
```
        "dst_netmas
        "dst_port":
        "id": 1,
        "protocol":
        "src_net":
        "src_netmas
        "verdict":
      }
    ]
  }
},
"hostname": "mGuard
"network": {
  "LAN0": {
    "address": "192
    "mask": 24,
    "router_mode":
  },
  "WAN": {
    "address": "10.
    "gateway": "10.
    "mask": 24,
    "router_mode":
  },
  "routes": [
```


FL MGUARD 1000
RESTful Configuration API
mGuardNT 1.8.x

Anwenderhandbuch

UM DE MGUARD NT CONFIG API

PHOENIX CONTACT
INSPIRING INNOVATIONS

Anwenderhandbuch

FL MGUARD 1000 - RESTful Configuration API - mGuardNT 1.8.x

UM DE MGUARD NT CONFIG API, Revision 11 2024-05-16

Dieses Handbuch ist gültig für:

Bezeichnung	Artikel-Nr.
FL MGUARD 1102	1153079
FL MGUARD 1105	1153078

Firmware-Version mGuardNT 1.8.x

Für weitere Informationen siehe mGuardNT 1.8.x Firmware – Release Notes.

108898_de_11

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit

Lesen Sie dieses Handbuch sorgfältig und bewahren Sie es für späteres Nachschlagen auf.

1.1 Kennzeichnung der Warnhinweise

Dieses Symbol mit dem Signalwort **ACHTUNG** warnt vor Handlungen, die zu einem Sachschaden oder einer Fehlfunktion führen können.

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Über dieses Handbuch

Folgende Elemente werden in diesem Handbuch verwendet:

Fett	Bezeichnung von Bedienelementen, Variablennamen oder sonstige Hervorhebungen
Kursiv	– Produkt- und Komponentenbezeichnungen (z. B. *tftpd64.exe*, *Config API*) – Fremdsprachliche Bezeichnungen oder Eigennamen – Sonstige Hervorhebungen
–	Unnummerierte Aufzählung
1.	Nummerierte Aufzählung
•	Handlungsanweisung
⇒	Ergebnis einer Handlung

1.3 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

– Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.
– Qualifizierte Anwendungsprogrammierer und Software-Ingenieure. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.

1.4 Bestimmungsgemäße Verwendung

– Die Geräte der Serie FL MGUARD 1000 sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall. Sie eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen.
– Das Gerät ist für die Installation im Schaltschrank vorgesehen.

1.5 Veränderung des Produkts

Modifikationen an der Hard- und Firmware des Geräts sind nicht zulässig.

– Unsachgemäße Arbeiten oder Veränderungen am Gerät können Ihre Sicherheit gefährden oder das Gerät beschädigen. Sie dürfen das Gerät nicht reparieren. Wenn das Gerät einen Defekt hat, wenden Sie sich an Phoenix Contact.

1.6 IT-Sicherheit

Sie müssen Komponenten, Netzwerke und Systeme vor unberechtigten Zugriffen schützen und die Datenintegrität gewährleisten. Hierzu müssen Sie bei netzwerkfähigen Geräten, Lösungen und PC-basierter Software organisatorische und technische Maßnahmen ergreifen.

Phoenix Contact empfiehlt dringend den Einsatz eines Managementsystems für Informationssicherheit (ISMS) zur Verwaltung aller infrastrukturellen, organisatorischen und personellen Maßnahmen, die zur Erhaltung der Informationssicherheit notwendig sind.

Darüber hinaus empfiehlt Phoenix Contact, mindestens die folgenden Maßnahmen zu berücksichtigen.

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten (letzter Zugriff am 15.04.2024):

– bsi.bund.de/it-sik.html
– ics-cert.us-cert.gov/content/recommended-practices

Verwenden Sie die jeweils aktuelle Firmware-Version

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Verfügbare Firmware-Updates finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

Verwenden Sie aktuelle Sicherheits-Software

- Um Sicherheitsrisiken wie Viren, Trojaner und andere Schad-Software zu erkennen und auszuschalten, installieren Sie auf allen PCs eine Sicherheits-Software.
- Stellen Sie sicher, dass die Sicherheits-Software immer auf dem aktuellen Stand ist und die neuesten Datenbanken nutzt.
- Nutzen Sie Whitelist-Tools zur Überwachung des Gerätekontexts.
- Um die Kommunikation Ihrer Anlage zu prüfen, nutzen Sie ein Intrusion-Detection-System.

Führen Sie regelmäßige Bedrohungsanalysen durch

- Um festzustellen, ob die von Ihnen getroffenen Maßnahmen Ihre Komponenten, Netzwerke und Systeme noch ausreichend schützen, ist eine regelmäßige Bedrohungsanalyse erforderlich.
- Führen Sie regelmäßige Bedrohungsanalysen durch.

Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Um Ihre Komponenten, Netzwerke und Systeme zu schützen, ist es nicht ausreichend, isoliert betrachtete Maßnahmen zu ergreifen. Defense-in-Depth-Mechanismen umfassen mehrere, aufeinander abgestimmte und koordinierte Maßnahmen, die Betreiber, Integratoren und Hersteller miteinbeziehen.

- Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Deaktivieren Sie nicht benötigte Kommunikationskanäle

- Deaktivieren Sie nicht benötigte Kommunikationskanäle (z. B. SNMP, FTP, BootP, DCP etc.) an den von Ihnen eingesetzten Komponenten.

Binden Sie Komponenten und Systeme nicht in öffentliche Netzwerke ein

- Vermeiden Sie es, Ihre Komponenten und Systeme in öffentliche Netzwerke einzubinden.
- Wenn Sie Ihre Komponenten und Systeme über ein öffentliches Netzwerk erreichen müssen, verwenden Sie ein VPN (Virtual Private Network).

Beschränken Sie die Zugangsberechtigung zum Gerät

- Beschränken Sie die Zugangsberechtigung zu Komponenten, Netzwerken und Systemen auf die Personen, für die eine Berechtigung unbedingt notwendig ist.
- Deaktivieren Sie nicht genutzte Benutzerkonten.

Sichern Sie den Zugriff ab

- Ändern Sie voreingestellte Passwörter während der ersten Inbetriebnahme.
- Verwenden Sie sichere Passwörter, deren Komplexität und Lebensdauer dem Stand der Technik entsprechen (z. B. mit einer Länge von mindestens zehn Zeichen und einer Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).
- Verwenden Sie Passwort-Manager mit zufällig erzeugten Passwörtern.
- Ändern Sie Passwörter entsprechend der für Ihre Anwendung geltenden Regeln.
- Verwenden Sie, sofern möglich, zentrale Benutzerverwaltungen zur Vereinfachung des User Managements und der Anmeldeinformationen.

Verwenden Sie bei Fernzugriff sichere Zugriffswege

- Verwenden Sie für einen Fernzugriff sichere Zugriffswege wie VPN (Virtual Private Network) oder HTTPS.

Verwenden Sie eine Firewall

- Richten Sie eine Firewall ein, um Ihre Netzwerke und darin eingebundene Komponenten und Systeme vor ungewollten Netzwerkzugriffen zu schützen.
- Verwenden Sie eine Firewall, um ein Netzwerk zu segmentieren oder bestimmte Komponenten (z. B. Steuerungen) zu isolieren.

Aktivieren Sie eine sicherheitsrelevante Ereignisprotokollierung (Logging)

- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung (Logging) gemäß der Sicherheitsrichtlinie und der gesetzlichen Bestimmungen zum Datenschutz.

Schützen Sie den Zugriff auf die SD-Karte

Geräte mit SD-Karten benötigen Schutz gegen unerlaubte physische Zugriffe. Eine SD-Karte kann mit einem herkömmlichen SD-Kartenleser jederzeit ausgelesen werden. Wenn Sie die SD-Karte nicht physisch gegen unbefugte Zugriffe schützen (z. B. mithilfe eines gesicherten Schaltschranks), sind somit auch sensible Daten für jeden abrufbar.

- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.
- Stellen Sie bei der Vernichtung der SD-Karte sicher, dass die Daten nicht wiederhergestellt werden können.

1.7 Aktuelle Sicherheitshinweise zu Ihrem Produkt

Product Security Incident Response Team (PSIRT)

Das Phoenix Contact PSIRT ist das zentrale Team für Phoenix Contact und dessen Tochterunternehmen, dessen Aufgabe es ist, auf potenzielle Sicherheitslücken, Vorfälle und andere Sicherheitsprobleme im Zusammenhang mit Produkten, Lösungen sowie Diensten von Phoenix Contact zu reagieren.

Das Phoenix Contact PSIRT leitet die Offenlegung, Untersuchung und interne Koordination und veröffentlicht Sicherheitshinweise zu bestätigten Sicherheitslücken, bei denen Maßnahmen zur Abschwächung oder Behebung verfügbar sind.

Die PSIRT-Webseite (phoenixcontact.com/psirt) wird regelmäßig aktualisiert. Zusätzlich empfiehlt Phoenix Contact, den PSIRT-Newsletter zu abonnieren.

Jeder kann per E-Mail Informationen zu potenziellen Sicherheitslücken beim Phoenix Contact PSIRT einreichen.

1.8 Support

Zusätzliche Informationen zum Gerät sowie Release Notes, Anwenderhilfen und Software-Updates finden Sie unter folgender Internet-Adresse: phoenixcontact.net/product/<Artikelnummer>.

Bei Problemen mit Ihrem Gerät oder der Bedienung Ihres Geräts wenden Sie sich bitte an Ihre Bezugsquelle.

Um in einem Fehlerfall schnelle Hilfe zu erhalten, erstellen Sie, falls möglich, beim Auftreten des Fehlers umgehend einen Snapshot der Gerätekonfiguration (siehe Kapitel 3.10, „Endpunkt "snapshot""), den Sie dem Support zur Verfügung stellen können.

2 RESTful Configuration API verwenden

2.1 Einleitung

Neben der Konfiguration über das Web-based Management, kann das Gerät auch über die *RESTful Configuration API* (kurz: *Config API*) konfiguriert werden.

Die Verwendung der *Config API* sollte auf erfahrene Anwender beschränkt werden.

Als Maschine-zu-Maschine-Interface ermöglicht die *RESTful Configuration API* eine automatisierte und dynamische Steuerung und Konfiguration des Geräts.

Die *Config API* wird über einen RESTful-Webserver des Geräts bereitgestellt.

Die Übertragung der Daten erfolgt über das HTTP(S)-Protokoll, das auch zum Abrufen von Webseiten verwendet wird (siehe Bild 2-1).

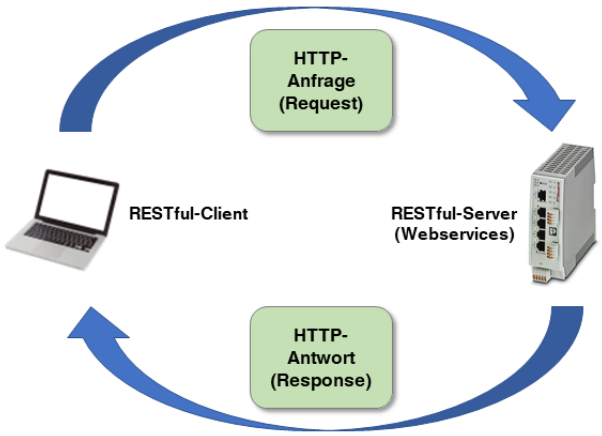

Bild 2-1 Datenaustausch zwischen RESTful-Client und RESTful-Server (REST = *Representational State Transfer*)

Der Zugriff auf den RESTful-Server kann mithilfe unterschiedlicher RESTful-Clients erfolgen, um z. B. die Konfiguration des Geräts mittels *GET-Request* abzufragen oder mittels *POST-Request* zu ändern.

Als RESTful-Client kann z. B. eine entsprechende Managementsoftware, ein Kommandozeilentool (z. B. *curl*), ein grafischer RESTful-Client für Windows (z. B. *Nightingale*) oder eine Webbrowser-Erweiterung (z. B. *YARC!* für *Google Chrome*) verwendet werden, die separat bezogen bzw. installiert werden müssen.

ACHTUNG: Software von Drittanbietern
Phoenix Contact übernimmt keine Garantie oder Haftung bei der Verwendung von Produkten von Drittanbietern. Verweise auf oder Beschreibungen von Drittanbieter-Software stellen keine Empfehlung dar, sondern sind Beispiele für grundsätzlich verwendbare Programme.

Die *RESTful Configuration API* sowie Anwendungsbeispiele zu den verfügbaren Endpunkten, werden in den folgenden Kapiteln beschrieben:

- Kapitel 2.2, „Aufbau von HTTP-Requests“
- Kapitel 2.3, „Beispiele“
- Kapitel 3, „Beschreibung der Endpunkte“

2.2 Aufbau von HTTP-Requests

In einem *HTTP-Request* werden bestimmte Elemente an einen RESTful-Server übergeben (siehe auch Beispiele in Tabelle 2-1).

URL escaping
Um zu verhindern, dass Sonderzeichen in JSON-Strings vom Server falsch interpretiert werden, müssen die Zeichen gegebenenfalls umkodiert werden (*URL escape*).

2.3 Beispiele

2.3.1 Anmeldung: CSRF-Token und Session-Cookie erzeugen

Für die sichere Konfiguration und Administration des Geräts über die *Config API* muss bei der Anmeldung des Benutzers zunächst ein *CSRF-Token* und ein sicheres *Session-Cookie* vom Gerät (= RESTful-Server) generiert und an den RESTful-Client übertragen werden.

CSRF-Token und **Session-Cookie** müssen in späteren Requests erneut angegeben werden: Speichern Sie die Informationen an einem geeigneten Ort ab.

Schritt 1

1) CSRF-Token anfordern (Endpunkt "csrf")

Ein **Login-Cookie** und ein **CSRF-Token** zur Absicherung einer Session (Sitzung) werden vom Gerät (= RESTful-Server) erzeugt und an den RESTful-Client übermittelt.

Gehen Sie wie folgt vor:

- GET-Request auf den Endpunk "csrf".

⇒ Ein *CSRF-Token* und ein *Login-Cookie* (z. B. *login_cookie*) werden erzeugt.

- Speichern bzw. kopieren Sie das *CSRF-Token* und ggf. auch das *Login-Cookie*.

Beispiel:

curl **-c** *login_cookie* -k -X GET https://192.168.1.1:443/api/v1/csrf

Antwort:

{"content":"ImIzYzk3N2UyYjFiYThlZmY5Yzc1M2FhZTQxYmE1MmYxZDQwZjQ3ZWYi_l2dMwHYPyJeVR1rFgli0Tww","envelope":{"identifier":{"contentID":"d2c01a66","functionalID":"d2c01a66"},"version":1},"error":[],"schemes":[],"status":0}

CSRF-Token: Das *CSRF-Token* wird als "*content*" zurückgeliefert und ist nur in Verbindung mit einem *Session-Cookie* gültig, das im nächsten Schritt über den Endpunkt "*login*" erzeugt werden muss.
Das aktuelle CSRF-Token muss in allen nachfolgenden *POST-Requests* innerhalb der laufenden Session angegeben werden.

Login-Cookie: Das *Login-Cookie* wird bei der Verwendung von *curl* mittels der Option *-c <login_cookie_name>* auf dem Konfigurations-Rechner abgespeichert.
Bei der Verwendung von grafischen RESTful-Clients wird das Cookie häufig automatisch gespeichert.

Schritt 2

2) Anmelden und Sitzung starten (Endpunkt "login")

Im Rahmen der Benutzer-Anmeldung müssen folgende Angaben gemacht werden:

- **Header:**
  - **Content-Type**: *application/json*
  - **X-CSRF-TOKEN**: das zuvor erzeugte <*CSRF-Token*> bzw. die Variable
- **Login-Cookie (**geschieht ggf. automatisch): das zuvor erzeugte <*login_cookie*>
- **Benutzername/Passwort** (als Content)

Gehen Sie wie folgt vor:

- POST-Request auf den Endpunk "login".

⇒ **Session-Cookie** (*session_cookie*) wird erzeugt.

- Speichern bzw. kopieren Sie ggf. das *Session-Cookie.*

⇒ Das *Session-Cookie* ist notwendig, um nachfolgende *GET*- und *POST-Requests* durchzuführen.

Beispiel:

curl **-b** *login_cookie* **-c** *session_cookie* -k -X POST https://192.168.1.1:443/api/v1/login -H "**X-CSRF-Token**: ImIzYzk3N2UyYjFiYThlZmY5Yzc1M2FhZTQxYmE1MmYxZDQwZjQ3ZWYi_l2dMwHYPyJeVR1rFgIi0Tww" -H "Content-Type: application/json" -d '{"**content**": {"username": "admin", "password": "private"}, "envelope": {"version": 1}}'

Antwort:

{"content":{},"envelope":{"identifier":{"contentID":"a3a6bf43","functionalID":"a3a6bf43"},"version":1},"error":[],"schemes":[{"name":"login.login.c1a52347","url":"/v1/login/scheme/login.login.c1a52347"}],"status":0}

Session-Cookie: Ein mittels *Login-Cookie* und C*SRF-Token* abgesichertes *Session-Cookie* wird erzeugt und (bei der Verwendung von *curl*) mithilfe der Option *-c <session_cookie_name>* auf dem Konfigurations-Rechner abgespeichert.

GET- und POST-Requests
In allen folgenden GET- und *POST-Requests* innerhalb einer Sitzung, muss *curl* mit der Option *-b <session_cookie_name>* aufgerufen werden, um das gespeicherte *Session-Cookie* zu verwenden.

Verwendung verschiedener RESTful-Clients

curl

Siehe Kapitel 3.3, „Endpunkt "csrf" / "login" / "logout"“.

YARC!

Siehe Kapitel 2.5, „RESTful-Client „YARC!“ verwenden (Chrome)“.

Nightingale

Beim **RESTful-Client „Nightingale“** (für Microsoft Windows) erfolgt die Erzeugung und Verwendung von *CSRF-Token* und *Session-Cookie* ähnlich wie bei *YARC!*.

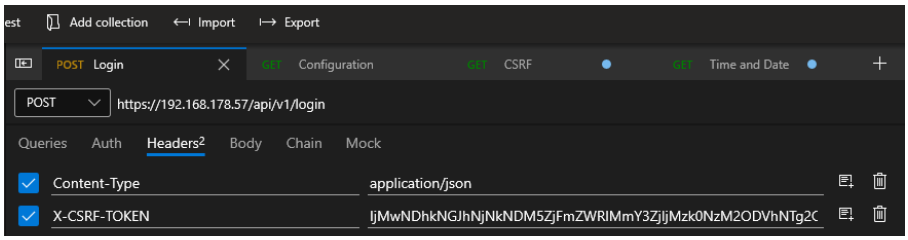

Bild 2-2 Beispiel: RESTful-Client „*Nightingale*“

2.3.2 Gerätekonfiguration ändern (POST-Request)

Wenn Sie eine Variable der Gerätekonfiguration im Endpunkt "*configuration*" mittels *POST-Request* ändern möchten, müssen Sie auch die Variablen (d. h. alle *keys* des *Frames*), die nicht geändert werden sollen, mit dem gleichen *POST-Request* an den RESTful-Server übergeben.

Das bedeutet beispielsweise, dass bei einer Änderung des *Hostnamens* auch bereits vorhandene *Firewall-Regeln*, *Netzwerkeinstellungen* etc. im *POST-Request* angegeben werden müssen (siehe unten: „Beispiel“).

Empfohlenes Vorgehen

- Führen Sie einen *GET-Request* auf den Endpunkt "*v1/configuration*" durch, um die aktuelle Gerätekonfiguration anzuzeigen.
- Editieren Sie die gewünschten Variablen.
- Kopieren Sie die Konfiguration in einen POST-Request.
- Senden Sie die geänderte Konfiguration als *POST-Request* an das Gerät.

Bitte beachten Sie:

Je nach verwendetem RESTful-Client müssen Sie den *POST-Request* vor dem Senden weiter anpassen.

Einige Teile der Antwort auf den *GET-Request* dürfen nicht in einem *POST-Request* gesendet werden. Ein *POST-Request* mittels RESTful-Client *curl* endet z. B. mit dem Eintrag: *"envelope": {"version": 1}}*'

Beachten Sie die korrekte Verwendung der Hochkommata zu Beginn und am Ende des Inhaltsblocks (content): ... -d '{"content": {"firewall“ ... “env*elope": {"version": 1}}*'

Beispiel

Eine Änderung des Hostnamens des Geräts sieht beispielsweise wie folgt aus.

(In diesem Beispiel wird der RESTful-Client *curl* über die Linux-Kommandozeile verwendet.)

1. Fragen Sie die aktuellen Werte des Endpunktes "configuration" ab (**GET-Request**).

GET-Request:

curl -k **-b** *session_cookie* -X GET https://192.168.1.1:443/api/v1/configuration

Antwort: (Für eine strukturierte Ansicht des Beispiels mit Firmware 1.8.0), siehe Kapitel 4.2.)

{"content": {"fileinfo": {"devtype": "0001010111020000", "firmware": "1.4.1"}, "**firewall**": {"forward": {"log_all_matches": "ON", "log_policy": "ON", "sanity_check": "ON", "stealth_allow_dhcp": "ON", "tables": [{"in_netzone": "NETZONE1", "out_netzone": "NETZONE2", "rules": []}, {"in_netzone": "NETZONE2", "out_netzone": "NETZONE1", "rules": [{"comment": "", "dst_network": "0.0.0.0/0", "dst_port": "ALL", "id": 0, "log": "OFF", "protocol": "ALL", "src_network": "0.0.0.0/0", "verdict": "ACCEPT"}]}], "testmode": "ON"}, "input": {"rules": [{"id": 0, "log": "OFF", "service": "HTTPS", "source": "NETZONE2", "verdict": "ACCEPT"}, {"id": 1, "log": "OFF", "service": "HTTPS", "source": "NETZONE1", "verdict": "ACCEPT"}]}, "port_forward": {"rules": [{"comment": "", "dst_ip": "0.0.0.0", "dst_port": 443, "inc_port": 5000, "protocol": "TCP", "src_interface": "NETZONE1"}, {"comment": "", "dst_ip": "0.0.0.0", "dst_port": 102, "inc_port": 5001, "protocol": "UDP", "src_interface": "NETZONE1"}]}}, "**logging**": {"remote": {"address": "syslog.my-mguard.com", "port": 513, "protocol": "UDP", "status": "ON"}}, "**network**": {"mode": "ROUTER", "nat": {"1_1_nat": [{"comment": "", "id": 0, "real_network": "192.168.1.100", "virt_network": "10.1.0.101"}, {"comment": "", "id": 1, "real_network": "192.168.1.200", "virt_network": "10.1.0.102"}], "masquerading": [{"from_ip": "0.0.0.0/0", "id": 0, "outgoing_on_if": "NETZONE1"}]}, "netzone1": {"mode": "DHCP"}, "netzone2": {"address": "192.168.1.1", "netmask": 24}, "routing": {"routes": [{"comment": "Production3", "gateway": "192.168.1.10", "network": "192.168.10.0/24"}]}, "stealth": {"management_address": "192.168.1.1", "management_gateway": "192.168.1.254", "management_netmask": 24}}, "**service**": {"dhcp_server": {"dns": "192.168.1.1", "gateway": "192.168.1.1", "lease_time": "12h", "netmask": 24, "range_high": "192.168.1.254", "range_low": "192.168.1.2", "status": "ON", "wins_server": ""}, "dnscache": {"allowed_requests": ["NETZONE2", "NETZONE1"], "dns_servers": "USER_DEFINED", "log": "ON", "user_defined": [{"comment": "", "ip": "212.2.220.212"}]}, "ntp": {"allow_client_requests": ["NETZONE2"], "server": [{"address": "0.pool.ntp.org", "comment": "", "port": 123}, {"address": "1.pool.ntp.org", "comment": "", "port": 123}, {"address": "2.pool.ntp.org", "comment": "", "port": 123}], "status": "ON"}, "snmp": {"allow_requests_from": ["NETZONE2"], "ro_community_string": "public", "status_v2c": "ON", "status_v3": "ON", "user": {"username": "snmp-v3-user"}}, "web": {"session_timeout": 450}}, "**system**": {"hostname": "OldName", "store_config_on_sdcard": "OFF", "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited."}, "**zoneinfo**": "UTC"}, "envelope": {"identifier": {"contentID": "8effd771", "functionalID": "dc5a1dcc"}, "version": 1}, "error": [], "schemes": [{"name": "common.4710ab60", "url": "/v1/configuration/scheme/common.4710ab60"}, {"name": "common.types.f0bf23da", "url": "/v1/configuration/scheme/common.types.f0bf23da"}, {"name": "configuration.fileinfo.b3afd1b0", "url": "/v1/configuration/scheme/configuration.fileinfo.b3afd1b0"}, {"name": "configuration.firewall.62d07c99", "url": "/v1/configuration/scheme/configuration.firewall.62d07c99"}, {"name": "configuration.hostname.27e2cb1c", "url": "/v1/configuration/scheme/configuration.hostname.27e2cb1c"}, {"name": "configuration.logging.fce1b9ba", "url": "/v1/configuration/scheme/configuration.logging.fce1b9ba"}, {"name": "configuration.network.0edde642", "url": "/v1/configuration/scheme/configuration.network.0edde642"}, {"name": "configuration.service.69f74574", "url": "/v1/configuration/scheme/configuration.service.69f74574"}, {"name": "configuration.system.9df06664", "url": "/v1/configuration/scheme/configuration.system.9df06664"}, {"name": "configuration.zoneinfo.e8437e00", "url": "/v1/configuration/scheme/configuration.zoneinfo.e8437e00"}], "status": 0}

2. Kopieren Sie die modifizierte Antwort in einen **POST-Request**.

URL escaping

– Beachten Sie die korrekte Verwendung der Hochkommata zu Beginn und am Ende des Inhaltsblocks (*content*): ... -d '{"content": {"fileinfo“ ... “envelope": {"version": 1}}'

– Prüfen Sie, ob bestimmte von Ihnen verwendete Zeichen gegebenenfalls mittels *URL escaping* umcodiert werden müssen.

POST-Request:

curl -k **-b** *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/configuration -d '{{"content": {"fileinfo": {"devtype": "0001010111020000", "firmware": "1.4.1"}, "**firewall**": {"forward": {"log_all_matches": "ON", "log_policy": "ON", "sanity_check": "ON", "stealth_allow_dhcp": "ON", "tables": [{"in_netzone": "NETZONE1", "out_netzone": "NETZONE2", "rules": []}, {"in_netzone": "NETZONE2", "out_netzone": "NETZONE1", "rules": [{"comment": "", "dst_network": "0.0.0.0/0", "dst_port": "ALL", "id": 0, "log": "OFF", "protocol": "ALL", "src_network": "0.0.0.0/0", "verdict": "ACCEPT"}]}], "testmode": "ON"}, "input": {"rules": [{"id": 0, "log": "OFF", "service": "HTTPS", "source": "NETZONE2", "verdict": "ACCEPT"}, {"id": 1, "log": "OFF", "service": "HTTPS", "source": "NETZONE1", "verdict": "ACCEPT"}]}, "port_forward": {"rules": [{"comment": "", "dst_ip": "0.0.0.0", "dst_port": 443, "inc_port": 5000, "protocol": "TCP", "src_interface": "NETZONE1"}, {"comment": "", "dst_ip": "0.0.0.0", "dst_port": 102, "inc_port": 5001, "protocol": "UDP", "src_interface": "NETZONE1"}]}}, "**logging**": {"remote": {"address": "syslog.mymguard.com", "port": 513, "protocol": "UDP", "status": "ON"}}, "**network**": {"mode": "ROUTER", "nat": {"1_1_nat": [{"comment": "", "id": 0, "real_network": "192.168.1.100", "virt_network": "10.1.0.101"}, {"comment": "", "id": 1, "real_network": "192.168.1.200", "virt_network": "10.1.0.102"}], "masquerading": [{"from_ip": "0.0.0.0/0", "id": 0, "outgoing_on_if": "NETZONE1"}]}, "netzone1": {"mode": "DHCP"}, "netzone2": {"address": "192.168.1.1", "netmask": 24}, "routing": {"routes": [{"comment": "Production3", "gateway": "192.168.1.10", "network": "192.168.10.0/24"}]}, "stealth": {"management_address": "192.168.1.1", "management_gateway": "192.168.1.254", "management_netmask": 24}}, "**service**": {"dhcp_server": {"dns": "192.168.1.1", "gateway": "192.168.1.1", "lease_time": "12h", "netmask": 24, "range_high": "192.168.1.254", "range_low": "192.168.1.2", "status": "ON", "wins_server": ""}, "dnscache": {"allowed_requests": ["NETZONE2", "NETZONE1"], "dns_servers": "USER_DEFINED", "log": "ON", "user_defined": [{"comment": "", "ip": "212.2.220.212"}]}, "ntp": {"allow_client_requests": ["NETZONE2"], "server": [{"address": "0.pool.ntp.org", "comment": "", "port": 123}, {"address": "1.pool.ntp.org", "comment": "", "port": 123}, {"address": "2.pool.ntp.org", "comment": "", "port": 123}], "status": "ON"}, "snmp": {"allow_requests_from": ["NETZONE2"], "ro_community_string": "public", "status_v2c": "ON", "status_v3": "ON", "user": {"username": "snmp-v3-user"}}, "web": {"session_timeout": 450}}, "**system**": {{"hostname": "NewName", "store_config_on_sdcard": "OFF", "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited."}, "**zoneinfo**": "UTC"}, "envelope": {"version": 1}}'

Antwort: (Für eine strukturierte Ansicht des Beispiel (Request und Antwort) mit Firmware 1.8.0, siehe Kapitel 4.3)

2.3.3 Gerätefirmware updaten (POST-Request)

In diesem Beispiel wird der RESTful-Client *curl* über die Linux-Kommandozeile verwendet.

Sie können die Firmware des Geräts mittels *POST-Request* mit einer lokal gespeicherten Update-Datei updaten.

```
curl -v -b session_cookie -H "X-CSRF-Token: <TOKEN>" -H "Content-Type:multipart/form-data" -X POST -F update_info='{"content": {}, "envelope": {"version": 1}}' -F update_file=@/home/update/mGuard-image-1.8.0.mguard3.update.signed -k https://192.168.1.1:443/api/v1/update
```

Anmerkung

– Der Parameter *update_info* enthält keine Daten über den JSON-Frame und wird leer übergeben.
– Der Parameter *update_file* enthält den Pfad zur Update-Datei.

2.3.4 Tabellenzeilen in die JSON-Datei einfügen

Einzelne Tabellenzeilen (z. B. Firewall-Regeln), werden durch Kommata voneinander abgetrennt.

Beispiel (Auszug)

*{"***firewall***": {"forward": {"rules": [*

– *{*"dst_network": " 0.0.0.0/0*", "dst_port": "* ALL*", "id": 0, "protocol": "*ALL*", "*src_network": " *192.168.1.0/24, "verdict": "ACCEPT"},*
{"dst_network": " 0.0.0.0/0*", "dst_port": "* ALL*", "id": 1, "protocol": "*ALL*", "*src_network": " *192.168.2.0/24, "verdict": "DROP"}*

2.4 RESTful-Client „curl“ verwenden (Linux)

ACHTUNG: Software von Drittanbietern
Phoenix Contact übernimmt keine Garantie oder Haftung bei der Verwendung von Produkten von Drittanbietern. Verweise auf oder Beschreibungen von Drittanbieter-Software stellen keine Empfehlung dar, sondern sind Beispiele für grundsätzlich verwendbare Programme.

Tabelle 2-1 Elemente, die bei einer Anfrage an einen RESTful-Server verwendet werden können (z. B. Client = *curl*)

Element	Optionen	Beschreibung
RESTful-Client *(curl)*	*-k* *--insecure*	Sorgt dafür, dass das HTTPS-Sicherheitszertifikat des Geräts nicht geprüft wird.
	-H *--header*	Fügt einen zusätzlichen Header in die HTTP-Anfrage von *curl* ein. Für einen *POST-Request* an den RESTful-Server des Geräts, muss zum Ändern der Konfiguration z. B. der Header "*Content-Type: application/json*" angegeben werden, für das Hochladen einer Update-Datei der "*Content-Type: multi-part/form-data*".
	-X <cmd> *--request <cmd>*	Gibt eine benutzerdefinierte Anforderungsmethode an.
	-c <Dateiname> *--cookie-jar*	Speichert das vom RESTful-Server übertragene *Session-Cookie* auf dem Konfigurations-Rechner.
	-b <Dateiname> *--cookie*	Verwendet das gespeicherte *Session-Cookie* im Cookie-Header eines *GET-*, oder *POST-Requests* an den RESful-Server.
	-d *--data*	Sendet die angegebenen Daten in einem *POST-Request* an den RESTful-Server in der Form, in der ein Webbrowser ein ausgefülltes HTML-Formular senden würde (siehe auch Option: *-F / --form*).
	-O *--remote-name*	Die Ausgabe wird in eine lokale Datei geschrieben und im aktuellen Arbeitsverzeichnis gespeichert. Der Dateiname wird aus der angegebenen URL extrahiert. Wenn der Dateiname vom Server, also vom Gerät, bestimmt werden soll, müssen Sie zusätzlich die Option *-J / --remote-header-name* verwenden. Die Option *-o / --output <filename>* muss in diesem Fall nicht verwendet werden.
	-J *--remote-header-name*	Die Option -J kann nur zusammen mit der Option -O verwendet werden. Die Option *-O / --remote-name* wird dabei angewiesen, den vom Server angegebenen Dateinamen zu verwenden, anstatt einen Dateinamen aus der URL zu extrahieren. Die Option *-o / --output <filename>* muss in diesem Fall nicht verwendet werden.
	-o <file> *--output <file>*	Schreibt die Ausgabe in die Datei *<file>* und nicht nach *stdout*.
	-v *--verbose*	Führt dazu, dass *curl* zusätzliche Informationen zu einem laufenden *Request* zurückgibt (z. B. Warnungen oder Informationen zu gesendeten Daten).
	-F *--form*	Führt dazu, dass *curl* Daten mit Hilfe des "*Content-Type:multipart/form-data*" mittels *POST-Request* senden kann (siehe auch Option: -d / --data).

Tabelle 2-1 Elemente, die bei einer Anfrage an einen RESTful-Server verwendet werden können (z. B. Client = *curl*)

Element	Optionen	Beschreibung
Content-Type	*application/json*	Um mittels *POST-Request* Dateien im JSON-Format zu ändern, muss im Header der Anfrage an den RESTful-Server "*Content-Type:application/json"* angegeben werden.
	multipart/form-data	Um mittels *POST-Request* das Hochladen von Dateien zu initiieren, muss im Header der Anfrage an den RESTful-Server "*Content-Type:multiform/form-data*" angegeben werden. Der in der Anfrage enthaltene *form-data key* "*update_info*" enthält einen leeren JSON-Frame, der *form-data key "update_file*" die eigentliche Update-Datei.
HTTP-Request (Methode)	*GET*	Der RESTful-Server wird angewiesen, die im *HTTP-Request* eindeutig spezifizierten Daten (Objekte) an den RESTful-Client zu übermitteln. Beispiel: Die Konfiguration des Geräts wird ausgelesen.
	POST	Inhalte (Objekte) werden vom RESTful-Client in einem Datenblock an den RESTful-Server übertragen. Beispiel: Die Konfiguration des Geräts wird neu erstellt oder geändert.
URL	*https://username:password@<IP-Adresse>:<Port>/api/v1/<Endpunkt>* Die Adresse, über die die *Config API* des Geräts erreicht werden kann. Die Konfiguration von Variablen finden in den *Endpunkten* statt. Die Authentifizierung erfolgt mittels Benutzernamen und Passwort.	
Endpunkt	Bestandteil der URL zum Aufrufen des RESTful-Webservices. Die Konfiguration der Geräte-Variablen findet in den Schlüsseln (*keys*) eines Frames der verfügbaren Endpunkte statt (siehe Kapitel 3).	
Argument	*content*	Enthält die Daten des Frames (die Struktur wird in den *schemes* definiert).
	envelope	Enthält allgemeine Informationen über den Frame.
	version	Version der *Config API* (ist ebenfalls Teil des Endpunkts, z. B. v1/configuration).
	identifier	Enthält zwei Hash-Werte, mit deren Hilfe Änderungen in der Konfiguration erkannt werden können.
	contentID	Beschreibt einen Hash-Wert über eine allgemein formatierte (und geordnete) Eingabedatei, um damit auf jegliche Änderung der monolithischen Konfiguration hinzuweisen.
	functionalID	Beschreibt einen Hash-Wert über die effektiv konfigurierte Funktionalität des Geräts, um damit auf jegliche Änderungen der Funktionalität (Berechtigungen eines Benutzers) hinzuweisen.
	error	Enthält eine Fehlerbeschreibung (siehe „Fehlermeldungen (RESTful-Server)“)
	schemes	Enthält den Verweis zu den Schemata (*schemes*) für den aktuellen Endpunkt.
	status	Enthält den Status der aktuellen Anfrage (*request*) (bezogen auf den Fehlerindex). Zeigt bei einem Fehler die minimale Fehler-ID aus der Fehlerliste an. Bei Erfolg wird die *0* angezeigt.

2.5 RESTful-Client „YARC!“ verwenden (Chrome)

Mittels der Browser-Erweiterung *YARC!* für *Google Chrome* können einfache *GET*- und *POST-Requests* im Webbrowser durchgeführt werden. (Zuletzt getestet: Oktober 2021)

ACHTUNG: Software von Drittanbietern
Phoenix Contact übernimmt keine Garantie oder Haftung bei der Verwendung von Produkten von Drittanbietern. Verweise auf oder Beschreibungen von Drittanbieter-Software stellen keine Empfehlung dar, sondern sind Beispiele für grundsätzlich verwendbare Programme.

2.5.1 Abgesicherte Sitzung starten und Benutzer anmelden

Bevor Sie die Konfiguration mittels *GET*- bzw. *POST-Request* abrufen oder ändern können, müssen Sie den Benutzer *admin* innerhalb einer abgesicherten Sitzung anmelden. Das dabei verwendete *Session-Cookie* wird automatisch vom Webbrowser gespeichert.

Gehen Sie wie folgt vor:

1. **CSRF-Token erzeugen**

– **Request**: GET
– **URL**: *https://192.168.1.1/api/v1/csrf*
– Der Token wird in der Antwort als *content* angegeben:
Response*: "content":* "ImI1ZTY5NzhjNjhlO-WY2ZDk4N2JjMDVkYmRkNTQ4NjgwZGViZDY-wODgi.ESghMQ.vUlJDwWK20p8OJYbs5GVhzcvwM8"

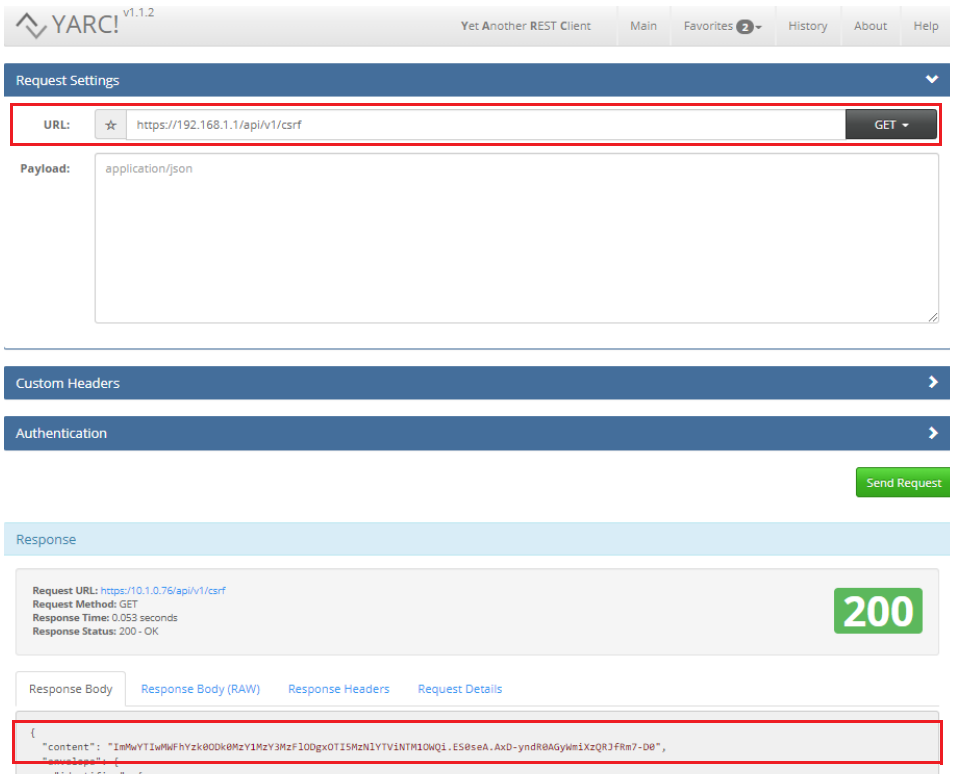

Bild 2-3 *GET-Request* auf Endpunkt *csrf*: CSRF-Token erzeugen

2. **Anmelden**

– **Request**: POST
– **URL**: *https://192.168.1.1/api/v1/login*
– **Payload**: {"content": {"username": "admin", "password": "private"}, "envelope": {"version": 1}}
– **Custom Headers**:
  – Content-Type: application/json
  – X-CSRF-Token: ImMwYTIwMWFhYzk0ODk0MzY22MZY3MzFlOSgxOTISMzNlYTViNTM1OWQi.ES0seA.AxD-yndRoAGyWmiXzQRJfRm7-D0

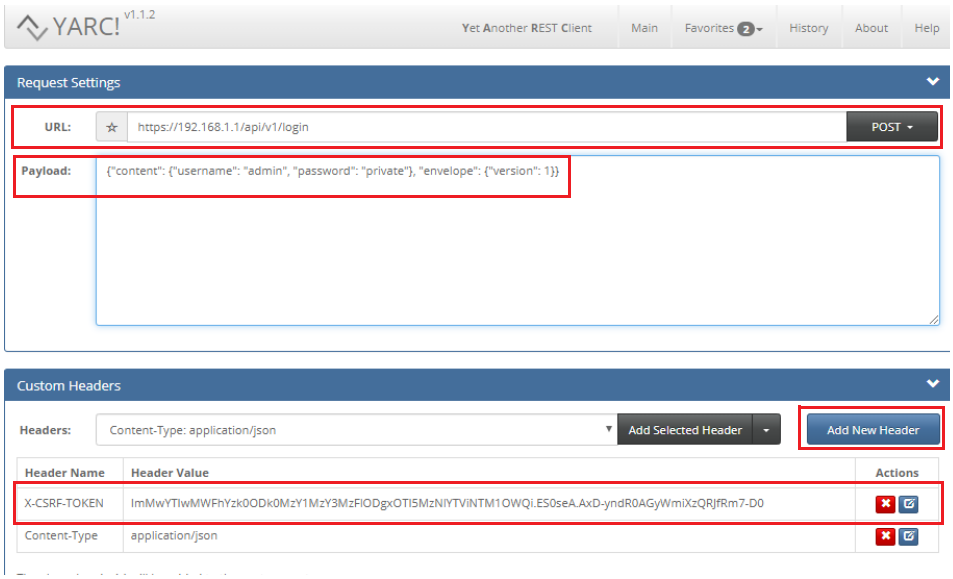

Bild 2-4 *POST-Request* auf Endpunkt *login*: Benutzer anmelden (mit CSRF-Token)

⇒ Nach einem erfolgreichem POST-Request auf den Endpunk *login* wurde ein *Session-Cookie* erzeugt.
⇒ Sie können nun *GET-* und *POST-Requests* innerhalb einer abgesicherten Sitzung (Session) senden.

3. **GET- und POST-Requests senden** (siehe Kapitel 2.5.2)

– **Request**: GET
– **URL**: *https://192.168.1.1/api/v1/configuration*
– **Payload**: leer (GET) bzw. Inhalt (POST)
– **Custom Headers** (nur *POST-Requests*):
  – Content-Type: application/json
  – X-CSRF-Token: ImMwYTIwMWFhYzk0ODk0MzY22MZY3MzFlOSgxOTISMzNlYTViNTM1OWQi.ES0seA.AxD-yndRoAGyWmiXzQRJfRm7-D0

2.5.2 Beispiel: Konfiguration mittels POST-Request ändern

- Melden Sie sich an, indem Sie ein *CSRF-Token* und ein *Session-Cookie* erzeugen.
- Führen Sie einen *GET-Request* auf den Endpunkt *configuration* durch (siehe Bild 2-5).

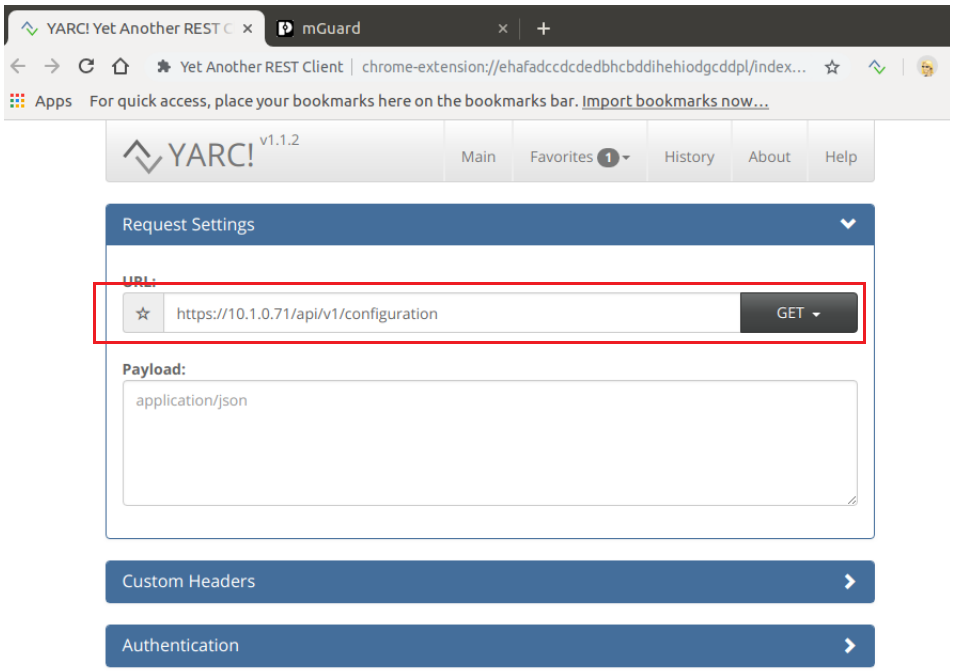

Bild 2-5 *GET-Request* auf den Endpunkt *configuration.*

⇒ Die Antwort des *GET-Requests* wird angezeigt (siehe Bild 2-6).

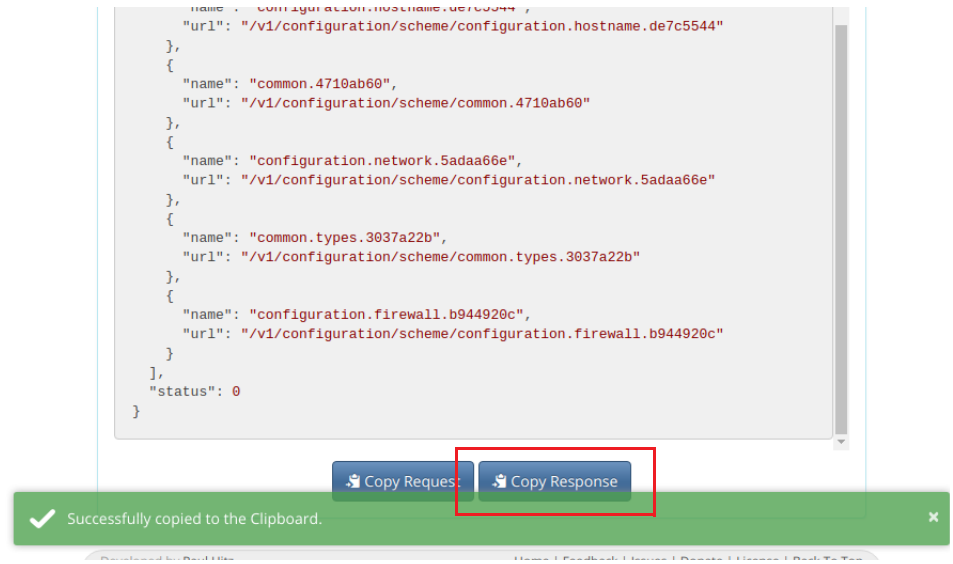

Bild 2-6 Antwort auf *GET-Request* wird angezeigt und kann kopiert werden

- Kopieren Sie die Antwort in den Bereich *Payload* (siehe Bild 2-6 und 2-7).

- Ändern Sie in der Antwort die Variablen-Werte, die Sie neu konfigurieren möchten (siehe Bild 2-7).
- Löschen Sie in der Antwort alle Keys, die in einem POST-Request nicht erlaubt sind. Das sind z. B. die keys *error*, *shemes* und *status*. Der Inhalt der Anwort muss mit dem key *envelope* wie folgt beendet werden:
  "envelope": {"version": 1}}
- Wählen Sie *POST* aus dem Drop-Down-Menü (*Request Settings*), um einen *POST-Request* zu senden.
- Klicken Sie auf **Send Request**.

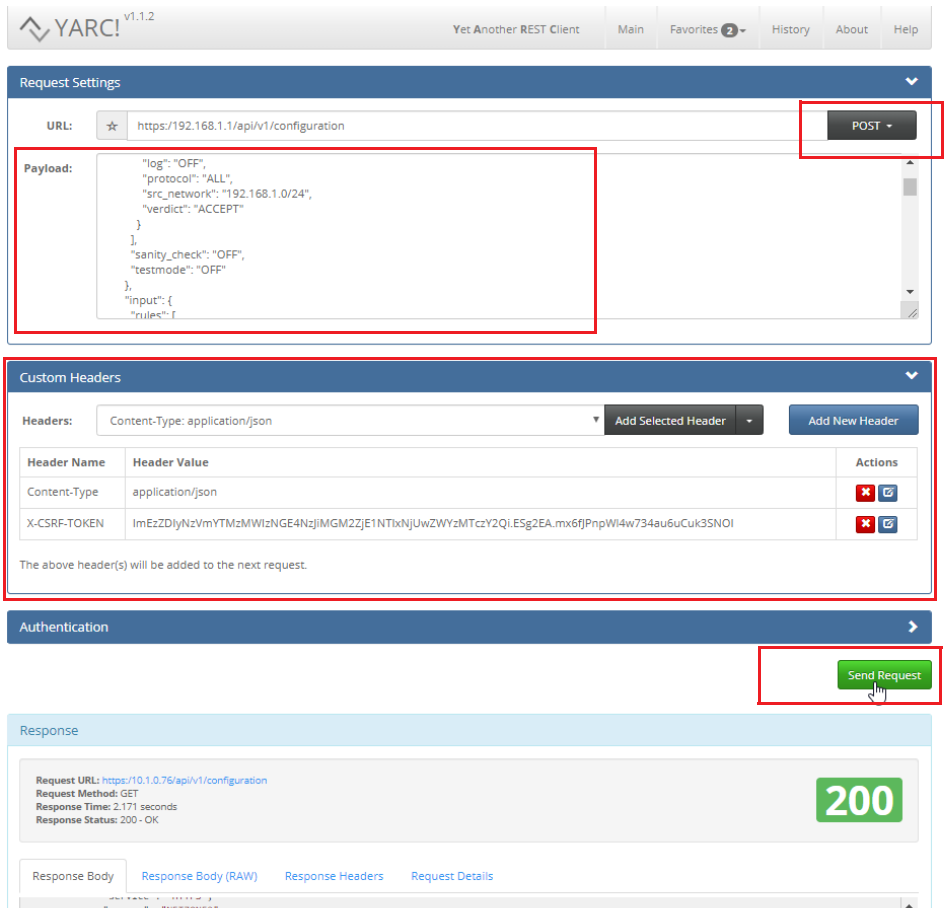

Bild 2-7 Angepasste Konfiguration als *POST-Request* senden (*Payload*-Fenster)

⇒ Die gesamte Konfiguration wird mit den geänderten Variablen-Werten an den RESTful-Server gesendet und die Gerätekonfiguration entsprechend geändert.

- Prüfen Sie mit einem erneuten *GET-Request*, ob die Änderungen wie gewünscht übernommen wurden.

2.6 Häufige Fehler (Troubleshooting)

1. **CSRF-Token**

   Vor der Anmeldung des Benutzers (über den Endpunkt *"login"*) muss ein *CSRF-Token* über den Endpunkt *"csrf"* generiert werden. Das *CSRF-Token* muss bei der Anmeldung und bei jedem weiteren *POST-Request* angegeben werden (siehe Kapitel 3.3).

2. **Login-Cookie**

   Mit der Erzeugung des *CSRF-Tokens* (siehe oben) wird ein *Login-Cookie* erzeugt, das bei der Anmeldung des Benutzers (siehe unten) zur Erzeugung des Sessions-Cookies verwendet werden muss (siehe Kapitel 3.3).

3. **Session-Cookie**

   Bei der Anmeldung des Benutzers über den Endpunkt *"login"* muss ein *Session-Cookie* erzeugt werden. Das zuvor erzeugte *CSRF-Token* muss in diesem Schritt ebenfalls angegeben werden (siehe oben).

   Das *Session-Cookie* muss nach erfolgter Anmeldung (= Start der Session) bei jedem GET- und *POST-Request* angegeben werden (siehe Kapitel 3.3).

4. **Anführungszeichen**

   Prüfen Sie bei einer fehlerhaften Eingabe die richtige Verwendung von Anführungszeichen. Beachten Sie, dass manche Variablen-Werte ohne Anführungszeichen angegeben werden müssen (z. B. Netzmasken).

5. **Klammern**

   Prüfen Sie bei einer fehlerhaften Eingabe, ob alle Klammern korrekt geöffnet und geschlossen wurden.

6. **URL escaping**

– Prüfen Sie die korrekte Verwendung der Hochkommata zu Beginn und am Ende des Inhaltsblocks (*content*): ... *-d '{"content": {"firewall“ ... “envelope": {"version": 1}}'*

– Prüfen Sie, ob bestimmte von Ihnen verwendete Zeichen gegebenenfalls mittels *URL escaping* umcodiert werden müssen.

7. **Nicht zugelassene keys in POST-Requests**

   POST-Request mit nicht zugelassenen Einträgen (*keys*) werden abgelehnt.

   Die z. B. durch einen GET-Request auf den Endpunkt *"configuration"* zurückgelieferten keys *identifier, error*, *shemes* und *status* dürfen in einem POST-Request auf den Endpunkt: *configuration*) nicht verwendet werden.

   Der Inhalt eines POST-Request muss mit dem key *envelope* wie folgt beendet werden: *“envelope": {"version": 1}}'* oder *“envelope": {"version": 1}}*

2.7 Fehlermeldungen (RESTful-Server)

Tabelle 2-2 RESTful Configuration API – Fehlermeldungen (RESTful-Server)

ID (status)	Fehlermeldung
0	OK – No error: Request successful
1	Request error
2	Interface not found
3	Server Error
4	Necessary key is missing from the request
5	The Firewall Assistant is running. Only GET- and HEAD-requests are allowed
6	No valid user session
7	Too many sessions
8	CSRF Token invalid or missing
9	Unauthorized
10001	IO Error
10002	Unknown Schema
10003	Validation Error
10004	Callback Error
10005	Apply Error
10006	System Error
10007	IP change is in progress, new IP will be:
20001	No Data entry found
20002	Wrong or missing envelope version
20003	No envelope
20010	Unexpected data entry found
20011	Duplicate JSON keys found
30001	Validation Error
30002	Schema Error
30003	Error on applying the configuration
30004	Gateway with address and netmask do not match
30005	The networks of the net zones 1 and 2 are not allowed to overlap.
40001	Something went wrong in the updater script
40002	Content-Type needs to be multipart/form-data
40003	File is too small
40004	File could not be saved
40006	Updater script can't be reached
50001	Validation Error
50002	Schema Error
50003	Error on applying the passwords

Tabelle 2-2 RESTful Configuration API – Fehlermeldungen (RESTful-Server)

ID (status)	Fehlermeldung
50004	Error on updating eds node
50005	Error: only on device managed users are allowed to change their password
60001	Validation Error
60002	Schema Error
60003	Error on applying the datetime
60004	Error on syncing datetime to RTC
70001	Unknown module requested
80001	Snapshot Error
90001	Software License Error
100001	Can't start ping
100002	Invalid arguments
110001	Can't start tcpdump
110002	Can't stop tcpdump
110003	Can't delete tcpdump
110004	No data available
110005	Tcpdump is already running
110006	Invalid arguments passed
120001	Validation Error
120002	Login failed
120003	Unknown username or password
120004	„“
130001	Logout failed
140001	Internal Error
150001	Use Notification Error
160001	Validation Error
160002	Schema Error
160003	Error on applying the user changes
160004	Error on updating eds node
170001	Cannot start the Firewall Assistant
170002	Cannot stop the Firewall Assistant
180001	Validation Error
180002	Schema Error
180003	Error reading log information
190001	Error while generating certificate
190002	Error getting certificate
190003	Error reloading/restarting logger
200001	Error while storing configurations
210001	Can't start unblockUser action

Tabelle 2-2 RESTful Configuration API – Fehlermeldungen (RESTful-Server)

ID (status)	Fehlermeldung
210002	Invalid arguments
210003	User is manual blocked by admin. Automatically blocking state can not resolved. Please unblock user by change 'block_user' in users config
210004	User not found in Database
220001	Error while migrating the configuration
220002	Validation error after migration
220003	The configuration has no valid firmware version for migration
230001	Error while rebooting via configapi

3 Beschreibung der Endpunkte

In den Endpunkten der mGuard RESTful Configuration API werden die einzelnen Variablen (*keys*) der Firmware konfiguriert.

Endpunkte stellen dabei unterschiedliche Bereiche der Firmware dar, in denen z. B. ein Firmware-Update gestartet oder die Konfiguration der Firewall geändert werden kann.

In diesem Kapitel werden die RESTful-Variablen beschrieben und den entsprechenden Menüpunkten im Web-based Management (WBM) zugeordnet (siehe Kapitel 3.1).

3.1 Verfügbare Endpunkte

Tabelle 3-1 Verfügbare Endpunkte des RESTful-Servers (mGuardNT 1.8.x)

Endpunkt	Methode	Was wird angezeigt / konfiguriert	Beschreibung
v1/csrf	**GET**	Ein *Login-Cookie* und ein *CSRF-Token* zur Absicherung einer Session (Sitzung) werden vom RESTful-Server erzeugt und an den RESTful-Client übermittelt.	Kapitel 3.3
v1/login	**POST**	Ein Benutzer wird mit seinen Zugangsdaten (*Benutzername* und *Passwort*) angemeldet. Die Sitzung wird gestartet und ein *Session-Cookie* wird erzeugt.	
v1/logout	**POST**	Der angemeldete Benutzer wird abgemeldet. Alle Informationen zur aktuellen Sitzung (*session data*) und das *Session-Cookie* werden gelöscht.	
v1/configuration	**GET**	Die Konfiguration in den Bereichen *Netzwerk*, *Firewall* und *System* wird angezeigt oder geändert.	Kapitel 3.4
	POST		
v1/configuration/default	**GET**	Die Konfiguration der werkseitigen Voreinstellung des Geräts im Bereich *Netzwerk*, *Firewall* und *System* wird angezeigt oder wiederhergestellt.	Kapitel 3.5
	POST		
v1/users	**GET**	Die Eigenschaften bestehender Benutzer werden angezeigt.	Kapitel 3.6
	POST	Benutzer werden neu hinzugefügt, editiert oder gelöscht.	
v1/password	**POST**	Das Passwort des angemeldeten Benutzers wird geändert.	Kapitel 3.7
v1/update	**POST**	Das Hochladen einer Firmwareupdate-Datei und das anschließende Ausführen des Firmwareupdates wird initiiert.	Kapitel 3.8
v1/datetime	**GET**	Das aktuelle Datum und die Uhrzeit des Geräts werden angezeigt oder geändert.	Kapitel 3.9
	POST		
v1/snapshot	**GET**	Ein Snapshot der aktuellen Gerätekonfiguration wird erstellt und heruntergeladen.	Kapitel 3.10
v1/logging	**GET**	Alle Log-Einträge auf dem Gerät werden abgerufen und angezeigt.	Kapitel 3.11
	POST	Nur Log-Einträge von Ereignissen, die die Firewall betreffen, werden abgerufen und angezeigt.	

Tabelle 3-1 [...]Verfügbare Endpunkte des RESTful-Servers (mGuardNT 1.8.x)

Endpunkt	Methode	Was wird angezeigt / konfiguriert	Beschreibung
v1/status	**GET**	Die Status-Informationen zu bestimmten Funktionen des Geräts werden abgerufen (z. B. aktuelle Firmware-Version).	Kapitel 3.12
v1/actions/fwassist/start	**POST**	Das Erfassen der Verbindungsdaten mittels *Firewall Assistant* wird gestartet.	Kapitel 3.13
v1/actions/fwassist/stop	**POST**	Das Erfassen der Verbindungsdaten mittels *Firewall Assistant* wird gestoppt. Erfasste Verbindungen werden automatisch in Firewall-Regeln umgewandelt.	
v1/actions/ping	**POST**	Eine ICMP-Anfrage wird an verbundene Netzwerk-Clients gesendet.	Kapitel 3.14
v1/actions/tcpdump/start	**POST**	Der Inhalt von Netzwerkpaketen wird analysiert (*tcpdump*). Die Analyse kann durch die Angabe von Filteroptionen eingeschränkt werden.	Kapitel 3.15
v1/actions/tcpdump/stop	**POST**	Die Analyse der Netzwerkpakete wird gestoppt. Das Ergebnis der Analyse wird automatisch in einer Datei (**.pcap*) gespeichert und heruntergeladen.	
v1/actions/pki/renew/logging	**GET**	Das Client-Zertifikat, das für die Authentifizierung des Geräts gegenüber einem Remote-Syslog-Server verwendet wird, wird erstellt und/oder heruntergeladen.	Kapitel 3.16
	POST		
v1/actions/storeconfig/sdcard	**POST**	Die aktuell auf dem Gerät gespeicherte Konfiguration wird auf die eingesetzte SD-Karte geschrieben.	Kapitel 3.17
v1/actions/reboot	**POST**	Das Gerät wird neu gestartet.	Kapitel 3.18
v1/actions/unblockuser	**POST**	Ein automatisch gesperrter Benutzer wird entsperrt.	Kapitel 3.19
v1/actions/migration	**POST**	Eine Konfiguration, die mit einer älteren Firmware-Version erstellt wurde, wird in eine Konfiguration migriert, die der aktuellen Firmware-Version entspricht.	Kapitel 3.20
v1/usenotification	**GET**	Die Systembenachrichtigung wird angezeigt.	Kapitel 3.21
v1/softwarelicense	**GET**	Die *Software License Terms* (SLT) für das Produkt werden erstellt und heruntergeladen.	Kapitel 3.22
v1/licenses	**GET**	Die auf dem Gerät verwendeten Software-Komponenten (Module) von Drittanbietern werden angezeigt.	Kapitel 3.23
v1/licenses/module/ <module name>	**GET**	Die Lizenzinformationen der auf dem Gerät verwendeten Software-Komponenten (Module) von Drittanbietern werden angezeigt.	Kapitel 3.24

3.2 Nomenklatur

Tabelle 3-2 Verwendete Nomenklatur in der Beschreibung der Endpunkte

Format	Beschreibung
<ip>	IPv4-Adresse (in Anführungszeichen) *Beispiel: "192.168.1.102"*
<nw_cidr>	IPv4-Netzwerk in CIDR-Schreibweise (in Anführungszeichen) *Beispiel: "192.168.1.0/24"* **Hinweis:** Für die Angabe einer IP-Adresse <ip> darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss ohne Netzmaske angegeben werden (siehe oben).
<nm_num>	Subnetzmaske in numerischer-Schreibweise *Beispiel: 24*
<num>	Numerischer Wert *Beispiel: 443*
<string>	Alphanumerischer Wert (in Anführungszeichen) *Beispiel: "mGuard-076"* Die erlaubten Sonderzeichen sind von der jeweils konfigurierten Variablen abhängig.
<YYYY-MM-DD_hh:mm:ss>	Datum und Uhrzeit (in Anführungszeichen) – YYYY = Jahr | MM = Monat | DD = Tag – hh = Stunde | mm = Minute | ss = Sekunde *Beispiel: "2018-06-24_18:05:09"*
<time_dhm>	Zeitangabe (in Anführungszeichen) Alphanumerischer Wert ungleich Null, mit dem die Zeit alternativ in Tagen, Stunden **oder** Minuten angegeben werden kann. d =Tag, h = Stunde, m = Minute *Beispiel: "12h"*
<time_minute>	Zeitangabe in Minuten Numerischer Wert ungleich Null, mit dem die Zeit in Minuten angegeben werden kann. *Beispiel: 60*
<timezone>	Die Zeitzone wird entsprechend der harmonisierten internationalen Zeitzonen angegeben (siehe Anhang: Kapitel 5.1).
<start:end>	Manche Werte können als Bereich angegeben werden. Die Eingabe eines Bereichs erfolgt, indem der Anfang und das Ende des Bereichs durch einen Doppelpunkt getrennt angegeben werden (Start:Ende). *Beispiel: "110:220"*

3.3 Endpunkt "csrf" / "login" / "logout"

Für die sichere Konfiguration und Administration des Geräts bzw. der Firmware muss zunächst ein sicheres *Session-Cookie* vom Gerät (RESTful-Server) generiert und an den RESTful-Client (z. B. Webbrowser) übertragen werden.

Zur Verhinderung von CSRF-Angriffen (*Cross-Site-Request-Forgery*) wird jede Sitzung (*Session*) zusätzlich über ein *CSRF-Token* abgesichert.

Vorgehen

1. *CSRF-Token* anfordern.
2. Benutzer anmelden und mit *CSRF-Token* abgesicherte Sitzung starten (*Session-Cookie*).
3. GET- und *POST-Requests* innerhalb der aktuellen Sitzung durchführen.

CSRF-Token anfordern

Ein *GET-Request* an den Endpunkt "*csrf*" erzeugt ein *CSRF-Token* und mittels der Option -c ein *Login-Cookie* (siehe Kapitel 3.3.1).

Das *CSRF-Token* muss anschließend bei der Anmeldung des Benutzers (Endpunkt "*login*") und in allen weiteren *POST-Requests* innerhalb der Sitzung angegeben werden.

Benutzer anmelden und Session-Cookie erstellen

Ein *POST-Request* an den Endpunkt "*login*", der das *Login-Cookie*, das *CSRF-Token,* sowie den Benutzernamen (*admin*) und das Benutzerpasswort (z. B. *private*) enthält, generiert ein *Session-Cookie* und startet die Sitzung (siehe Kapitel 3.3.2).

Das *Session -Cookie* muss anschließend bei allen *POST-* und *GET-Requests* innerhalb der Sitzung angegeben werden, um deren Integrität sicherzustellen.

Das *Session-Cookie* wird gelöscht, wenn ein *POST-Request* an den Endpunkt "*logout*" gesendet wird. Damit endet auch die Sitzung.

GET- und POST-Requests innerhalb einer Sitzung durchführen (siehe Kapitel 3.4)

GET-Request: Nur das *Session-Cookie* muss angegeben werden.

POST-Request: Das *Session-Cookie* und das *CSRF-Token* müssen angegeben werden.

3.3.1 Endpunkt "csrf"

Ein *Login-Cookie* und ein *CSRF-Token* zur Absicherung einer Session (Sitzung) werden vom RESTful-Server erzeugt und an den RESTful-Client übermittelt.

Das *Login-Cookie* wird mittels der Option *-c <login_cookie>* auf dem Konfigurations-Rechner abgespeichert.

Das *CSRF-Token* wird als "*content*" zurückgeliefert und ist nur in Verbindung mit dem *Session-Cookie* gültig, das im nächsten Schritt über den Endpunkt "*login*" erzeugt wird.

Beispiel

curl -k **-c** *login_cookie* -X GET https://192.168.1.1:443/api/v1/csrf

Antwort:

{"content":"ImIzYzk3N2UyYjFiYThlZmY5Yzc1M2FhZTQxYmE1MmYxZDQwZjQ3ZWYi.ESVZMA.wKC_l2dMwHYPyJeVR1rFgli0Tww","envelope":{"identifier":{"contentID":"d2c01a66","functionalID":"d2c01a66"},"version":1},"error":[],"schemes":[],"status":0}

3.3.2 Endpunkt "login"

Über diesen Endpunkt kann ein Benutzer mit seinen Zugangsdaten (Benutzername und Passwort) angemeldet werden.

Ein durch *Login-Cookie* und C*SRF-Token* abgesichertes *Session-Cookie* wird erzeugt und mittels der Option *-c <session_cookie_name>* auf dem Konfigurations-Rechner abgespeichert.

In allen folgenden GET- und *POST-Requests* innerhalb einer Sitzung, muss *curl* mit der Option *-b <session_cookie_name>* aufgerufen werden, um das gespeicherte *Session-Cookie* zu verwenden.

Beispiel

curl -k -X POST https://192.168.1.1:443/api/v1/login **-b** *login_cookie* **-c** *session_cookie* -H "**X-CSRF-Token**: ImIzYzk3N2UyYjFiYThlZmY5Yzc1M2FhZTQxYmE1MmYxZDQwZjQ3ZWYi.ESVZMA.wKC_l2dMwHYPyJeVR1rFgli0Tww" -H "Content-Type: application/json" -d '{"**content**": {"username": "admin", "password": "private"}, "envelope": {"version": 1}}'

Antwort:

{"content":{},"envelope":{"identifier":{"contentID":"a3a6bf43","functionalID":"a3a6bf43"},"version":1},"error":[],"schemes":[{"name":"login.login.c1a52347","url":"/v1/login/scheme/login.login.c1a52347"}],"status":0}

3.3.3 Endpunkt "configuration" (GET-Request)

Beispiel (GET "configuration")

curl -k **-b** *session_cookie* -X GET https://192.168.1.1:443/api/v1/configuration

Antwort:

siehe Kapitel 4.2, „GET-Request (Endpunkt: "configuration")“

3.3.4 Endpunkt "logout"

Über diesen Endpunkt kann ein angemeldeter Benutzer abgemeldet werden.

Alle Informationen zur Sitzung (*session data*) werden zusammen mit dem *Session-Cookie* gelöscht. Bei einer erneuten Anmeldung müsste ein neues *CSRF-Token* und ein neues *Session-Cookie* erzeugt werden.

Beispiel

curl -k -X POST https://192.168.1.1:443/api/v1/logout **-b** *session_cookie* -H "**X-CSRF-Token**: ImIzYzk3N2UyYjFiYThlZmY5Yzc1M2FhZTQxYmE1MmYxZDQwZjQ3ZWYi.ESVZMA.wKC_l2dMwHYPyJeVR1rFgli0Tww" -H "Content-Type: application/json" -d '{"content": {}, "envelope": {"version": 1}}'

Antwort:

{"content":{},"envelope":{"identifier":{"contentID":"a3a6bf43","functionalID":"a3a6bf43"},"version":1},"error":[],"schemes":[],"status":0}

3.4 Endpunkt "configuration"

Über diesen Endpunkt kann die Konfiguration der Elemente des Endpunkts

1. angezeigt (*GET-Request*) oder
2. geändert (*POST-Request*) werden.

Lokal gespeicherte Passwörter werden bei einem GET-Request nicht übermittelt.

Bei einem POST-Request gilt:

1. Die Konfiguration darf nicht mit einer Minor-Version erstellt worden sein, die höher ist als die, die bereits auf dem Gerät installiert ist.
2. Wird auf dem Gerät eine Konfiguration wiederhergestellt, die mit einer älteren Firmware-Version erstellt wurde, werden die Variablen-Werte, die in der älteren Firmware-Version noch nicht vorhanden waren, beibehalten.

Folgende Elemente sind Bestandteil des Endpunkts

- Firewall (durchgehender Datenverkehr) (Kapitel 3.4.1)
- Eingangs-Firewall (Gerätezugriff) (Kapitel 3.4.2)
- Port-Weiterleitung (Kapitel 3.4.3)
- Remote-Logging (Kapitel 3.4.4)
- Netzwerkmodus (Kapitel 3.4.5)
- Netzwerkkonfiguration (Kapitel 3.4.6)
- NAT-Masquerading (Kapitel 3.4.7)
- 1:1-NAT (Kapitel 3.4.8)
- Standard-Gateway (Kapitel 3.4.9)
- Zusätzliche statische Routen (Kapitel 3.4.10)
- Netzwerkdienste:
  - DHCP-Server (Kapitel 3.4.11)
  - DNS-Server / DNS-Cache (Kapitel 3.4.12)
  - NTP-Server / NTP-Client (Kapitel 3.4.13)
  - SNMP-Server (Kapitel 3.4.14)
  - Web (Session Timeout) (Kapitel 3.4.15)
- System (Kapitel 3.4.16)
  - Hostname des Geräts
  - Konfiguration automatisch speichern
  - Systembenachrichtigung
- Zeitzone (Kapitel 3.4.17)

Beispiel: Konfiguration anzeigen (GET)

curl -k **-b** *session_cookie* -X GET https://192.168.1.1:443/api/v1/configuration

Antwort:

⇒ (Ergebnis/Antwort: siehe Kapitel 4.2)

Beispiel (1.4.1): Konfiguration ändern (POST)

curl -k **-b** *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/configuration -d '{{"content": {"fileinfo": {"devtype": "0001010111020000", "firmware": "1.4.1"}, "**firewall**": {"forward": {"log_all_matches": "ON", "log_policy": "ON", "sanity_check": "ON", "stealth_allow_dhcp": "ON", "tables": [{"in_netzone": "NETZONE1", "out_netzone": "NETZONE2", "rules": []}, {"in_netzone": "NETZONE2", "out_netzone": "NETZONE1", "rules": [{"comment": "", "dst_network": "0.0.0.0/0", "dst_port": "ALL", "id": 0, "log": "OFF", "protocol": "ALL", "src_network": "0.0.0.0/0", "verdict": "ACCEPT"}]}], "testmode": "ON"}, "input": {"rules": [{"id": 0, "log": "OFF", "service": "HTTPS", "source": "NETZONE2", "verdict": "ACCEPT"}, {"id": 1, "log": "OFF", "service": "HTTPS", "source": "NETZONE1", "verdict": "ACCEPT"}]}, "port_forward": {"rules": [{"comment": "", "dst_ip": "0.0.0.0", "dst_port": 443, "inc_port": 5000, "protocol": "TCP", "src_interface": "NETZONE1"}, {"comment": "", "dst_ip": "0.0.0.0", "dst_port": 102, "inc_port": 5001, "protocol": "UDP", "src_interface": "NETZONE1"}]}}, "**hostname**": "NewName", "**logging**": {"remote": {"address": "syslog.my-mguard.com", "port": 513, "protocol": "UDP", "status": "ON"}}, "**network**": {"mode": "ROUTER", "nat": {"1_1_nat": [{"comment": "", "id": 0, "real_network": "192.168.1.100", "virt_network": "10.1.0.101"}, {"comment": "", "id": 1, "real_network": "192.168.1.200", "virt_network": "10.1.0.102"}], "masquerading": [{"from_ip": "0.0.0.0/0", "id": 0, "outgoing_on_if": "NETZONE1"}]}, "netzone1": {"mode": "DHCP"}, "netzone2": {"address": "192.168.1.1", "netmask": 24}, "routing": {"routes": [{"comment": "Production3", "gateway": "192.168.1.10", "network": "192.168.10.0/24"}]}, "stealth": {"management_address": "192.168.1.1", "management_gateway": "192.168.1.254", "management_netmask": 24}}, "**service**": {"dhcp_server": {"dns": "192.168.1.1", "gateway": "192.168.1.1", "lease_time": "12h", "netmask": 24, "range_high": "192.168.1.254", "range_low": "192.168.1.2", "status": "ON", "wins_server": ""}, "dnscache": {"allowed_requests": ["NETZONE2", "NETZONE1"], "dns_servers": "USER_DEFINED", "log": "ON", "user_defined": [{"comment": "", "ip": "212.2.220.212"}]}, "ntp": {"allow_client_requests": ["NETZONE2"], "server": [{"address": "0.pool.ntp.org", "comment": "", "port": 123}, {"address": "1.pool.ntp.org", "comment": "", "port": 123}, {"address": "2.pool.ntp.org", "comment": "", "port": 123}], "status": "ON"}, "snmp": {"allow_requests_from": ["NETZONE2"], "ro_community_string": "public", "status_v2c": "ON", "status_v3": "ON", "user": {"username": "snmp-v3-user"}}, "web": {"session_timeout": 450}}, "**system**": {"store_config_on_sdcard": "OFF", "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited."}, "**zoneinfo**": "UTC"}, "envelope": {"version": 1}}'

Antwort: (Für eine strukturierte Ansicht mit mGuardNT 1.8.0, siehe Kapitel 4.3)

3.4.1 Firewall (für durchgehenden Datenverkehr)

Einstellmöglichkeiten

1. „Logging“
2. „Konsistenzprüfung“
3. „Weiterleitung von DHCP-Paketen“
4. „Connection-Tracking-Helper (FTP)“
5. „Firewall-Tabellen“
6. „Firewall-Regeln“
7. „Firewall-Test-Mode“

Beispiel

"**firewall**": {"**forward**": {"**log_all_matches**": "ON", "**log_policy**": "ON", "**sanity_check**": "ON", "**stealth_allow_dhcp**": "ON", "**ftp_allow_field**": "ON", "**tables**": [{"in_netzone": "NETZONE2", "out_netzone": "NETZONE1", "**rules**": [{"dst_network": "0.0.0.0/0", "dst_port": "ALL", "id": 0, "protocol": "ALL", "src_network": "192.168.1.0/24, "verdict": "ACCEPT", "log": "OFF“, “comment“: ““}, {"dst_network": "192.168.1.55", "dst_port": 443, "id": 1, "protocol": "TCP", "src_network": "0.0.0.0", "src_netmask": 0, "verdict": "ACCEPT", "log": "OFF“, “comment“: “This rule belongs to the machine B“}]}, {"in_netzone": "NETZONE1", "out_netzone": "NETZONE2", "**rules**": [] }], "**testmode**": "ON"}}

Logging

Tabelle 3-3 Endpunkt **configuration**, Key(s): **firewall >> forward**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward)	log_all_matches	"ON" "OFF"	**Alle konfigurierten Regeln loggen** Bei aktivierter Funktion wird für jede Datenverbindung, auf die eine beliebige Firewall-Regel zutrifft, ein entsprechender Log-Eintrag erstellt. Das gilt auch für die Regeln, in denen das Logging mittels der Funktion „*Log*“ deaktiviert ist. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Log-Präfix: *fw-forward-* *Beispiel: "OFF"*
	log_policy	"ON" "OFF"	**Unbekannte Verbindungsversuche loggen** Bei aktivierter Funktion wird für jede Datenverbindung, auf die keine konfigurierte Firewall-Regel zutrifft, ein entsprechender Log-Eintrag erstellt. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Log-Präfix: *fw-forward-policy-* *Beispiel: "OFF"*

Konsistenzprüfung

Tabelle 3-4 Endpunkt **configuration**, Key(s): **firewall >> forward >> (sanity_check)**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward)	sanity_check	"ON" "OFF"	**TCP/UDP/ICMP-Konsistenzprüfung** Die Konsistenzprüfung erhöht den Schutz von angebundenen Netzwerk-Clients vor *Denial of Service* (DoS)-Angriffen. Bei aktivierter Funktion werden Datenpakete, die durch das Gerät geroutet und an angebundene Netzwerk-Clients weitergeleitet werden, auf das Vorhandensein schadhafter Elemente geprüft: **ICMP-Pakete** Nur bekannter ICMP-Code wird verwendet. **UDP-Pakete** Zielport im UDP-Paket ist ungleich Null. **TCP-Pakete** Quell- und Zielport im TCP-Paket sind ungleich Null. **IPv4-Pakete** Protokoll ist nicht auf Null gesetzt. Datenpakete, die den vorgegebenen Anforderungen nicht genügen, werden von der Firewall verworfen. *Beispiel:* "*ON*"

Weiterleitung von DHCP-Paketen

Tabelle 3-5 Endpunkt **configuration**, Key(s): **firewall >> forward >> (stealth_allow_dhcp)**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward)	stealth_allow_dhcp	"ON" "OFF"	**Weiterleitung von DHCP-Paketen erlauben** Im Stealth-Modus gilt: Bei aktivierter Funktion können Clients in Netzzone 2 ihre IP-Konfiguration **automatisch und unabhängig von den Einstellungen in den Firewall-Tabellen** von einem DHCP-Server in Netzzone 1 beziehen. In den Firewall-Tabellen konfigurierte Firewall-Regeln, die diesen DHCP-Datenverkehr blockieren würden, werden nicht beachtet. Eine manuelle Konfiguration von Firewall-Regeln, um DHCP-Datenverkehr zu erlauben, ist nicht erforderlich. *Beispiel:* "*ON*"

Connection-Tracking-Helper (FTP)

Tabelle 3-6 Endpunkt **configuration**, Key(s): **firewall >> forward >> (ftp_allow_field)**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward)	ftp_allow_field	"ON" "OFF"	**Connection-Tracking-Helper (FTP)** Die Aktivierung der Funktion hilft dabei, erwünschte, von der Firewall jedoch blockierte Datenverbindungen über das FTP-Protokoll, zu ermöglichen. Wird eine Verbindung über das FTP-Protokoll hergestellt, kann die Datenübertragung auf zwei Wegen erfolgen: 1. Beim „aktiven FTP“ stellt der angerufene FTP-Server im Gegenzug eine zusätzliche Verbindung zum Anrufer (FTP-Client) her, um über diese Verbindung die Daten zu übertragen. 2. Beim „passiven FTP“ baut der Anrufer (FTP-Client) eine zusätzliche Verbindung zum Server auf, um die Daten zu übertragen. Damit die zusätzliche Verbindung nicht von der Firewall blockiert wird, muss der Connection-Tracking-Helper für FTP in beiden Fällen aktiviert sein. Die aktivierte Funktion wird auch auf Datenpakete angewendet, die mittels Port-Weiterleitung weitergeleitet werden. **ACHTUNG: Keine Verbindung im Stealth-Modus bei „aktivem FTP“.** Bei Verbindungen im Stealth-Modus mit „aktivem FTP“ wird auch mit aktiviertem Connection-Tracking-Helper keine Verbindung aufgebaut. Verwenden Sie in diesem Fall entweder „passives FTP“ oder erstellen Sie eine zusätzliche Firewall-Regel, die eine Datenverbindung vom Server zum Client Ihren Anforderungen entsprechend erlaubt (z. B. Erlauben: *Netzzone 1 → Netzzone 2,* Protokoll: *TCP*, Von IP: *192.168.1.100*, Nach IP: *192.168.1.200*). *Beispiel:* "*ON*"

Firewall-Tabellen

Tabelle 3-7 Endpunkt **configuration**, Key(s): **firewall >> forward >> tables**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward, tables)	in_netzone	"NETZONE1" "NETZONE2"	**Netzzone X → Netzzone Y** Die Firewall-Regeln werden je nach Richtung des initialen Datenverkehrs in zwei unterschiedlichen Tabellen konfiguriert: – *Netzzone 1 → Netzzone 2* *(in_netzone → out_netzone)* – *Netzzone 2 → Netzzone 1* (*in_netzone → out_netzone*) Die Regeln in einer Firewall-Tabelle werden ausschließlich auf den Datenverkehr angewendet, der entsprechend der angegebenen Richtung von der einen in die andere Netzzone durch das Gerät durchgeleitet (*geroutet*) wird. Über den key **firewall >> forward >> tables** wird für jede Tabelle die Richtung des Datenverkehrs definiert, auf die die nachfolgend konfigurierten Regeln angewendet werden. **Hinweis**: 1. Beide Tabellen müssen konfiguriert werden (siehe „Beispiel“). 2. Die Werte für die Variablen *in_netzone* und *out_netzone* müssen innerhalb einer Tabelle unterschiedlich sein. *Beispiel:* "*NETZONE1*"
	out_netzone	"NETZONE1" "NETZONE2"	

Firewall-Regeln

Tabelle 3-8 Endpunkt **configuration**, Key(s): **firewall >> forward >> tables >> rules**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward, tables, rules)	dst_network	<nw_cidr> <ip>	**Nach IP/Netzwerk** Ziel (Netzwerk oder IP-Adresse), an das Datenpakete gesendet werden müssen, damit die Regel in diesem Punkt zutrifft. Wird als Subnetzmaske eine „0“ angegeben, trifft die Regel in diesem Punkt auf alle Quellen (alle IP-Adressen und Netzwerke) zu. **Hinweis:** Für die Angabe einer IP-Adresse <ip> darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss ohne Netzmaske angegeben werden. *Beispiel: "10.1.0.0/24"* *Beispiel: "10.1.0.50"*
	dst_port	<num> "ALL" <start:end>	**Nach Port** Ziel-Port oder Port-Bereich, an den Datenpakete gesendet werden müssen, damit die Regel in diesem Punkt zutrifft. "ALL" = alle Ports *Beispiel: 443* *Beispiel (Portbereich): 110:120*
	id	<num>	**ID** Identifikationsnummer der Regel Die ID bestimmt die Reihenfolge, in der die Regeln abgefragt werden, beginnend mit der niedrigsten ID. *Beispiel: 33*
	log	"ON" "OFF"	**Log** Bei aktivierter Funktion wird für jede Datenverbindung, auf die die Regel zutrifft, ein Log-Eintrag erstellt. Für Regeln, in denen die Funktion deaktiviert ist, wird kein Log-Eintrag erstellt, es sei denn, die Funktion *„Alle konfigurierten Regeln loggen“* ist aktiviert. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Log-Präfix: *fw-forward-* *Beispiel: "OFF"*

Tabelle 3-8 Endpunkt **configuration**, Key(s): **firewall >> forward >> tables >> rules**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	protocol	"TCP" "UDP" "ICMP" "GRE" "ALL"	**Protokoll** Netzwerkprotokoll, das für die Übertragung der Datenpakete verwendet werden muss, damit die Regel in diesem Punkt zutrifft. "ALL" = alle Protokolle *Beispiel: "TCP"*
	src_network	<nw_cidr> <ip>	**Von IP/Netzwerk** Quelle (Netzwerk oder IP-Adresse), von der aus Datenpakete gesendet werden müssen, damit die Regel in diesem Punkt zutrifft. **Hinweis:** Für die Angabe einer IP-Adresse <ip> darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss ohne Netzmaske angegeben werden. Wird als Subnetzmaske eine „0“ angegeben, trifft die Regel in diesem Punkt auf alle Quellen (alle IP-Adressen und Netzwerke) zu. *Beispiel: "192.168.1.0/24"* *Beispiel: "10.168.1.50"*
	verdict	"ACCEPT" "DROP" "REJECT"	**Aktion** Aktion, die ausgeführt wird, wenn alle in der Zugriffsregel konfigurierten Parameter auf ein Paket zutreffen. **Annehmen:** Die Datenpakete dürfen passieren. **Abweisen:** Die Datenpakete werden zurückgewiesen. Der Absender wird informiert. **Verwerfen:** Die Datenpakete werden verworfen. Der Absender wird nicht informiert. **Hinweis (Stealth-Modus):** Im *Stealth-Modus* führt die Auswahl der Aktion *Abweisen* zum gleichen Verhalten wie die Auswahl der Aktion *Verwerfen.* Da das Gerät im *Stealth-Modus* über keine eigene IP-Adresse verfügt, werden Datenpakete in beiden Fällen verworfen und der Absender nicht informiert. In den Log-Einträgen wird in diesen Fällen als Aktion „*drop*“ und nicht „*reject*“ protokolliert. *Beispiel: "ACCEPT"*
	comment	<string>	**Kommentar** Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

Firewall-Test-Mode

Tabelle 3-9 Endpunkt **configuration**, Key(s): **firewall >> forward >> testmode**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (forward)	testmode	"ON" "OFF"	**Firewall-Test-Mode** Ungewollt durch die Firewall abgelehnter Datenverkehr kann einfach identifiziert und durch die automatisierte Erstellung entsprechender Firewall-Regeln erlaubt werden. **ACHTUNG: Die Firewall wird deaktiviert.** Im *Firewall-Test-Mode* werden Datenpakete, die durch keine der bereits konfigurierten Firewall-Regeln erfasst werden, anders als üblich nicht verworfen, sondern weitergeleitet. **Voraussetzung** Damit der *Firewall-Test-Mode* Einträge erzeugen kann, darf in der bestehenden Firewall-Tabelle keine abschließende Regel vorhanden sein, die jeglichen Datenverkehr ablehnt. **Funktionsweise** Bei aktivierter Funktion wird der durch das Gerät durchgeleitete (*geroutete*) Datenverkehr von der Firewall analysiert. Trifft eine bereits konfigurierte Firewall-Regel auf ein Datenpaket zu, wird die Regel **wie üblich** auf das Datenpaket angewendet (*Annehmen, Abweisen* oder *Verwerfen*). Trifft keine der konfigurierten Regeln auf ein Datenpaket zu, wird das Paket **anders als üblich** nicht verworfen, sondern weitergeleitet. Gleichzeitig wird der Benutzer über das Ereignis informiert: 1. Die LED „PF2“ des Geräts leuchtet rot. 2. Der Schaltausgang „O1“ auf der COMBICON-Steckverbindung „XG2“ des Geräts nimmt *High-Pegel* ein. (Eine angeschlossene Signallampe würde in diesem Fall leuchten„Endpunkt "status"“.) 3. Im „Endpunkt "status"“ wird ein Eintrag erstellt, der vom Benutzer analysiert werden kann. Soll der Datenverkehr, der einen *Test-Mode-Alarm* ausgelöst hat, in Zukunft erlaubt werden, kann der Benutzer über das **Web-based Management** aus dem zugehörigen Eintrag in der Tabelle *Test-Mode-Alarme* (WBM) automatisch eine entsprechende Firewall-Regel erstellen. (Siehe Anwenderhandbuch „UM DE MGUARD NT“ unter phoenixcontact.net/product/1153079)

Tabelle 3-9 Endpunkt **configuration**, Key(s): **firewall >> forward >> testmode**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
			Erstellen von Firewall-Regeln aus Test-Mode-Alarmen Im **Web-based Management** können Einträge in der Tabelle *Test-Mode-Alarme* ausgewählt und automatisch als neue Firewall-Regeln am Ende der bestehenden Firewall-Tabellen eingefügt werden. Die neu eingefügten Regeln würden den entsprechenden Datenverkehr zukünftig erlauben (*Aktion* = *Annehmen*).
			Firewall-Test-Mode deaktivieren Wird der *Firewall-Test-Mode* deaktiviert, werden alle entsprechenden Einträge im „Endpunkt "status""bzw. in der Tabelle *Test-Mode-Alarme* gelöscht und eine Signalisierung durch die LED „PF2“ und den Schaltausgang „O1“ beendet.

3.4.2 Eingangs-Firewall (Gerätezugriff)

Einstellmöglichkeiten

1. „Logging“
2. „Eingangs-Firewall-Regeln“

Beispiel

"**firewall**": {"**input**": {"log_all_matches": "ON", "log_policy": "ON", "**rules**": [{"id": 0, "service": "HTTPS", "source": "NETZONE2", "verdict": "ACCEPT"}, {"id": 1, "service": "HTTPS", "source": "NETZONE1", "verdict": "ACCEPT", "log": "ON“}]}}

Logging

Tabelle 3-10 Endpunkt **configuration**, Key(s): **firewall >> input >> (log_all_matches / log_policy)**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (input)	log_all_matches	"ON" "OFF"	**Alle konfigurierten Regeln loggen** Bei aktivierter Funktion wird für jede Datenverbindung, auf die eine beliebige Eingangs-Firewall-Regel zutrifft, ein Log-Eintrag erstellt. Das gilt auch für die Regeln, in denen das Logging mittels der Funktion „*Log*“ deaktiviert ist. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Log-Präfix: *fw-input-* *Beispiel: "OFF"*
	log_policy	"ON" "OFF"	**Unbekannte Verbindungsversuche loggen** Bei aktivierter Funktion wird für jede Datenverbindung, auf die keine konfigurierte Eingangs-Firewall-Regel zutrifft, ein Log-Eintrag erstellt. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Log-Präfix: *fw-input-policy-* *Beispiel: "OFF"*

Eingangs-Firewall-Regeln

Tabelle 3-11 Endpunkt **configuration**, Key(s): **firewall >> input >> rules**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (input, rules)	id	<num>	**ID** Identifikationsnummer der Regel Die ID bestimmt die Reihenfolge, in der die Regeln abgefragt werden, beginnend mit der niedrigsten ID. *Beispiel: 33*
	log	"ON" "OFF"	**Log** Bei aktivierter Funktion wird für jede Datenverbindung, auf die die Regel zutrifft, ein Log-Eintrag erstellt. Für Regeln, in denen die Funktion deaktiviert ist, wird kein Log-Eintrag erstellt, es sei denn, die Funktion *„Alle konfigurierten Regeln loggen“* ist aktiviert. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Log-Präfix: *fw-input-* *Beispiel: "OFF"*
	service	"HTTPS"	**Dienst** Auf dem Gerät laufender Netzwerkdienst, für den eine Zugriffsregel erstellt werden soll. Über HTTPS kann auf den Web-Server des Geräts (Web-based Management und *Config API*) zugegriffen werden. *Beispiel: HTTPS*
	source	"NETZONE1" "NETZONE2"	**HTTPS-Zugang aus Netzzone 1/2** Der Zugriff auf den Web-Server (HTTPS) des Geräts aus der angegebenen Netzzone wird erlaubt (TCP-Port 443). *Beispiel: "NETZONE2"*
	verdict	"ACCEPT"	**Aktion** Aktion, die ausgeführt wird, wenn alle in der Zugriffsregel konfigurierten Parameter auf ein Paket zutreffen. *Beispiel: "ACCEPT"*

3.4.3 Port-Weiterleitung

Port-Weiterleitungs-Regeln werden vor Firewall-Regeln angewendet
Die Regeln zur Port-Weiterleitung werden angewendet und ausgeführt, bevor die konfigurierten Firewall-Regeln für durchgehenden/gerouteten Datenverkehr angewendet werden (siehe Kapitel 3.4.1).

Das heißt, eine Firewall-Regel, die allen eingehenden Datenverkehr blockiert, würde beim Zutreffen einer Port-Weiterleitungs-Regel nicht angewendet.

Beispiel

"**firewall**": "**port_forward**": {"**rules**": [{"dst_ip": "192.168.1.200", "dst_port": 5000, "inc_port": 115, "protocol": "ALL", "src_interface": "NETZONE1", “comment“: “This rule refers to production B“}]}

Tabelle 3-12 Endpunkt **configuration**, Key(s): **firewall >> port_forward >> rules**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
firewall (port_forward, rules)	inc_port	<num>	**Eingehender Port** Netzwerk-Port des Geräts, an den Datenpakete gesendet werden müssen, damit die Regel angewendet wird. Datenpakete, die an diesen Port gesendet werden, werden an die in der Regel definierte Ziel-IP-Adresse (*dst_ip*) und den definierten Ziel-Port (*dst_port*) weitergeleitet: – Die Ziel-IP-Adresse im Header des Datenpakets wird auf die in der Regel definierte Ziel-IP-Adresse (*dst_ip*) umgeschrieben. – Der Ziel-Port im Header des Datenpakets wird auf den in der Regel definierten Ziel-Port (*dst_port*) umgeschrieben. **Hinweis:** Mögliche Ports sind 1 – 65535, unter Ausschluss folgender Ports, da sie von Diensten des Geräts verwendet werden: DNS (53), HTTPS (443), NTP (123), SNMP (161), DHCP (67, 68) *Beispiel: 115*
	protocol	"TCP" "UDP"	**Protokoll** Netzwerkprotokoll, das für die Übertragung der Datenpakete verwendet werden muss, damit die Regel angewendet wird. *Beispiel: "TCP"*
	src_interface	“NETZONE1“ “NETZONE2“	**Aus** Netzzone, aus der Datenpakete an das Gerät gesendet werden müssen, damit die Regeln angewendet wird. *Beispiel: "NETZONE1"*

Tabelle 3-12 Endpunkt **configuration**, Key(s): **firewall >> port_forward >> rules**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	dst_ip	<ip>	**Nach IP** IP-Adresse des Ziel-Clients, an die eingehende Datenpakete weitergeleitet werden, wenn die Regel angewendet wird. Die Original-Ziel-Adresse im Header des Datenpakets wird auf diese IP-Adresse umgeschrieben. *Beispiel: "192.168.1.200"*
	dst_port	<num>	**Nach Port** Netzwerk-Port, an den eingehende Datenpakete weitergeleitet werden, wenn die Regel angewendet wird. Der Original-Ziel-Port im Header des Datenpakets (siehe *„inc_port"*) wird auf diesen Port umgeschrieben. *Beispiel: 5000*
	comment	<string>	**Kommentar** Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

3.4.4 Remote-Logging

Beispiel

"**logging**": {"remote": {"address": "192.168.1.254", "port": 514, "protocol": "TLS", "ca": "*-----BEGIN CERTIFICATE-----\nMIID4jdQibqcmC/Q9xueMwDQYJKoZIhvcNAQEL\nBQAw-bDELMAkG [...] g92ibqcaZmC/Q9Oys=\n-----END CERTIFICATE-----", "status": "OFF"}}*

Tabelle 3-13 Endpunkt **configuration**, Key(s): **logging**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
logging (remote)	address	<ip> <string>	**IP/Hostname (Log-Server)** IP-Adresse oder Hostname des Remote-Servers (*Syslog*-Server), an den Log-Einträge gesendet werden sollen. *Beispiel: "192.168.1.254"*
	port	<num>	**Port (Log-Server)** Netzwerk-Port, auf dem der Remote-Server Datenpakete annimmt (Standard-Port: *514/UDP*). *Beispiel: 514*
	status	"ON" "OFF"	**Remote-Logging** Bei aktivierter Funktion werden alle Log-Einträge des Geräts, dem *Syslog*-Protokoll entsprechend (siehe RFC 5424), an einen entfernten Remote-Server übertragen (siehe oben). Die Übertragung erfolgt wahlweise über das unverschlüsselte UDP- oder verschlüsselt über das TCP-Protokoll. *Beispiel: "OFF"*
	protocol	"UDP" "TLS"	**Übertragungsprotokoll** Netzwerkprotokoll, das für den Verbindungsaufbau zum Remote-Server (*Syslog*-Server) verwendet wird. **Hinweis:** Aus Sicherheitsgründen sollte immer eine verschlüsselte TLS-Verbindung zwischen dem Gerät (mGuard) und dem *Syslog*-Server genutzt werden. **UDP** Die Daten werden unverschlüsselt über das UDP-Protokoll übertragen. Eine gegenseitige Authentifizierung von Gerät und Remote-Server findet nicht statt. **TLS über TCP** Die Daten werden verschlüsselt über eine TCP-Verbindung übertragen. Eine gegenseitige Authentifizierung von Gerät und Remote-Server erfolgt mittels X.509-Zertifikaten. Das benötigte Client-Zertifikat kann über den folgenden Endpunkt angezeigt oder neu erzeugt werden: „Endpunkt "actions/pki/renew/logging"“

Tabelle 3-13 Endpunkt **configuration**, Key(s): **logging**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
			Voraussetzung: Um die Integrität und Authentizität der verschlüsselten TCP-Verbindung sicherzustellen, muss 1. ein Server-Zertifikat (CA-Zertifikat) des Remote-Servers auf dem Gerät installiert werden (siehe unten), 2. ein Client-Zertifikat auf dem Gerät erzeugt, heruntergeladen und auf dem Remote-Server installiert werden (siehe Kapitel 3.16). *Beispiel: "TLS"*
	ca	<string>	**Server-CA-Zertifikat auf das Gerät hochladen** Das CA-Zertifikat, mit dem der Remote-Server (*Syslog*-Server) authentifiziert wird, wird auf das Gerät hochgeladen. Das CA-Zertifikat wird vom Betreiber des Remote-Servers bereitgestellt und muss auf das Gerät hochgeladen werden (X.509-Zertifikat mit *öffentlichem* Schlüssel). Eine verschlüsselte TCP-Verbindung zum Remote-Server kann nur dann erfolgreich aufgebaut werden, wenn dieser seinerseits ein vom CA-Zertifikat ausgestelltes Zertifikat (mit dem *geheimen* Schlüssel) oder eine gültige Zertifikatskette, mit dem CA-Zertifikat als oberste Instanz, vorzeigt. **Format:** Die maximal erlaubte Dateigröße beträgt 1 MB. *Beispiel:* *"-----BEGIN CERTIFICATE-----\nMIID4jCCAsqgAwIBAgIUfFtWt2Ytv88GdQibqcmC/Q9xueMwDQYJKoZIhvcNA* [...] *EmQxzWgTz8ljR4VgmTXFOC2yqXOys=\n-----END CERTIFICATE-----"*

3.4.5 Netzwerk (Modus)

Beispiel **"network":** {"mode": "STEALTH"}

Tabelle 3-14 Endpunkt **configuration**, Key(s): **network >> mode >> stealth**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network	mode	ROUTER STEALTH	**Modus** Das Gerät kann in zwei Netzwerk-Modi betrieben werden. **ROUTER** Befindet sich das Gerät im Router-Modus, arbeitet es als Gateway zwischen verschiedenen Subnetzen. Der Datenverkehr wird dabei zwischen den beiden Netzwerkinterfaces (Netzzonen) des Geräts weitergeleitet (*geroutet*). Clients in Subnetz der einen Netzzone können mit Clients im Subnetz der andern Netzzone kommunizieren und Daten austauschen. Die Sicherheits- und Firewall-Funktionen des Geräts werden auf eingehenden und durchgeleiteten (*gerouteten*) Datenverkehr angewendet. **STEALTH** Der Stealth-Modus wird dazu verwendet, einen einzelnen oder mehrere lokale Clients in einem bestehenden Subnetz (z. B. die Maschinensteuerungen in einem Produktions-Netzwerk) vor unerwünschten Netzwerkzugriffen zu schützen, ohne dass deren IP-Einstellungen geändert werden müssen. Das Gerät wird dazu über seine beiden Netzwerkinterfaces (Netzzonen) zwischen den Clients und dem umgebenden Subnetz eingefügt, sodass der gesamte Datenverkehr von und zu den Clients durch das Gerät geleitet wird. Die Netzwerkkonfiguration der angeschlossenen Clients muss nicht geändert werden. Die Serverdienste DHCP-, NTP- und DNS-Server sind auf dem Gerät deaktiviert. Die Sicherheits- und Firewall-Funktionen des Geräts werden auf eingehenden und durchgeleiteten Datenverkehr (z. B. DHCP-*Requests*) angewendet. Die Konfiguration des Geräts erfolgt über die *Stealth-Management-IP-Adresse*, über die auf das WBM und die *Config API* des Geräts zugegriffen werden kann.

Mode: STEALTH

Beispiel **"network": {"mode":** "STEALTH", "stealth": {"management_address": "192.168.1.1", "management_netmask": 24, "management_gateway": "192.168.1.254"}}

Tabelle 3-15 Endpunkt **configuration**, Key(s): **network >> mode >> (STEALTH) >> stealth**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: STEALTH) (stealth)	management_ address	<ip>	**Management-IP-Adresse** IP-Adresse, über die das Gerät im Stealth-Modus erreichbar ist und administriert werden kann. Die Management-IP-Adresse ist auf allen Netzwerkinterfaces (Netzzonen) verfügbar. Die Konfiguration des Geräts erfolgt über das WBM oder die *Config API*. **Hinweis:** Das Ändern der IP-Adresse, über die Sie aktuell auf das Gerät zugreifen, führt dazu, dass das Gerät nach dem Speichern der Konfiguration unter dieser Adresse nicht mehr erreichbar ist. Melden Sie sich über die geänderte IP-Adresse erneut an. *Beispiel: "192.168.1.1"*
	management_ netmask	<nm_num>	**Netzmaske** Subnetzmaske, die definiert, in welchem Subnetz das Gerät im Stealth-Modus über die Management-IP-Adresse erreichbar ist. *Beispiel: 16*
	management_ gateway	<ip>	**Standard-Gateway** IP-Adresse des Standard-Gateways, an das das Gerät Verbindungsanfragen sendet, um unbekannte Subnetze oder das Internet zu erreichen. Im Stealth-Modus ist es dem Gerät damit möglich, als Client z. B. Anfragen an einen NTP- oder DNS-Server zu senden. Wird eine Management-IP-Adresse vergeben, muss das Standard-Gateway des Netzes, in dem sich das Gerät befindet, angegeben werden. Das Standard-Gateway kann sowohl über Netzzone 1 (XF1) als auch über Netzzone 2 (XF2–XF5) erreichbar sein. *Beispiel: "192.168.1.254"*

Mode: ROUTER Die einzelnen Funktionen im Router-Modus werden in getrennten Kapiteln beschreiben.

Tabelle 3-16 Endpunkt **configuration**, Key(s): **network >> mode >> (ROUTER)**

Key(s)	Variable (key)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER)	netzone1 netzone2	Siehe: – Kapitel 3.4.6, „Netzwerk (Netzzone 1/2)“
	nat	Siehe: – Kapitel 3.4.7, „Netzwerk (NAT, IP-Masquerading)“ – Kapitel 3.4.8, „Netzwerk (NAT, 1:1-NAT)“
	routing	Siehe: – Kapitel 3.4.9, „Netzwerk (Routing, Gateway)“ – Kapitel 3.4.10, „Netzwerk (Routing, Zusätzliche Routen)“

3.4.6 Netzwerk (Netzzone 1/2)

Beispiel

"network": "netzone1": {"mode": "DHCP"}, "netzone2": {"address": "192.168.1.1", "netmask": 24}

Die über DHCP oder statisch konfigurierten Netzwerke der beiden Netzzonen dürfen sich nicht überlappen.

Netzzone 1

Tabelle 3-17 Endpunkt **configuration**, Key(s): **network >> netzone1**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER) (netzone1)	mode	"DHCP" "STATIC"	**Router-Modus** Modus, mit dem festgelegt wird, wie der Netzzone eine Netzwerkkonfiguration zugewiesen wird. **DHCP** Der Netzzone wird eine Netzwerkkonfiguration (IP-Adresse, Subnetzmaske und optional ein Standard-Gateway und DNS-Server) automatisch von einem DHCP-Server zugewiesen, wenn ein DHCP-Server im Netzwerk vorhanden ist. **Statisch** Der Netzzone muss eine statische Netzwerkkonfiguration vom Benutzer manuell zugewiesen werden (IP-Adresse, Subnetzmaske und optional ein Standard-Gateway). *Beispiel:* "*STATIC*"
	address	<ip>	**IP-Adresse** IP-Adresse des Netzwerkinterface XF1 (Netzzone 1). **Hinweis:** Das Ändern der IP-Adresse, über die Sie aktuell auf das Gerät zugreifen, führt dazu, dass das Gerät nach dem Speichern der Konfiguration unter dieser Adresse nicht mehr erreichbar ist. Melden Sie sich über die geänderte IP-Adresse erneut an. *Beispiel:* "*10.1.0.100*"
	netmask	<nm_num>	**Netzmaske** Subnetzmaske, die definiert, in welchem Subnetz sich das Gerät befindet. *Beispiel: 16*

Netzzone 2

Tabelle 3-18 Endpunkt **configuration**, Key(s): **network >> netzone2**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER) (netzone2)	address	<ip>	**IP-Adresse** IP-Adresse des Netzwerkinterface XF2–XF5 (Netzzone 2). **Hinweis:** Das Ändern der IP-Adresse, über die Sie aktuell auf das Gerät zugreifen, führt dazu, dass das Gerät nach dem Speichern der Konfiguration unter dieser Adresse nicht mehr erreichbar ist. Melden Sie sich über die geänderte IP-Adresse erneut an. *Beispiel: "192.168.1.1"*
	netmask	<nm_num>	**Netzmaske** Subnetzmaske, die definiert, in welchem Subnetz sich das Gerät befindet. *Beispiel: 24*

3.4.7 Netzwerk (NAT, IP-Masquerading)

Abweichende Einstellungen in Config API und WBM sind möglich

IP-Masquerading kann über das Web-based Management für jede Netzzone aktiviert oder deaktiviert werden.

In der *Config API* kann darüber hinaus festgelegt werden, dass nur der Datenverkehr aus definierten Netzwerken maskiert wird.

Eine solche Konfiguration würde vom Gerät angewendet, im Web-based Management jedoch nicht angezeigt werden!

Beispiel

"**network**": {"**nat**": {"**masquerading**": [{"from_ip": "0.0.0.0/0", "id": 0, "outgoing_on_if": "NETZONE1"}, {"from_ip": "0.0.0.0/0", "id": 1, "outgoing_on_if": "NETZONE2"}, {"from_ip": "10.1.1.0/24", "id": 2, "outgoing_on_if": "NETZONE2"}]}}

Tabelle 3-19 Endpunkt **configuration**, Key(s): **network >> nat >> masquerading**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER) (nat, masquerading)	id	<num>	Identifikationsnummer der Regel Die ID bestimmt die Reihenfolge, in der die Regeln angewendet werden, beginnend mit der niedrigsten ID. *Beispiel: 0*
	from_ip	<nw_cidr>	Die NAT-Masquerading-Regel wird auf Datenpakete angewendet, die aus dem angegebenen Netzwerk gesendet und durch das Gerät durchgeleitet (*geroutet*) werden. Wird als Subnetzmaske die „0“ (z. B. 0.0.0.0/0) angegeben, wird die NAT-Regel auf alle IP-Adressen und Netzwerke angewendet. **Hinweis:** Wird die Funktion im **Web-based Management** aktiviert, wird der Variablen der Wert 0.0.0.0/0 zugeordnet. *Beispiel: "10.1.1.0/24"*
	outgoing_on_if	"NETZONE1" "NETZONE2"	**Maskiere in Richtung Netzzone 1/2** Die NAT-Masquerading-Regel wird auf Datenpakete (Anfragen) angewendet, die das Gerät auf dem ausgewählten Netzwerkinterface (Netzzone) verlassen. Die IP-Adresse des Absenders wird im Datenpaket auf die IP-Adresse des ausgewählten Netzwerkinterface (Netzzone) umgeschrieben. *Beispiel: "NETZONE1"*

3.4.8 Netzwerk (NAT, 1:1-NAT)

Beispiel

"**network**": {"**nat**": {"**1_1_nat**": [{"id": 0, "real_network": "192.168.1.0/24", "virt_network": "10.1.0.0/24", “comment“: “This rule refers to to production B“}]}}

Tabelle 3-20 Endpunkt **configuration**, Key(s): **network >> nat >> 1_1_nat**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER) (nat, 1_1_nat)	id	<num>	**ID** Identifikationsnummer der Regel Die ID bestimmt die Reihenfolge, in der die Regeln angewendet werden, beginnend mit der niedrigsten ID.
	real_network	<nw_cidr> <ip>	**Reale IP/Netzwerk** Der Datenverkehr, der von oder an Netzwerk-Clients des realen Netzwerks gesendet wird, unterliegt der 1:1-NAT-Regel. **1:1-NAT** Beim 1:1-NAT wird der Netzwerkteil (rot) der IP-Adressen von Clients im realen Netzwerk auf den Netzwerkteil eines anderen (übersetzten) Netzwerks umgeschrieben (siehe Beispiel). Der den Clients zugeordnete Hostteil (grün) der IP-Adressen wird unverändert beibehalten. **Beispiel** **1:1-NAT-Regel:** 192.168.1.0/**24** <-> 10.1.0.0/**24** ⇒ **Übersetzung:** 192.168.1.100 <-> 10.1.0.100 ⇒ **Übersetzung:** 192.168.1.200 <-> 10.1.0.200 Der Netzwerk- und der Hostteil einer IP-Adresse werden durch die Subnetzmaske definiert (z. B. 192.168.70.80/**16** oder 10.1.1.30/**24**). **Reale IP** Ist die Netzmaske 32, werden einzelne IP-Adressen und keine Netzwerke durch die 1:1-NAT-Regel übersetzt: **Hinweis:** Für die Angabe einer IP-Adresse <ip> darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss ohne Netzmaske angegeben werden. **1:1-NAT-Regel:** 192.168.1.40 <-> 10.1.5.40 ⇒ **Übersetzung:** 192.168.1.40 <-> 10.1.5.40 **Praxis** Clients in beiden Netzwerken können in beide Richtungen miteinandern kommunizieren. Dabei ist das reale (zumeist private) Netzwerk im anderen (zumeist öffentlichen) Netzwerk nicht sichtbar:

Tabelle 3-20 Endpunkt **configuration**, Key(s): **network >> nat >> 1_1_nat**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
			– Als Absenderadresse der Clients im realen Netzwerk erscheint den Netzwerkteilnehmern im anderen Netzwerk jeweils deren übersetzte IP-Adresse. – Um Clients im realen Netzwerk aus dem anderen Netzwerk zu erreichen, muss deren übersetzte IP-Adresse verwendet werden. – ARP-Anfragen an die übersetzten IP-Adressen der Clients im realen Netzwerk werden automatisch und stellvertretend vom Gerät beantwortet. **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. – Firewall-Regeln werden grundsätzlich auch auf übersetzte IP-Adressen angewendet. *Beispiel:* "*192.168.1.0/24*" *Beispiel:* "*192.168.1.50*"
	virt_network	<nw_cidr> <ip>	**Übersetzte IP/Netzwerk** Das Netzwerk, auf das die realen IP-Adressen der Clients aus dem realen Netzwerk umgeschrieben werden sollen (siehe „real_network“). **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. **Übersetzte IP** Ist die Netzmaske 32, werden einzelne IP-Adressen und keine Netzwerke durch die 1:1-NAT-Regel übersetzt. **Hinweis:** Bei Konfigurationsänderungen über die Config API darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss stattdessen ohne Netzmaske angegeben werden. **Eingabeformat:** IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation) *Beispiel:* "*192.168.2.0/24*" *Beispiel:* "*10.1.0.50*"

Tabelle 3-20 Endpunkt **configuration**, Key(s): **network >> nat >> 1_1_nat**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
			– Als Absenderadresse der Clients im realen Netzwerk erscheint den Netzwerkteilnehmern im anderen Netzwerk jeweils deren übersetzte IP-Adresse. – Um Clients im realen Netzwerk aus dem anderen Netzwerk zu erreichen, muss deren übersetzte IP-Adresse verwendet werden. – ARP-Anfragen an die übersetzten IP-Adressen der Clients im realen Netzwerk werden automatisch und stellvertretend vom Gerät beantwortet. **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. – Firewall-Regeln werden grundsätzlich auch auf übersetzte IP-Adressen angewendet. *Beispiel:* "*192.168.1.0/24*" *Beispiel:* "*192.168.1.50*"
	virt_network	<nw_cidr> <ip>	**Übersetzte IP/Netzwerk** Das Netzwerk, auf das die realen IP-Adressen der Clients aus dem realen Netzwerk umgeschrieben werden sollen (siehe „real_network“). **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. **Übersetzte IP** Ist die Netzmaske 32, werden einzelne IP-Adressen und keine Netzwerke durch die 1:1-NAT-Regel übersetzt. **Hinweis:** Bei Konfigurationsänderungen über die Config API darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss stattdessen ohne Netzmaske angegeben werden. **Eingabeformat:** IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation) *Beispiel:* "*192.168.2.0/24*" *Beispiel:* "*10.1.0.50*"

Tabelle 3-20 Endpunkt **configuration**, Key(s): **network >> nat >> 1_1_nat**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
			– Als Absenderadresse der Clients im realen Netzwerk erscheint den Netzwerkteilnehmern im anderen Netzwerk jeweils deren übersetzte IP-Adresse. – Um Clients im realen Netzwerk aus dem anderen Netzwerk zu erreichen, muss deren übersetzte IP-Adresse verwendet werden. – ARP-Anfragen an die übersetzten IP-Adressen der Clients im realen Netzwerk werden automatisch und stellvertretend vom Gerät beantwortet. **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. – Firewall-Regeln werden grundsätzlich auch auf übersetzte IP-Adressen angewendet. *Beispiel:* "*192.168.1.0/24*" *Beispiel:* "*192.168.1.50*"
	virt_network	<nw_cidr> <ip>	**Übersetzte IP/Netzwerk** Das Netzwerk, auf das die realen IP-Adressen der Clients aus dem realen Netzwerk umgeschrieben werden sollen (siehe „real_network“). **Voraussetzung** – Das reale und das übersetzte Netzwerk müssen die gleiche Subnetzmaske verwenden. – Die übersetzten IP-Adressen der Clients im realen Netzwerk dürfen im anderen (übersetzten) Netzwerk noch nicht vergeben sein. **Übersetzte IP** Ist die Netzmaske 32, werden einzelne IP-Adressen und keine Netzwerke durch die 1:1-NAT-Regel übersetzt. **Hinweis:** Bei Konfigurationsänderungen über die Config API darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss stattdessen ohne Netzmaske angegeben werden. **Eingabeformat:** IPv4-Adresse, IPv4-Netzwerk (CIDR-Notation) *Beispiel:* "*192.168.2.0/24*" *Beispiel:* "*10.1.0.50*"

Tabelle 3-20 Endpunkt **configuration**, Key(s): **network >> nat >> 1_1_nat**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	comment	<string>	**Kommentar** Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

3.4.9 Netzwerk (Routing, Gateway)

Beispiel

"**network**": "**routing**": {"**gateway**": "192.168.1.144", "routes": [{"network": "10.2.2.0/24", "gateway": "192.168.1.200", “comment“: “This route leads to cell B“}]}

Tabelle 3-21 Endpunkt **configuration**, Key(s): **network >> routing >> gateway**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER) (routing, gateway)	gateway	<ip>	**Standard-Gateway** IP-Adresse des Standard-Gateways, an das das Gerät Verbindungsanfragen sendet, um unbekannte Subnetze oder das Internet zu erreichen. Als Standard-Gateway kann sowohl ein Gerät im Subnetz der Netzzone 1 (XF1) als auch im Subnetz der Netzzone 2 (XF2–XF5) angegeben werden. **Hinweis:** Muss nur für den Router-Modus „Statisch“ angegeben werden (siehe Kapitel 3.4.6). *Beispiel: "10.1.0.254"*

3.4.10 Netzwerk (Routing, Zusätzliche Routen)

Beispiel

"**network**": "**routing**": {"gateway": "192.168.1.144", "**routes**": [{"network": "192.168.3.0/24", "gateway": "192.168.1.200", “comment“: “This route leads to cell B“}]}

Tabelle 3-22 Endpunkt **configuration**, Key(s): **network >> routing >> routes**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
network (mode: ROUTER) (routing, routes)	network	<nw_cidr> <ip>	**IP/Netzwerk** Ziel (Netzwerk oder IP-Adresse), das über eine zusätzliche Route erreicht werden soll. **Hinweis:** Bei Konfigurationsänderungen über die Config API darf die Netzmaske **/32** nicht verwendet werden. Eine IP-Adresse muss stattdessen ohne Netzmaske angegeben werden. *Beispiel: "192.168.3.0/24"* *Beispiel: "192.168.4.100"*
	gateway	<ip>	**Gateway** IP-Adresse des Gateways, über das das Ziel über die zusätzliche Route erreichbar ist. *Beispiel: "192.168.1.200"*
	comment	<string>	**Kommentar** Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

3.4.11 Service (DHCP-Server)

Beispiel

"**service**": {"**dhcp_server**": {"dns": "192.168.1.1", "gateway": "192.168.1.1", "lease_time": "12h", "range_high": "192.168.1.254", "range_low": "192.168.1.2", "status": "ON", "wins_server": "192.168.1.252"}}

Tabelle 3-23 Endpunkt **configuration**, Key(s): **service >> dhcp_server**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (dhcp_server)	dns	<ip>	**DNS-Server** IP-Adresse eines DNS-Servers, die der DHCP-Server anfragenden Clients zuweist. Ein DNS-Server (DNS = *Domain Name Service*) ermöglicht es Clients, Hostnamen in IP-Adressen aufzulösen. Wenn der DNS-Server des Geräts genutzt werden soll, muss die IP-Adresse der Netzzone angegeben werden, auf der dieser Dienst aktiv ist (werkseitige Voreinstellung: Netzzone 2 = 192.168.1.1). *Beispiel: "192.168.1.1"*
	gateway	<ip>	**Standard-Gateway** IP-Adresse des Standard-Gateways, die der DHCP-Server anfragenden Clients zuweist. Dies ist in der Regel die interne IP-Adresse des Geräts. *Beispiel: "192.168.1.1"*
	lease_time	<time_dhm>	Zeitraum, in dem die einem Client zugewiesene Netzwerkkonfiguration für diesen gültig bleibt. Auch wenn der Client vorübergehende keinen Netzwerkverbindung zum DHCP-Server hat, wird ihm bei einer erneuten Anfrage innerhalb des Zeitraums immer die gleiche Netzwerkkonfiguration zugewiesen. Kurz vor Ablauf des Zeitraums sollte der Client seinen Anspruch auf die ihm zugeteilte Konfiguration erneuern. Ansonsten wird die Konfiguration unter Umständen einem anderen Client zugewiesen. Der Zeitraum kann alternativ in Tagen (d), Stunden (h) **oder** Minuten (m) abgegeben werden. *Beispiel: "12h"*
	netmask	<nm_num>	**Lokale Netzmaske** Subnetzmaske, die der DHCP-Server anfragenden Clients zuweist. Der Bereich, aus dem Netzwerk-Clients IP-Adressen zugewiesen werden, solle so gewählt werden, dass die IP-Adressen in dem zugewiesenen Subnetz erreichbar sind (siehe keys: *range_low, range_high*). *Beispiel: 24*

Tabelle 3-23 Endpunkt **configuration**, Key(s): **service >> dhcp_server**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	range_low	<ip>	**Anfang IP-Adressbereich** Anfang des IP-Adressbereichs, aus dem der DHCP-Server anfragenden Clients IP-Adressen zuweist. Der Bereich sollte so gewählt werden, dass die in ihm enthaltenen IP-Adressen in dem zugewiesenen Subnetz erreichbar sind (siehe key *netmask*). *Beispiel:* "*192.168.1.2*"
	range_high	<ip>	**Ende IP-Adressbereich** Ende des IP-Adressbereichs, aus dem der DHCP-Server anfragenden Clients IP-Adressen zuweist. Der Bereich sollte so gewählt werden, dass die in ihm enthaltenen IP-Adressen in dem zugewiesenen Subnetz erreichbar sind (siehe key *netmask*). *Beispiel:* "*192.168.1.249*"
	status	"ON" "OFF"	**DHCP-Server für Netzzone 2** Bei aktivierter Funktion wird anfragenden Clients, die über Netzzone 2 mit dem Gerät verbunden sind, eine Netzwerkkonfiguration zugewiesen. **Hinweis:** Die Anfragen an den UDP-Port 67 werden unabhängig von den Einstellungen in den Firewall-Tabellen des Geräts immer angenommen, wenn der DHCP-Server aktiviert ist. Der Server weist den Clients dann IP-Adressen aus dem konfigurierten IP-Adressbereich zu. *Beispiel:* "*ON*"
	wins_server	<ip>	**WINS-Server** IP-Adresse eines WINS-Servers, die der DHCP-Server anfragenden Clients zuweist. Ein WINS-Server (*Windows Internet Naming Service*) ermöglicht es Clients, Hostnamen (*NetBIOS*-Namen) in IP-Adressen aufzulösen. *Beispiel:* "*192.168.1.252*"

3.4.12 Service (DNS-Cache/DNS-Server)

Beispiel

"**service**": "dnscache": {"allowed_requests": ["NETZONE1", "NETZONE2"], "dns_servers": "USER_DEFINED", "log": "ON", "user_defined": [{"ip": "192.168.1.150", “comment“: “Company DNS server A“}, {"ip": "192.168.1.160", “comment“: “DNS server fallback“}]}

Tabelle 3-24 Endpunkt **configuration**, Key(s): **service >> dnscache**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (dnscache)	allowed_requests	"NETZONE1" "NETZONE2"	**DNS-Server erreichbar aus Netzzone 1/2** Der Zugriff auf den DNS-Server des Geräts aus der angegebenen Netzzone wird erlaubt (UDP/TCP-Port 53). *Beispiel: "NETZONE2"*
	dns_servers	"USER_DEFINED" "ROOT_DNS_SERVER"	Der Benutzer kann auswählen, ob im Gerät voreingestellte „Root-DNS-Server“ oder „benutzerdefinierte DNS-Server“ zur Auflösung von Hostnamen verwendet werden. **Hinweis:** Diese Auswahlmöglichkeit besteht nur, wenn das Gerät seine Netzwerkkonfiguration **nicht von einem DHCP-Server** bezieht (siehe Kapitel 3.4.6). **Root-DNS-Server** **Nur** die im Gerät voreingestellten Root-DNS-Server werden zur Auflösung von Hostnamen verwendet. Der erste erreichbare Root-DNS-Server wird verwendet. **Benutzerdefiniert** **Nur** die benutzerdefinierten DNS-Server werden zur Auflösung von Hostnamen verwendet. Es können mehrere DNS-Server angegeben werden. Wird kein DNS-Server angegeben, werden Hostnamen nicht aufgelöst. *Beispiel: "ROOT_DNS_SERVER"*
	log	"ON" "OFF"	**DNS-Anfragen loggen** Bei aktivierter Funktion wird für alle Anfragen (UDP/TCP) an den DNS-Server des Geräts ein Log-Eintrag erstellt. Log-Einträge können über den Endpunkt *logging* (siehe Kapitel 3.11) oder in der Datei *journal* analysiert werden, die über einen Snapshot erzeugt und heruntergeladen werden kann (siehe Kapitel 3.10). Für erlaubte Anfragen (Variable „*allowed_requests*“): – Log-Präfix: *fw-input-dnscache-* Für alle anderen Anfragen: – Log-Präfix: *fw-input-policy-* *Beispiel: "OFF"*

Tabelle 3-24 Endpunkt **configuration**, Key(s): **service >> dnscache**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (dnscache, user_defined)	ip	<ip>	**Benutzerdefinierte DNS-Server** IP-Adresse eines oder mehrerer DNS-Server, die vom Gerät zur Auflösung von Hostnamen angefragt werden. *Beispiel:* "*46.182.19.48*"
	comment	<string>	**Kommentar** Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

3.4.13 Service (NTP-Server/NTP-Client)

Beispiel

"**service**": "ntp": {"allow_client_requests": ["NETZONE1", "NETZONE2"], "server": [{"address": "0.pool.ntp.org", "port": 123, “comment“: “Company NTP 1“}, {"address": "1.pool.ntp.org", "port": 123, “comment“: “Company NTP fallback“}], "status": "ON"}

Tabelle 3-25 Endpunkt **configuration**, Key(s): **service >> ntp**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (ntp)	status	“ON“ “OFF“	**NTP** Mit dieser Funktion kann der NTP-Client und der NTP-Server des Geräts aktiviert werden. Der NTP-Server des Geräts wird erst dann aktiviert, wenn der Zugriff auf den NTP-Server aus mindestens einer Netzzone erlaubt ist (siehe *„allow_client_requests“*). **NTP-Client** Bei aktivierter Funktion bezieht das Gerät seine Systemzeit (Uhrzeit und Datum) von einem oder mehreren NTP-Servern und synchronisiert sich fortlaufend mit ihnen. Der NTP-Server überträgt die *Koordinierte Weltzeit* (UTC). Die Zeit auf dem Gerät (Systemzeit) wird der konfigurierten Zeitzone entsprechend angezeigt und verwendet (z. B. in Log-Einträgen). Die *Real-Time-Clock (RTC)* des Geräts wird automatisch mit den erhaltenen Zeitangaben der NTP-Server synchronisiert. Die initiale Zeitsynchronisation kann bis zu 15 Minuten oder länger dauern. Während dieser Zeitspanne vollzieht das Gerät immer wieder Vergleiche zwischen den Zeitangaben der externen NTP-Server und der eigenen Systemzeit, um diese so präzise wie möglich abzustimmen. **NTP-Server** Bei aktivierter Funktion können verbundene Netzwerk-Clients ihre Systemzeit über den NTP-Server des Geräts synchronisieren. Der NTP-Server überträgt die *Koordinierte Weltzeit* (UTC). Der Zugriff auf den NTP-Server kann auf ausgewählte Quellen (Netzzonen, IP-Adressen oder Netzwerke) beschränkt werden (siehe *„„allow_client_requests““*). *Beispiel:* "*ON*"
	allow_client_requests	"NETZONE1" "NETZONE2"	**NTP-Server erreichbar aus Netzzone 1/2** Der Zugriff auf den NTP-Server des Geräts aus der angegebenen Netzzone wird erlaubt (UDP-Port 123). Der NTP-Server des Geräts wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist. *Beispiel: "NETZONE1"*

Tabelle 3-25 Endpunkt **configuration**, Key(s): **service >> ntp**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (ntp, server)	address	<ip> <string>	**IP/Hostname** IP-Adresse oder Hostname des externen NTP-Servers (Zeit-Server), an den das Gerät NTP-Anfragen senden soll, um die aktuelle Zeit (Uhrzeit und Datum) zu beziehen. Sind mehrere NTP-Server angegeben, verbindet sich das Gerät automatisch mit allen Servern, um aus allen erhaltenen Werten die aktuelle Zeit zu berechnen. **Eingabeformat:** IPv4-Adresse oder Hostname *Beispiel: "0.pool.ntp.org"*
	port	<num> (oder leer)	**Port** Port, auf dem der externe NTP-Server NTP-Anfragen entgegennimmt. Die Angabe eines Ports ist optional *Beispiel: 123*
	comment	<string>	**Kommentar** Frei wählbarer Kommentar. Erlaubte Zeichen: max. 128

3.4.14 Service (SNMP-Server)

Beispiel

"**service**": "snmp": {"allow_requests_from": ["NETZONE1", "NETZONE2"], ro_community_string": "public", "status_v2c": "ON", "status_v3": "ON", "user": {"new_password": "My-Password_123", "repeat_password": "My-Password_123", "username": "SNMP-mGuard_01"}}

Tabelle 3-26 Endpunkt **configuration**, Key(s): **service >> snmp**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (snmp)	allow_request_from	"NETZONE1" "NETZONE2“	**SNMP-Server erreichbar aus Netzzone 1/2** Der Zugriff auf den SNMP-Server des Geräts aus der angegebenen Netzzone wird erlaubt (UDP-Port 161). Der SNMP-Server wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist. *Beispiel: "NETZONE1"*
	ro_community_string	<string>	**Read-only community** SNMP kodiert bei der Version SNMPv1/SNMPv2c die Zugangsdaten als Teil einer sogenannten *Community*. Der *Read-only community* string wird dabei wie ein Passwort oder Zugangsschlüssel verwendet. Die Authentifizierung mittels *Read-only community* string ermöglicht einen beschränkten SNMP-Lesezugriff. **Eingabeformat:** Der String muss mit einem Buchstaben beginnen. Erlaubte Zeichen (min. 6, max. 255): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_- *Beispiel: "public"*
	status_v2c	“ON“ “OFF“	**SNMPv2c** Bei aktivierter Funktion kann das Gerät über das Protokoll SNMPv2c überwacht werden (Lesezugriff). **ACHTUNG: Unsicheres Protokoll** Das unverschlüsselte SNMPv1/2-Protokoll sollte nur in einer sicheren Netzwerkumgebung verwendet werden, die gänzlich unter der Kontrolle des Betreibers steht. Bei der Aktivierung von SNMPv2c wird das Protokoll SNMPv1 ebenfalls unterstützt. Der SNMP-Server wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist (siehe oben). *Beispiel: “OFF“*

Tabelle 3-26 Endpunkt **configuration**, Key(s): **service >> snmp**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	status_v3	“ON“ “OFF“	**SNMPv3** Bei aktivierter Funktion kann das Gerät über das Protokoll SNMPv3 überwacht werden (Lesezugriff). Im Gegensatz zu den Protokollen SNMPv1/v2c gilt das SNMPv3-Protokoll als sicher, da es die Möglichkeit zur Benutzerauthentifizierung und zur Verschlüsselung bietet. Verwendete Verschlüsselungs- und Hash-Algorithmen: – AES-128 – SHA-2 (SHA-256) mit SNMPv3 USM Der SNMP-Server wird erst aktiviert, wenn der Zugriff aus mindestens einer Netzzone erlaubt ist (siehe oben). *Beispiel: “OFF“*
service (snmp, user)	new_password	<string>	**Passwort** Das Passwort des zugehörigen SNMP-Benutzers. **Hinweis:** Nach dem Speichern der Konfiguration wird das konfigurierte Passwort nicht mehr angezeigt. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 8, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ *Beispiel: "My-Password_123"*
	repeat_password	<string>	**Passwort bestätigen** Wiederholte Eingabe des Passworts.
	username		**Benutzername** Benutzername des SNMPv3-Benutzers, der über das SNMPv3-Protokoll auf den SNMP-Server des Geräts zugreifen möchte. Das Hinzufügen weiterer SNMPv3-Benutzer wird nicht unterstützt. **Eingabeformat:** Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.- *Beispiel: "SNMP-mGuard_01"*

3.4.15 Service (Session timeout)

Beispiel "**service**": "web": {"session_timeout“: 60, "user_blocking_time": 10, "user_max_failed_logins": 5}

Tabelle 3-27 Endpunkt **configuration**, Key(s): **service >> web**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
service (web)	session_timeout	<time_minute>	**Ablauf der Sitzung (hh:mm)** Länge des *Session Timeouts* (Zeitspanne). Die Sitzung eines Benutzers wird durch einen *Session timeout* zeitlich begrenzt. Die konfigurierbare Zeitspanne des *Session Timeouts* liegt zwischen 5 Minuten und 8 Stunden. Nach Ablauf der Sitzung wird der Benutzer automatisch abgemeldet. Der *Session timeout* startet mit der Anmeldung des Benutzers (werkseitige Voreinstellung: 30 Minuten). Führt der Benutzer während einer laufenden Sitzung eine Aktion durch, wird der *Session timeout* jeweils auf den konfigurierten Ausgangswert zurückgesetzt. **Eingabeformat:** Minuten (min. 5, max. 480) *Beispiel: 60*
	user_blocking_time	<time_minute>	**Zeitraum, für den ein Benutzer gesperrt wird (hh:mm)** Zeitraum, für den ein Benutzer nach erfolglosen Anmeldeversuchen gesperrt wird. Ein Benutzer wird nach einer konfigurierbaren Anzahl erfolgloser Anmeldeversuche (falsche Passworteingabe) automatisch für den konfigurierten Zeitraum gesperrt (siehe unten). **Hinweis:** Diese Sperre kann durch einem Administrator mit der Rolle „*Super Admin*“ vorzeitig aufgehoben werden (siehe Kapitel 3.19). **Hinweis:** Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben. **Eingabeformat:** Minuten (min. 1, max. 480) *Beispiel: 10*

Tabelle 3-27 Endpunkt **configuration**, Key(s): **service >> web**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	user_max_failed_logins	<string>	**Anzahl erfolgloser Anmeldeversuche, bis ein Benutzer gesperrt wird** Anzahl erfolgloser Anmeldeversuche, bis ein Benutzer gesperrt wird. Ein Benutzer wird nach der konfigurierten Anzahl erfolgloser Anmeldeversuche (falsche Passworteingabe) automatisch für bis zu 8 Stunden gesperrt (siehe oben). **Hinweis:** Diese Sperre kann durch einem Administrator mit der Rolle „*Super Admin*“ vorzeitig aufgehoben werden (siehe Kapitel 3.19). **Hinweis:** Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben. **Eingabeformat:** Ziffer (min. 5, max. 200) *Beispiel: 3*

3.4.16 System

Über den Endpunkt "*System*" können Sie

1. den Hostnamen des Geräts ändern,
2. die aktuelle Konfiguration auf SD-Karte speichern (z.B. für einen Gerätetausch),
3. die Systembenachrichtigung konfigurieren.

Beispiel

"**system**": {"hostname": "mGuard-production-01", "store_config_on_sdcard": "ON", "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited."}

Tabelle 3-28 Endpunkt **configuration**, Key(s): **system**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
system	hostname	<string>	**Hostname** Name, unter dem das Gerät im Netzwerk grundsätzlich sichtbar und erreichbar ist. Wird der Hostname über das *Domain Name System* (DNS) aufgelöst, können Netzwerkteilnehmer das Gerät direkt über seinen Hostnamen ansprechen. **Eingabeformat:** Der Name muss mit einem Buchstaben oder einer Ziffer beginnen und enden. Erlaubte Zeichen (min. 1, max. 63): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789- *Beispiel: "mGuard-production-01"*
	usenotification	<string>	**Systembenachrichtigung** Frei wählbarer Text für eine Systembenachrichtigung, die vor einer Anmeldung am Gerät angezeigt wird (maximal 512 Zeichen). Wird angezeigt bei: – Anmeldung über das Web-based Management (WBM) *Beispiel: “The usage of this mGuard security appliance is reserved to authorized staff only.“*

Tabelle 3-28 Endpunkt **configuration**, Key(s): **system**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	store_config_on_sdcard	"ON" "OFF"	**Konfiguration automatisch speichern** Bei aktivierter Funktion wird jede Konfigurationsänderung, die im WBM oder über die *Config API* gespeichert wird, automatisch auf die eingesetzte SD-Karte geschrieben. Es werden drei Dateien gespeichert: – *users_pass.json* – *snmp-pass.conf* – *configuration.json* **Gespeicherte Konfiguration via SD-Karte erneut in ein Gerät importieren:** Für alle **neuen Geräte** oder Geräte, die mittels Smart-Mode auf Werkseinstellungen zurückgesetzt wurden, gilt: Eine auf der eingesetzten SD-Karte gespeicherte Konfiguration/Benutzerverwaltung wird beim Start bzw. der Inbetriebnahme des Geräts automatisch in das Gerät importiert und dort angewendet. **Voraussetzung:** – Firmware-Version „SD-Karte“ ist in der Minor-Version kleiner/gleich Firmware-Version „Gerät“. – Die drei Dateien sind auf der SD-Karte enthalten (einzeln oder in gepackter Form als *mGuard.tar.gz:* Die Einzeldateien werden priorität verwendet!). Tritt während des Imports ein Fehler auf, startet das Gerät in der werkseitigen Voreinstellung. Die LEDs FAIL und PF1 leuchten zusätzlich rot.

3.4.17 Zeitzone

Beispiel "**zoneinfo**": "Europe/Berlin"

Tabelle 3-29 Endpunkt **configuration**, Key(s): **zoneinfo**

Key(s)	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
system	zoneinfo	<timezone>	**Zeitzone** Die manuell eingestellte oder per NTP bezogene Systemzeit wird der konfigurierten Zeitzone entsprechend angezeigt und verwendet (z. B. in Log-Einträgen). Verfügbare Zeitzonen: siehe Kapitel 5.1 *Beispiel: "Europe/Berlin"*

3.5 Endpunkt "configuration/default"

Über diesen Endpunkt kann die werkseitige Voreinstellung der Elemente des Endpunkts

1. angezeigt (*GET-Request*) oder
2. wiederhergestellt (*POST-Request*) werden.

Das aktuelle Administrator-Passwort und Zertifikate bleiben erhalten.

Beispiel: Konfiguration anzeigen (GET)

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/configuration/default

Antwort:

⇒ (Ergebnis/Antwort: siehe Kapitel 4.1)

Beispiel: Werkseinstellung anwenden (POST)

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -X POST https://192.168.1.1:443/api/v1/configuration/default

3.6 Endpunkt "users"

Nur sichtbar für Benutzer mit der Benutzerrolle *Super Admin*.

Lokal gespeicherte Passwörter werden bei einem GET-Request nicht übermittelt.

Über diesen Endpunkt können folgende Einstellungen vorgenommen werden:

– ein externer LDAP-Server kann konfiguriert werden (**key: ldap**, siehe Kapitel 3.6.1, „Benutzer >> LDAP“),
– die Eigenschaften bestehender lokaler Benutzer können angezeigt sowie lokale Benutzer neu hinzugefügt, editiert oder gelöscht werden (**key: user_mgmt**, siehe Kapitel 3.6.2, „Benutzer >> Benutzerverwaltung“).

Benutzerrollen und Berechtigungen

Tabelle 3-30 Benutzerrollen und Berechtigungen

Berechtigung / Rolle	Super Admin	Admin	Audit
Benutzer verwalten	x		
LDAP konfigurieren	x		
Konfiguration ändern	x	x	
Aktionen durchführen	x	x	
Firmware-Updates installieren	x	x	
Konfiguration prüfen	x	x	x
Eigenes Passwort ändern	x	x	x
Gerätestatus abfragen	x	x	x
Log-Einträge lesen	x	x	x

Beispiel: Konfiguration – LDAP-Server/Benutzermanagement – anzeigen (GET)

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/users

Antwort:

{"content":

{"**ldap**": {"ldap_server": {"base_dn": "DC=mguard,DC=management", "ca": "-----BEGIN CERTIFICATE-----\nMII [...] nF\nBW5/87JeonwLYiT0JjajXDGLAf0t4O\n-----END CERTIFICATE-----\n", "hostname": "192.168.2.100", "port": 389, "tls": "ON", "username": "admin_ldap" }, "status": "ON", "user_role_mapping": {"admin": "Role_2", "audit": "Role_3", "ldap_attribute": "Role", "super_admin": "Role_1" } },

"**user_mgmt**": {"current_user": "admin",

"**users**": [{"block_user": "OFF", "name": "", "old_username": "admin", "role": "SUPERADMIN", "username": "admin" }, {"block_user": "OFF", "name": "", "old_username": "admin_production", "role": "ADMIN", "username": "admin_production" }] } },

"**envelope**": {"identifier": {"contentID": "4b7a11b1", "functionalID": "4b7a11b1" }, "version": 1 }, "error": [], "schemes": [{"name": "users.manageusers.e52f65cd", "url": "/v1/users/scheme/users.manageusers.e52f65cd" }], "status": 0 }

Antwort: (Für eine strukturierte Ansicht eines anderen Beispiels, siehe Kapitel 4.5)

Beispiel: Benutzereigenschaften und Passwörter ändern (POST)

Der Standard-Benutzer "*admin*" (Rolle: *Super Admin*) ist angemeldet und möchte mit einem POST-Request

1. seinen Benutzernamen zu "*superadmin*" ändern,
2. das Passwort des Benutzers "*admin_production*" ändern
3. den Benutzer "*audit_production*" mit der entsprechenden Rollen hinzufügen,
4. (Die Einstellungen zum LDAP-Server (key: "*ldap*") werden nicht geändert. Die Angabe des LDAP-Passworts ist nur bei einer Änderung notwendig!)

```
curl -k -b session_cookie -H "X-CSRF-Token: <TOKEN>" -H "Content-Type:application/json" -X POST
https://192.168.1.1:443/api/v1/users -d

'{"content": {"ldap": {"ldap_server": {"base_dn": "DC=mguard,DC=management", "ca": "-----BEGIN CERTIFICATE-----
\nMII [...] nF\nBW5/87JeonwLYiT0JjajXDGLAf0t4O\n-----END CERTIFICATE-----\n", "hostname": "192.168.2.100",
"password": "ldap_server_password", "port": 389, "tls": "ON", "username": "server-admin"}, "status": "ON", "user_ro-
le_mapping": {"ldap_attribute":"Role", "admin": "Role_2", "audit": "Role_3", "super_admin": "Role_1"}},

"user_mgmt": {"old_password": "private", "current_user": "admin",

"users": [{"block_user": "OFF", "name": "", "old_username": "admin", "role": "SUPERADMIN", "username": "superadmin"},
{"block_user": "OFF", "name": "", "old_username": "admin_production", "role": "ADMIN", "username": "admin_production",
"new_password": "secret_production_password","repeat_password": "secret_production_password" },{ "block_user":
"OFF", "name": "", "old_username": "", "role": "AUDIT", "username": "secret_audit_production","new_password": "sec-
ret_audit_password","repeat_password": "secret_audit_password"}]}}, "envelope": { "version": 1 }}'
```

3.6.1 Benutzer >> LDAP

Tabelle 3-31 Endpunkt **users**, Key(s): **ldap**

Endpunkt	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
users, ldap (ldap_server)	base_dn	<string>	**Base-DN** Basisadresse im Verzeichnis auf dem LDAP-Server. Die Suche nach den gewünschten Objekten (z. B. Benutzerdaten) wird auf einen kleineren Bereich im Verzeichnisbaum des LDAP-Servers eingeschränkt. Sie erfolgt ausschließlich unterhalb der angegebenen Basisadresse (Knotenpunkt). **Eingabeformat:** Verzeichnispfad (*DC=x,DC=y,DC=z*) Erlaubte Zeichen (min. 1, max. 1024): Die Eingabe muss mit einem der folgenden Zeichen beginnen: ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789._ Diese Zeichen können jeweils durch eines der folgenden vier Zeichen verbunden werden: -_=, **Beispiel:** DC=mguard,DC=management,DC=user
	hostname	<ip> <string>	**IP/Hostname** IP-Adresse oder Hostname des externen LDAP-Servers, an den das Gerät Anfragen zur Benutzer-Authentisierung senden soll. **Eingabeformat:** IPv4-Adresse oder Hostname *Beispiel: "my-ldap-server.com"*
	password	<string>	**Passwort** Passwort, mit dem sich das Gerät beim LDAP-Server anmeldet und authentifiziert. **Hinweis:** Nach dem Speichern der Konfiguration wird das konfigurierte Passwort nicht mehr angezeigt. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 6, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!#$%&()*+,-./:;<=>?[]^_`{|}~@ *Beispiel: "ldap_password_183"*

Tabelle 3-31 Endpunkt **users**, Key(s): **ldap**

Endpunkt	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	port	<num>	**Port** Port, auf dem der externe LDAP-Server Anfragen entgegennimmt. *Beispiel: 389*
	username	<string>	**Benutzername** Benutzername, mit dem sich das Gerät beim LDAP-Server anmeldet und authentifiziert. Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.- *Beispiel: "mGuard_183"*
	tls	"ON" "OFF"	**LDAP über TLS** Bei aktivierter Funktion werden die Daten verschlüsselt über eine TCP-Verbindung übertragen. **Hinweis:** Aus Sicherheitsgründen sollte immer eine verschlüsselte TLS-Verbindung zwischen dem Gerät (mGuard) und dem LDAP-Server verwendet werden. **Voraussetzung:** Um die Integrität und Authentizität der verschlüsselten TCP-Verbindung sicherzustellen, muss das Server-Zertifikat (CA-Zertifikat) des Remote-Servers auf dem Gerät installiert werden (siehe unten).
	ca	<string>	**Server-CA-Zertifikat auf das Gerät hochladen** CA-Zertifikat, mit dem der Remote-Server (LDAP-Server) gegenüber dem Gerät authentifiziert wird. Das CA-Zertifikat wird vom Betreiber des Remote-Servers bereitgestellt und muss auf das Gerät hochgeladen werden (X.509-Zertifikat mit öffentlichem Schlüssel). Eine verschlüsselte TCP-Verbindung zum Remote-Server kann nur dann erfolgreich aufgebaut werden, wenn dieser seinerseits ein vom CA-Zertifikat ausgestelltes Zertifikat (mit dem geheimen Schlüssel) oder eine gültige Zertifikatskette, mit dem CA-Zertifikat als oberste Instanz, vorzeigt. **Format:** Die maximal erlaubte Dateigröße beträgt 1 MB.

Tabelle 3-31 Endpunkt **users**, Key(s): **ldap**

Endpunkt	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
users, ldap (status)	status	″ON″ ″OFF″	**LDAP-Authentifizierung** Bei aktivierter Funktion kann das Gerät über das LDAP-Protokoll auf einen konfigurierten LDAP-Server zugreifen. Auf dem LDAP-Server verwaltete Benutzer können bei der Anmeldung am Gerät über das LDAP-Protokoll und die Eingabe ihrer LDAP-Zugangsdaten authentisiert werden. Bei der Anmeldung eines Benutzers (Login) prüft das Gerät als Erstes, ob der Benutzer als **lokaler Benutzer** auf dem Gerät vorhanden ist. Ist dies der Fall, kann der lokale Benutzer nur mit dem l**okal konfigurierten Benutzer-Passwort** angemeldet werden. Eine Abfrage beim LDAP-Server findet in diesem Fall nicht mehr statt. Ein über LDAP angemeldeter Benutzer wird automatisch abgemeldet, wenn die Funktion während der laufenden Sitzung deaktiviert wird. *Beispiel: "ON"*
users, ldap (user_role_mapping)	ldap_attribute	<string>	**LDAP-Attribut** Name des Attributs, in dem die Rollen/Benutzerklassen für jeden LDAP-Benutzer festgelegt werden. Damit die Zuordnung der Rollen stattfinden kann, müssen diese sowohl auf dem LDAP-Server als auch auf dem Gerät dem gleichen LDAP-Attribut zugeordnet werden. **Beispielkonfiguration:** Konfiguration auf dem LDAP-Server**:** – **Role:** *Role_1* – **Role:** *Role_2* – **Role:** *Role_3* Anzugebendes LDAP-Attribut auf dem mGuard-Gerät**:** – *Role* Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.- *Beispiel: "Role"*

Tabelle 3-31 Endpunkt **users**, Key(s): **ldap**

Endpunkt	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	admin	<string>	Bei einer Anmeldung über LDAP muss die dem LDAP-Benutzer auf dem LDAP-Server zugewiesene Benutzerrolle (oder Benutzerrollen) mindestens einer der drei verfügbaren Benutzerrollen auf dem Gerät zugeordnet werden (siehe auch„Benutzerrollen und Berechtigungen“ auf Seite 77). Kann die Benutzerrolle des LDAP-Benutzers nicht zugeordnet werden, ist eine Anmeldung nicht möglich. **Beispiel:** **Gerät <-> LDAP-Server** Super Admin <-> Role_1 Admin <-> Role_2 Audit <-> Role_3 Sind einem LDAP-Benutzer mehrere Benutzerrollen zugeordnet, wird er bei der Anmeldung mit der Rolle mit den weitestgehenden Berechtigungen angemeldet. Erlaubte Zeichen (min. 1, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.- *Beispiel: "Role_1"*
	audit	<string>	
	super_admin	<string>	

3.6.2 Benutzer >> Benutzerverwaltung

Tabelle 3-32 Endpunkt **users,** Keys: **user_mgmt**

Endpunkt	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
user_mgmt (current_users)	old_password	<string>	Das Passwort des angemeldeten Benutzers muss angegeben werden, wenn Änderungen im Endpunkt "users" vorgenommen und mit einem POST-Request an das Gerät gesendet werden sollen. **Hinweis:** Nach dem Speichern der Konfiguration wird das konfigurierte Passwort nicht mehr angezeigt. *Beispiel: "current_password"*
	current_user	<string>	Der Benutzername des angemeldeten Benutzers.
user_mgm (users)	username	<string>	**Benutzername** Eindeutiger Benutzername, mit dem sich der Benutzer beim Gerät anmeldet. **Eingabeformat:** Der Name muss mit einem Buchstaben oder einer Ziffer beginnen. Er darf nicht mit einem Punkt enden. Erlaubte Zeichen (min. 2, max. 200): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789_.- *Beispiel: "admin_01_dep-1.15"*
	role	SUPERADMIN ADMIN AUDIT	**Rolle** Mit der Auswahl einer Benutzerrolle werden dem Benutzer bestimmte Berechtigungen zugewiesen. Der Standard-Benutzer in der werkseitigen Voreinstellung „admin“ besitzt die Rolle „*Super Admin*“. Ein Benutzer mit der Rolle „*Super Admin*“ kann sich nicht selber löschen. *Beispiel: "SUPERADMIN"*
	name	<string> (oder leer)	**Richtiger Name** Frei zu vergebender Name zur Vereinfachung der Administration. *Beispiel: "Administrator 01"*

Tabelle 3-32 Endpunkt **users,** Keys: **user_mgmt**

Endpunkt	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
	new_password	<string>	**Neues Passwort** Das neue Passwort des zugehörigen Benutzers. **Hinweis:** Nach dem Speichern der Konfiguration wird das konfigurierte Passwort nicht mehr angezeigt. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 6, max. 64): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ *Beispiel: "My-Password_123"*
	repeat_password	<string>	**Neues Passwort bestätigen** Wiederholte Eingabe des neuen Passworts.
	block_user	"ON" "OFF"	**Benutzer sperren** Bei aktivierter Funktion ist der zugehörige Benutzer gesperrt und kann sich nicht erneut am Gerät anmelden. Eine Benutzer kann sich nicht selber sperren. **Hinweis:** Ein angemeldeter Benutzer bleibt innerhalb seiner laufenden Sitzung auch dann angemeldet, wenn er von einer anderen Instanz aus gesperrt wird. **Hinweis:** Benutzer, die über einen LDAP-Server authentisiert werden, können nur über die Benutzerverwaltung des LDAP-Servers gesperrt werden. *Beispiel: "ON"*

3.7 Endpunkt "password"

Über diesen Endpunkt kann das Passwort des angemeldeten Benutzers geändert werden.

Lokal gespeicherte Passwörter werden bei einem GET-Request nicht übermittelt.

Beispiel

```
curl -k -b session_cookie -H "X-CSRF-Token: <TOKEN>" -H "Content-Type:application/json" -X POST
https://192.168.1.1:443/api/v1/password -d '{"content": {"old_password": "private", "new_password": "My-Pass-
word_123", "repeat_password": "My-Password_123"}, "envelope": {"version": 1}}'
```

Tabelle 3-33 Endpunkt **password**

Endpunkt	Methode	Variable (key)	Wert (Format)	Bezeichnung (WBM) / Beschreibung
password	**POST**	old_password	<string> (password in plain format)	**Aktuelles Passwort** Das bestehende Passwort des angemeldeten Benutzers, das geändert werden soll.
		new_password	<string> (password in plain format)	**Neues Passwort** Das neue Passwort für den angemeldeten Benutzer. **Hinweis:** Nach dem Speichern der Konfiguration wird das konfigurierte Passwort nicht mehr angezeigt. **Eingabeformat:** Um die Sicherheit zu erhöhen, sollte das Passwort Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Erlaubte Zeichen (min. 6, max. 64): ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 0123456789!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ *Beispiel:* "*My-Password_123*"
		repeat_password	<string> (password in plain format)	**Neues Passwort bestätigen** Wiederholte Eingabe des neuen Passworts.

3.8 Endpunkt "update"

Über diesen Endpunkt kann das Hochladen einer von Phoenix Contact bereitgestellten signierten Update-Datei initiiert und das Firmwareupdate gestartet werden.

Alle Einstellungen, Passwörter und Zertifikate bleiben auf dem Gerät erhalten.

Ein Downgrade von einer höheren auf eine niedrigere Firmware-Version ist nicht möglich.

Beispiel

```
curl -v -b session_cookie -H "X-CSRF-Token: <TOKEN> "-H "Content-Type:multipart/form-data" -X POST -F update_info='{"content": {}, "envelope": {"version": 1}}' -F update_file=@/home/update/mGuard-image-1.8.0.mguard3.update.signed -k https://192.168.1.1:443/api/v1/update
```

Nach erfolgter Installation des Updates startet das Gerät nach einigen Sekunden automatisch neu. **Warten Sie, bis das Gerät vollständig gestartet wurde.**

Anmerkung

- Der Parameter *update_info* enthält keine Daten über den JSON-Frame und wird leer übergeben.
- Der Parameter *update_file* enthält den Pfad zur Update-Datei.

3.8.1 Unterscheidung von Update-Typen

Tabelle 3-34 Unterscheidung von Update-Typen (Beispiel)

Update-Typ	Eigenschaft	Auswirkung auf die bestehende Konfiguration
Patch-Release **Patch-Update**	Behebt Fehler aus den Vorversionen. Die Versionsnummer ändert sich an der dritten Stelle: – Die Version 1.7.**2** ist z. B. ein Patch-Release zu den Versionen 1.7.**1** oder 1.7.**0**.	Die bestehende Konfiguration wird unverändert beibehalten.
Minor-Release **Minor-Update**	Ergänzt das Gerät zusätzlich um neue Eigenschaften und Funktionen. Die Versionsnummer ändert sich an der zweiten Stelle: Die Version 1.**8**.0 ist z. B. ein Minor-Release zu den Versionen 1.**7**.2 oder 1.**6**.2.	1. Befindet sich das Gerät in der Werkseinstellung, gilt: – Das Gerät wird nach dem Update mit der werkseitigen Voreinstellung der **neuen** Firmware-Version konfiguriert. – Es ist möglich, dass sich Standardwerte der bestehenden Firmware-Version ändern oder Eigenschaften und Variablen hinzugefügt oder entfernt werden. 2. Wurden bereits Änderungen an der bestehenden Konfiguration des Geräts vorgenommen, gilt: – Die bestehende Konfiguration wird unverändert übernommen. – Neue Eigenschaften und Variablen aus der **neuen** Firmware-Version werden zur bestehenden Konfiguration hinzugefügt (in der Werkseinstellung). **Hinweis:** Damit das Update ausgeführt werden kann, müssen vor dem Update gegebenenfalls Anpassungen an der bestehenden Konfiguration vorgenommen werden. **Hinweis:** Sollte das Update aufgrund einer nicht kompatiblen Konfiguration fehlschlagen, wird der Benutzer über eine Fehlermeldung und/oder einen Log-Eintrag über den Grund des Fehlers informiert.
Major-Release **Major-Update**	Fügt dem Gerät zusätzlich grundlegende neue Eigenschaften und Funktionen hinzu. Die Versionsnummer ändert sich an der ersten Stelle: Die Version **2**.0.0 ist z. B. ein Major-Release zu den Versionen **1**.5.0 oder **1**.4.2.	

3.9 Endpunkt "datetime"

Über diesen Endpunkt kann die aktuelle Zeit (UTC) des Geräts

1. angezeigt (*GET-Request*) oder
2. eingestellt (*POST-Request*) werden.

Mittels *GET-Request* wird die manuell eingestellte oder per NTP bezogene Zeit (UTC) der ausgewählten Zeitzone entsprechend angezeigt.
Die **Zeitzone** kann im Endpunkt „*configuration*“ geändert werden (siehe Kapitel 3.4.17).

Um die Zeit manuell mittels *POST-Request* einzustellen, muss zunächst der NTP-Client deaktiviert werden (siehe Kapitel 3.4.13).

Beispiel: Zeit anzeigen (GET)

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/datetime

Antwort:

{"content": {"datetime": "2018-03-28_14:04:59"}, "envelope": {"identifier": {"contentID": "00bfc976", "functionalID": "00bfc976"}, "version": 1}, "error": [], "schemes": [{"name": "datetime.datetime.0020c25e", "url": "/v1/datetime/scheme/datetime.datetime.0020c25e"}], "status": 0}

Beispiel: Zeit einstellen (POST)

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type:application/json" -X POST https://192.168.1.1:443/api/v1/datetime -d '{"content": {"datetime": "2018-03-28_14:04:59"}, "envelope": {"version": 1}}'

Tabelle 3-35 Endpunkt **datetime**

Endpunkt	Methode	Key	Wert (Format)	Bezeichnung (WBM) / Beschreibung
datetime	**POST**	datetime	<YYYY-MM-DD_hh:mm:ss>	**Zeit und Datum einstellen** Die Systemzeit des Geräts wird konfiguriert und in der *Real-Time-Clock* (RTC) abgespeichert. Erlaubter Bereich: >= 2018-01-01_00:00:00 <= 2069-01-01_00:00:00 Die Systemzeit wird der konfigurierten Zeitzone entsprechend angezeigt und verwendet (z. B. in Log-Einträgen). *Beispiel: "2018-03-28_14:04:59"*

3.10 Endpunkt "snapshot"

Über diesen Endpunkt kann ein Snapshot erstellt und heruntergeladen werden.

Der Snapshot kann zur Fehlerdiagnose und bei der Kommunikation mit dem Support verwendet werden. Er enthält die aktuelle Konfiguration, Informationen zur Benutzerverwaltung und andere Systeminformationen des Geräts (siehe Tabelle 3-36):

Tabelle 3-36 Inhalt eines Snapshots

Dateiname	Inhalt / Beschreibung
Dateiformat: *json*	
config.json	Zeigt die aktuelle Gerätekonfiguration.
serdata.json	Zeigt die Serialisierungsdaten, die bei der Herstellung mit dem Gerät verknüpft wurden.
ldap.json	Zeigt die aktuelle Konfiguration zur LDAP-Authentifizierung via LDAP-Server.
users.json	Zeigt aktuelle Informationen über die lokalen Benutzer auf dem Gerät.
Dateiformat: *txt*	
bootloader_version	Zeigt die Version des aktuell installierten Bootloaders.
conntrack	Zeigt den aktuellen Inhalt der Zustandstabelle (*connection tracking table*).
df	Zeigt die aktuelle Belegung des Dateisystems.
eds	Zeigt aktuelle dynamische Status-Informationen zu bestimmten Funktionen des Geräts.
ethtool_eth0	Zeigt Informationen über den Ethernet-Port *eth0* (XF1 / Netzzone 1).
ethtool_eth1	Zeigt Informationen über den Ethernet-Port *eth1* (XF2–5 / Netzzone 2).
ipset_list	Zeigt Informationen über das aktuell verwendete IP-Set.
ip_neight	Zeigt aktuelle Verbindungsinformationen zu angeschlossenen (*benachbarten)* Geräten.
ip_route	Zeigt die aktuelle Routing-Tabelle.
ip_link	Zeigt den aktuellen Verbindungsstatus der Netzwerkinterfaces.
ip_addr	Zeigt die aktuelle Netzwerkkonfiguration.
issue	Informationen zum Firmware-Image.
journal	Zeigt die aktuelle Log-Datei des Systems.
ls_mnt_hfs	Zeigt die aktuell im Dateisystem des Geräts (/mnt/hfs) vorhandenen Dateien und Verzeichnisse.
mount	Zeigt die eingehängten Dateisysteme.
nft_ruleset	Zeigt die aktuell konfigurierten Firewall-Regeln.
nft_tables	Zeigt die aktuell konfigurierten Firewall-Tabellen.
proc_net_dev	Zeigt aktuelle Informationen über den Netzwerkverkehr aller Netzwerk-Interfaces (Datei */proc/net/dev*).
proc_net_snmp	Zeigt Informationen über den Netzwerkverkehr über das SNMP-Protokoll (Datei */proc/net/snmp*).
pstree	Zeigt Informationen über aktuell laufende Prozesse.
services	Zeigt die aktuell auf dem System gestarteten Dienste (*systemd)*.
tpm2_fixed	Zeigt nicht veränderbare Informationen über den TPM-Chip.
tpm2_variable	Zeigt veränderbare Informationen des TPM-Chips.

Tabelle 3-36 [...]Inhalt eines Snapshots

Dateiname	Inhalt / Beschreibung
uptime	Zeigt die aktuelle Betriebszeit und den Load Average des Systems.
userid	Zeigt die User-ID und die Gruppenmitgliedschaft.
version	Zeigt die aktuell installierte Firmware-Version.

Sensitive Daten und sicherheitsrelevante Informationen (z. B. Passwörter oder geheime kryptografische/gehashte Schlüssel) sind im Snapshot nicht enthalten.

Beispiel: Snapshot erstellen und herunterladen

curl -k -O -J -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/snapshot

Antwort:

```
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 31225  100 31225    0     0   4158      0  0:00:07  0:00:07 --:--:--  7256
curl: Saved to filename 'snapshot_2019-12-24_22_00_00.tar.gz'
```

Der Zeitpunkt der Snapshot-Erstellung wird im Dateinamen wie folgt angegeben: <YYYY-MM-DD_hh:mm:ss> (siehe auch Kapitel 3.2)

3.11 Endpunkt "logging"

Über diesen Endpunkt können alle oder ausgewählte Log-Einträge auf dem Gerät abgerufen und angezeigt werden.

Firewall-Logging
Log-Einträge werden nur für Pakete mit dem *Ether-Type IPv4* erstellt. Pakete mit anderen *Ether-Types* (z. B. *ARP, IPv6*) werden nicht in den Log-Dateien protokolliert. (Ausnahme: Einträge, die das Rate-Limit betreffen – *fw-input-rate-limit*)

Bei Datenverbindungen (z. B. UDP, TCP oder ICMP) wird nur das erste Paket der Verbindung geloggt (wenn Logging aktiviert ist), da die Verbindung dem *Connection Tracking* unterliegt.

Remote-Logging (Log-Server)
Die Konfiguration eines Remote-Servers (*Syslog*-Server) erfolgt im Endpunkt „*configuration*“ (siehe Kapitel 3.4.4).

In seltenen Fällen kann es bei der Generierung vieler Log-Eintrage dazu kommen, dass ein Log-Eintrag nicht übertragen wird. Um dies nachprüfen zu können, wird jeder Log-Eintrag, wie im Syslog-Protokoll beschrieben, mit einer fortlaufenden Sequenz-ID versehen (z. B. meta sequenceId="728").

Sensitive Daten und sicherheitsrelevante Informationen (z. B. Passwörter oder geheime kryptografische/gehashte Schlüssel) sind in den Log-Dateien nicht enthalten.

Anders als im WBM wird der Zeitpunkt, an dem der Log-Eintrag erstellt wurde, unabhängig von der eingestellten Zeitzone immer in UTC angezeigt.

Beispiel: Alle Log-Einträge abrufen (GET)

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/logging

Antwort:

{"content":{"logging":{"logs" :"Jan 27 08:09:44 kernel:

[…]

Jan 27 08:13:32 configapi[1963]:127.0.0.1 - - [27/Jan/2020 08:13:32] \"GET /v1/logging HTTP/1.1\" 200 -\n"}}, "error":[], "envelope":{ "version":1, "identifier":{ "contentID":"66db9094", "functionalID":"66db9094" }}, "status":0, "schemes":[{ "url":"/v1/logging/scheme/logging.logging.17ef3f7f", "name":"logging.logging.17ef3f7f" }]}

Beispiel: Nur Firewall-Log-Einträge abrufen (POST)

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/logging -d '{"content": {"logging": {"features": ["firewall"]}}, "envelope": {"version":1}}'

Antwort:

{"content": {"logging": {"logs":"Mar 28 14:12:00 systemd[1]: Started Firewall Logger.\nMar 28 14:14:32 firewall-log[1618]: fw-forward-policy: IPv4 PROTO=ICMP SRC=10.1.0.68 DST=192.168.1.2 SPT=0 DPT=0\nMar 28 14:14:32 firewall-log[1618]: fw-forward-policy: IPv4 PROTO=ICMP SRC=10.1.0.68 DST=192.168.1.2 SPT=0 DPT=0\nMar 28 14:14:34 firewall-log[1618]: fw-forward-policy: IPv4 PROTO=ICMP SRC=10.1.0.68 DST=192.168.1.2 SPT=0 DPT=0\nMar 28 14:14:34 firewall-log[1618]: fw-forward-policy: IPv4 PROTO=ICMP SRC=10.1.0.68 DST=192.168.1.2 SPT=0 DPT=0\nMar 28 14:14:36 firewall-log[1618]: fw-forward-policy: IPv4 PROTO=ICMP SRC=10.1.0.68 DST=192.168.1.2 SPT=0 DPT=0\nMar 28 14:14:36 firewall-log[1618]: fw-forward-policy: IPv4 PROTO=ICMP SRC=10.1.0.68 DST=192.168.1.2 SPT=0 DPT=0\n"}}, envelope": {"identifier": {"contentID":"993a659f","functionalID":"993a659f"},"version": 1},"error":[],"schemes": [{"name": "logging.logging.17ef3f7f","url":"/v1/logging/scheme/logging.logging.17ef3f7f"}],"status": 0}

Tabelle 3-37 Endpunkt **logging**

Endpunkt	Methode	Key	Wert (Format)	Bezeichnung (WBM) / Beschreibung
logging	**POST**	"features"	"firewall"	**Nur Firewall** Nur Log-Einträge von Ereignissen, die die Firewall betreffen, werden abgerufen und angezeigt. *Beispiel: "firewall"*

3.12 Endpunkt "status"

Über diesen Endpunkt können dynamische Status-Informationen zu bestimmten Funktionen des Geräts im JSON-Format abgerufen und angezeigt werden.

Zum Beispiel:

– Aktuelle Firmware-Version
– Test-Mode-Alarme
– Status des *Firewall Assistant*
– DHCP-Client (vom DHCP-Server empfangene Daten zur Netzwerkkonfiguration)

Beispiel: Dynamische Statusinformationen abrufen (GET)

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/status


```
{ "content": {
   "firewall": {
    "forward": {
     "testmode": {
      "hit": ""} } },
   "fwassist": {
    "status": "OFF"
   },
   "network": {
    "dhcp": "",
    "noroute": "0",
    "ntp_state": "NOT_SYNCED"
   },
   "system": {
    "admin_password_is_default": "FALSE",
    "firmwareversion": "1.8.0"
   },
   "tcpdump": {
    "status": "OFF"
   },
   "users": {
    "admin": {
     "block_start_time": "",
     "block_status": "UNBLOCKED"
    },
    "admin_extern": {
     "block_start_time": "",
     "block_status": "BLOCKED_BY_ADMIN"
    },
    "audit_production": {
     "block_start_time": "",
     "block_status": "BLOCKED_BY_AUTO"
   } } }, "envelope": { "identifier": { "contentID": "facbc43c", "functionalID": "facbc43c" }, "version": 1 }, "error": [], "schemes": [], "status": 0}
```

3.13 Endpunkt "actions/fwassist"

Über die Endpunkte "*/v1/actions/fwassist/start*" und "*/v1/actions/fwassist/stop* " kann der *Firewall Assistant* gestartet und gestoppt werden.

Beschreibung

Der *Firewall Assistant* analysiert und erfasst im aktivierten Zustand den Datenverkehr, der durch das Gerät durchgeleitet (*geroutet*) wird (**Netzzone 1 ⟷ Netzzone 2**).

Die Firewall ist dabei in beide Richtungen geöffnet.

Aus den erfassten Paketdaten werden Firewall-Regeln abgeleitet, die beim Beenden des *Firewall Assistant* automatisch in die entsprechenden Firewall-Tabellen des Geräts eingetragen werden.

Der in diesen Firewall-Regeln definierte Datenverkehr wird künftig erlaubt (**Aktion = Annehmen**). Alle anderen Verbindungen werden verworfen.

Die mittels *Firewall Assistant* erstellten Firewall-Tabellen können beliebig angepasst und erweitert werden.

Tabelle 3-38 Firewall Assistant: Umwandlung von Paketdaten in Firewall-Regeln

Header-Eintrag	Eintrag in Firewall-Regel	Beispiel
Quell-IP-Adresse	**src_network**	*10.1.1.55*
Ziel-IP-Adresse	**dst_network**	*192.168.1.100*
Die jeweilige Netzmaske des Quell- und des Ziel-Netzwerks wird nicht erfasst. Es werden lediglich einzelne IP-Adressen erfasst und in die Firewall-Regel übernommen.		
Ziel-Port	**dst_port**	*443*
Wird kein Ziel-Port übertragen (wie z. B. beim *ICMP*-Protokoll), wird in der Firewall-Regel kein Wert eingetragen.		
Protokoll	**protocol**	*ALL*
Folgende Protokolle können als Wert in die Firewall-Regel übernommen werden: – *TCP, UDP, ICMP, GRE, ESP* Für alle anderen Protokolle wird in der Firewall-Regel der Wert „*ALL*" eingetragen.		
—	**verdict**	*ACCEPT*
In alle mittels *Firewall Assistant* oder *Firewall-Test-Mode* erstellten Firewall-Regeln wird als Aktions-Wert grundsätzlich immer „*Annehmen*" eingetragen.		

3.13.1 Firewall Assistant starten ("actions/fwassist/start")

ACHTUNG: Die Firewall wird deaktiviert.
Wenn der *Firewall Assistant* aktiviert ist, werden angebundene Netzwerk-Clients nicht mehr durch die Firewall geschützt.

Der *Firewall Assistant* kann nur gestartet werden, wenn vorher **alle Firewall-Regeln** in allen Firewall-Tabellen gelöscht wurden (siehe Kapitel 3.4.1).

Über diesen Endpunkt kann der *Firewall Assistant* aktiviert werden:

⇒ Der Datenverkehr wird analysiert und erfasst.

⇒ Die Firewall ist in beide Richtungen geöffnet.

Beispiel:

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/fwassist/start

Antwort:

{"content":{},"envelope":{"identifier":{"contentID":"a3a6bf43","functionalID":"a3a6bf43"},"version":1},"error":[],"schemes":[],"status":0}

3.13.2 Firewall Assistant stoppen ("actions/fwassist/stop")

ACHTUNG: Die automatisch erstellten Firewall-Regeln sind ungeprüft aktiv.
Prüfen Sie umgehend die neu erstellten Firewall-Regeln und passen Sie diese Ihren Sicherheitsanforderungen entsprechend an.

Über diesen Endpunkt kann der aktivierte *Firewall Assistant* gestoppt werden:

⇒ Aus den erfassten Paketdaten werden automatisch Firewall-Regeln erstellt und in die entsprechenden Firewall-Tabellen eingetragen (WBM-Menü: **Netzwerksicherheit >> Firewall >> Regeln**, siehe Tabelle 3-8).

⇒ Die eingetragenen Regeln erlauben den entsprechenden Datenverkehr umgehend und permanent (**Aktion = Annehmen**) (siehe Tabelle 3-38).

Beispiel:

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/fwassist/stop

Antwort (Ausschnitt):

{"content": "{\"fileinfo\": {\"devtype\": \"0001010111020000\", \"firmware\": \"1.8.0\"}, \"firewall\": {\"forward\": {\"sanity_check\": \"ON\", \"stealth_allow_dhcp\": \"ON\", \"tables\": [{\"in_netzone\": \"NETZONE1\", \"out_netzone\": \"NETZONE2\", \"rules\": [{\"dst_network\": \"192.168.1.1\", \"dst_port\": \"ALL\", \"id\": 1, \"protocol\": \"ALL\", \"src_network\": \"10.1.0.68\", \"verdict\": \"ACCEPT\"}]}, {\"in_netzone\": \"NETZONE2\", \"out_netzone\": \"NETZONE1\", \"rules\": []}], \"testmode\": \"OFF\"},

...

3.14 Endpunkt "actions/ping"

Über diesen Endpunkt kann geprüft werden, ob ein Netzwerk-Client über seine IP-Adresse mit einem Interface des Geräts verbunden und über das ICMP-Protokoll erreichbar ist.

Beispiel

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/ping -d '{"content": {"dst_ip": "192.168.1.3"}, "envelope": {"version": 1}}'

Antwort:

{"content": {

"result": "PING 192.168.1.3 (192.168.1.3): 56 data bytes\n64 bytes from 192.168.1.3: seq=0 ttl=128 time=1.801 ms\n64 bytes from 192.168.1.3: seq=1 ttl=128 time=1.670 ms\n64 bytes from 192.168.1.3: seq=2 ttl=128 time=1.521 ms\n64 bytes from 192.168.1.3: seq=3 ttl=128 time=1.515 ms\n64 bytes from 192.168.1.3: seq=4 ttl=128 time=1.486 ms\n\n--- 192.168.1.3 ping statistics ---\n5 packets transmitted, 5 packets received, 0% packet loss\nround-trip min/avg/max = 1.486/1.598/1.801 ms\n"

},

"envelope": {

"identifier": {

"contentID": "28e2909c",

"functionalID": "28e2909c"

},

"version": 1

},

"error": [],

"schemes": [],

"status": 0

}

Tabelle 3-39 Endpunkt **actions/ping**

Endpunkt	Methode	Key	Wert (Format)	Bezeichnung (WBM) / Beschreibung
actions/ping	**POST**	dst_ip	<ip>	**Ping** Eine Ping-Anfrage (*ICMP request*) wird an die angegebene IP-Adresse eines Netzwerk-Clients gesendet. Ist der Client über eine beliebige Netzzone des Geräts über das ICMP-Protokoll erreichbar, sendet er eine Antwort an das Gerät zurück. *Beispiel: "192.168.1.254"*

3.15 Endpunkt "actions/tcpdump"

Über diesen Endpunkt kann der Inhalt von Netzwerkpaketen analysiert werden, die über ein ausgewähltes Netzwerkinterface gesendet oder empfangen werden (*tcpdump*).

Welche Netzwerkpakete analysiert werden, wird über Filteroptionen bestimmt.

Das Ergebnis der Analyse wird in einer Datei (**.pcap*) gespeichert, heruntergeladen und auf dem Gerät gelöscht.

Wird das Gerät währen einer laufenden Analyse neu gestartet, werden die bis dahin gesammelten Daten gelöscht.

Wenn die Datei (**.pcap*) eine Größe von 50 MB überschreitet, wird die Analyse mit einem Fehler abgebrochen. Die bis dahin gesammelten Daten werden gelöscht.

3.15.1 Netzwerkanalyse starten ("actions/tcpdump/start")

Über diesen Endpunkt kann die Paketanalyse (*tcpdump*) aktiviert werden.

Beispiel: Daten erfassen

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/tcpdump/start -d '{"content": {"interface": "eth0", "options": "tcp and net 192.168.1.0/24 and not port 443"}, "envelope": {"version": 1}}'

Antwort:

{"content":{},"envelope":{"identifier":{"contentID":"a3a6bf43","functionalID":"a3a6bf43"},"version":1},"error":[],"schemes":[],"status":0}

Tabelle 3-40 Endpunkt **actions/tcpdump/start**

Endpunkt	Methode	Key	Wert (Format)	Bezeichnung (WBM) / Beschreibung
actions/tcpdump/start	**POST**	interface	*“lan(n)“* *“eth(n)“*	Nur Datenpakete, die über das ausgewählte Netzwerk-Interface gesendet oder empfangen werden, werden analysiert. *Beispiel: "eth0“*
		Durch die Angabe von Optionen kann die Paketanalyse auf eine Auswahl der unten stehenden Elemente beschränkt werden. Optionen können über die logischen Verknüpfungen „*and*, *or*, *not*“ verknüpft werden. *Beispiel: "tcp and net 192.168.1.0/24 and not port 443"*		
		options	tcp	TCP-Protokoll
			udp	UDP-Protokoll
			arp	ARP-Protokoll
			icmp	ICMP-Protokoll
			esp	ESP-Protokoll
			host <ip>	IPv4-Adresse
			port <1-65535>	Netzwerkport (einzelne Portnummer)
			net <nw_cidr>	Netzwerk (in CIDR-Schreibweise, z. B. 192.168.1.0/24)
			and, or, not	Logische Verknüpfungen

3.15.2 Netzwerkanalyse stoppen ("actions/tcpdump/stop")

Über diesen Endpunkt kann eine laufende Analyse (*tcpdump*) gestoppt werden. Die erfassten Paketinhalte werden in einer Datei (**.pcap*) zusammengefasst und automatisch vom Gerät heruntergeladen. Anschließend wird die Datei auf dem Gerät gelöscht.

Beispiel: Datenerfassung stoppen und Daten herunterladen

curl -k -J -O -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/tcpdump/stop

Antwort:

```
% Total    % Received % Xferd  Average     Speed   Time    Time     Time  Current
                                 Dload     Upload   Total   Spent    Left  Speed
100 361    100 361    0  0      4158             0  0:00:07  0:00:07 --:--:--  7256
curl: Saved to filename 'tcpdump_2019-12-24_18_20_53.pcap'
```

Der Zeitpunkt des Herunterladens der Datei wird im Dateinamen wie folgt angegeben: <YYYY-MM-DD_hh:mm:ss> (siehe auch Kapitel 3.2)

3.16 Endpunkt "actions/pki/renew/logging"

Über diesen Endpunkt kann das Client-Zertifikat, das für die Authentifizierung des Geräts gegenüber einem Remote-Syslog-Server verwendet wird, heruntergeladen oder neu erzeugt werden.

Das selbstsignierte Client-Zertifikat, mit dem sich das Gerät gegenüber dem Remote-Server (*Syslog*-Server) authentifiziert, wird auf dem Gerät erzeugt und dort gespeichert.

Es muss heruntergeladen und vom Betreiber des Remote-Servers auf den Remote-Server hochgeladen werden (X.509-Zertifikat mit *öffentlichem* Schlüssel).

GET-Request: Das bestehende Zertifikat wird heruntergeladen

POST-Request: Das Zertifikat wird neu erzeugt und heruntergeladen. Das bestehende Zertifikat wird verworfen.

ACHTUNG: Das aktuelle Zertifikat wird gelöscht
Wenn Sie ein neues Client-Zertifikat erzeugen, wird das aktuell auf dem Gerät gespeicherte Zertifikat unwiderruflich gelöscht. Das neu erzeugte Zertifikat muss erneut auf den Remote-Server hochgeladen werden.

3.16.1 Client-Zertifikat herunterladen/anzeigen

Beispiel: Client-Zertifikat herunterladen/anzeigen (GET)

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/actions/pki/renew/logging

Antwort:

{ "content": {

"result": "-----BEGIN CERTIFICATE-----
\nMIIC+jCCAoCgAwIBAgIUYAZPkn8RAgJAmkIOnLDm+onXOScwCgYIKoZIzj0EAwIw\ngY4xIzAhBgNVBAMMGjB4ZDc1ZmFiMDhfOUIraTVVNnJfc3lzbG9nMScwJQYDVQQK\nDB5QSE9FTklYIENPTlRBQ1QgQ3liZXIgU2VjdXJpdHkxDzANBgNVBAsMBm1HdWFy\nZDEPMA0GA1UEBwwGQmVybGluMQ8wDQYDVQQIDAZCZXJsaW4xCzAJBgNVBAYTAkRF\nMB4XDTIwMDkyMzA5MDQwMloXDTIxMDkyMzA5MDQwMlowgY4xIzAhBgNVBAMMGjB4\nZDc1ZmFiMDhfOUIraTVVNnJfc3lzbG9nMScwJQYDVQQKDB5QSE9FTklYIENPTlRB\nQ1QgQ3liZXIgU2VjdXJpdHkxDzANBgNVBAsMBm1HdWFyZDEPMA0GA1UEBwwGQmVy\nbGluMQ8wDQYDVQQIDAZCZXJsaW4xCzAJBgNVBAYTAkRFMHYwEAYHKoZIzj0CAQYF\nK4EEACIDYgAEZ6tFsUk5fQFCz/9BiCUWnpugLfMukOFqvA7LxTfgCrm/m205vFjB\n8XioQ/6K7l/u46QxFkvFRVFCReSp42igsQPIB9UovrTS5QHFl1co8bZ0olHEYret\nc9mPYokYCRYIo4GcMIGZMB0GA1UdDgQWBBQsGCVeZr4OqdwrUFNg+YeFB7mYPTAf\nBgNVHSMEGDAWgBQsGCVeZr4OqdwrUFNg+YeFB7mYPTAPBgNVHRMBAf8EBTADAQH/\nMEYGA1UdEQQ/MD2CBm1HdWFyZIIJbG9jYWxob3N0hxD+gAAAAAAAAAAAAAAAAAAB\nhwR/AAABhxAAAAAAAAAAAAAAAAAAAABMAoGCCqGSM49BAMCA2gAMGUCMQDsbX2a\nyUmuqqjOQD+5AzMNiAFl5haDmHkl0pEmvcLY9f8nNHQ8Me58PuZyw4VgKowCMDL3\nnBsYB4Kc3flirQUy7hn0RjV2OH1OQjGNS2cHopSQXC9IneNrTjuWfVe9Hr2RzKA==\n-----END CERTIFICATE-----\n"

},

"envelope": {"identifier": {"contentID": "d90879c6", "functionalID": "d90879c6"}, "version": 1}, "error": [], "schemes": [], "status": 0}

3.16.2 Client-Zertifikat neu erzeugen und herunterladen/anzeigen

Beispiel: Client-Zertifikat neu erzeugen und herunterladen/anzeigen (POST)

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/pki/renew/logging

Antwort:

{"content":{"result":"-----BEGIN CERTIFICATE-----
\nMIIC/jCCAoOgAwIBAgIUOqSd61vLE05FFS3HTUj7R95SLQowCgYIKoZIzj0EAwIw\ngY4xIzAhBgNVBAMMGjB4ZDdhN2M1MDhfU3BNMVpVLWdfc3lzbG9nMScwJQYDVQQK\nDB5QSE9FTklYIENPTlRBQ1QgQ3liZXIgU2VjdXJpdHkxDzANBgNVBAsMBm1HdWFy\nZDEPMA0GA1UEBwwGQmVybGluMQ8wDQYDVQQIDAZCZXJsaW4xCzAJBgNVBAYTAkRF\nMB4XDTIwMDkyNDA4MzUyMloXDTIxMDkyNDA4MzUyMlowgY4xIzAhBgNVBAMMGjB4\nZDdhN2M1MDhfU3BNMVpVLWdfc3lzbG9nMScwJQYDVQQKDB5QSE9FTklYIENPTlRB\nQ1QgQ3liZXIgU2VjdXJpdHkxDzANBgNVBAsMBm1HdWFyZDEPMA0GA1UEBwwGQmVy\nbGluMQ8wDQYDVQQIDAZCZXJsaW4xCzAJBgNVBAYTAkRFMHYwEAYHKoZIzj0CAQYF\nK4EEACIDYgAEbfRgAuCxBh6iOq38GZVKbdlxC7OLSOZRB+C8RYDUu+f/+bzon/bP\nMZhjmuWhwhVFmFm0CBjRa4DuEN1LhJwKwmpTmKX4W2x8UCdLhEaAtbSXrFelCYo8\ngZSVs/Em8415o4GfMIGcMB0GA1UdDgQWBBT/HhB3tU2HOs0Xm3wg/PRGaAhvcjAf\nBgNVHSMEGDAWgBT/HhB3tU2HOs0Xm3wg/PRGaAhvcjAPBgNVHRMBAf8EBTADAQH/\nMEkGA1UdEQRCMECCCXRyZXRzdHN0c4IJbG9jYWxob3N0hxD+gAAAAAAAAAAAAAAA\nAAABhwR/AAABhxAAAAAAAAAAAAAAAAAAAABMAoGCCqGSM49BAMCA2kAMGYCMQD4\ncX0FsoGCrfCD5kkxr9TDZzul9bCu9O6mw6/BahwNmtVbKOflNrPXcYNIrNhgc7sC\nMQCsAvMxmMzkxVQoTLL2CDTCfQmyc-cZufdF5lSjHq6Hd+VVUls+2xUxs1R63D9sb\nsqE=\n-----END CERTIFICATE-----
\n"},"envelope":{"identifier":{"contentID":"e039f5fa","functionalID":"e039f5fa"},"version":1},"error":[],"schemes":[],"status":0}

3.17 Endpunkt "actions/storeconfig/sdcard"

Über diesen Endpunkt kann die aktuell auf dem Gerät gespeicherte Konfiguration auf die eingesetzte SD-Karte geschrieben werden.

Es werden drei Dateien gespeichert:

– *users_pass.json, snmp-pass.conf, configuration.json*

Stellen Sie sicher, dass nur befugte Personen auf die SD-Karte zugreifen können.

Entnehmen Sie die SD-Karte erst, wenn der Schreibvorgang abgeschlossen ist.

Gespeicherte Konfiguration via SD-Karte erneut in ein Gerät importieren

Für alle **neuen Geräte** oder Geräte, die mittels Smart-Mode auf Werkseinstellungen zurückgesetzt wurden, gilt:

Eine auf der eingesetzten SD-Karte gespeicherte Konfiguration/Benutzerverwaltung wird beim Start bzw. der Inbetriebnahme des Geräts automatisch in das Gerät importiert und dort angewendet.

Voraussetzung:

– Firmware-Version „SD-Karte“ ist in der Minor-Version kleiner/gleich Firmware-Version „Gerät“.
– Die drei Dateien sind auf der SD-Karte enthalten (einzeln oder in gepackter Form als *mGuard.tar.gz:* Die Einzeldateien werden prioritär verwendet!).

Tritt während des Imports ein Fehler auf, startet das Gerät in der werkseitigen Voreinstellung. Die LEDs FAIL und PF1 leuchten zusätzlich rot.

Die gespeicherte Konfiguration enthält sicherheitsrelevante Informationen, wie z. B. lokale Benutzer, Berechtigungen, Passwörter (hashed) und Zertifikate (öffentliche Schlüssel). Das Password für den LDAP-Server ist im Klartext enthalten.
Ausnahme: Private Schlüssel sind in der Konfiguration nicht enthalten.

Beispiel: Aktuell gespeicherte Konfiguration auf SD-Karte schreiben

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/storeconfig/sdcard

Antwort:

{ "content": "",
"envelope": {
"identifier": {
"contentID": "330b153b",
"functionalID": "330b153b"
}, "version": 1}, "error": [], "schemes": [], "status": 0}

3.18 Endpunkt "actions/reboot"

Über diesen Endpunkt kann das Gerät neu gestartet werden.

Alle nicht gespeicherten Änderungen gehen verloren.

Beispiel: Gerät neu starten

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/reboot

Antwort:


```
{
  "content": "",
  "envelope": {
    "identifier": {
      "contentID": "330b153b",
      "functionalID": "330b153b"
    },
    "version": 1
  },
  "error": [],
  "schemes": [],
  "status": 0
}
```

3.19 Endpunkt "actions/unblockuser"

Über diesen Endpunkt kann ein automatisch gesperrter Benutzer (siehe Kapitel 3.4.15) von einem Benutzer mit der Rolle "*Super Admin*" vor Ablauf der Sperrzeit entsperrt werden.

Beispiel: Benuter admin2 entsperren

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/unblockuser -d '{"content": {"username": "admin2"}, "envelope": {"version": 1}}'

Antwort:

{"content":{"result":true},"envelope":{"identifier":{"contentID":"a3a6bf43","functionalID":"a3a6bf43"},"version":1},"error":[],
"schemes":[
{
"name": "unblockuser.unblockuser.228955d0",
"url": "/v1/actions/unblockuser/scheme/unblockuser.unblockuser.228955d0"
}
],"status":0}

Tabelle 3-41 Endpunkt **actions/tcpdump/start**

Endpunkt	Methode	Key	Wert (Format)	Bezeichnung (WBM) / Beschreibung
actions/unblockuser	**POST**	username	<string>	Ein automatisch gesperrter Benutzer wird vor Ablauf der Sperrzeit entsperrt. Der Status des Benutzers im Endpunkt "Status" wechselt von "BLOCKED_BY_AUTO" zu "UNBLOCKED" (siehe Kapitel 3.12). **Hinweis:** Eine automatische Sperre wird ebenfalls durch einen Neustart des Geräts aufgehoben.

3.20 Endpunkt "actions/migration"

Über diesen Endpunkt kann eine Konfiguration, die mit einer älteren Firmware-Version erstellt wurde, in eine Konfiguration migriert werden, die der aktuell installierten Firmware-Version auf dem Gerät entspricht.

Die migrierte Konfiguration wird als Antwort auf den POST-Request lediglich angezeigt. Das Hochladen und Aktivieren einer Konfiguration erfolgt über den Endpunkt "*configuration*" (siehe Kapitel 3.4).

Die migrierte Konfiguration kann mit einem Text-Editor angepasst und anschließend über den Endpunkt "*configuration*" auf das Gerät hochgeladen und dort aktiviert werden.

Beispiel: Konfiguration (1.5.1) auf ein Gerät mit installierter Firmware-Version 1.8.0 migrieren

```
curl -k -b session_cookie -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST
https://192.168.1.1:443/api/v1/actions/migration -d '
{{"content": {
   "fileinfo": {
    "devtype": "0001010111020000",
    "firmware": "1.5.1"
   },
   "firewall": {
    "forward": {
     "log_all_matches": "OFF",
     "log_policy": "OFF",
[...]
```

Antwort: (Die Antwort zeigt die migrierte Konfiguration an: Für eine strukturierte Ansicht siehe Kapitel 4.4)

```
"content": {
   "fileinfo": {
    "devtype": "0001010111020000",
    "firmware": "1.8.0"
   },
   "firewall": {
    "forward": {",
     "ftp_allow_field": "OFF",
     "log_all_matches": "OFF",
     "log_policy": "OFF",
[...]
```

3.21 Endpunkt "usenotification"

Über diesen Endpunkt kann die Systembenachrichtigung angezeigt werden.

Session-Cookie und *Session-Token* sind bei einem *GET-Request* auf diesen Endpunkt nicht erforderlich.

Die **Konfiguration der Systembenachrichtigung** erfolgt im Endpunkt "*configuration/system*" (siehe Kapitel 3.4.16).

Beispiel: Systembenachrichtigung anzeigen (GET)

curl -k -X GET https://192.168.1.1:443/api/v1/usenotification

Antwort:

{"content": "The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited.", "envelope": {"identifier": {"contentID": "00bfc976", "functionalID": "00bfc976"}, "version": 1}, "error": [ ], "schemes": [ ], "status": 0}

3.22 Endpunkt "softwarelicense"

Über diesen Endpunkt können die aktuell gültigen *Software License Terms* (SLT) für das Produkt erstellt und heruntergeladen werden. Die SLT werden als PDF-Datei bereitgestellt.

Beispiel:

curl -k -O -J -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/softwarelicense

Antwort:

% Total	% Received	% Xferd	Average Dload	Speed Upload	Time Total	Time Spent	Time Left	Current Speed
100 2186k	100 2186k	0 0	12.4M	0	0:00:07	0:00:07	--:--:--	12.3M

curl: Saved to filename 'Phoenix_Contact_Software_License_Terms_date_of_May_2018.pdf'

3.23 Endpunkt "licenses"

Über diesen Endpunkt können die auf dem Gerät verwendeten Software-Komponenten (Module) von Drittanbietern angezeigt werden.

Beispiel:

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/licenses

Antwort:

{"content": {"modules": ["acl", "attr", "base-files", "base-passwd", "busybox", "bzip2", "ca-certificates", "conntrack-tools", "cracklib", "curl", "dbus", "dbus-glib", "dtc", "e2fsprogs", "ethtool", "expat", "gcc-runtime", "gdbm", "glib-2.0", "glibc", "gmp", "gnutls", "gptfdisk", "jq", "kmod", "libcap", "libffi", "libgcc", "libgcrypt", "libgpg-error", "libidn2", "libmnl", "libnetfilter-conntrack", "libnetfilter-cthelper", "libnetfilter-cttimeout", "libnfnetlink", "libnftnl", "libpam", "libpcre", "libseccomp", "libunistring", "libxcrypt", "libxml2", "linux-yocto", "mdio-tool", "ncurses", "netbase", "nettle", "nftables", "nginx", "openssh", "openssl", "opkg-utils", "os-release", "packagegroup-core-boot", "packagegroup-tpm2", "parted", "perl", "popt", "python3", "python3-click", "python3-flask", "python3-itsdangerous", "python3-jinja2", "python3-jsonmerge", "python3-jsonpointer", "python3-jsonschema", "python3-markupsafe", "python3-rfc3987", "python3-setuptools", "python3-simplejson", "python3-strict-rfc3339", "python3-werkzeug", "readline", "rng-tools", "run-postinsts", "shadow", "shadow-securetty", "shared-mime-info", "sqlite3", "systemd", "systemd-compat-units", "systemd-conf", "systemd-serialgetty", "tpm2-abrmd", "tpm2-tools", "tpm2-tss", "tpm2-tss-engine", "u-boot-tools", "update-rc.d", "util-linux", "volatile-binds", "xz", "zlib"]}, "envelope": {"identifier": {"contentID": "39632d7a", "functionalID": "39632d7a"}, "version": 1}, "error": [], "schemes": [{"name": "licenses.licenses.1362f8b6", "url": "/v1/licenses/scheme/licenses.licenses.1362f8b6"}], "status": 0}

3.24 Endpunkt "licenses/module/<module name>"

Über diesen Endpunkt können die Lizenzinformationen der auf dem Gerät verwendeten Software-Komponenten (Module) von Drittanbietern angezeigt werden.

Beispiel: Lizenzinformationen der Komponente „curl“ anzeigen

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/licenses/module/curl | python -m json.tool

Antwort:


```
{
  "content": {
    "license": [
      "COPYRIGHT AND PERMISSION NOTICE\n\nCopyright (c) 1996 - 2018, Daniel Stenberg, <daniel@haxx.se>, and many\ncontributors, see the THANKS file.\n\nAll rights reserved.\n\nPermission to use, copy, modify, and distribute this software for any purpose\nwith or without fee is hereby granted, provided that the above copyright\nnotice and this permission notice appear in all copies.\n\nTHE SOFTWARE IS PROVIDED \"AS IS\", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR\nIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,\nFITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN\nNO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM,\nDAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR\nOTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE\nOR OTHER DEALINGS IN THE SOFTWARE.\n\nExcept as contained in this notice, the name of a copyright holder shall not\nbe used in advertising or otherwise to promote the sale, use or other dealings\nin this Software without prior written authorization of the copyright holder.",
      "MIT License\n\nCopyright (c) <year> <copyright holders>\n\nPermission is hereby granted, free of charge, to any person obtaining a copy\nof this software and associated documentation files (the \"Software\"), to deal\nin the Software without restriction, including without limitation the rights\nto use, copy, modify, merge, publish, distribute, sublicense, and/or sell\ncopies of the Software, and to permit persons to whom the Software is\nfurnished to do so, subject to the following conditions:\n\nThe above copyright notice and this permission notice shall be included in\nall copies or substantial portions of the Software.\n\nTHE SOFTWARE IS PROVIDED \"AS IS\", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR\nIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,\nFITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE\nAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER\nLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,\nOUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN\nTHE SOFTWARE."
    ]
  },
  "envelope": {
    "identifier": {
      "contentID": "ed097814",
      "functionalID": "ed097814"
    },
    "version": 1
  },
  "error": [],
  "schemes": [
    {
      "name": "licenses.licenses.1362f8b6",
      "url": "/v1/licenses/scheme/licenses.licenses.1362f8b6"
    }
  ],
  "status": 0
}
```

4 Beispiele

4.1 GET-Request (Endpunkt: "configuration/default")

Befehl:

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/configuration/default

Antwort:


```
{
  "content": {
    "fileinfo": {
      "devtype": "0001010111020000",
      "firmware": "1.8.0"
    },
    "firewall": {
      "forward": {
        "ftp_allow_field": "OFF",
        "log_all_matches": "OFF",
        "log_policy": "OFF",
        "sanity_check": "ON",
        "stealth_allow_dhcp": "ON",
        "tables": [
          {
            "in_netzone": "NETZONE2",
            "out_netzone": "NETZONE1",
            "rules": [
              {
                "comment": "",
                "dst_network": "0.0.0.0/0",
                "dst_port": "ALL",
                "id": 0,
                "log": "OFF",
                "protocol": "ALL",
                "src_network": "0.0.0.0/0",
                "verdict": "ACCEPT"
              }
            ]
          },
          {
            "in_netzone": "NETZONE1",
            "out_netzone": "NETZONE2",
```

```
      "rules": []
     }
    ],
    "testmode": "OFF"
   },
   "input": {
    "rules": [
     {
      "id": 0,
      "log": "OFF",
      "service": "HTTPS",
      "source": "NETZONE2",
      "verdict": "ACCEPT"
     }
    ]
   },
   "port_forward": {
    "rules": []
   }
  },
  "logging": {
   "remote": {
    "address": "192.168.1.254",
    "port": 514,
    "protocol": "UDP",
    "status": "OFF"
   }
  },
  "network": {
   "mode": "ROUTER",
   "nat": {
    "1_1_nat": [],
    "masquerading": [
     {
      "from_ip": "0.0.0.0/0",
      "id": 0,
      "outgoing_on_if": "NETZONE1"
     }
    ]
   },
   "netzone1": {
    "mode": "DHCP"
   },
```

```
  "netzone2": {
    "address": "192.168.1.1",
    "netmask": 24
  },
  "routing": {
    "routes": []
  },
  "stealth": {
    "management_address": "192.168.1.1",
    "management_gateway": "192.168.1.254",
    "management_netmask": 24
  }
 },
 "service": {
  "dhcp_server": {
    "dns": "192.168.1.1",
    "gateway": "192.168.1.1",
    "lease_time": "12h",
    "netmask": 24,
    "range_high": "192.168.1.254",
    "range_low": "192.168.1.2",
    "status": "ON",
    "wins_server": ""
  },
  "dnscache": {
    "allowed_requests": [
      "NETZONE2"
    ],
    "dns_servers": "ROOT_DNS_SERVER",
    "log": "OFF",
    "user_defined": []
  },
  "ntp": {
    "allow_client_requests": [
      "NETZONE2"
    ],
    "server": [
      {
        "address": "0.pool.ntp.org",
        "comment": "",
        "port": 123
      },
      {
```

```
        "address": "1.pool.ntp.org",
        "comment": "",
        "port": 123
       },
       {
        "address": "2.pool.ntp.org",
        "comment": "",
        "port": 123
       },
       {
        "address": "3.pool.ntp.org",
        "comment": "",
        "port": 123
       }
      ],
      "status": "ON"
     },
     "snmp": {
      "allow_requests_from": [
       "NETZONE2"
      ],
      "ro_community_string": "public",
      "status_v2c": "OFF",
      "status_v3": "OFF"
     },
     "web": {
      "session_timeout": 30,
      "user_blocking_time": 10,
      "user_max_failed_logins": 5
     }
    },
    "system": {
     "hostname": "mGuard",
     "store_config_on_sdcard": "OFF",
     "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only.
Any intrusion and its attempt without permission is illegal and strictly prohibited."
    },
    "zoneinfo": "UTC"
   },
   "envelope": {
    "identifier": {
     "contentID": "72f6b081",
     "functionalID": "be532724"
```

```
  },
  "version": 1
},
"error": [],
"schemes": [
  {
    "name": "common.4710ab60",
    "url": "/v1/configuration/scheme/common.4710ab60"
  },
  {
    "name": "common.types.f0bf23da",
    "url": "/v1/configuration/scheme/common.types.f0bf23da"
  },
  {
    "name": "configuration.fileinfo.b3afd1b0",
    "url": "/v1/configuration/scheme/configuration.fileinfo.b3afd1b0"
  },
  {
    "name": "configuration.firewall.62d07c99",
    "url": "/v1/configuration/scheme/configuration.firewall.62d07c99"
  },
  {
    "name": "configuration.logging.fce1b9ba",
    "url": "/v1/configuration/scheme/configuration.logging.fce1b9ba"
  },
  {
    "name": "configuration.network.0edde642",
    "url": "/v1/configuration/scheme/configuration.network.0edde642"
  },
  {
    "name": "configuration.service.1f00d993",
    "url": "/v1/configuration/scheme/configuration.service.1f00d993"
  },
  {
    "name": "configuration.system.ef2e081a",
    "url": "/v1/configuration/scheme/configuration.system.ef2e081a"
  },
  {
    "name": "configuration.zoneinfo.e8437e00",
    "url": "/v1/configuration/scheme/configuration.zoneinfo.e8437e00"
  }
],
"status": 0
```

}

4.2 GET-Request (Endpunkt: "configuration")

GET-Request:

curl -k -b *session_cookie* -X GET https://192.168.1.1:443/api/v1/configuration

Antwort:


```
{
  "content": {
    "fileinfo": {
      "devtype": "0001010111020000",
      "firmware": "1.8.0"
    },
    "firewall": {
      "forward": {
        "ftp_allow_field": "ON",
        "log_all_matches": "ON",
        "log_policy": "ON",
        "sanity_check": "ON",
        "stealth_allow_dhcp": "ON",
        "tables": [
          {
            "in_netzone": "NETZONE1",
            "out_netzone": "NETZONE2",
            "rules": [
              {
                "comment": "",
                "dst_network": "192.168.1.20",
                "dst_port": "ALL",
                "id": 0,
                "log": "OFF",
                "protocol": "ALL",
                "src_network": "0.0.0.0/0",
                "verdict": "REJECT"
              },
              {
                "comment": "Office",
                "dst_network": "0.0.0.0/0",
                "dst_port": "ALL",
                "id": 1,
                "log": "ON",
                "protocol": "ALL",
                "src_network": "192.168.2.0/24",
                "verdict": "ACCEPT"
              },
              {
```

```
        "comment": "Production",
        "dst_network": "192.168.1.0/24",
        "dst_port": "ALL",
        "id": 2,
        "log": "ON",
        "protocol": "ALL",
        "src_network": "10.10.0.0/24",
        "verdict": "ACCEPT"
       }
     ]
    },
    {
     "in_netzone": "NETZONE2",
     "out_netzone": "NETZONE1",
     "rules": [
      {
       "comment": "",
       "dst_network": "0.0.0.0/0",
       "dst_port": "ALL",
       "id": 0,
       "log": "OFF",
       "protocol": "ALL",
       "src_network": "0.0.0.0/0",
       "verdict": "ACCEPT"
      }
     ]
    }
  ],
  "testmode": "ON"
},
"input": {
  "log_all_matches": "OFF",
  "log_policy": "OFF",
  "rules": [
    {
     "id": 1,
     "log": "OFF",
     "service": "HTTPS",
     "source": "NETZONE1",
     "verdict": "ACCEPT"
    }
  ]
},
"port_forward": {
  "rules": [
    {
```

```
        "comment": "",
        "dst_ip": "192.168.5.99",
        "dst_port": 162,
        "inc_port": 1515,
        "protocol": "TCP",
        "src_interface": "NETZONE1"
       }
      ]
     }
    },
    "logging": {
     "remote": {
      "address": "192.168.1.254",
      "ca": "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAlc5enlYQSFe-
KohrV0cjaOOmnC1NgnSCENMp0Yt16iKtUuYSl\nLl3xxrBmmeaYcRvWpuy3WDUYrHPMglyWdmpF
XhxxK2oO3g1eqsNKnvYQAXUQeIdS\nbbMZejfwsgrsFo0gK3dU9AXZe20FCGdfnmzhfrmVNlIZAMJ
ZhwSz2RvbsQss2gPF\nHddJC6nHzsmrEnoEQN+Z0173N9OhUQKG5WSZOPsOKDflHLBvFxsmm
6oisTZM4g+w\n9eXG4EhWVfkxJmFUMWXa+nFm37Px1eTDFEW5hpJC1/SPUPEO51/nhrAtxre/FR
Rg\nAuh26x/D8+t/cAxtLpB2eht21Cfo/l9F7kwdywIDAQABAoIBAGeSsgpo2IMbu2bO\nhOyxIGde7D
ZBZDfepmlVXFiKZlCdnEtTnU6oqPPFPHrFWrpBFAx+91hOBYwd19M8\n4D5oxSMHKRtqDXNq7Pv
FYA89ct1/EW8zqELeJAxDJvAB6y7ATfCfZaX9cVsLigJA\nbnS7NMCIEOjopA7JUFqwXqQJxb/GOm
DrENr9eTC4fp8elCgDF+gyBY6bcc19L4ab\nFDF5fcAb+mRFG4GNE1NIToBi5R5bZchjwt1wp174HA
4XyY4cBS+9COMON74MFM6t\nWvnxACzh0UCB7PvrONgSj0yZ9UfZ3OvVYXURxdxtKN8G3LYYR
PSEFumjFY/sTWFA\nW7+xHwkCgYEAxkFBu+RozZ1m39EMNjYSrs2YlRJLDKwxv3Fr0erFw5fM78
SZ9wAo\nig5EzqprD+qAitnee4rAvDZajdeYnH/gREco6ca6bCx37ksMewCDtMo6SlWSRieY\nuEHKz
gGa8/DWp04FXgpYwhkRwye32cJucDUtPBxlLQi66nSYBJ9RAW8CgYEAwXCP\n/bLG6wleRal+f61
T54lhu8qr1R2vvcWnCrH85EyB64Q8YBJDBKSzmSSuKF5U9swN\nXsqLhQHx7KPkouwoZcQFcidL
ur+Bww/kXldujAzTX7OsEegsSEcQXafyVrxI4Ela\nhCV7YOtTiiIF6iM3/cWigmuIFp+8fdGlm/cxw2UCg
YBcaEBOZslexXYU7qiFgDC3\nH4dAKvmmP4C0nhZGcuqZH2FbhMTK91zt9Han6ZEbiw89KQ3lga
gSUjdlE8/DamtL\nB+wPAx0TnKqN/JclofjBxNzklvwmDQDHKYtw+BiUiXZT5y7jRWlXlz3LO/Ea4+B8\
nFp0t/ol+Omp9K7lLtkKYqwKBgBjronFBpeTDuTRqSJS0RLnwdfnWe1qiT3C4VPPI\nyFa1ElvB5nFO
CPpBKa4SDqm+tV1yHkrW9zB0drFQz/S5Td8GaNky/MubPmFd28LX\nqrM6N8T9ha5s5b+OACrAp
zTLXuweJx4dlg7zYjjLZmlqjh0QaAY7SjX38DWZW6eD\nKhMNAoGBAKD7QKKk7UoVTbocOlTdxak
5DUTmO5NPbnoHo3aj5rq57v1STutHNi2w\nZiYHgDGvIfIyHzwU2MEIXV0S3ZEVI76kaffZn7Nmyhc
6ByibbbqRmyDqzTqnwzSR\ntLUEox056XsJRfKrBNhj0e9utJ1wLrPmAF7EqqCT1+2IXmGbTFU3\n--
---END RSA PRIVATE KEY-----\n-----BEGIN CERTIFICATE-----\nMIIDhTCCAm2gAwIBAgIBFzANBg-
kqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJERTEN\nMAsGA1UECBMEdGVzdDENMAsGA1U
EBxMEdGVzdDENMAsGA1UEChMEdGVzdDENMAsG\nA1UECxMEdGVzdDEVMBMGA1UEAxM
Mc2VydmVyLmlwLmRlMRswGQYJKoZIhvcNAQkB\nFgx0ZXN0QHRlc3QuZGUwHhcNMjAxMTAyM
TAyNDAwWhcNMjExMTAyMTAyNDAwWjB9\nMQswCQYDVQQGEwJERTENMAsGA1UECBMEd
GVzdDENMAsGA1UEBxMEdGVzdDENMAsG\nA1UEChMEdGVzdDENMAsGA1UECxMEdGVzdD
EVMBMGA1UEAxMMc2VydmVyLmlwLmRl\nMRswGQYJKoZIhvcNAQkBFgx0ZXN0QHRlc3QuZG
UwggEiMA0GCSqGSIb3DQEBAQUA\nA4IBDwAwggEKAoIBAQCVzl6eVhBIV4qiGtXRyNo46acLU2
CdIIQ0ynRi3Xqlq1S5\nhIgsjfHGsGaZ5phxG9am7LdYNRisc8yAjJZ2akVeHHErag7eDV6qw0qe9hA
BdRB4\nh1Jtsxl6N/CyCuwWjSArd1T0Bdl7bQUlZ1+ebOF+uZU2UhkAwlmHBLPZG9uxCyza\nA8Ud
10kLqcfOyasSegRA35nTXvc306FRAoblZJk4+w4oN8gcsG8XGyabqiKxNkzi\nD7D15cbgSFZV+TE
mYVQxZdr6cWbfs/HV5MMURbmGkkLX9I9Q8Q7nX+eGsC3Gt78V\nFGAC6HbrH8Pz639wDG0ukH
Z6G3bUJ+j8j0XuTB3LAgMBAAGjEDAOMAwGA1UdEwQF\nMAMBAf8wDQYJKoZIhvcNAQELBQA
DggEBACYKsvmIu0Yqb+YBrXGbpCm36S0dfgms\n74KbIqYTKRrx2aMQc7HAhyJgCbnZPrZ/reDHb
sMjAvhMc+uXmuDbsamlvP90G80E\nj/2eCKafcPbvnqI1mU4eV7VcjDlkqN2x3NTAUcRHTWssFolG
g5DYW0vN1KjKjjly\nHEaFW71o6iQwxWWrC5gJKP+t6HZ8sfJKvGT2jHIOuLwqI3WUsas5DTh5pyu
bGxQS\nb6ngF3YV/t/PuC43i3UkYcGtczrVLrA3WJB1Eyncu6kMQKJp87+bCUlY2ajn1twc\nkx1HCr9
vXeTBolubJgsPfeDEYEihsBHbrlhRRcNBO4EZfY4LMebN820=\n-----END CERTIFICATE-----\n",
      "port": 514,
      "protocol": "TLS",
```

```
    "status": "ON"
   }
  },
  "network": {
   "mode": "ROUTER",
   "nat": {
    "1_1_nat": [
     {
      "comment": "",
      "id": 0,
      "real_network": "192.168.180.0/24",
      "virt_network": "192.168.5.0/24"
     }
    ],
    "masquerading": [
     {
      "from_ip": "0.0.0.0/0",
      "id": 0,
      "outgoing_on_if": "NETZONE1"
     }
    ]
   },
   "netzone1": {
    "address": "192.168.178.57",
    "mode": "DHCP",
    "netmask": 24
   },
   "netzone2": {
    "address": "192.168.1.1",
    "netmask": 24
   },
   "routing": {
    "gateway": "192.168.178.1",
    "routes": [
     {
      "comment": "Route to Machine Net 2",
      "gateway": "192.168.1.1",
      "network": "192.168.5.0/24"
     }
    ]
   },
   "stealth": {
    "management_address": "192.168.178.57",
    "management_gateway": "192.168.178.1",
    "management_netmask": 24
   }
```

```
},
"service": {
 "dhcp_server": {
  "dns": "192.168.1.1",
  "gateway": "192.168.1.1",
  "lease_time": "12h",
  "netmask": 24,
  "range_high": "192.168.1.254",
  "range_low": "192.168.1.2",
  "status": "ON",
  "wins_server": ""
 },
 "dnscache": {
  "allowed_requests": [
   "NETZONE2"
  ],
  "dns_servers": "USER_DEFINED",
  "log": "OFF",
  "user_defined": []
 },
 "ntp": {
  "allow_client_requests": [
   "NETZONE2"
  ],
  "server": [
   {
    "address": "0.pool.ntp.org",
    "comment": "",
    "port": 123
   },
   {
    "address": "1.pool.ntp.org",
    "comment": "",
    "port": 123
   },
   {
    "address": "2.pool.ntp.org",
    "comment": "",
    "port": 123
   },
   {
    "address": "3.pool.ntp.org",
    "comment": "",
    "port": 123
   }
  ],
```

```
      "status": "ON"
    },
    "snmp": {
      "allow_requests_from": [
        "NETZONE2"
      ],
      "ro_community_string": "public",
      "status_v2c": "ON",
      "status_v3": "ON",
      "user": {
        "username": "snmp-user-mGuardNT"
      }
    },
    "web": {
      "session_timeout": 90,
      "user_blocking_time": 30,
      "user_max_failed_logins": 4
    }
  },
  "system": {
    "hostname": "OldName",
    "store_config_on_sdcard": "OFF",
    "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only.
Any intrusion and its attempt without permission is illegal and strictly prohibited."
  },
  "zoneinfo": "Europe/Berlin"
 },
 "envelope": {
  "identifier": {
    "contentID": "66e8539e",
    "functionalID": "59d3ff2b"
  },
  "version": 1
 },
 "error": [],
 "schemes": [
  {
    "name": "common.4710ab60",
    "url": "/v1/configuration/scheme/common.4710ab60"
  },
  {
    "name": "common.types.f0bf23da",
    "url": "/v1/configuration/scheme/common.types.f0bf23da"
  },
  {
    "name": "configuration.fileinfo.b3afd1b0",
```

```
    "url": "/v1/configuration/scheme/configuration.fileinfo.b3afd1b0"
   },
   {
    "name": "configuration.firewall.62d07c99",
    "url": "/v1/configuration/scheme/configuration.firewall.62d07c99"
   },
   {
    "name": "configuration.logging.fce1b9ba",
    "url": "/v1/configuration/scheme/configuration.logging.fce1b9ba"
   },
   {
    "name": "configuration.network.0edde642",
    "url": "/v1/configuration/scheme/configuration.network.0edde642"
   },
   {
    "name": "configuration.service.1f00d993",
    "url": "/v1/configuration/scheme/configuration.service.1f00d993"
   },
   {
    "name": "configuration.system.ef2e081a",
    "url": "/v1/configuration/scheme/configuration.system.ef2e081a"
   },
   {
    "name": "configuration.zoneinfo.e8437e00",
    "url": "/v1/configuration/scheme/configuration.zoneinfo.e8437e00"
   }
  ],
  "status": 0
}
```

4.3 POST-Request (Endpunkt "configuration")

(Für die Antwort auf den POST-Request; siehe unten „**Antwort:**“.)

POST-Request:

curl -k **-b** *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/configuration -d '


```
{
  "content": {
    "fileinfo": {
      "devtype": "0001010111020000",
      "firmware": "1.8.0"
    },
    "firewall": {
      "forward": {
        "ftp_allow_field": "ON",
        "log_all_matches": "ON",
        "log_policy": "ON",
        "sanity_check": "ON",
        "stealth_allow_dhcp": "ON",
        "tables": [
          {
            "in_netzone": "NETZONE1",
            "out_netzone": "NETZONE2",
            "rules": [
              {
                "comment": "",
                "dst_network": "192.168.1.20",
                "dst_port": "ALL",
                "id": 0,
                "log": "OFF",
                "protocol": "ALL",
                "src_network": "0.0.0.0/0",
                "verdict": "REJECT"
              },
              {
                "comment": "Office",
                "dst_network": "0.0.0.0/0",
                "dst_port": "ALL",
                "id": 1,
                "log": "ON",
                "protocol": "ALL",
                "src_network": "192.168.2.0/24",
```

```
        "verdict": "ACCEPT"
       },
       {
        "comment": "Production",
        "dst_network": "192.168.1.0/24",
        "dst_port": "ALL",
        "id": 2,
        "log": "ON",
        "protocol": "ALL",
        "src_network": "10.10.0.0/24",
        "verdict": "ACCEPT"
       }
      ]
     },
     {
      "in_netzone": "NETZONE2",
      "out_netzone": "NETZONE1",
      "rules": [
       {
        "comment": "",
        "dst_network": "0.0.0.0/0",
        "dst_port": "ALL",
        "id": 0,
        "log": "OFF",
        "protocol": "ALL",
        "src_network": "0.0.0.0/0",
        "verdict": "ACCEPT"
       }
      ]
     }
    ],
    "testmode": "ON"
   },
   "input": {
    "log_all_matches": "OFF",
    "log_policy": "OFF",
    "rules": [
     {
      "id": 1,
      "log": "OFF",
      "service": "HTTPS",
      "source": "NETZONE1",
      "verdict": "ACCEPT"
```

```
      }
     ]
    },
    "port_forward": {
     "rules": [
      {
       "comment": "",
       "dst_ip": "192.168.5.99",
       "dst_port": 162,
       "inc_port": 1515,
       "protocol": "TCP",
       "src_interface": "NETZONE1"
      }
     ]
    }
   },
   "logging": {
    "remote": {
     "address": "192.168.1.254",
     "ca": "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAlc5enlYQSFe-
KohrV0cjaOOmnC1NgnSCENMp0Yt16iKtUuYSl\nLl3xxrBmmeaYcRvWpuy3WDUYrHPMglyWdmpF
XhxxK2oO3g1eqsNKnvYQAXUQeIdS\nbbMZejfwsgrsFo0gK3dU9AXZe20FCGdfnmzhfrmVNllZAMJ
ZhwSz2RvbsQss2gPF\nHddJC6nHzsmrEnoEQN+Z0173N9OhUQKG5WSZOPsOKDfIHLBvFxsmm
6oisTZM4g+w\n9eXG4EhWVfkxJmFUMWXa+nFm37Px1eTDFEW5hpJC1/SPUPEO51/nhrAtxre/FR
Rg\nAuh26x/D8+t/cAxtLpB2eht21Cfo/l9F7kwdywIDAQABAoIBAGeSsgpo2IMbu2bO\nhOyxIGde7D
ZBZDfepmlVXFiKZlCdnEtTnU6oqPPFPHrFWrpBFAx+91hOBYwd19M8\n4D5oxSMHKRtqDXNq7Pv
FYA89ct1/EW8zqELeJAxDJvAB6y7ATfCfZaX9cVsLigJA\nbnS7NMCIEOjopA7JUFqwXqQJxb/GOm
DrENr9eTC4fp8elCgDF+gyBY6bcc19L4ab\nFDF5fcAb+mRFG4GNE1NlToBi5R5bZchjwt1wp174HA
4XyY4cBS+9COMON74MFM6t\nWvnxACzh0UCB7PvrONgSj0yZ9UfZ3OvVYXURxdxtKN8G3LYYR
PSEFumjFY/sTWFA\nW7+xHwkCgYEAxkFBu+RozZ1m39EMNjYSrs2YlRJLDKwxv3Fr0erFw5fM78
SZ9wAo\nig5EzqprD+qAitnee4rAvDZajdeYnH/gREco6ca6bCx37ksMewCDtMo6SlWSRieY\nuEHKz
gGa8/DWp04FXgpYwhkRwye32cJucDUtPBxlLQi66nSYBJ9RAW8CgYEAwXCP\n/bLG6wleRal+f61
T54lhu8qr1R2vvcWnCrH85EyB64Q8YBJDBKSzmSSuKF5U9swN\nXsqLhQHx7KPkouwoZcQFcidL
ur+Bww/kXldujAzTX7OsEegsSEcQXafyVrxI4Ela\nhCV7YOtTiiIF6iM3/cWigmuIFp+8fdGlm/cxw2UCg
YBcaEBOZslexXYU7qiFgDC3\nH4dAKvmmP4C0nhZGcuqZH2FbhMTK91zt9Han6ZEbiw89KQ3lga
gSUjdlE8/DamtL\nB+wPAx0TnKqN/JclofjBxNzklvwmDQDHKYtw+BiUiXZT5y7jRWlXlz3LO/Ea4+B8\
nFp0t/ol+Omp9K7lLtkKYqwKBgBjronFBpeTDuTRqSJS0RLnwdfnWe1qiT3C4VPPl\nyFa1ElvB5nFO
CPpBKa4SDqm+tV1yHkrW9zB0drFQz/S5Td8GaNky/MubPmFd28LX\nqrM6N8T9ha5s5b+OACrAp
zTLXuweJx4dIg7zYjjLZmlqjh0QaAY7SjX38DWZW6eD\nKhMNAoGBAKD7QKKk7UoVTbocOlTdxak
5DUTmO5NPbnoHo3aj5rq57v1STutHNi2w\nZiYHgDGvIfIyHzwU2MEIXV0S3ZEVI76kaffZn7Nmyhc
6ByibbbqRmyDqzTqnwzSR\ntLUEox056XsJRfKrBNhj0e9utJ1wLrPmAF7EqqCT1+2IXmGbTFU3\n-
---END RSA PRIVATE KEY-----\n-----BEGIN CERTIFICATE-----\nMIIDhTCCAm2gAwIBAgIBFzANBg-
kqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJERTEN\nMAsGA1UECBMEdGVzdDENMAsGA1U
EBxMEdGVzdDENMAsGA1UEChMEdGVzdDENMAsG\nA1UECxMEdGVzdDEVMBMGA1UEAxM
Mc2VydmVyLmlwLmRlMRswGQYJKoZIhvcNAQkB\nFgx0ZXN0QHRlc3QuZGUwHhcNMjAxMTAyM
TAyNDAwWhcNMjExMTAyMTAyNDAwWjB9\nMQswCQYDVQQGEwJERTENMAsGA1UECBMEd
GVzdDENMAsGA1UEBxMEdGVzdDENMAsG\nA1UEChMEdGVzdDENMAsGA1UECxMEdGVzdD
EVMBMGA1UEAxMMc2VydmVyLmlwLmRl\nMRswGQYJKoZIhvcNAQkBFgx0ZXN0QHRlc3QuZG
UwggEiMA0GCSqGSIb3DQEBAQUA\nA4IBDwAwggEKAoIBAQCVzl6eVhBIV4qiGtXRyNo46acLU2
CdIIQ0ynRi3XqIq1S5\nhIgsjfHGsGaZ5phxG9am7LdYNRisc8yAjJZ2akVeHHErag7eDV6qw0qe9hA
BdRB4\nh1JtsxI6N/CyCuwWjSArd1T0Bdl7bQUlZ1+ebOF+uZU2UhkAwlmHBLPZG9uxCyza\nA8Ud
10kLqcfOyasSegRA35nTXvc306FRAoblZJk4+w4oN8gcsG8XGyabqiKxNkzi\nD7D15cbgSFZV+TE
```

mYVQxZdr6cWbfs/HV5MMURbmGkkLX9I9Q8Q7nX+eGsC3Gt78V\nFGAC6HbrH8Pz639wDG0ukH
Z6G3bUJ+j8j0XuTB3LAgMBAAGjEDAOMAwGA1UdEwQF\nMAMBAf8wDQYJKoZIhvcNAQELBQA
DggEBACYKsvmIu0Yqb+YBrXGbpCm36S0dfgms\n74KbIqYTKRrx2aMQc7HAhyJgCbnZPrZ/reDHb
sMjAvhMc+uXmuDbsamlvP90G80E\nj/2eCKafcPbvnqI1mU4eV7VcjDlkqN2x3NTAUcRHTWssFolG
g5DYW0vN1KjKjjly\nHEaFW71o6iQwxWWrC5gJKP+t6HZ8sfJKvGT2jHIOuLwqI3WUsas5DTh5pyu
bGxQS\nb6ngF3YV/t/PuC43i3UkYcGtczrVLrA3WJB1Eyncu6kMQKJp87+bCUlY2ajn1twc\nkx1HCr9
vXeTBolubJgsPfeDEYEihsBHbrlhRRcNBO4EZfY4LMebN820=\n-----END CERTIFICATE-----\n",


```
      "port": 514,
      "protocol": "TLS",
      "status": "ON"
    }
  },
  "network": {
    "mode": "ROUTER",
    "nat": {
      "1_1_nat": [
        {
          "comment": "",
          "id": 0,
          "real_network": "192.168.180.0/24",
          "virt_network": "192.168.5.0/24"
        }
      ],
      "masquerading": [
        {
          "from_ip": "0.0.0.0/0",
          "id": 0,
          "outgoing_on_if": "NETZONE1"
        }
      ]
    },
    "netzone1": {
      "address": "192.168.178.57",
      "mode": "DHCP",
      "netmask": 24
    },
    "netzone2": {
      "address": "192.168.1.1",
      "netmask": 24
    },
    "routing": {
      "gateway": "192.168.178.1",
      "routes": [
        {
          "comment": "Route to Machine Net 2",
```

```
        "gateway": "192.168.1.1",
        "network": "192.168.5.0/24"
       }
      ]
     },
     "stealth": {
      "management_address": "192.168.178.57",
      "management_gateway": "192.168.178.1",
      "management_netmask": 24
     }
    },
    "service": {
     "dhcp_server": {
      "dns": "192.168.1.1",
      "gateway": "192.168.1.1",
      "lease_time": "12h",
      "netmask": 24,
      "range_high": "192.168.1.254",
      "range_low": "192.168.1.2",
      "status": "ON",
      "wins_server": ""
     },
     "dnscache": {
      "allowed_requests": [
       "NETZONE2"
      ],
      "dns_servers": "USER_DEFINED",
      "log": "OFF",
      "user_defined": []
     },
     "ntp": {
      "allow_client_requests": [
       "NETZONE2"
      ],
      "server": [
       {
        "address": "0.pool.ntp.org",
        "comment": "",
        "port": 123
       },
       {
        "address": "1.pool.ntp.org",
        "comment": "",
```

```
        "port": 123
       },
       {
        "address": "2.pool.ntp.org",
        "comment": "",
        "port": 123
       },
       {
        "address": "3.pool.ntp.org",
        "comment": "",
        "port": 123
       }
      ],
      "status": "ON"
     },
     "snmp": {
      "allow_requests_from": [
       "NETZONE2"
      ],
      "ro_community_string": "public",
      "status_v2c": "ON",
      "status_v3": "ON",
      "user": {
       "username": "snmp-user-mGuardNT"
      }
     },
     "web": {
      "session_timeout": 90,
      "user_blocking_time": 30,
      "user_max_failed_logins": 4
     }
    },
    "system": {
     "hostname": "NewName",
     "store_config_on_sdcard": "OFF",
     "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only.
Any intrusion and its attempt without permission is illegal and strictly prohibited."
    },
    "zoneinfo": "Europe/Berlin"
   },
"envelope":  {"version": 1}}'
```

Antwort:


```
{
  "content": {
    "fileinfo": {
      "devtype": "0001010111020000",
      "firmware": "1.8.0"
    },
    "firewall": {
      "forward": {
        "ftp_allow_field": "ON",
        "log_all_matches": "ON",
        "log_policy": "ON",
        "sanity_check": "ON",
        "stealth_allow_dhcp": "ON",
        "tables": [
          {
            "in_netzone": "NETZONE1",
            "out_netzone": "NETZONE2",
            "rules": [
              {
                "comment": "",
                "dst_network": "192.168.1.20",
                "dst_port": "ALL",
                "id": 0,
                "log": "OFF",
                "protocol": "ALL",
                "src_network": "0.0.0.0/0",
                "verdict": "REJECT"
              },
              {
                "comment": "Office",
                "dst_network": "0.0.0.0/0",
                "dst_port": "ALL",
                "id": 1,
                "log": "ON",
                "protocol": "ALL",
                "src_network": "192.168.2.0/24",
                "verdict": "ACCEPT"
              },
              {
                "comment": "Production",
                "dst_network": "192.168.1.0/24",
                "dst_port": "ALL",
```

```
        "id": 2,
        "log": "ON",
        "protocol": "ALL",
        "src_network": "10.10.0.0/24",
        "verdict": "ACCEPT"
       }
      ]
     },
     {
      "in_netzone": "NETZONE2",
      "out_netzone": "NETZONE1",
      "rules": [
       {
        "comment": "",
        "dst_network": "0.0.0.0/0",
        "dst_port": "ALL",
        "id": 0,
        "log": "OFF",
        "protocol": "ALL",
        "src_network": "0.0.0.0/0",
        "verdict": "ACCEPT"
       }
      ]
     }
    ],
    "testmode": "ON"
   },
   "input": {
    "log_all_matches": "OFF",
    "log_policy": "OFF",
    "rules": [
     {
      "id": 1,
      "log": "OFF",
      "service": "HTTPS",
      "source": "NETZONE1",
      "verdict": "ACCEPT"
     }
    ]
   },
   "port_forward": {
    "rules": [
     {
```

```
        "comment": "",
        "dst_ip": "192.168.5.99",
        "dst_port": 162,
        "inc_port": 1515,
        "protocol": "TCP",
        "src_interface": "NETZONE1"
       }
      ]
     }
    },
    "logging": {
     "remote": {
      "address": "192.168.1.254",
      "ca": "-----BEGIN RSA PRIVATE KEY-----\nMIIEowIBAAKCAQEAlc5enlYQSFe-
KohrV0cjaOOmnC1NgnSCENMp0Yt16iKtUuYSl\nLl3xxrBmmeaYcRvWpuy3WDUYrHPMgIyWdmpF
XhxxK2oO3g1eqsNKnvYQAXUQeIdS\nbbMZejfwsgrsFo0gK3dU9AXZe20FCGdfnmzhfrmVNIlZAMJ
ZhwSz2RvbsQss2gPF\nHddJC6nHzsmrEnoEQN+Z0173N9OhUQKG5WSZOPsOKDfIHLBvFxsmm
6oisTZM4g+w\n9eXG4EhWVfkxJmFUMWXa+nFm37Px1eTDFEW5hpJC1/SPUPEO51/nhrAtxre/FR
Rg\nAuh26x/D8+t/cAxtLpB2eht21Cfo/l9F7kwdywlDAQABAoIBAGeSsgpo2lMbu2bO\nhOyxIGde7D
ZBZDfepmlVXFiKZlCdnEtTnU6oqPPFPHrFWrpBFAx+91hOBYwd19M8\n4D5oxSMHKRtqDXNq7Pv
FYA89ct1/EW8zqELeJAxDJvAB6y7ATfCfZaX9cVsLigJA\nbnS7NMClEOjopA7JUFqwXqQJxb/GOm
DrENr9eTC4fp8elCgDF+gyBY6bcc19L4ab\nFDF5fcAb+mRFG4GNE1NlToBi5R5bZchjwt1wp174HA
4XyY4cBS+9COMON74MFM6t\nWvnxACzh0UCB7PvrONgSj0yZ9UfZ3OvVYXURxdxtKN8G3LYYR
PSEFumjFY/sTWFA\nW7+xHwkCgYEAxkFBu+RozZ1m39EMNjYSrs2YlRJLDKwxv3Fr0erFw5fM78
SZ9wAo\nig5EzqprD+qAitnee4rAvDZajdeYnH/gREco6ca6bCx37ksMewCDtMo6SlWSRieY\nuEHKz
gGa8/DWp04FXgpYwhkRwye32cJucDUtPBxlLQi66nSYBJ9RAW8CgYEAwXCP\n/bLG6wleRal+f61
T54lhu8qr1R2vvcWnCrH85EyB64Q8YBJDBKSzmSSuKF5U9swN\nXsqLhQHx7KPkouwoZcQFcidL
ur+Bww/kXldujAzTX7OsEegsSEcQXafyVrxI4Ela\nhCV7YOtTiiIF6iM3/cWigmuIFp+8fdGlm/cxw2UCg
YBcaEBOZslexXYU7qiFgDC3\nH4dAKvmmP4C0nhZGcuqZH2FbhMTK91zt9Han6ZEbiw89KQ3lga
gSUjdlE8/DamtL\nB+wPAx0TnKqN/JclofjBxNzklvwmDQDHKYtw+BiUiXZT5y7jRWlXlz3LO/Ea4+B8\
nFp0t/ol+Omp9K7lLtkKYqwKBgBjronFBpeTDuTRqSJS0RLnwdfnWe1qiT3C4VPPl\nyFa1ElvB5nFO
CPpBKa4SDqm+tV1yHkrW9zB0drFQz/S5Td8GaNky/MubPmFd28LX\nqrM6N8T9ha5s5b+OACrAp
zTLXuweJx4dIg7zYjjLZmlqjh0QaAY7SjX38DWZW6eD\nKhMNAoGBAKD7QKKk7UoVTbocOlTdxak
5DUTmO5NPbnoHo3aj5rq57v1STutHNi2w\nZiYHgDGvIfIyHzwU2MEIXV0S3ZEVI76kaffZn7Nmyhc
6ByibbbqRmyDqzTqnwzSR\ntLUEox056XsJRfKrBNhj0e9utJ1wLrPmAF7EqqCT1+2IXmGbTFU3\n-
----END RSA PRIVATE KEY-----\n-----BEGIN CERTIFICATE-----\nMIIDhTCCAm2gAwIBAgIBFzANBg-
kqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJERTEN\nMAsGA1UECBMEdGVzdDENMAsGA1U
EBxMEdGVzdDENMAsGA1UEChMEdGVzdDENMAsG\nA1UECxMEdGVzdDEVMBMGA1UEAxM
Mc2VydmVyLmlwLmRlMRswGQYJKoZIhvcNAQkB\nFgx0ZXN0QHRlc3QuZGUwHhcNMjAxMTAyM
TAyNDAwWhcNMjExMTAyMTAyNDAwWjB9\nMQswCQYDVQQGEwJERTENMAsGA1UECBMEd
GVzdDENMAsGA1UEBxMEdGVzdDENMAsG\nA1UEChMEdGVzdDENMAsGA1UECxMEdGVzdD
EVMBMGA1UEAxMMc2VydmVyLmlwLmRl\nMRswGQYJKoZIhvcNAQkBFgx0ZXN0QHRlc3QuZG
UwggEiMA0GCSqGSIb3DQEBAQUA\nA4IBDwAwggEKAoIBAQCVzl6eVhBIV4qiGtXRyNo46acLU2
CdIIQ0ynRi3Xqlq1S5\nhIgsjfHGsGaZ5phxG9am7LdYNRisc8yAjJZ2akVeHHErag7eDV6qw0qe9hA
BdRB4\nh1Jtsxl6N/CyCuwWjSArd1T0Bdl7bQUlZ1+ebOF+uZU2UhkAwlmHBLPZG9uxCyza\nA8Ud
10kLqcfOyasSegRA35nTXvc306FRAoblZJk4+w4oN8gcsG8XGyabqiKxNkzi\nD7D15cbgSFZV+TE
mYVQxZdr6cWbfs/HV5MMURbmGkkLX9l9Q8Q7nX+eGsC3Gt78V\nFGAC6HbrH8Pz639wDG0ukH
Z6G3bUJ+j8j0XuTB3LAgMBAAGjEDAOMAwGA1UdEwQF\nMAMBAf8wDQYJKoZIhvcNAQELBQA
DggEBACYKsvmlu0Yqb+YBrXGbpCm36S0dfgms\n74KblqYTKRrx2aMQc7HAhyJgCbnZPrZ/reDHb
sMjAvhMc+uXmuDbsamlvP90G80E\nj/2eCKafcPbvnqI1mU4eV7VcjDlkqN2x3NTAUcRHTWssFolG
g5DYW0vN1KjKjjly\nHEaFW71o6iQwxWWrC5gJKP+t6HZ8sfJKvGT2jHIOuLwql3WUsas5DTh5pyu
bGxQS\nb6ngF3YV/t/PuC43i3UkYcGtczrVLrA3WJB1Eyncu6kMQKJp87+bCUlY2ajn1twc\nkx1HCr9
vXeTBolubJgsPfeDEYEihsBHbrlhRRcNBO4EZfY4LMebN820=\n-----END CERTIFICATE-----\n",
      "port": 514,
```

```
    "protocol": "TLS",
    "status": "ON"
   }
  },
  "network": {
   "mode": "ROUTER",
   "nat": {
    "1_1_nat": [
     {
      "comment": "",
      "id": 0,
      "real_network": "192.168.180.0/24",
      "virt_network": "192.168.5.0/24"
     }
    ],
    "masquerading": [
     {
      "from_ip": "0.0.0.0/0",
      "id": 0,
      "outgoing_on_if": "NETZONE1"
     }
    ]
   },
   "netzone1": {
    "address": "192.168.178.57",
    "mode": "DHCP",
    "netmask": 24
   },
   "netzone2": {
    "address": "192.168.1.1",
    "netmask": 24
   },
   "routing": {
    "gateway": "192.168.178.1",
    "routes": [
     {
      "comment": "Route to Machine Net 2",
      "gateway": "192.168.1.1",
      "network": "192.168.5.0/24"
     }
    ]
   },
   "stealth": {
```

```
    "management_address": "192.168.178.57",
    "management_gateway": "192.168.178.1",
    "management_netmask": 24
   }
  },
  "service": {
   "dhcp_server": {
    "dns": "192.168.1.1",
    "gateway": "192.168.1.1",
    "lease_time": "12h",
    "netmask": 24,
    "range_high": "192.168.1.254",
    "range_low": "192.168.1.2",
    "status": "ON",
    "wins_server": ""
   },
   "dnscache": {
    "allowed_requests": [
     "NETZONE2"
    ],
    "dns_servers": "USER_DEFINED",
    "log": "OFF",
    "user_defined": []
   },
   "ntp": {
    "allow_client_requests": [
     "NETZONE2"
    ],
    "server": [
     {
      "address": "0.pool.ntp.org",
      "comment": "",
      "port": 123
     },
     {
      "address": "1.pool.ntp.org",
      "comment": "",
      "port": 123
     },
     {
      "address": "2.pool.ntp.org",
      "comment": "",
      "port": 123
```

```
        },
        {
          "address": "3.pool.ntp.org",
          "comment": "",
          "port": 123
        }
      ],
      "status": "ON"
    },
    "snmp": {
      "allow_requests_from": [
        "NETZONE2"
      ],
      "ro_community_string": "public",
      "status_v2c": "ON",
      "status_v3": "ON",
      "user": {
        "username": "snmp-user-mGuardNT"
      }
    },
    "web": {
      "session_timeout": 90,
      "user_blocking_time": 30,
      "user_max_failed_logins": 4
    }
  },
  "system": {
    "hostname": "NewName",
    "store_config_on_sdcard": "OFF",
    "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only.
Any intrusion and its attempt without permission is illegal and strictly prohibited."
  },
  "zoneinfo": "Europe/Berlin"
 },
 "envelope": {
  "identifier": {
    "contentID": "d311f50a",
    "functionalID": "ec2a59bf"
  },
  "version": 1
 },
 "error": [],
 "schemes": [
```

```
    {
      "name": "common.4710ab60",
      "url": "/v1/configuration/scheme/common.4710ab60"
    },
    {
      "name": "common.types.f0bf23da",
      "url": "/v1/configuration/scheme/common.types.f0bf23da"
    },
    {
      "name": "configuration.fileinfo.b3afd1b0",
      "url": "/v1/configuration/scheme/configuration.fileinfo.b3afd1b0"
    },
    {
      "name": "configuration.firewall.62d07c99",
      "url": "/v1/configuration/scheme/configuration.firewall.62d07c99"
    },
    {
      "name": "configuration.logging.fce1b9ba",
      "url": "/v1/configuration/scheme/configuration.logging.fce1b9ba"
    },
    {
      "name": "configuration.network.0edde642",
      "url": "/v1/configuration/scheme/configuration.network.0edde642"
    },
    {
      "name": "configuration.service.1f00d993",
      "url": "/v1/configuration/scheme/configuration.service.1f00d993"
    },
    {
      "name": "configuration.system.ef2e081a",
      "url": "/v1/configuration/scheme/configuration.system.ef2e081a"
    },
    {
      "name": "configuration.zoneinfo.e8437e00",
      "url": "/v1/configuration/scheme/configuration.zoneinfo.e8437e00"
    }
  ],
  "status": 0
}
```

4.4 POST-Request (Endpunkt "actions/migration")

POST-Request:

curl -k **-b** *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type: application/json" -X POST https://192.168.1.1:443/api/v1/actions/migration -d '


```
{"content": {
   "fileinfo": {
    "devtype": "0001010111020000",
    "firmware": "1.5.1"
   },
   "firewall": {
    "forward": {
     "log_all_matches": "OFF",
     "log_policy": "OFF",

[...]

},"envelope":  {"version": 1}}'
```


Antwort:


```
{
  "content": {
   "fileinfo": {
    "devtype": "0001010111020000",
    "firmware": "1.8.0"
   },
   "firewall": {
    "forward": {
     "ftp_allow_field": "OFF",
     "log_all_matches": "OFF",
     "log_policy": "OFF",
     "sanity_check": "ON",
     "stealth_allow_dhcp": "ON",
     "tables": [
      {
       "in_netzone": "NETZONE2",
       "out_netzone": "NETZONE1",
       "rules": []
      },
      {
       "in_netzone": "NETZONE1",
       "out_netzone": "NETZONE2",
       "rules": []
      }
```

```
      ],
      "testmode": "ON"
    },
    "input": {
      "rules": [
        {
          "id": 0,
          "log": "OFF",
          "service": "HTTPS",
          "source": "NETZONE2",
          "verdict": "ACCEPT"
        },
        {
          "id": 1,
          "log": "OFF",
          "service": "HTTPS",
          "source": "NETZONE1",
          "verdict": "ACCEPT"
        }
      ]
    },
    "port_forward": {
      "rules": []
    }
  },
  "logging": {
    "remote": {
      "address":
"a.123456ddddd7890ddddddddddddddddddddddddd1234567890123456789.AAA1234567890123
456789012345678901234567890123456789012345678901234567890.AAA1234567890123456789012345678
901234567890123456789012345678901234567890.AAA1234567890123456789012345678901234567890123
45678901234567890",
      "port": 513,
      "protocol": "UDP",
      "status": "ON"
    }
  },
  "network": {
    "mode": "ROUTER",
    "nat": {
      "1_1_nat": [],
      "masquerading": [
        {
          "from_ip": "0.0.0.0/0",
```

```
      "id": 0,
      "outgoing_on_if": "NETZONE1"
     }
    ]
   },
   "netzone1": {
    "mode": "DHCP"
   },
   "netzone2": {
    "address": "10.1.1.1",
    "netmask": 24
   },
   "routing": {
    "routes": []
   },
   "stealth": {
    "management_address": "192.168.1.1",
    "management_gateway": "192.168.1.254",
    "management_netmask": 24
   }
  },
  "service": {
   "dhcp_server": {
    "dns": "192.168.1.1",
    "gateway": "192.168.1.1",
    "lease_time": "12h",
    "netmask": 24,
    "range_high": "192.168.1.254",
    "range_low": "192.168.1.2",
    "status": "OFF",
    "wins_server": ""
   },
   "dnscache": {
    "allowed_requests": [],
    "dns_servers": "USER_DEFINED",
    "log": "OFF",
    "user_defined": [
     {
      "comment": "",
      "ip": "212.2.220.212"
     }
    ]
   },
```

```
  "ntp": {
    "allow_client_requests": [
      "NETZONE2",
      "NETZONE1"
    ],
    "server": [
      {
        "address": "0.pool.ntp.org",
        "comment": "",
        "port": 123
      },
      {
        "address": "1.pool.ntp.org",
        "comment": "",
        "port": 123
      },
      {
        "address": "2.pool.ntp.org",
        "comment": "",
        "port": 123
      },
      {
        "address": "1.2.3.4",
        "comment": "",
        "port": 123
      }
    ],
    "status": "OFF"
  },
  "snmp": {
    "allow_requests_from": [
      "NETZONE2"
    ],
    "ro_community_string": "public",
    "status_v2c": "OFF",
    "status_v3": "OFF"
  },
  "web": {
    "session_timeout": 90,
    "user_blocking_time": 30,
    "user_max_failed_logins": 4
  }
},
```

```
    "system": {
      "hostname": "mGuard",
      "store_config_on_sdcard": "OFF",
      "usenotification": "The usage of this mGuard security appliance is reserved to authorized staff only.
Any intrusion and its attempt without permission is illegal and strictly prohibited."
    },
    "zoneinfo": "Europe/Berlin"
  },
  "envelope": {
    "identifier": {
      "contentID": "5cc1731e",
      "functionalID": "d78399a9"
    },
    "version": 1
  },
  "error": [],
  "schemes": [],
  "status": 0
}
```

4.5 GET-Request (Endpunkt: "users")

GET-Request:

curl -k **-b** *session_cookie* -X GET https://192.168.1.1:443/api/v1/users

Antwort:


```
{
  "content": {
    "ldap": {
      "ldap_server": {
        "base_dn": "DC=mguard,DC=management",
        "ca": "-----BEGIN CERTIFICATE-----\nMIIDmzCCAoOgAwIBAgIU-
WYcWnmC15gUbcfq6Zx7c9MgYviEwDQYJKoZIhvcNAQEL\nBQAwXTELMAkGA1UEBhMCQlkxCz
AJBgNVBAgMAkJZMQ4wDAYDVQQHDAVNaW5zazEM\nMAoGA1UECgwDU0FNMQswCQYDVQ
QLDAJRQTEWMBQGA1UEAwwNMTkyLjE2OC4xLjEx\nNTAeFw0yMDEwMjkxMTE0NDBaFw0zM
DEwMjcxMTE0NDBaMF0xCzAJBgNVBAYTAkJZ\nMQswCQYDVQQIDAJCWTEOMAwGA1UEBww
FTWluc2sxDDAKBgNVBAoMA1NBTTELMAkG\nA1UECwwCUUExFjAUBgNVBAMMDTE5Mi4xNjg
uMS4xMTUwggEiMA0GCSqGSIb3DQEB\nAQUAA4IBDwAwggEKAoIBAQCyY2f6XAZoRkv2wIRv8
LQfXs+rkhxLQsy62oQcmMPt\nwVkg3NAgC69t3ESk91zFUZvhE7Of2NJbFQmtfJlUZlJWhYNg4gVR
28X/VrsKgkps\npzqemiKmj4aWWvk9+8IjPpvdng9TP5F4zTDF3W3Xy3v3THr3YixY80LqMHbPNFp
O\n7GnGe7YQMrWt3rZFkSEG3k3q4nTS8znPUS78qE96GAgspxLllcsdVKe6/9K8yYSb\nv5l0L6r8c
Cj+zel3EV9UxatyC1hGbZjcO+QfwNhz/nJb+5HOF6Kpxexl6rsIe/28\njE9LadvXAl+DDiX2gcStGj0Lw
9h7Uuu3hDkQVezyLKzrAgMBAAGjUzBRMB0GA1Ud\nDgQWBBSqPqzTnykG0FHJdijV7WeJLC5B
GzAfBgNVHSMEGDAWgBSqPqzTnykG0FHJ\ndijV7WeJLC5BGzAPBgNVHRMBAf8EBTADAQH/M
A0GCSqGSIb3DQEBCwUAA4IBAQBv\n4vnhipL0JOOoLwNsp6vW9Gzx9nVlkdSmlD3e6zqg5m2HlI
NbCvlf1fxMtKq5m+cR\n1tnb3fNUjp+Au30B/iPQD9LFaX0458XinOxYpyQcKRWDrXLgnMfSixUv96G
NQzoZ\ndjLI3O8IDFU0GsitQNAfepyH94+GDSsP2oKdAPTIUO5jgPKM5deSqeh0qCND8rhW\nYN6
viunYRKz/9y9pDDM6iLkBwZpjAzjj1e17tB06QPkrfwOn5ofYY0vcqRK6LsnF\nBW5/87JeogTAN2iLD
gVIlVuSe9+Q/Wm+okFObilbECoh2L6zqojLwpp8GEqv3NhD\nwLYiT0JjajXDGLAf0t4O\n-----END
CERTIFICATE-----\n",
        "hostname": "192.168.2.100",
        "port": 389,
        "tls": "ON",
        "username": "admin_ldap"
      },
      "status": "ON",
      "user_role_mapping": {
        "admin": "Role_2",
        "audit": "Role_3",
        "ldap_attribute": "Role",
        "super_admin": "Role_1"
      }
    },
    "user_mgmt": {
      "current_user": "admin",
      "users": [
        {
          "block_user": "OFF",
```

```
        "name": "",
        "old_username": "admin",
        "role": "SUPERADMIN",
        "username": "admin"
       },
       {
        "block_user": "OFF",
        "name": "",
        "old_username": "admin_production",
        "role": "ADMIN",
        "username": "admin_production"
       }
      ]
     }
    },
    "envelope": {
     "identifier": {
      "contentID": "4b7a11b1",
      "functionalID": "4b7a11b1"
     },
     "version": 1
    },
    "error": [],
    "schemes": [
     {
      "name": "users.manageusers.e52f65cd",
      "url": "/v1/users/scheme/users.manageusers.e52f65cd"
     }
    ],
    "status": 0
}
```

4.6 POST-Request (Endpunkt "users")

POST-Request:

curl -k -b *session_cookie* -H "X-CSRF-Token: <TOKEN>" -H "Content-Type:application/json" -X POST https://192.168.1.1:443/api/v1/users -d '


```
{
 "content": {
  "ldap": {
   "ldap_server": {
    "base_dn": "DC=mguard,DC=management",
    "ca": "-----BEGIN CERTIFICATE-----\nMIIDmzCCAoOgAwIBAgIU-
WYcWnmC15gUbcfq6Zx7c9MgYviEwDQYJKoZIhvcNAQEL\nBQAwXTELMAkGA1UEBhMCQlkxCz
AJBgNVBAgMAkJZMQ4wDAYDVQQHDAVNaW5zazEM\nMAoGA1UECgwDU0FNMQswCQYDVQ
QLDAJRQTEWMBQGA1UEAwwNMTkyLjE2OC4xLjEx\nNTAeFw0yMDEwMjkxMTE0NDBaFw0zM
DEwMjcxMTE0NDBaMF0xCzAJBgNVBAYTAkJZ\nMQswCQYDVQQIDAJCWTEOMAwGA1UEBww
FTWluc2sxDDAKBgNVBAoMA1NBTTELMAkG\nA1UECwwCUUExFjAUBgNVBAMMDTE5Mi4xNjg
uMS4xMTUwggEiMA0GCSqGSIb3DQEB\nAQUAA4IBDwAwggEKAoIBAQCyY2f6XAZoRkv2wIRv8
LQfXs+rkhxLQsy62oQcmMPt\nwVkg3NAgC69t3ESk91zFUZvhE7Of2NJbFQmtfJlUZlJWhYNg4gVR
28X/VrsKgkps\npzqemiKmj4aWWvk9+8IjPpvdng9TP5F4zTDF3W3Xy3v3THr3YixY80LqMHbPNFp
O\n7GnGe7YQMrWt3rZFkSEG3k3q4nTS8znPUS78qE96GAgspxLllcsdVKe6/9K8yYSb\nv5l0L6r8c
Cj+zel3EV9UxatyC1hGbZjcO+QfwNhz/nJb+5HOF6KpxexI6rsIe/28\njE9LadvXAI+DDiX2gcStGj0Lw
9h7Uuu3hDkQVezyLKzrAgMBAAGjUzBRMB0GA1Ud\nDgQWBBSqPqzTnykG0FHJdijV7WeJLC5B
GzAfBgNVHSMEGDAWgBSqPqzTnykG0FHJ\ndijV7WeJLC5BGzAPBgNVHRMBAf8EBTADAQH/M
A0GCSqGSIb3DQEBCwUAA4IBAQBv\n4vnhipL0JOOoLwNsp6vW9Gzx9nVlkdSmlD3e6zqg5m2HlI
NbCvlf1fxMtKq5m+cR\n1tnb3fNUjp+Au30B/iPQD9LFaX0458XinOxYpyQcKRWDrXLgnMfSixUv96G
NQzoZ\ndjLI3O8IDFU0GsitQNAfepyH94+GDSsP2oKdAPTIUO5jgPKM5deSqeh0qCND8rhW\nYN6
viunYRKz/9y9pDDM6iLkBwZpjAzjj1e17tB06QPkrfwOn5ofYY0vcqRK6LsnF\nBW5/87JeogTAN2iLD
gVIIVuSe9+Q/Wm+okFObilbECoh2L6zqojLwpp8GEqv3NhD\nwLYiT0JjajXDGLAf0t4O\n-----END
CERTIFICATE-----\n",
    "hostname": "192.168.2.100",
    "password": "ldap_server_password",
    "port": 389,
    "tls": "ON",
    "username": "admin_ldap"
   },
   "status": "ON",
   "user_role_mapping": {
    "admin": "Role_2",
    "audit": "Role_3",
    "ldap_attribute": "Role",
    "super_admin": "Role_1"
   }
  },
  "user_mgmt": {
   "current_user": "admin", "old_password": "private",
   "users": [
    {
     "block_user": "OFF",
```

```
        "name": "",
        "old_username": "admin",
        "role": "SUPERADMIN",
        "username": "superadmin"
       },
       {
        "block_user": "OFF",
        "name": "",
        "old_username": "admin_production",
        "role": "ADMIN",
        "username": "admin_production",
        "new_password": "secret_production_password",
        "repeat_password": "secret_production_password"
       },
{
        "block_user": "OFF",
        "name": "",
        "old_username": "",
        "role": "AUDIT",
        "username": "secret_audit_production",
        "new_password": "secret_audit_password",
        "repeat_password": "secret_audit_password"

       }
     ]
   }
 },
 "envelope": {"version": 1}}'
```

5 Anhang

5.1 Verfügbare Zeitzonen

In alphabetischer Reihenfolge:

Africa

Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek

America

America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Ensenada, America/Fort_Nelson, America/Fort_Wayne, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox_IN, America/Kralendijk, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Lower_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Beulah, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Porto_Velho, America/Puerto_Rico,

	America/Punta_Arenas, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio_Branco, America/Rosario, America/Santa_Isabel, America/Santarem, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St_Barthelemy, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife
Antarctica	Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen
Asia	Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Atyrau, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Choibalsan, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Famagusta, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho_Chi_Minh, Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qostanay, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung_Pandang, Asia/Ulaanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yangon, Asia/Yekaterinburg, Asia/Yerevan
Atlantic	Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley
Australia	Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna
Brazil	Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West
CET/CST6CDT	CET, CST6CDT
Canada	Canada/Atlantic, Canada/Central, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon
Chile	Chile/Continental, Chile/EasterIsland
Cuba	Cuba

EET, EST, EST5EDT	EET, EST, EST5EDT
Egypt	Egypt, Eire
Etc	Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu
Europe	Europe/Amsterdam, Europe/Andorra, Europe/Astrakhan, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Kirov, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Saratov, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Ulyanovsk, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich
Factory	Factory
GB	GB, GB-Eire
GMT	GMT, GMT+0, GMT-0, GMT0
Greenwich	Greenwich
HST	HST
Hongkong	Hongkong
Iceland	Iceland
Indian	Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion
Iran	Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT
Pacific	Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap

Poland	Poland
Portugal	Portugal
ROC	ROC
ROK	ROK
Singapore	Singapore
Turkey	Turkey
UCT	UCT
US	US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Samoa
UTC	UTC
Universal	Universal
W-SU	W-SU
WET	WET
Zulu	Zulu

Bitte beachten Sie folgende Hinweise

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:
phoenixcontact.net/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

108898_de_11
Order No. —11

INSPIRING INNOVATIONS