1e0b-e46d-80886df0d7ff		
GIT Version	3.3.0		
IP Address	192.168.62.172		
MAC-Address	00:50:56:a6:08:79		
Maintenance Mode	disabled		
OS Version	7.9		
Product Name	VMware Virtual Platform		
Total Memory	7.638 GB		
Uptime	95 Hour(s) 51 Minute(s) 52 Second(s)		
Virtualization Role	guest		
Container Networks	[-]		
Container Networks	bridge	Subnet	10.0.0.0/25
Container Networks	mdnetwork	Subnet	10.0.0.128/25
Component Information	[-]		

MediData

Si le réseau au sein duquel opère l’Appliance est 'caché’ derrière une plage d’adresses IP 172.16.0.0/12 (172.16.0.0 – 172.31.255.255), le réseau interne devra être configuré via le menu 'internal Network'. Mais ceci ne devrait être nécessaire que dans des cas isolés.

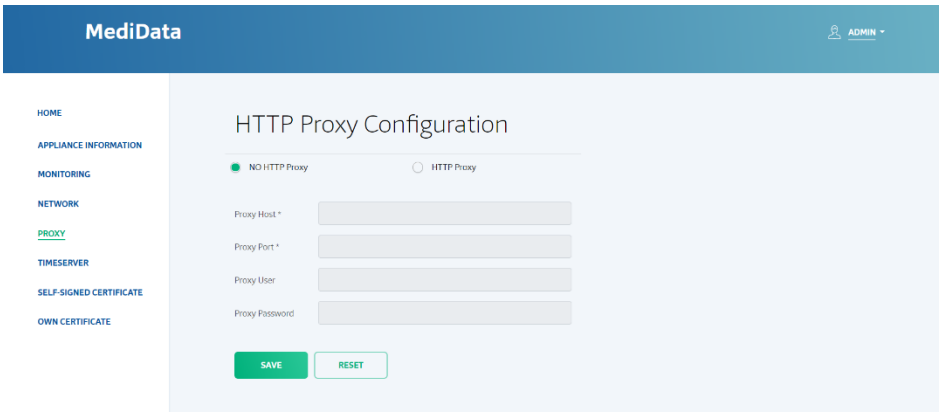
Après l’entrée des adresses et la sauvegarde, l’utilisateur doit se déconnecter. Il peut le faire par le biais du dialogue suivant. L’Appliance redémarrera.



Configurer le serveur proxy

Ce menu permet de configurer un proxy HTTP propre.

La MediData Appliance est préparamétrée comme «NO http Proxy». Si vous souhaitez néanmoins accéder à Internet via un serveur proxy, vous devez modifier la configuration proxy.



Une fois les paramètres enregistrés, l'utilisateur doit se déconnecter. Il peut passer par le dialogue suivant. L'Appliance procède alors à un redémarrage. L'opération peut prendre quelques minutes.

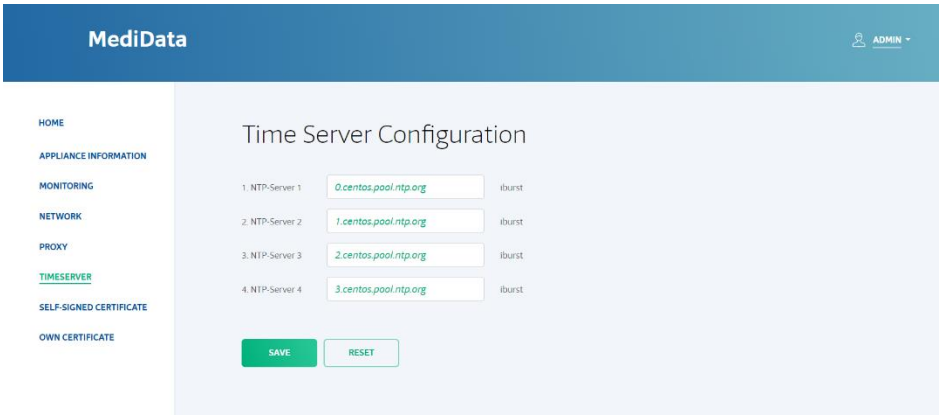
Le serveur proxy peut être configuré et programmé de plusieurs façons pour vérifier automatiquement la connexion SSL (SSL Interception). La MediData Appliance reçoit alors le certificat du serveur proxy pour la connexion au serveur MediData.

L'utilisation d'un tel proxy est déconseillé car il correspond par son comportement à une attaque de l'homme du milieu.

Configuration du serveur temporel

Pour la synchronisation temporelle, CentOS utilise l'infrastructure de réseau proposée par le projet https://www.ntppool.org/de/.

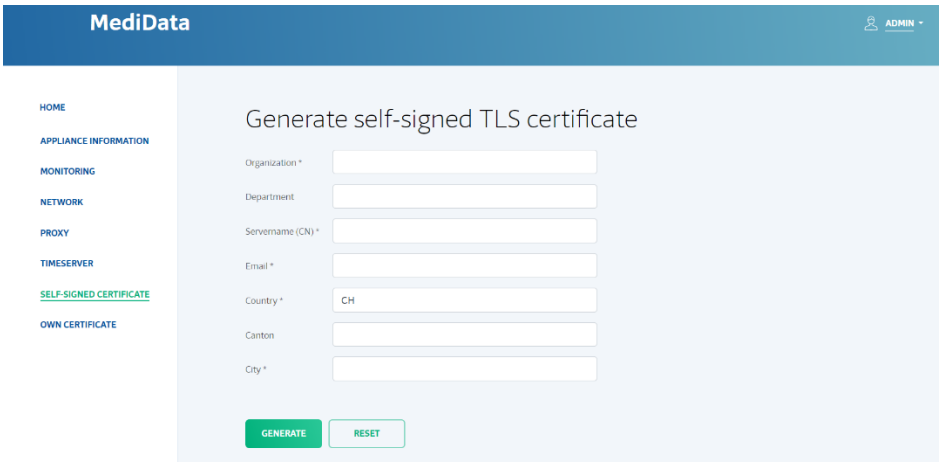
Si vous souhaitez utiliser votre propre serveur temporel pour l'Appliance, passez par le menu suivant. Plusieurs serveurs peuvent être configurés.



MediData

Créer son propre certificat autosigné

Un certificat TLS autosigné de MediData est intégré par défaut au Client. Une fonction est à votre disposition si vous souhaitez remplacer ce certificat par votre propre certificat autosigné avec les informations correspondantes.



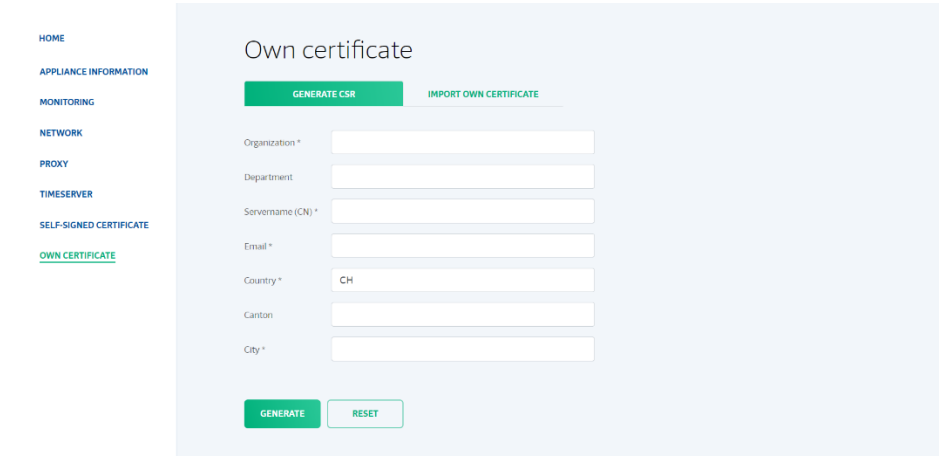
Les champs suivis d'un * doivent être complétés.

Le certificat sera rapidement actif après un clic sur 'Generate'.

Créer un certificat d'organisation

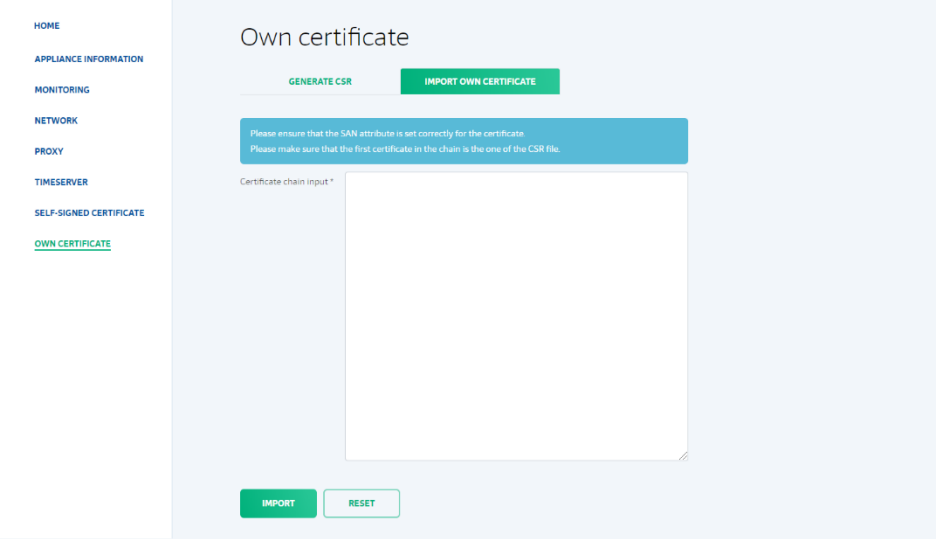
Des certificats de votre organisation peuvent aussi être lus en utilisant le menu suivant.

Il faut commencer par créer un CertificateSigningRequest. Saisissez les données requises. Les champs marqués d'un * sont obligatoires.



En cliquant sur le bouton 'generate', vous générerez la 'certificate chain'. Copiez-la.

Ouvrez ensuite l’onglet 'Import own certificate'.



Vous pouvez à présent y copier le certificat reçu de l’organisme de certification. Cliquez ensuite sur le bouton 'Import'.