

Allegato tecnico Appliance MediData

Le presenti istruzioni presuppongono conoscenze a livello di rete e di sistema operativo. Eventualmente consultare il referente del software utilizzato nello studio medico o lo specialista addetto al sistema di rete (se disponibile).

Cronistoria modifiche

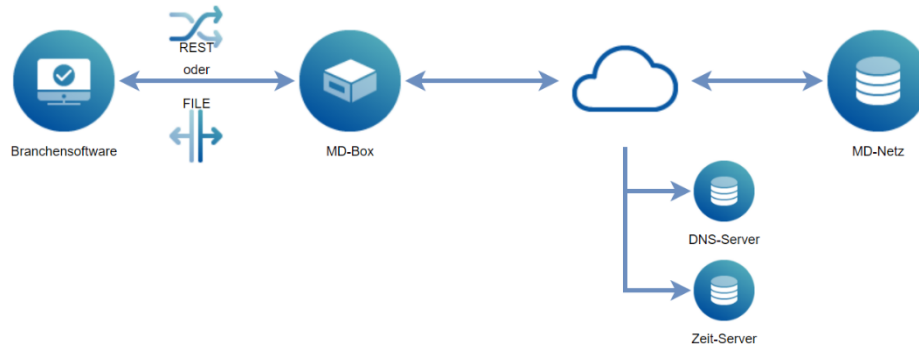
Versione rev.	Descrizione della modifica	Data modifica	Autore
0.1	Prima versione della documentazione	20 lug 2021	Manuel Gebistorf (gem)
1.0	Pubblicazione	7 set 2021	Manuel Gebistorf (gem)
1.1	Intervallo IP 172.x.x.x Integrazione della descrizione	8 set 2021	Manuel Gebistorf (gem)

Sommario:

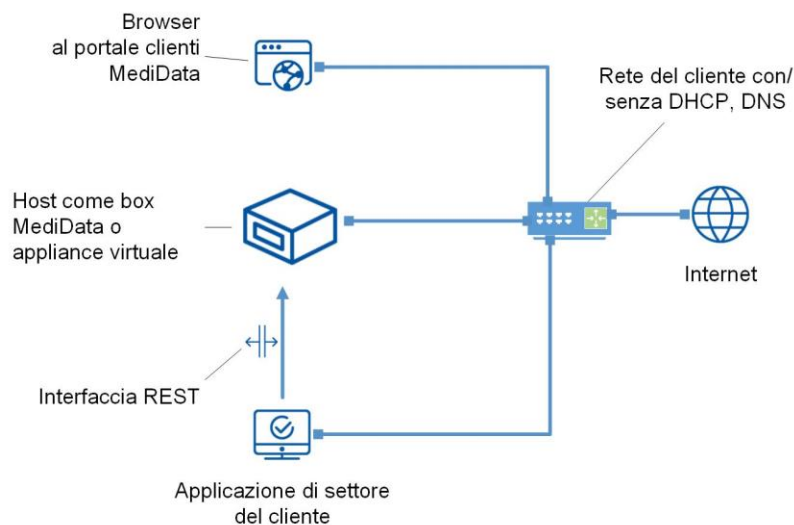
- [Requisiti](#)
 - [Schema della rete del cliente](#)
 - [Raggiungibilità](#)
 - [Pagina di accesso per la configurazione](#)
 - [Messaggi sullo stato](#)
 - [Informazioni sull'Appliance](#)
 - [Metriche dell'Appliance \(Monitoring\)](#)
 - [Configurazione della rete](#)
 - [Rete Docker interna](#)
 - [Configurazione del server proxy](#)
 - [Impostazioni del Time Server](#)
 - [Creazione di un certificato autofirmato](#)
 - [Creazione di un certificato dell'organizzazione](#)
-

Requisiti

L'Appliance MediData deve essere accesa e collegata a Internet.



Schema della rete del cliente



Raggiungibilità

I seguenti indirizzi vengono raggiunti tramite le porte elencate. Si accerti che nella rete le porte siano libere.

Sistema produttivo

Destinazione	Porta	Scopo
sshmdclient.medidata.ch	TCP 9022	Collegamento di gestione a MediData (SSH)
wsr.medidata.ch	TCP 443	Collegamento di gestione a MediData (SSL)
Tutti*	UDP 123	Sincronizzazione temporale
Stabilito dal client DHCP	UDP 53	Risoluzione dei nomi

*Per la sincronizzazione temporale CentOS utilizza l'infrastruttura di rete messa a disposizione dal progetto <https://www.ntppool.org/it/>.

Sistema ACC

Destinazione	Porta	Scopo
sshmdclient-acc.medidata.ch	TCP 9022	Collegamento di gestione a MediData (SSH)
wsr-acc.medidata.ch	TCP 443	Collegamento di gestione a MediData (SSL)
Tutti*	UDP 123	Sincronizzazione temporale
Stabilito dal client DHCP	UDP 53	Risoluzione dei nomi

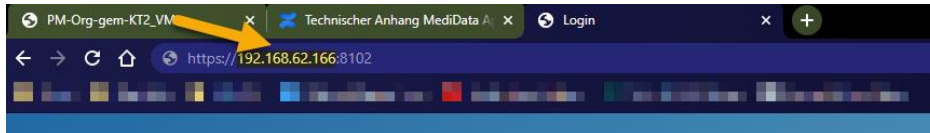
*Per la sincronizzazione temporale CentOS utilizza l'infrastruttura di rete messa a disposizione dal progetto <https://www.ntppool.org/it/>.

Pagina di accesso per la configurazione

Per effettuare la configurazione completa dell'Appliance MediData è disponibile una pagina di accesso protetta dedicata.

→ L'Appliance MediData deve essere accesa. Se l'Appliance MediData è spenta, è necessario accenderla e attendere che effettui la procedura di avvio.

→ Inserisca nel suo browser Internet il seguente URL.



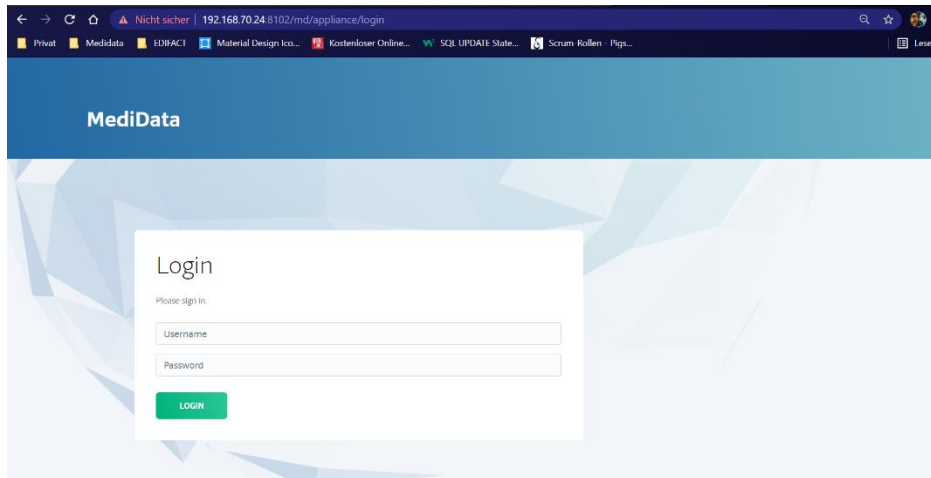
Attenzione, la parte marcata in giallo può variare. L'esempio visibile qui è solo a titolo di esempio. Per conoscere l'indirizzo IP corretto da inserire consultare ad esempio il portale per i clienti.

Rete senza DHCP

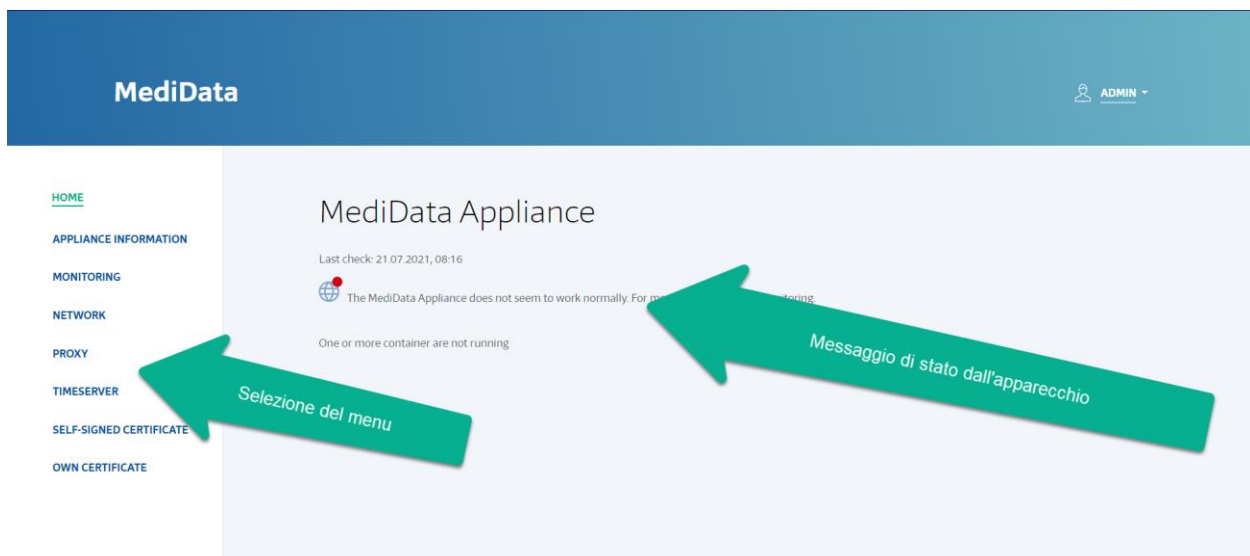
Se l'Appliance MediData si trova in una rete che non supporta DHCP, non viene assegnato alcun indirizzo IP. In tal caso, l'Appliance può essere raggiunta tramite l'indirizzo IP **169.254.99.198**.

→ Come passo successivo, può effettuare il login tramite l'apposita finestra nella Management UI (Management User Interface). L'Appliance viene fornita con le seguenti impostazioni di default: nome utente = admin, password = admin.

MediData



Dopo aver effettuato correttamente il login, le verrà visualizzata la pagina “Home” della Management UI.



Messaggi sullo stato

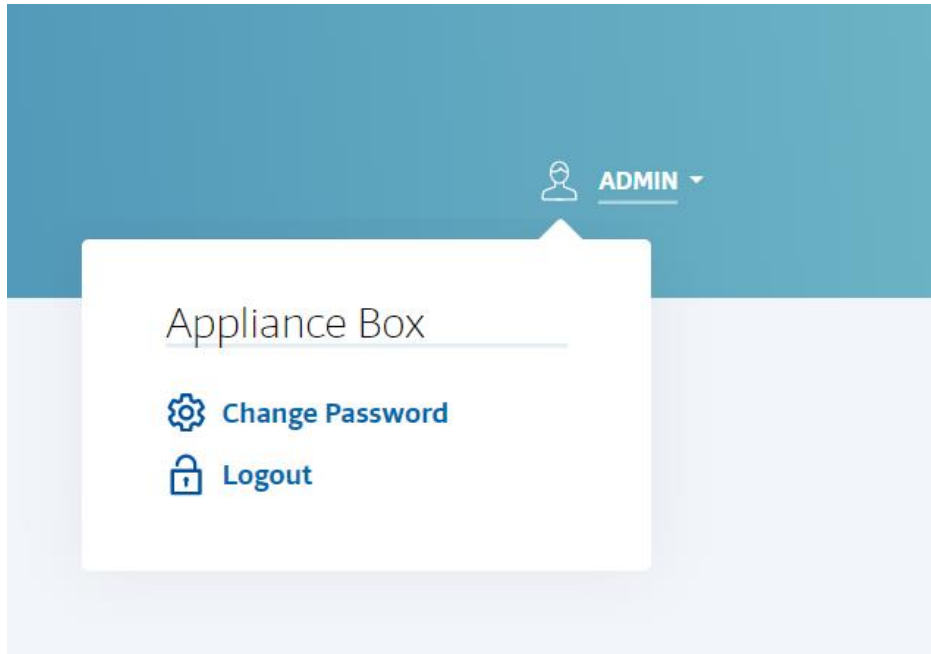
I messaggi sullo stato vengono scaricati a determinati intervalli e visualizzati nel menu “Home”.

- Last Check: marca temporale dell'ultima raccolta dati
- Stato: esistono due stati:
 - verde → tutto OK
 - rosso → ci sono problemi sulla Appliance che potrebbero compromettere la trasmissione dati. Ciò che non funziona correttamente nell'Appliance viene visualizzato in forma testuale.

Impostazioni dell'utente

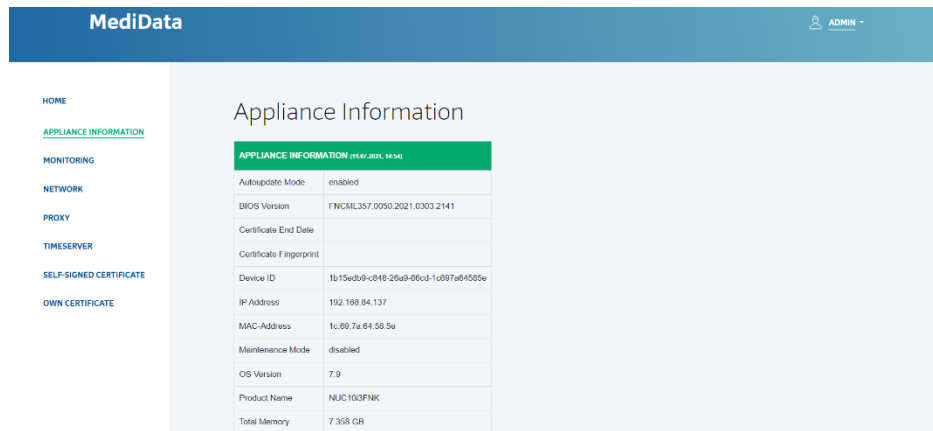
MediData

Cliccando sul pulsante "Admin" è possibile modificare la password per la Management UI o effettuare il logout.



Informazioni sull'Appliance (Appliance Information)

In questo menu vengono visualizzate (in genere in modo statico) informazioni sulla Appliance.

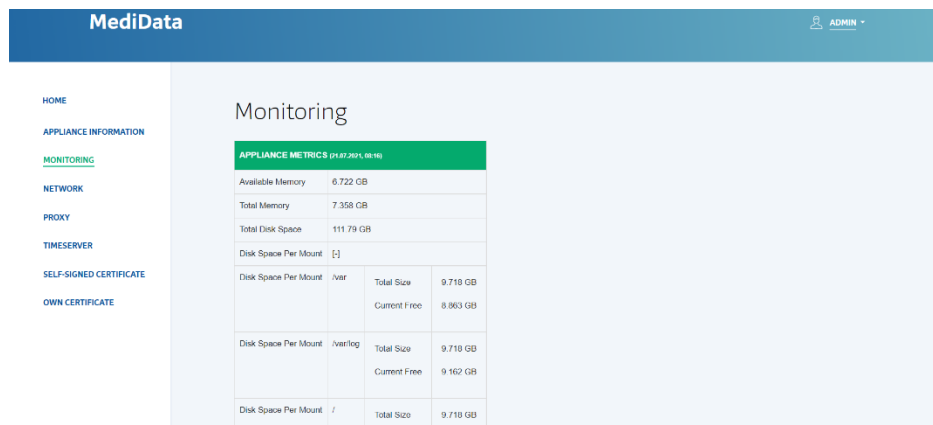


APPLIANCE INFORMATION (11:47:2021, 14:14)	
Autoupdate Mode	enabled
BIOS Version	F7NCML357.0050.2021.C303.2141
Certificate End Date	
Certificate Fingerprint	
Device ID	1b15e6d9-c648-26a9-86cd-1c097a64505e
IP Address	192.168.84.137
MAC Address	1c:60:7a:64:5b:5e
Maintenance Mode	disabled
OS Version	7.9
Product Name	NUC103FNK
Total Memory	7.358 GB

Queste informazioni possono essere visualizzate anche tramite l'interfaccia REST.

Metriche dell'Appliance (Monitoring)

In questo menu si trovano metriche (informazioni dinamiche come ad es. il consumo di memoria) relative all'Appliance.

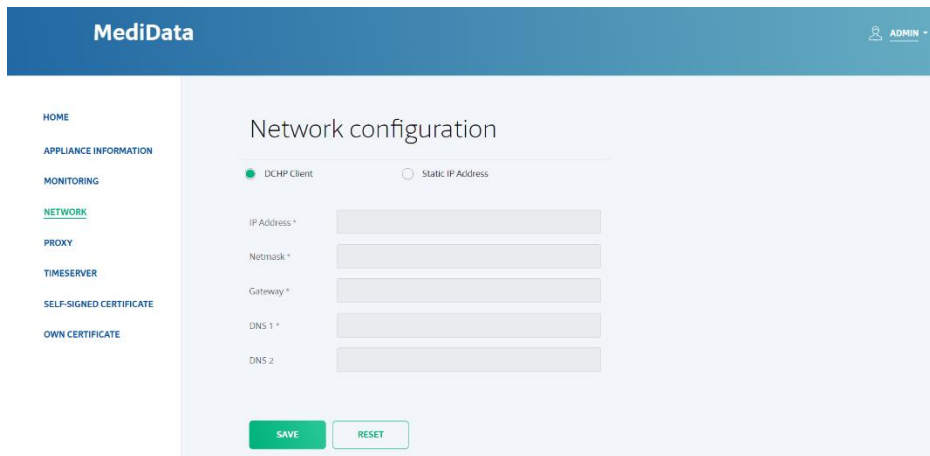


APPLIANCE METRICS (11:47:2621, 08:16)			
Available Memory	6.722 GB		
Total Memory	7.358 GB		
Total Disk Space	111.79 GB		
Disk Space Per Mount	[]		
Disk Space Per Mount /var	Total Size	9.710 GB	
	Current Free	8.863 GB	
Disk Space Per Mount /var/log	Total Size	9.710 GB	
	Current Free	9.162 GB	
Disk Space Per Mount /	Total Size	9.710 GB	

Queste informazioni possono essere visualizzate anche tramite l'interfaccia REST.

Configurazione della rete (Network configuration)

Nel menu “Network configuration” è possibile modificare l’impostazione dell’indirizzo IP dell’Appliance da DHCP a statico.



The screenshot shows the MediData management 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 sidebar on the left contains a menu with the following items: HOME, APPLIANCE INFORMATION, MONITORING, NETWORK (highlighted in green), PROXY, TIMESERVER, SELF-SIGNED CERTIFICATE, and OWN CERTIFICATE. The main content area is titled 'Network configuration'. It features two radio buttons: 'DHCP Client' (selected) and 'Static IP Address'. Below this, there are five input fields, each with an asterisk indicating it is required: 'IP Address *', 'Netmask *', 'Gateway *', 'DNS 1 *', and 'DNS 2'. At the bottom of the form, there are two buttons: a green 'SAVE' button and a white 'RESET' button.

Gli attributi sono contrassegnati da un asterisco (*) e la compilazione è obbligatoria.

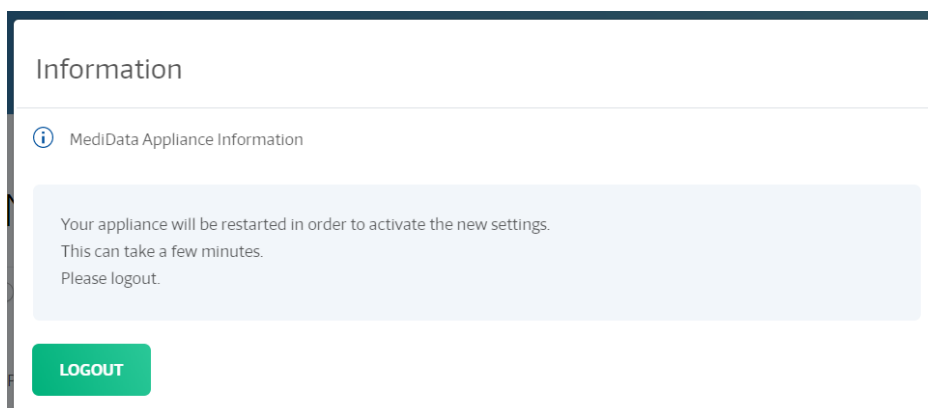
Rete Docker interna

L’intervallo di indirizzi IP 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) viene utilizzato per scopi interni. Se la rete presso il cliente è configurata in tale intervallo, l’Appliance al riavvio lo rileva e modifica la rete interna nel range 10.0.0.0/8. Nel menu “Appliance Information” della Management UI è possibile impostare quale intervallo di indirizzi deve essere utilizzato per l’intervallo interno.

APPLIANCE INFORMATION (07.09.2024, 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	1.1		

Se la rete in cui l'Appliance viene fatta funzionare deve essere "nascosta" dietro un intervallo di indirizzi IP 172.16.0.0/12 (172.16.0.0 – 172.31.255.255), è necessario configurare la rete interna tramite il menu "Internal Network". Ciò dovrebbe tuttavia essere necessario solo in singoli casi.

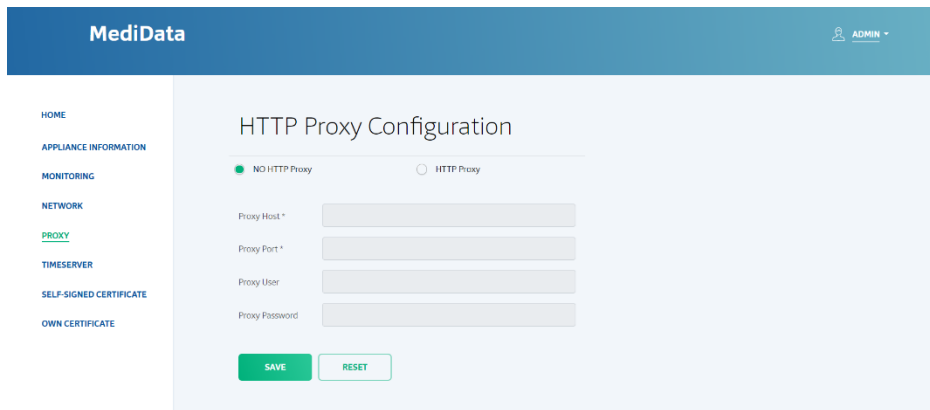
Dopo l'inserimento e il salvataggio degli indirizzi, l'utente deve effettuare il logout e lo può fare tramite la seguente finestra di dialogo. Dopo il logout l'Appliance esegue in riavvio.



Configurazione del server proxy (HTTP Proxy Configuration)

Tramite questo menu è possibile configurare un proprio proxy HTTP.

L'Appliance MediData è impostata di default come «NO http Proxy». Tuttavia, se desidera accedere a Internet attraverso un server proxy, occorre modificare la configurazione del proxy.



Se le impostazioni vengono salvate, l'utente deve effettuare il logout. Lo si può fare tramite la seguente finestra di dialogo. Dopo il logout, l'Appliance esegue un riavvio che può richiedere qualche minuto.

Se il server proxy è configurato in modo da ispezionare le connessioni SSL (intercettazione SSL), la connessione SSL viene terminata e decrittografata nel proxy. L'appliance MediData riceve quindi il certificato del server proxy per la connessione al server Medidata.

Tale proxy non dovrebbe essere usato perché corrisponde al comportamento di un attacco man-in-

the-middle.

Impostazioni del Time Server

Per la sincronizzazione temporale CentOS utilizza l'infrastruttura di rete messa a disposizione dal progetto <https://www.ntppool.org/it/>.

Se desidera poter utilizzare un proprio Time Server per l'Appliance, lo può fare tramite questo menu. È anche possibile configurare diversi server.

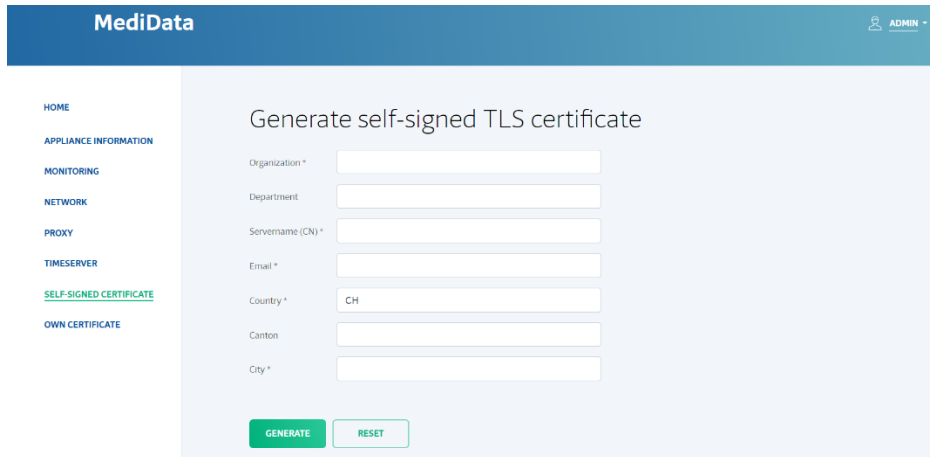
- HOME
- APPLIANCE INFORMATION
- MONITORING
- NETWORK
- PROXY
- TIMESERVER**
- SELF-SIGNED CERTIFICATE
- OWN CERTIFICATE

Time Server Configuration

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

Creazione di un certificato autofirmato

Nel client è integrato per default un certificato TLS autofirmato di MediData. Se desidera sostituire questo certificato con uno proprio autofirmato contenente le sue informazioni è disponibile un'apposita funzione.



The screenshot shows the MediData web interface. The top navigation bar includes the MediData logo and an 'ADMIN' user profile. A sidebar on the left lists various system components: 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' and contains a form with the following fields: Organization * (required), Department, Servername (CN) * (required), Email * (required), Country * (pre-filled with 'CH'), Canton, and City * (required). At the bottom of the form are two buttons: 'GENERATE' (in green) and 'RESET'.

Gli attributi contrassegnati con un asterisco (*) sono campi obbligatori.

Cliccando su “Generate” il certificato sarà attivo dopo breve tempo.

Creazione di un certificato dell'organizzazione

È possibile importare anche certificati della propria organizzazione

Come primo passo è necessario creare una “CertificateSigningRequest”. Inserisca i dati necessari a tale scopo. Gli attributi contrassegnati con un asterisco (*) sono campi obbligatori.

Own certificate

GENERATE CSR | **IMPORT OWN CERTIFICATE**

Organization *

Department

Servername (CN) *

Email *

Country *

Canton

City *

GENERATE | **RESET**

Cliccando sul pulsante “Generate” viene generata la “certificate chain”. Copi la “certificate chain”.

Al termine, passi al registro “Import own certificate”.

Own certificate

GENERATE CSR | **IMPORT OWN CERTIFICATE**

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.

Certificate chain input *

IMPORT | **RESET**

Ora può copiare qui il certificato che ha ricevuto dall'ufficio di certificazione e poi cliccare sul pulsante “Import”.