

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:

- [Conditions préalables](#)
 - [Schéma du réseau client](#)
 - [Joignabilité](#)
- [Page d'accueil de la configuration](#)
 - [Messages d'état](#)
- [Informations sur l'Appliance](#)
- [Métriques de l'Appliance \(monitoring\)](#)
- [Configuration réseau](#)
 - [Réseau docker interne](#)
- [Configurer le serveur proxy](#)
- [Configuration du serveur temporel](#)
- [Créer son propre certificat autosigné](#)
- [Créer un certificat d'organisation](#)

Conditions préalables

La MediData Appliance doit être allumée et connectée à Internet.

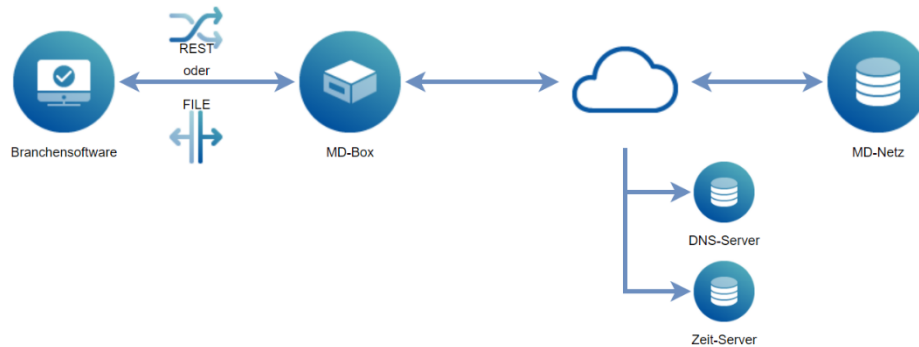
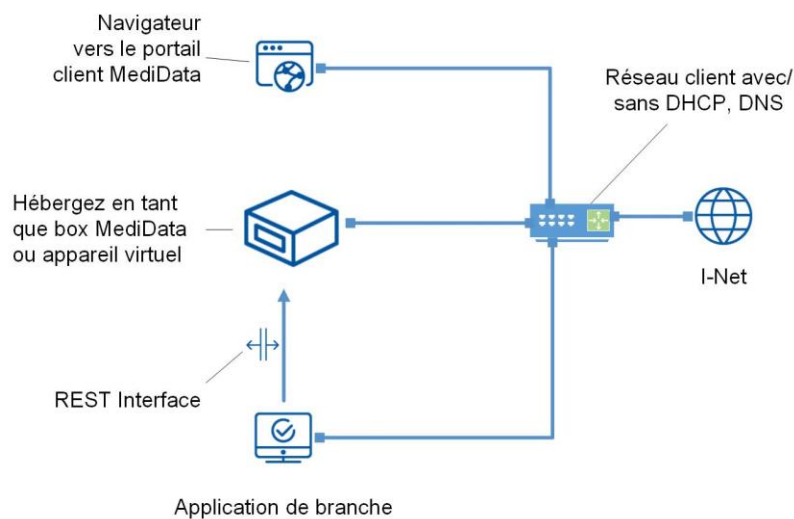


Schéma du réseau client



Joignabilité

Les adresses suivantes sont accessibles par l'intermédiaire des ports mentionnés. Veuillez 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/>.

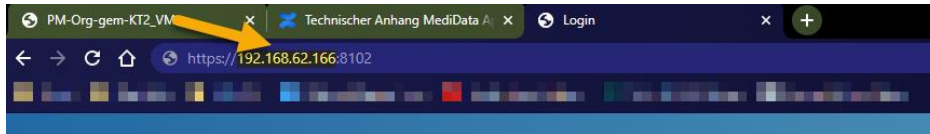
Page d'accueil de la configuration

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

MediData

→ 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.

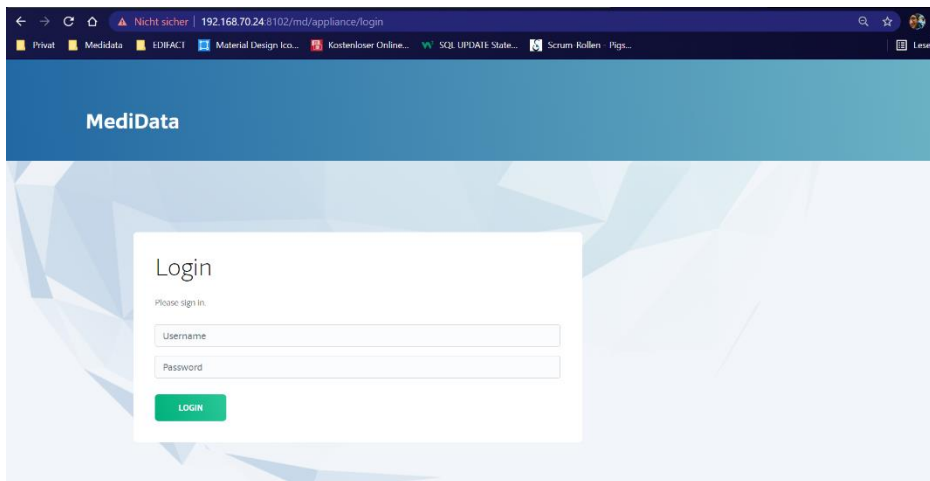


Notez que la partie marquée en jaune peut varier. L'URL entrée ici n'est qu'un exemple. Vous trouverez l'adresse IP correcte à entrer sur le portail clients p. ex.

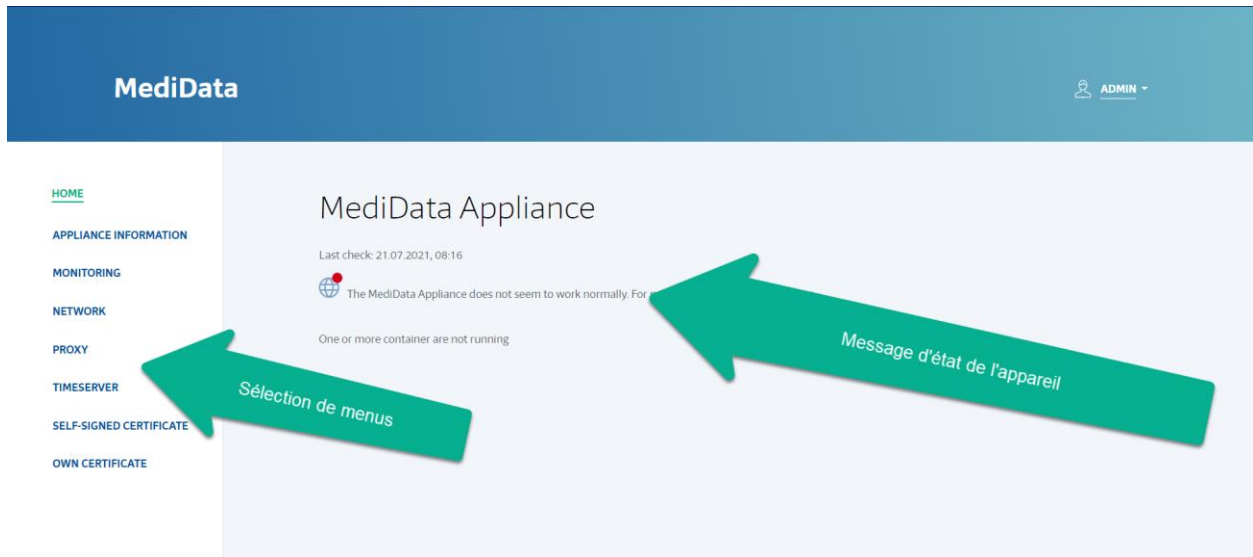
Réseau sans DHCP

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



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.

 ADMIN ▾

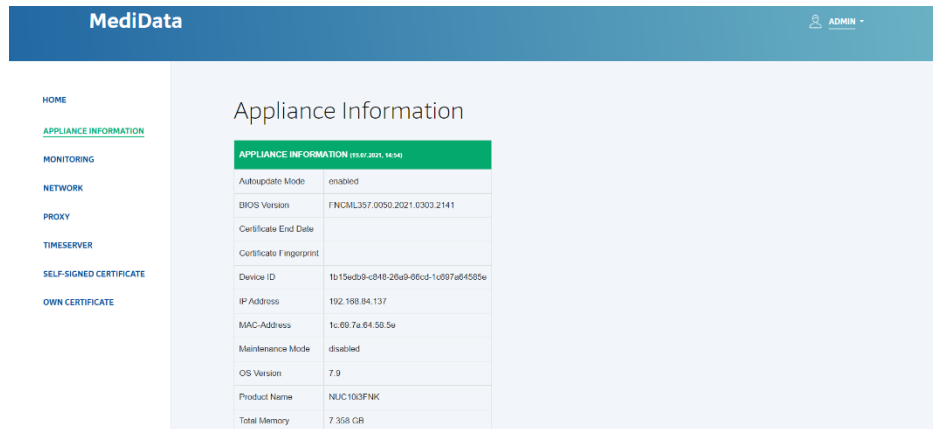
Appliance Box

 [Change Password](#)

 [Logout](#)

Informations sur l'Appliance

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

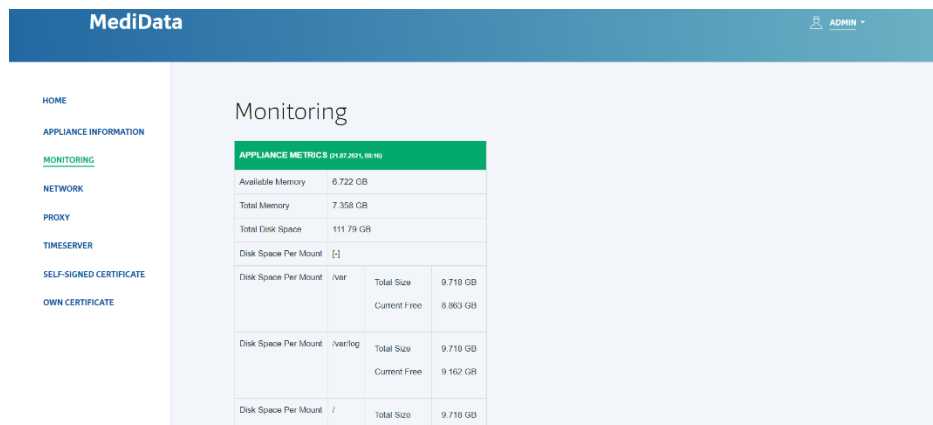


APPLIANCE INFORMATION (11.07.2021, 14:50)	
Autoupdate Mode	enabled
DIOS Version	FWGML357.0050.2021.0303.2141
Certificate End Date	
Certificate Fingerprint	
Device ID	1b15ed09-c848-26a9-06c1-1c097a04505e
IP Address	192.168.84.137
MAC-Address	1c:00:7a:04:50:5e
Maintenance Mode	disabled
OS Version	7.9
Product Name	NUC10QFNK
Total Memory	7.358 GB

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).



APPLIANCE METRICS (11.07.2021, 08:16)			
Available Memory	6.722 GB		
Total Memory	7.358 GB		
Total Disk Space	111.79 GB		
Disk Space Per Mount	[]		
Disk Space Per Mount	/var	Total Size	9.710 GB
		Current Free	8.863 GB
Disk Space Per Mount	/var/log	Total Size	9.710 GB
		Current Free	9.162 GB
Disk Space Per Mount	/	Total Size	9.710 GB

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

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

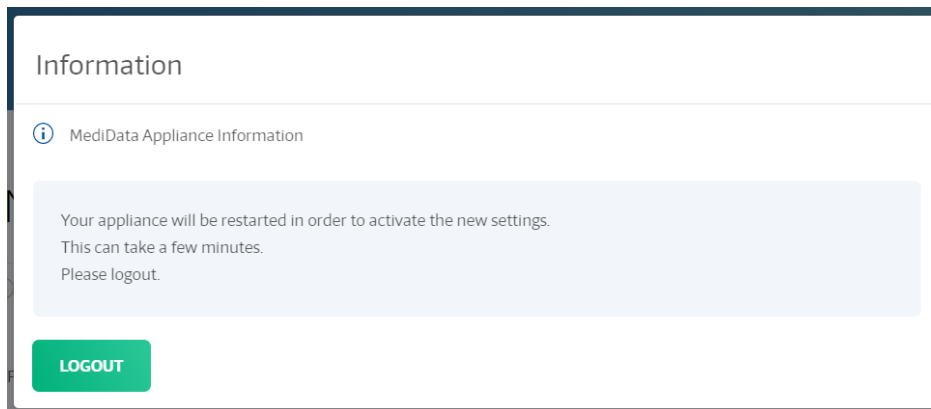
La plage d'adresses IP 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) est réservée à l'usage interne. Si le réseau côté client est configuré dans cette plage, l'Appliance le détectera lors d'un redémarrage et basculera le réseau interne sur la plage 10.0.0.0/8. La plage d'adresses utilisée pour le secteur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

APPLIANCE INFORMATION (07.09.2021, 13:27)			
Device ID	42260843-ada6-1e0b-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 [1]

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.

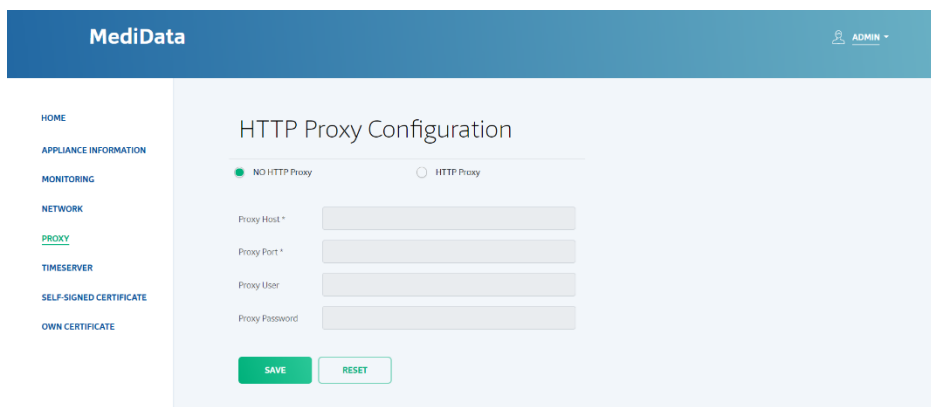
Après l'entrée des adresses et la sauvegarde, l'utilisateur doit se déconnecter. Il peut le faire par le biais du dialogue suivant. L'Appliance redémarrera.



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.

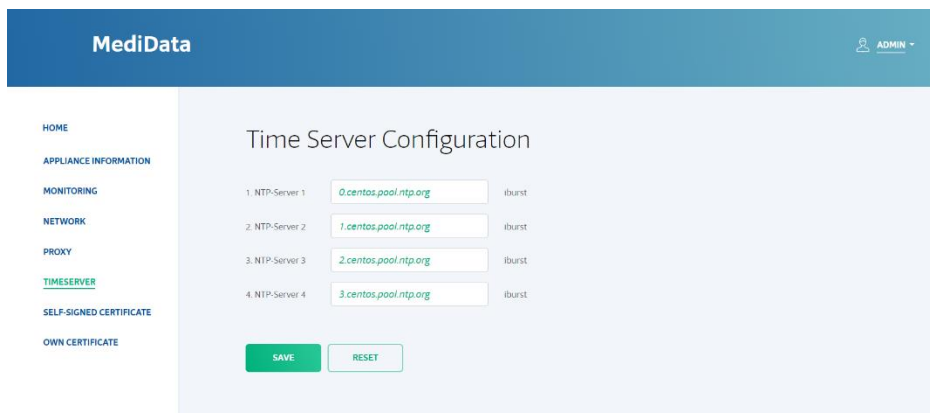
Le serveur proxy peut être configuré et programmé de plusieurs façons pour vérifier automatiquement la connexion SSL (SSL Interception). La MediData Appliance reçoit alors le certificat du serveur proxy pour la connexion au serveur MediData.

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.

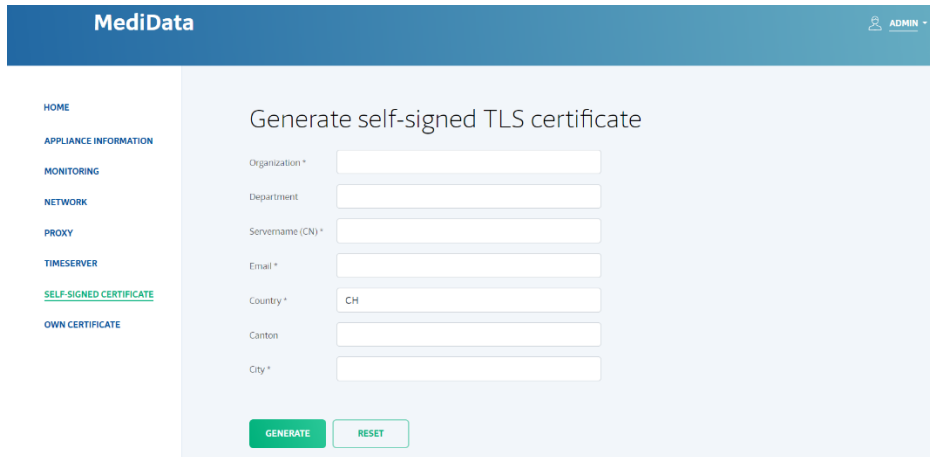


MediData		ADMIN
HOME	Time Server Configuration	
APPLIANCE INFORMATION		
MONITORING		
NETWORK		
PROXY		
TIMESERVER		
SELF-SIGNED CERTIFICATE		
OWN CERTIFICATE		

1. NTP-Server 1	<input type="text" value="0.centos.pool.ntp.org"/>	iburst
2. NTP-Server 2	<input type="text" value="1.centos.pool.ntp.org"/>	iburst
3. NTP-Server 3	<input type="text" value="2.centos.pool.ntp.org"/>	iburst
4. NTP-Server 4	<input type="text" value="3.centos.pool.ntp.org"/>	iburst

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.



The screenshot shows the MediData web interface. At the top, there is a blue header with the MediData logo on the left and an 'ADMIN' user profile on the right. A left sidebar contains a navigation menu with items: HOME, APPLIANCE INFORMATION, MONITORING, NETWORK, PROXY, TIMESERVER, SELF-SIGNED CERTIFICATE (highlighted in green), and OWN CERTIFICATE. The main content area is titled 'Generate self-signed TLS certificate'. It contains a form with the following fields: Organization * (text input), Department (text input), Servname (CN) * (text input), Email * (text input), Country * (text input with 'CH' selected), Canton (text input), and City * (text input). Below the form are two buttons: 'GENERATE' (green) and 'RESET' (light blue).

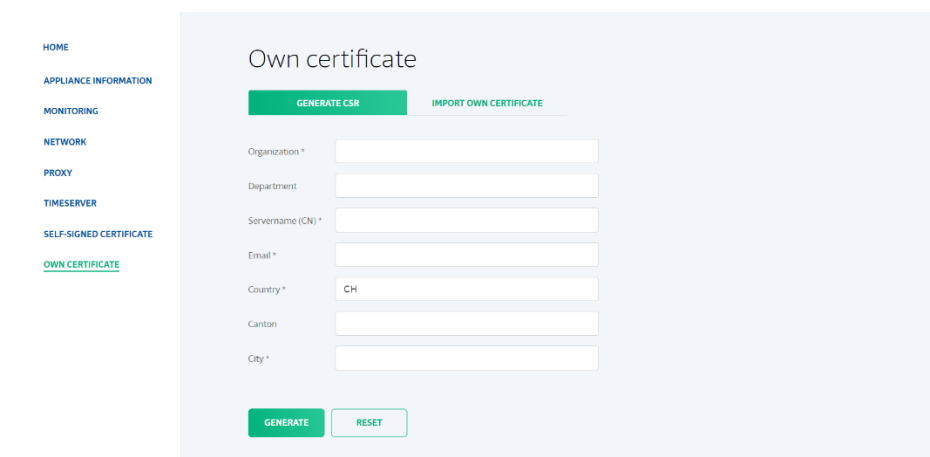
Les champs suivis d'un * doivent être complétés.

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.

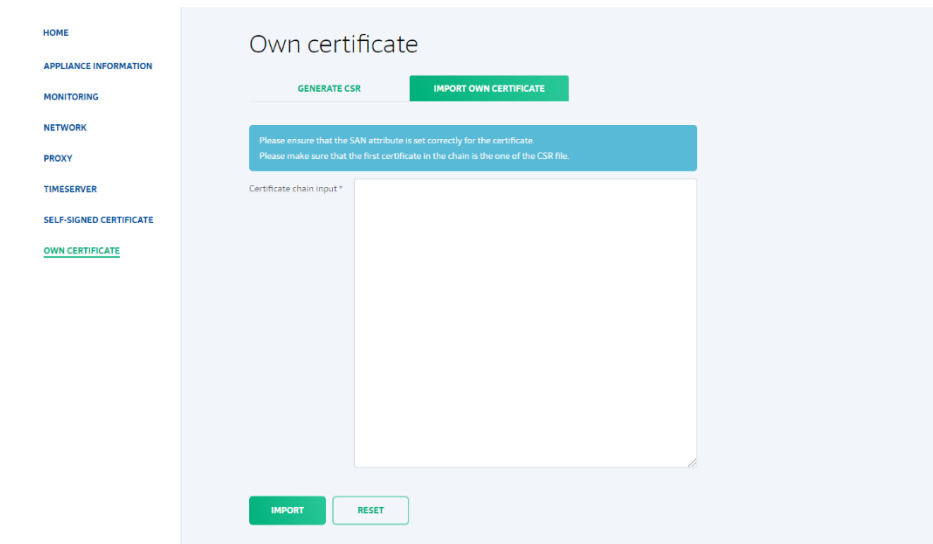
Il faut commencer par créer un CertificateSigningRequest. Saisissez les données requises. Les champs marqués d'un * sont obligatoires.



The screenshot shows the MediData web interface for generating an organization certificate. The left sidebar is identical to the previous screenshot, with 'OWN CERTIFICATE' highlighted in green. The main content area is titled 'Own certificate'. It features two tabs: 'GENERATE CSR' (active, green) and 'IMPORT OWN CERTIFICATE' (light blue). Below the tabs is a form with the following fields: Organization * (text input), Department (text input), Servname (CN) * (text input), Email * (text input), Country * (text input with 'CH' selected), Canton (text input), and City * (text input). At the bottom are 'GENERATE' (green) and 'RESET' (light blue) buttons.

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

Ouvrez ensuite l'onglet 'Import own certificate'.



The screenshot shows the 'Own certificate' page in the MediData interface. On the left is a navigation menu with the following items: HOME, APPLIANCE INFORMATION, MONITORING, NETWORK, PROXY, TIMESERVER, SELF-SIGNED CERTIFICATE, and OWN CERTIFICATE (which is highlighted in green). The main content area has the title 'Own certificate' and two buttons: 'GENERATE CSR' and 'IMPORT OWN CERTIFICATE' (highlighted in green). Below these buttons is a blue warning box with the text: 'Please ensure that the SAN attribute is set correctly for the certificate. Please make sure that the first certificate in the chain is the one of the CSR file.' Underneath the warning box is a text input field labeled 'Certificate chain input *' with a large empty area for pasting text. At the bottom of the form are two buttons: 'IMPORT' (highlighted in green) and 'RESET'.

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