

Technischer Anhang MediData Appliance (Deutsch)

Die folgende Anleitung setzt Kenntnisse auf Netzwerk- und Betriebssystemebene voraus. Bitte konsultieren Sie Ihren Ansprechpartner der Praxissoftware oder Ihre zuständige Fachperson für das Netzwerksystem (falls vorhanden).

Änderungshistorie

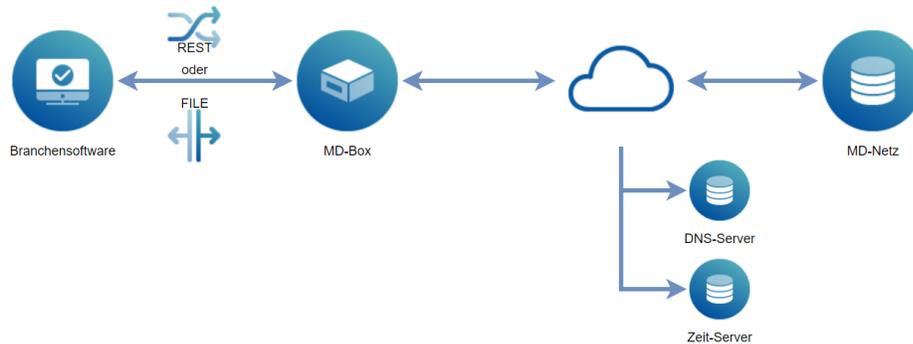
Rev. Version	Beschreibung der Änderung	Änderungsdatum	Ersteller
0.1	Erste Version des Dokumentation	Jul 20, 2021	Manuel Gebistorf (gem)
1.0	Veröffentlichung	Sep 7, 2021	Manuel Gebistorf (gem)
1.1	IP-Range 172.x.x.x Beschreib ergänzt	Sep 8, 2021	Manuel Gebistorf (gem)

Inhalt:

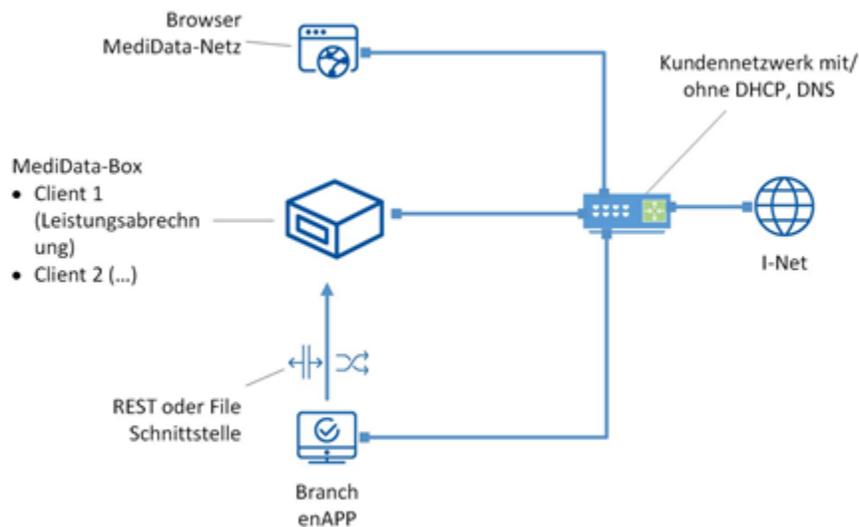
- [Voraussetzung](#)
 - [Schema Kunden-Netzwerk](#)
 - [Erreichbarkeit](#)
- [Einstiegsseite für die Konfiguration](#)
 - [Statusmeldungen](#)
- [Informationen über die Appliance](#)
- [Metriken der Appliance \(Monitoring\)](#)
- [Netzwerkeinstellungen](#)
 - [Internes Docker-Netzwerk](#)
- [Proxy-Server konfigurieren](#)
- [Time-Server Einstellungen](#)
- [Eigenes selbst signiertes Zertifikat erstellen](#)
- [Organisations Zertifikat erstellen](#)

Voraussetzung

Die MediData Appliance muss eingeschaltet und am Internet angeschlossen sein.



Schema Kunden-Netzwerk



Erreichbarkeit

Die folgenden Adressen werden über die aufgeführten Ports erreicht. Stellen Sie sicher, dass die Ports im Netzwerk frei sind:

Produktives System

Ziel	Port	Zweck
sshmdclient.medidata.ch	TCP 9022	Managementverbindung zur MediData (SSH)
wsr.medidata.ch	TCP 443	Managementverbindung zur MediData (SSL)
Alle*	UDP 123	Zeitsynchronisation
Vom DHCP Client vorgegeben	UDP 53	Namensauflösung

*Für die Zeitsynchronisation nutzt CentOS die vom Projekt <https://www.ntppool.org/de/> bereitgestellte Infrastruktur im Netz.

ACC-System

Ziel	Port	Zweck
sshmdclient-acc.medidata.ch	TCP 9022	Managementverbindung zur MediData (SSH)
wsr-acc.medidata.ch	TCP 443	Managementverbindung zur MediData (SSL)
Alle*	UDP 123	Zeitsynchronisation
Vom DHCP Client vorgegeben	UDP 53	Namensauflösung

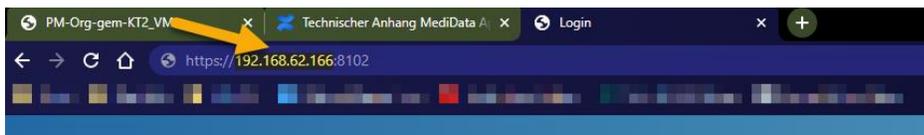
*Für die Zeitsynchronisation nutzt CentOS die vom Projekt <https://www.ntppool.org/de/> bereitgestellte Infrastruktur im Netz.

Einstiegsseite für die Konfiguration

Es gibt eine abgesicherte Einstiegsseite für die gesamte Konfiguration der MediData Appliance.

→ Die MediData Appliance muss eingeschaltet sein. Falls die MediData Appliance ausgeschaltet ist, schalten Sie die Appliance ein und warten Sie bis diese aufgestartet ist.

→ Geben Sie in Ihrem Internetbrowser die folgende URL ein.

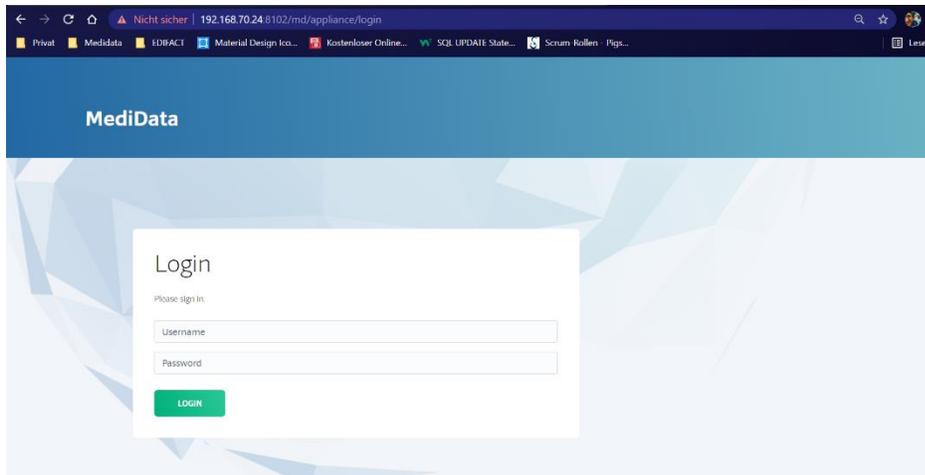


Beachten Sie, dass der gelb markierte Teil abweichend sein kann. Das hier ersichtliche Beispiel ist nur exemplarisch. Die korrekte IP-Adresse für die Eingabe entnehmen Sie z.B. dem Kundenportal.

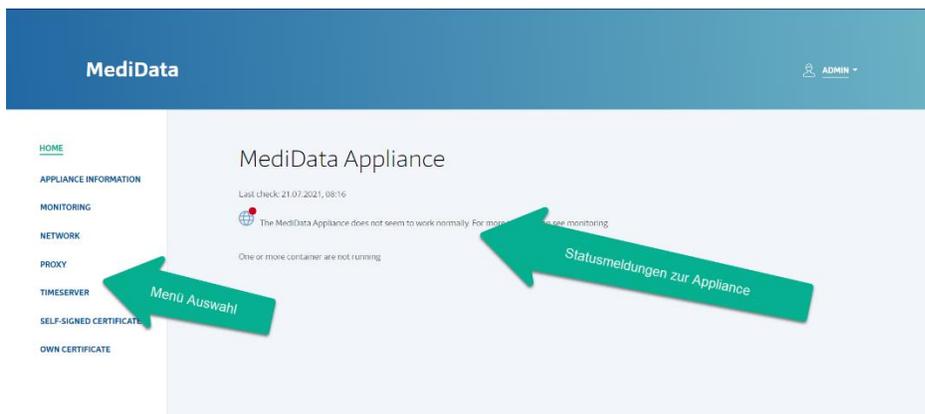
Netzwerk ohne DHCP

Befindet sich die MediData Appliance in einem Netzwerk welches kein DHCP unterstützt wird auch keine IP-Adresse vergeben. Ist dies der Fall können Sie die Appliance über die IP-Adresse **169.254.99.198** erreichen.

→ Als nächstes können Sie sich über das Login-Fenster im ManagementUI einloggen. Ausgeliefert wird die Appliance mit: Username = admin, Password = admin.



Nach erfolgreichem Login befinden Sie sich auf der 'Home' Seite des Management UI.



Statusmeldungen

Die Statusmeldungen werden in einem gewissen Interval abgerufen und im 'Home' Menü dargestellt.

- Last Check: Timestamp der letzten Datensammlung
- Status: Es gibt zwei Status;
 - Grün → alles ist okay
 - Rot → Es gibt Probleme auf der Appliance welche die Datenübermittlung beeinträchtigen könnten. Was mit der Appliance nicht in Ordnung ist wird als Text angezeigt.

Benutzereinstellungen

Mit einem Klick auf die Fläche 'Admin' können Sie das Passwort für das ManagementUI ändern oder sich ausloggen.

 ADMIN ▾

Appliance Box

 [Change Password](#)

 [Logout](#)

Informationen über die Appliance

In diesem Menü werden Informationen (meist statisch) über die Appliance angezeigt.

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-c848-26a9-06cd-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

Diese Informationen können auch über die REST-Schnittstelle abgerufen werden.

Metriken der Appliance (Monitoring)

In diesem Menü finden sich Metriken (dynamische Informationen wie z.B. Speicherverbrauch) über die Appliance.

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	over	Total Size	9.710 GB
		Current Free	8.863 GB
Disk Space Per Mount	over/leg	Total Size	9.710 GB
		Current Free	9.162 GB
Disk Space Per Mount	/	Total Size	9.710 GB

Diese Informationen können auch über die REST-Schnittstelle abgerufen werden.

Netzwerkeinstellungen

Im Menü 'Netzwerkeinstellungen' kann die IP-Adresse der Appliance von DHCP auf Fix eingestellt werden.

Die Attribute welche mit einem * versehen sind müssen zwingend befüllt werden.

Internes Docker-Netzwerk

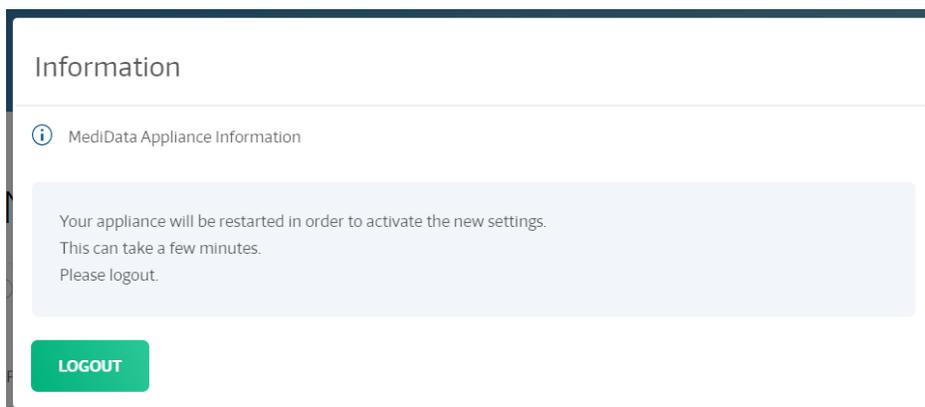
Der IP-Adressbereich 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) wird für interne Zwecke gebraucht. Ist das Netzwerk beim Kunden in diesem Bereich konfiguriert detektiert die Appliance bei einem Neustart dies und ändert das interne Netzwerk im Bereich 10.0.0.0/8. Welcher Adressbereich für den interne Bereich verwendet wird, kann im ManagementUI unter den 'Appliance Information' eingesehen werden.

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 1/1

Ist das Netzwerk, in welchem die Appliance betrieben wird, hinter einem IP-Adressbereich 172.16.0.0/12 (172.16.0.0 – 172.31.255.255) 'versteckt' muss das interne Netzwerk über das Menü 'internal Network' konfiguriert werden. Dies sollte aber nur in Einzelfällen nötig sein.

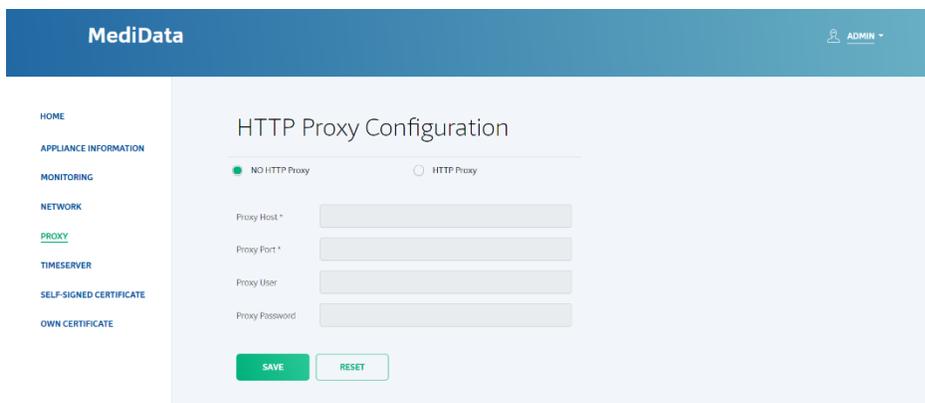
Nach der Eingabe der Adressen und dem Speichern muss der User ausloggen, dies kann über den folgenden Dialog gemacht werden. Die Appliance führt danach einen Neustart aus.



Proxy-Server konfigurieren

Über dieses Menü kann ein eigener HTTP-Proxy konfiguriert werden.

Die MediData Appliance ist als «NO http Proxy» vor eingestellt. Falls Sie jedoch über einen Proxy-Server aufs Internet zugreifen, die Proxy-Konfiguration angepasst werden.



Werden die Einstellungen gespeichert muss sich der Benutzer ausloggen. Dies kann über den folgenden Dialog gemacht werden. Die Appliance führt danach einen Neustart durch, dies kann ein paar Minuten dauern.

Ist der Proxy-Server so konfiguriert, dass dieser SSL Verbindungen inspiziert (SSL Interception) wird die SSL Verbindung beim Proxy terminiert und entschlüsselt. Die MediData Appliance bekommt dann das Zertifikat des Proxy-Server für die Verbindung zum Medidata-Server.

Ein solcher Proxy sollte nicht verwendet werden da dieser vom Verhalten einer Man-in-the-Middle Attacke entspricht.

Time-Server Einstellungen

Für die Zeitsynchronisation nutzt CentOS die vom Projekt <https://www.ntppool.org/de/> bereitgestellte Infrastruktur im Netz.

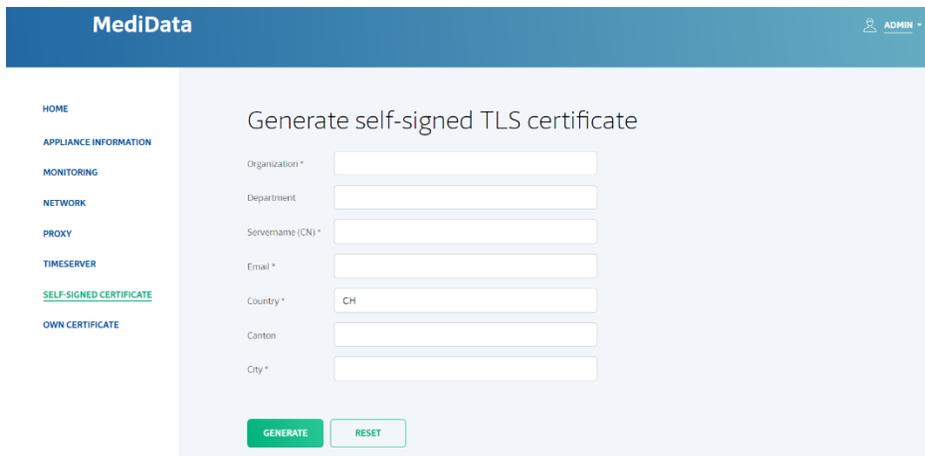
Möchten Sie einen eigenen Time-Server für die Appliance verwenden können Sie dies über dieses Menü machen. Es können auch mehrere Server eingestellt werden.

The screenshot shows the 'Time Server Configuration' page in the MediData admin interface. The page has a blue header with the 'MediData' logo and an 'ADMIN' user profile icon. A left sidebar contains navigation links: HOME, APPLIANCE INFORMATION, MONITORING, NETWORK, PROXY, **TIMESERVER** (highlighted), SELF-SIGNED CERTIFICATE, and OWN CERTIFICATE. The main content area is titled 'Time Server Configuration' and contains four rows of input fields for NTP servers. Each row has a label (1. NTP-Server 1 to 4), a text input field containing a URL (0.centos.pool.ntp.org to 3.centos.pool.ntp.org), and a 'iburst' checkbox. At the bottom of the configuration area are two buttons: 'SAVE' and 'RESET'.

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

Eigenes selbst signiertes Zertifikat erstellen

Auf dem Client ist ein selbst signiertes TLS-Zertifikat der MediData standardmässig integriert. Möchten Sie dieses Zertifikat durch ein eigenes selbst signiertes Zertifikat mit entsprechenden Einträgen ersetzen, steht Ihnen eine Funktion zur Verfügung.



The screenshot shows the MediData web interface. The top navigation bar is blue with the MediData logo on the left and an 'ADMIN' user profile on the right. A left sidebar contains a menu with the following 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' and contains a form with the following fields: Organization * (required), Department, Servename (CN) * (required), Email * (required), Country * (with 'CH' selected), Canton, and City * (required). At the bottom of the form are two buttons: 'GENERATE' (green) and 'RESET' (white).

Die Attribute welche mit einem * versehen sind, sind Pflichtfelder.

Mit einem Klick auf 'Generate' ist das Zertifikat nach kurzer Zeit aktiv.

Organisations Zertifikat erstellen

Es können auch Zertifikate Ihrer Organisation eingelesen werden, hierzu wird dieses Menü verwendet.

Als ersten Schritt muss ein CertificateSigningRequest erstellt werden. Geben Sie die nötigen Angaben dazu ein. Die mit einem * markierten Attribute sind Pflicht.

Own certificate

GENERATE CSR | **IMPORT OWN CERTIFICATE**

Organization *

Department

Servname (CN) *

Email *

Country *

Canton

City *

GENERATE | **RESET**

Mit einem Klick auf den Button 'generate' wird der 'certificate chain' generiert. Kopieren Sie diesen.

Anschliessend wechseln Sie in das Register '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**

Sie können nun das Zertifikat, welches Sie von der Zertifizierungsstelle erhalten haben reinkopieren und auf den Button 'Import' klicken.