



OctoGate[®]

Benutzerhandbuch

Änderungen von Daten und Angaben ohne vorherige Ankündigung vorbehalten.
Die in den Beispielen verwendeten Namen und Daten sind frei erfunden, soweit nichts anderes angegeben ist. Ohne ausdrückliche schriftliche Erlaubnis der OctoGate IT Security Systems GmbH darf kein Teil dieses Handbuchs vervielfältigt oder übertragen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln, elektronisch oder mechanisch, dies geschieht.

© OctoGate IT Security Systems GmbH. Alle Rechte vorbehalten.

Klingenderstraße 5, 33100 Paderborn, Germany

<http://www.octogate.de>

OctoGate ist eingetragenes Markenzeichen der

OctoGate IT Security Systems GmbH.

Alle genannten Markenzeichen stehen ausschließlich den jeweiligen Inhabern zu.

Für die Richtigkeit des Inhalts dieses Handbuchs wird keine Garantie übernommen.

Dieses Handbuch hat den Status

DRAFT

Diese Version ist noch unvollständig

Besuchen Sie regelmäßig

<http://www.octogate.de/support/downloads/>

für eine aktualisierte Version

Handbuch Version 4.01 DRAFT

Dieses Handbuch bezieht sich auf die Software Version 2.45/8.6.6 und
GUI-Version 4.00

Inhaltsverzeichnis

1	Einleitung.....	6
1.1	Systemvoraussetzungen.....	7
1.2	Virenschutz	7
1.3	Content-Filter	7
1.4	Spamschutz	8
1.5	Mail-Relay	8
2	Die Hardware Ihrer OctoGate.....	9
2.1	Lieferung der OctoGate.....	9
2.2	Anschlüsse der OctoGate	10
2.2.1	OctoGate DeskSolution 5/10 User	10
2.2.2	OctoGate RackSolution 10/20 User	10
2.2.3	OctoGate RackSolution 50-250 User.....	11
2.2.4	OctoGate RackSolution 500-1000 User	12
2.3	Anschließen Ihrer OctoGate.....	12
3	Ersteinrichtung Ihrer OctoGate	14
3.1	Installation vom USB-Stick.....	14
3.1.1	Allgemeine Angaben	14
3.1.2	Auswahl der Internetverbindung.....	15
3.1.3	Interne Netzwerkkonfiguration.....	16
3.2	Übertragen der Konfiguration auf die OctoGate	17
3.3	Sichere Aufbewahrung des USB-Stick	17
3.4	Einstellungen in Ihrem Netzwerk	18
3.4.1	DNS	18
3.4.2	Protokolle.....	18
3.4.3	Zeitsynchronisation (NTP).....	18
4	Das LC-Display der RackSolution-Serie.....	20
5	Die Konfigurationsoberfläche (WebGUI)	21
5.1	Allgemeines.....	21
5.2	Erstanmeldung / Inbetriebnahme.....	22
5.3	Übersicht	23
5.3.1	Status	23
5.4	Administration	24
5.4.1	Module.....	24
5.4.2	Benutzer	24
5.4.3	Wartung & Dienste	25
5.5	WAN.....	26
5.5.1	Verbindung	26
5.6	Webfilter (ohne aktiviertes User-Management)	27

5.6.1	Content-Filter	27
5.6.2	Pausen-Filter	28
5.7	Webfilter (Aktiviertes User-Management)	29
5.7.1	Allgemein	30
5.7.2	Active Directory	30
5.7.3	Benutzer-Verwaltung	31
5.7.4	Filter-Profile	33
5.7.5	Gruppen.....	34
5.7.6	Globale Whitelist.....	35
5.7.7	Globale Blacklist	35
5.7.8	Whitelist ohne Login	35
5.7.9	Inhaltsfilter Badwords	35
5.7.10	Pausen-Filter	35
5.8	Firewall	36
5.8.1	Portfreischaltungen.....	36
5.8.2	Portweiterleitungen.....	38
5.8.3	NAT	39
5.9	Netzwerk	41
5.9.1	IP-Adressen.....	41
5.9.2	DHCP	42
5.9.3	Routing	44
5.9.4	DNS	45
5.9.5	VLAN	45
5.10	VPN/Remote	46
5.10.1	OctoVPN-Clients	46
5.10.2	Fernzugriff	48
5.10.3	Mail-Relay.....	49
5.11	OctoScan	49
5.12	OctoGuest.....	51
5.12.1	Einstellungen	51
5.12.2	Zugangscodes	52
6	Berichte / Reporter.....	54
6.1	Zugriff auf Reports	54
6.1.1	Viren	54
6.1.2	Firewall	55
6.1.3	Webtraffic	57
7	Der OctoGate RemoteSupport.....	60
8	Der VPN-Client.....	61
8.1.1	Windows-Betriebssysteme	62
8.1.2	Windows Mobile	63

8.1.3	Linux, MacOS X.....	63
9	OctoScan Client	64
10	Fehlersuche.....	67
10.1	E-Mail Versand	67
10.1.1	Microsoft Outlook Express	67
10.1.2	Microsoft Office Outlook	67
10.1.3	Mozilla Thunderbird	67
10.2	Webzugang / Proxykonfiguration.....	68
10.2.1	Microsoft Internet Explorer	68
10.2.2	Mozilla Firefox	68
10.3	FTP	69
10.4	VoIP	69
10.5	Instant Messaging Services.....	69
10.6	VPN.....	69
10.7	DNS	69
10.8	Elster Steuersoftware	70
10.9	Java Applets	70
11	Anhang.....	71
11.1	Hinweise zum Datenschutz	71
11.1.1	Wissenswertes	71
11.2	Checklisten	72
11.2.1	Checkliste Datenschutz.....	72
11.2.2	Checkliste IT-Sicherheit	72
12	Index.....	74

1 Einleitung

Herzlichen Glückwunsch zum Erwerb Ihrer OctoGate! Sie haben mit der OctoGate eine Hochsicherheitsfirewall erworben, die Ihnen ein Höchstmaß an Sicherheit für Ihr Netzwerk bietet und Ihnen gleichzeitig alle Funktionen an die Hand gibt, Ihren Internetzugang so effizient wie möglich zu gestalten.

Der *Managed Service* sorgt dafür, dass Ihre OctoGate auch in Zukunft immer auf dem neuesten Stand der Sicherheitstechnik ist. Wir reagieren schnell und zuverlässig auf neu auftretende Bedrohungsszenarien und sorgen dafür, dass Ihre OctoGate jederzeit vor neuen Gefahren gewappnet ist.

Sollten Sie Fragen oder Wünsche zu Ihrer Firewall haben, so können Sie uns wie folgt kontaktieren:

Telefon: 05251 / 18040-0

E-Mail-Support: support@octogate.de

Wir empfehlen Ihnen, sich das Handbuch aufmerksam durchzulesen, um sich mit den vielfältigen Konfigurationsmöglichkeiten und Funktionen Ihrer OctoGate vertraut zu machen.

Das Handbuch erklärt Ihnen die grundlegenden Funktionen der Bedienungsoberfläche und richtet sich in seiner Struktur nach dem Menüaufbau.

Zu beachten ist, dass die verfügbaren Menüpunkte der Bedienungsoberfläche sich nach den Rechten des angemeldeten Benutzers richten. Beachten Sie daher die Hinweise im Text. Folgende Rollen stehen standardmäßig zur Verfügung:

- Als *Administrator* kann man sämtliche sicherheitsrelevanten Einstellungen der OctoGate, wie Setup der Firewallregeln, des Spamfilters, des Web-Content-Filters bzw. der benutzerbasierten Profile und des Black-/Whitelisting sowie der VPN-Clients vornehmen. Der Administrator kann keine weiteren Benutzer einrichten, die Zugriff auf alle oder einige Bereiche der WebGUI.
- Der *Reporter* hat vollen Zugriff auf alle Reportfunktionen der OctoGate, kann jedoch keine Konfigurationseinstellungen vornehmen (Kapitel 6)

Für spezielle Fragen steht Ihnen neben dem Support auch ein Online-Forum unter www.octogate.de zur Verfügung. Hier können Sie Fragen stellen oder bereits besprochene Fragen nachvollziehen. Ein Wiki erklärt Ihnen darüber hinaus Fachbegriffe und OctoGate-spezifische Themen.

In Kapitel 10 finden Sie Hilfestellungen zu typischen Fragen hinsichtlich des Betriebs der Firewall. Sollten Fragen offen bleiben, können Sie sich jederzeit an den Support wenden.

1.1 Systemvoraussetzungen

Internetbrowser: Internet Explorer ab Version 7, Mozilla Firefox ab Version 2, Opera, Google Chrome oder Apple Safari. Für eine optimale Anzeige empfehlen wir den Einsatz von Mozilla Firefox in der jeweils neuesten Version.

OctoScan erfordert Windows NT SP6, Windows 2000, XP, Vista, Windows 7 oder Windows Server ab Version 2003. OctoScan ist auch unter 64-bit Systemen lauffähig. Wir empfehlen einen Prozessor mit mindestens 1 Ghz und 1 GB RAM.

OctoGate VirtualAppliances sind optimiert für VMware-Umgebungen. Wir empfehlen den Betrieb unter VMware ESX-Server oder VMware Workstation. Für den Betrieb werden mindestens 4 GB Festplattenkapazität und 1 GB zugewiesener Arbeitsspeicher vorausgesetzt. Für die Verwaltung der Netze weisen Sie der VirtualAppliance mindestens 2 PCI-NICs (WAN, INT) zu.

1.2 Virenschutz

Die OctoGate prüft sämtlichen ein- und ausgehenden Datenverkehr transparent auf schädlichen Inhalt. Viren-, Trojaner- und Dialer-Erkennung erfolgt bereits beim Download. Eine mögliche Gefahrenquelle bleibt jedoch bestehen: Durch Wechselspeichermedien wie Disketten, USB-Sticks oder externe Laufwerke können Viren an der OctoGate vorbei in das interne Netzwerk gelangen. Aus diesem Grund bietet Ihnen die OctoGate einen zusätzlichen Virenschanner für alle an ihr angeschlossenen PCs. Dieser Virenschanner lässt sich zentral über die Administrationsoberfläche der OctoGate für alle PCs konfigurieren. Sie haben mit diesem lokalen Virenschanner weiterhin die Möglichkeit zentral für jeden PC zu bestimmen, ob externe Wechselmedien zugelassen werden sollen oder nicht (so genanntes „Device Lock“). Informationen hierzu finden Sie in Kapitel 5.11.

1.3 Content-Filter

Der in der OctoGate eingebaute Web-Content-Filter basiert auf einer integrierten Datenbank, die etwa 60 Mio. URLs verwaltet und diese in 24 Kategorien zusammenfasst. Diese Datenbank wird laufend automatisch auf dem neuesten Stand gehalten. Die Zusammenfassung der URLs in Kategorien erleichtert Ihnen die Konfiguration des Content-Filters, indem Sie einzelne Kategorien freigeben bzw. sperren können. Wenn eine gesperrte URL im Browser aufgerufen wird, zeigt die OctoGate anstelle der Webseite einen entsprechenden Hinweis auf die greifende Sperre der entsprechenden Kategorie an. Selbstverständlich kann der Content-Filter um benutzerdefinierte Black- und Whitelisten ergänzt werden. Näheres zur Konfiguration des Content-Filters finden Sie ab Seite 27.

1.4 Spamschutz

Die OctoGate verfügt über einen leistungsfähigen Spamfilter. Der Spamfilter arbeitet transparent und lässt sich durch den Benutzer trainieren, um die Erkennungsrate weiter zu erhöhen. Als Spam klassifizierte E-Mails werden von der OctoGate als Spam markiert und an den Empfänger ausgeliefert. Der Empfänger kann nun einfache Regeln in seinem Mailclient erstellen, die die markierten E-Mails aussortieren oder löschen.

1.5 Mail-Relay

Optional lässt sich die OctoGate um ein Mail-Relay erweitern. Dies ist insbesondere dann sinnvoll, wenn Ihr Netzwerk über einen eigenen Mailserver verfügt und/oder ein hohes Mailaufkommen bewältigt werden muss. Das Mail-Relay bietet eine verbesserte Performance bei der Spam- und Virenerkennung bei hohem Mailedurchsatz, da die OctoGate so selbst für die Annahme der Mails verantwortlich ist und geprüfte Mails ggf. an den internen Mailserver weiterleitet. Wird kein interner Mailserver angegeben, fungiert die OctoGate als vollwertiger Mailserver. Wie Sie das Mail-Relay konfigurieren, lesen Sie ab Seite 48.

2 Die Hardware Ihrer OctoGate

2.1 Lieferung der OctoGate

Folgendes muss sich in Ihrem Lieferumfang befinden:

- Die OctoGate (Einzelbeschreibungen im folgenden Abschnitt)
- Ein USB-Stick (1 GB Speicherkapazität)



- Ein Kaltgerätestecker



- Externes Netzteil (nur DeskSolution)



2.2 Anschlüsse der OctoGate¹

2.2.1 OctoGate DeskSolution 5/10 User

Frontansicht



Rückansicht



4 x Ethernet LAN 10/100 RJ 45

1 x serieller Port

2 x USB 2.0

1 x DC IN (5V)

2.2.2 OctoGate RackSolution 10/20 User

Frontansicht



2 x USB 2.0

1 x serieller Port

4 x Ethernet LAN 10/100 RJ-45

Rückansicht

¹ Die gezeigten Bilder können von Ihrem Gerät abweichen



- 1 x VGA Ausgang
- 1 x serieller Port (1)
- 2 x USB 2.0 (2)

2.2.3 OctoGate RackSolution 50-250 User

Frontansicht



- 2 x USB 2.0
- 1 x serieller Port RJ-45
- 8 x Ethernet LAN 10/100/1000 RJ-45

Rückansicht



- 1 x VGA

2.2.4 OctoGate RackSolution 500-1000 User

Frontansicht



2 x USB 2.0

1 x serieller Port über Adapter

8 x Ethernet LAN 10/100/1000 RJ 45

Rückansicht



1 x VGA

Redundante Netzteile

2 x HDD hot swapped

2.3 Anschließen Ihrer OctoGate

Bitte schließen Sie Ihre OctoGate an das Stromversorgungsnetz an und verbinden Sie die Ethernet-Anschlüsse folgendermaßen:

EXT → DSL-Modem, Standleitung

INT → Internes Netzwerk (Verbindungsaufbau grundsätzlich aus diesem Netz in die DMZ)

DMZ → Optionales physikalisch getrenntes Netzwerk (bspw. DMZ, die Demilitarisierte Zone)

WLAN → Optionales physikalisch getrenntes Netzwerk (bspw. WLAN-Router für separates, kabelloses Netz)

Port 5-8 (ab OctoGate RackSolution 50) → Optionale physikalisch voneinander getrennte Netzwerke

Im folgenden Kapitel wird die Erstinstallation Ihrer OctoGate beschrieben.

3 Ersteinrichtung Ihrer OctoGate

3.1 Installation vom USB-Stick

- Entfernen Sie ggf. den Schreibschutz des USB-Sticks (seitlichen Schalter am USB-Stick nach vorne schieben)
- Stecken Sie den USB-Stick in einen freien USB-Steckplatz Ihres PCs
- Öffnen Sie den Windows-Explorer
- Wählen Sie den USB-Stick aus
- Starten Sie *OctoGateInstaller(.exe)*

3.1.1 Allgemeine Angaben

Im Regelfall sind Ihre Daten in der Konfigurationsmaske bereits eingetragen. Andernfalls tragen Sie Ihre Daten in die entsprechenden Felder ein und klicken Sie auf „Weiter >“.

OctoGate Konfiguration-Tool Version: 1.0.0.19

OctoGate[®]
MANAGED SECURITY FIREWALL

Ablaufmenü

- ▶ Allgemein
- Fachhändler
- Internetdaten
- InternetDetails
- Abschluss

Firmenname Kunde: Karl Bray KG

Ansprech. Geschäftsführer: Hr Friesen

Ansprech. Technik: Frl Bunte

Seriennummer: xy34502z

Straße: Bockecke 4

Postleitzahl: 33014 Ort: Bad Driburg

Vorwahl + Rufnummer: 05253 / 527746

<Zurück Weiter>

In der zweiten Eingabemaske tragen Sie ggf. die Daten Ihres OctoGate-Partners ein und klicken Sie anschließend auf „Weiter >“.

OctoGate Konfiguration-Tool Version: 1.0.0.19

OctoGate[®]
MANAGED SECURITY FIREWALL

Ablaufmenü

- Allgemein
- Fachhändler**
- Internetdaten
- InternetDetails
- Abschluss

Firmenname Fachhändler: Rupprecht KG

Ansprech. Geschäftsführer: Hr Rupprecht

Ansprech. Technik Kunde: Hr Rupprecht

Straße: Ferdinandstrasse 76

Postleitzahl: 33102 Ort: Paderborn

Vorwahl + Rufnummer: 05251 / 668817

Fachhändlernummer: 33pb402

<Zurück >Weiter>

3.1.2 Auswahl der Internetverbindung

Bitte wählen Sie unter *Internetverbindung* die Art Ihres Internetzugangs aus. Halten Sie die Einwahldaten zu Ihrem Internet-Provider bereit und geben Sie diese dann in die entsprechenden Felder ein.

OctoGate Konfiguration-Tool Version: 1.0.0.19

OctoGate[®]
MANAGED SECURITY FIREWALL

Ablaufmenü

- Allgemein
- Fachhändler
- Internetdaten**
- InternetDetails
- Abschluss

Internetverbindung: DSL

Benutzername: rumpelstilz

Kennwort: ****

Verbindungs-Timeout: Freiminuten in Minuten

Freivolumen in min.: 300

<Zurück >Weiter>

Unter *Verbindungs-Timeout* stellen Sie Ihren Internettarif ein. Verfügen Sie über einen Flat-Tarif brauchen Sie hier nichts zu ändern. Andernfalls können Sie ein Freivolumen bzw. Freiminuten

eintragen (sollten Sie sich nicht sicher sein, welchen Tarif Sie nutzen, wenden Sie sich bitte an Ihren Internet-Provider).

Anmerkung: Eine Verbindung über ISDN ist nur als Backup-Lösung zu empfehlen, falls die DSL-Leitung einmal ausfällt. Dazu benötigen Sie ein ISDN-Modem, welches auch für die zusätzliche Fax-Option der OctoGate notwendig ist.

In diesem Falle können Sie über HSM ein ISDN-Modem beziehen oder alternativ auf dem freien Markt eine Fritz!Card USB 2.1 erwerben, welche über den USB-Anschluss mit ihrer OctoGate verbunden wird. Bei Selbsterwerb des ISDN-Modems erhalten Sie eine entsprechende Gutschrift bei Kauf der Faxoption.

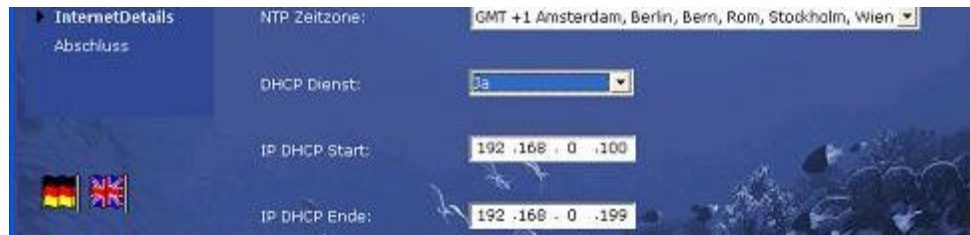
Klicken Sie anschließend auf „Weiter >“.

3.1.3 Interne Netzwerkkonfiguration



Hier konfigurieren Sie Ihr Netzwerk. Folgende Felder werden angezeigt:

- IP-Adresse der OctoGate: Vergeben Sie in diesem Feld eine IP-Adresse für Ihre OctoGate
- Subnetzmaske: Geben Sie die Subnetzmaske Ihres Netzwerks an.
- NTP Zeitzone: Geben Sie Ihre Zeitzone an. Für Deutschland wählen Sie GMT+1 (Voreinstellung)
- DHCP Dienst: Geben Sie hier an, ob Ihre OctoGate DHCP (Dynamic Host Configuration Protocol) nutzen soll. Wenn *Ja*, weist Ihre OctoGate den angeschlossenen PCs automatisch eine IP-Adresse zu, innerhalb des von Ihnen anzugebenden Adressbereichs (siehe Beispiel).



Klicken Sie nach Abschluss der Netzwerkkonfiguration auf *Weiter*. Ihre Einstellungen werden nun auf dem USB-Stick gespeichert. Danach teilt Ihnen der OctoGate Installer mit, wenn die Konfiguration abgeschlossen ist.



Klicken Sie nun auf *Beenden* und entfernen Sie dann den USB-Stick wie nachfolgend beschrieben.

3.2 Übertragen der Konfiguration auf die OctoGate

- Stecken Sie den USB-Stick in einen der USB-Anschlüsse Ihrer ausgeschalteten OctoGate
- Schalten Sie die OctoGate ein. Nun bootet die OctoGate und Ihre Konfiguration wird auf die OctoGate übertragen
- Nach Abschluss des Bootvorgangs gibt die OctoGate ein akustisches Signal. Nun können Sie den USB-Stick aus der OctoGate entfernen

3.3 Sichere Aufbewahrung des USB-Stick

Bitte schützen Sie nach der Verwendung den Stecker des USB-Sticks mit der zugehörigen Verschlusskappe und bewahren Sie ihn an einem sicheren Ort auf.

3.4 Einstellungen in Ihrem Netzwerk

3.4.1 DNS

Falls Sie DHCP benutzen, sind von Ihrer Seite keine weiteren Einstellungen nötig. Andernfalls müssen Sie in Ihrer Netzwerkkonfiguration die IP-Adresse Ihrer OctoGate als DNS-Server angeben.

3.4.2 Protokolle

Die standardmäßig freigeschalteten Protokolle der OctoGate sind:

- HTTP
- SMTP
- POP3
- HTTPS
- FTP

3.4.3 Zeitsynchronisation (NTP)

In einem lokalen Netzwerk ist es unbedingt notwendig, dass Rechner ihre Uhrzeit synchronisieren, damit beispielsweise die Zeitstempel von Dateien, die von einem gemeinsamen Dateiserver bezogen werden, konsistent bleiben. Daher ist es empfehlenswert, Ihre OctoGate die Uhrzeit der im lokalen Netz befindlichen Rechner synchronisieren zu lassen. Die OctoGate selbst synchronisiert ihre Uhrzeit mit Zeitservern im Internet und gewährleistet so eine stets korrekte Uhrzeit.

Folgendermaßen richten Sie die Zeitsynchronisation auf den lokalen Rechnern ein (ab Windows 2000 Server / Windows XP):

- Starten Sie *Start*→*Programme*→*Zubehör*→*Eingabeaufforderung* und geben Sie folgende Befehle ein:

```
„net stop w32time“  
„net time /setsntp:octo.octo“ ein.  
„net start w32time“
```

Nach Bestätigung mit *Enter* sollte die Meldung „Der Befehl wurde erfolgreich ausgeführt.“ erscheinen.

Ab Windows 2003 Server / Windows Vista:

- Starten Sie *Start*→*Programme*→*Zubehör*→*Eingabeaufforderung* und geben Sie folgende Befehle ein:



```
„w32tm /config /syncfromflags:manual /manualpeerlist:octo.octo“,  
„w32tm /config /update“,  
„w32tm /resync“
```

Jeweils nach Bestätigung mit *Enter* sollte die Meldung „Der Befehl wurde erfolgreich ausgeführt.“ erscheinen.

4 Das LC-Display der RackSolution-Serie

Bei Geräten mit LC-Display (nur Modelle der R-Serie) können Sie einige Funktionen über das Tastenfeld an der Frontseite des Gerätes auslösen.



Durch Drücken der Tasten  bzw.  gelangen Sie in das Menü. Dort steht Ihnen die folgenden Untermenüs zur Verfügung (mit *ENTER* gelangen Sie in das entsprechende Untermenü, mit *ESC* verlassen Sie es wieder):

SYSINFO → Anzeige aktueller Informationen zu Ihrer OctoGate:

- *Version*: Die Betriebssystemversion Ihrer OctoGate.
- *DSL-Log*: Zugewiesene IP-Adressen sowie primärer und sekundärer DNS-Server. Bei Problemen mit Ihrer Internetverbindung teilen Sie diese Daten bitte dem OctoGate-Support mit.
- *Ext. IP*: Die aktuelle externe IP-Adresse der OctoGate.
- *Einwahldaten*: Die Einwahldaten Ihres Providers in verschlüsselter Form. Teilen Sie diese Daten im Falle von Verbindungsproblemen dem OctoGate-Support mit.
- *Festplatte*: Die Festplattenausnutzung in %.
- *Traffic*: Das ein- und ausgehende Netzwerktraffic-Volumen.
- *Anz. Sessions*: Die Anzahl der aktuellen Verbindungen.

ADMIN → Wahrnehmen von Administratorfunktionen:

- *Konfiguration*: Erzwingt das Neueinlesen der Daten Ihres USB-Sticks (siehe Kapitel 2).
- *Neustart*: Führt einen Systemneustart durch. Bestätigen Sie mit *ENTER*.
- *Herunterfahren*: Führt die OctoGate herunter und schaltet sie aus. Bestätigen Sie mit *ENTER*.
- *USB-Backup*: Führt ein Backup auf einem angeschlossenen USB-Stick aus. Dabei wird der Stick zunächst formatiert (alle Daten auf dem Stick werden gelöscht!) und anschließend werden das grundlegende *Setup*, dieses *Handbuch* und sämtliche *Firewall-Einstellungen* Ihrer OctoGate gesichert.
- *USB-Restore*: Nach einem Geräteaustausch oder auf Anweisung des OctoGate-Supports stellt diese Funktion sämtliche Einstellungen Ihrer OctoGate wieder her. Dazu muss der USB-Stick an der OctoGate angeschlossen sein, auf den Sie zuvor das Backup ihrer Daten aufgespielt haben (siehe letzter Punkt). Wählen Sie diesen Menüpunkt und drücken *ENTER*.

5 Die Konfigurationsoberfläche (WebGUI)

5.1 Allgemeines

Die WebGUI der OctoGate ist auf optimale Bedienbarkeit hin entwickelt worden. Fehleingaben werden weitgehend durch Überprüfung der Eingaben vermieden. Sämtliche Regeln und Objekte, die Sie in der WebGUI konfigurieren können, sind in übersichtlichen Tabellen aufgeführt.

Aktionsleiste zum Bearbeiten/Löschen von markierten Elementen oder zum Verwerfen von vorgenommenen Änderungen

Wählen Sie einen Spaltennamen und geben Sie einen Begriff ein, nach dem die Einträge gefiltert werden sollen

The screenshot shows a configuration table with the following data:

Name	Beschreibung	Service	Akti
Mail Relay	Mail-Relay mit Spamfilter und Virenschanner	smtp	<input checked="" type="checkbox"/>
Spamfilter	Proxybasierter Spamfilter mit Virenschanner	pop3/smtp	<input type="checkbox"/>
Benutzer Management	Benutzersteuerung für wür den Web-Proxy	http/https/ftp	<input checked="" type="checkbox"/>
VPN-Server	VPN-Server für Token und Zertifikat	vpn	<input checked="" type="checkbox"/>
Virenschanner Server	Server für die OctoScan-Clients	Octoscan	<input checked="" type="checkbox"/>
Webfilter	Proxybasierter Webfilter mit Virenschanner	http/https/ftp	<input checked="" type="checkbox"/>

UI elements circled in red include: the 'Bearbeiten' and 'Verwerfen' buttons; the search filter dropdown; the 'Overview' and 'Changes' tabs; and the '6 / 6' page indicator.

Wählen Sie die Lasche *Changes* für die Ansicht aller Elemente, für die Sie bereits (noch nicht gespeicherte) Änderungen vorgenommen haben

Angezeigte/tatsächliche Anzahl von Elementen in der Tabelle

Sobald Sie Änderungen an der Konfiguration vorgenommen haben, die von der GUI explizit gespeichert werden müssen, erhalten Sie folgenden Hinweis:

The notification message reads: "Speicher-Liste" and "Kategorie *Module* wurde hinzugefügt!". The interface also shows navigation links: "Downloads", "Log-Viewer", "Speichern", and "Abmelden".

Die meisten Änderungen, die Sie im Laufe einer Sitzung vornehmen, werden in eine Speicher-Liste aufgenommen, so dass Sie diese Änderungen in einem Vorgang speichern können. Einige Änderun-

gen werden direkt an die OctoGate übertragen. In diesem Falle entfällt der Hinweis auf die erweiterte Speicherliste.

5.2 Erstanmeldung / Inbetriebnahme

In Ihrem Webbrowser rufen Sie die Benutzeroberfläche der OctoGate mit der Adresse „octo.octo“ auf. Beim ersten Zugriff müssen Sie sich als Administrator registrieren.

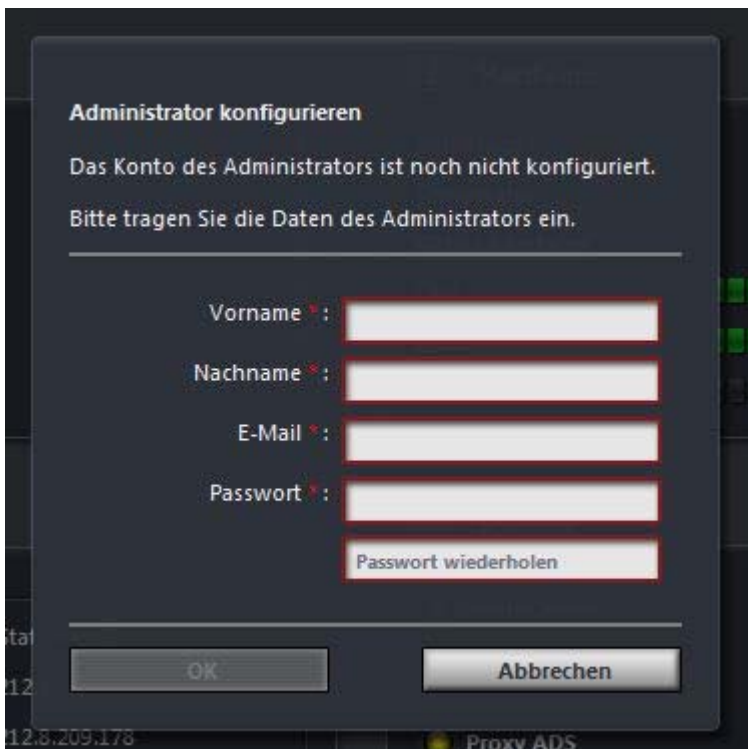


Das Login für die Erstanmeldung ist vorgegeben:

Kennung: admin

Passwort: system

Im folgenden Dialog müssen Sie sich als Administrator registrieren und das Passwort erneuern:



Wenn Sie jetzt/zukünftig mittels WebGUI auf Ihre OctoGate zugreifen, erscheint eine Login-Maske:

- Sie können sich mit Kennung „admin“ und Ihrem Passwort anmelden.

- Falls Sie Ihr Passwort vergessen haben, können Sie es sich über den Link „Passwort vergessen“ zuschicken lassen.
- ! **Anmerkung:** Geben Sie Ihr Passwort mehrfach falsch ein wird Ihr Zugang gesperrt! Wenden Sie sich zur Behebung dieses Problems an den OctoGate Support.

5.3 Übersicht

5.3.1 Status

Hier sehen Sie Detailinformationen zu Ihrer OctoGate wie Modellnummer, Versionsnummern, Ressourcenauslastung, Netzwerkinformationen und aktivierte Dienste. Des Weiteren sehen Sie statistische Daten über sicherheitsrelevante Vorfälle wie Firewallvents, gefilterte Viren und Spamnachrichten sowie Anzahl von Blockaden des Webfilters.

The screenshot displays the OctoGate WebGUI status overview page. The interface is organized into several sections:

- Übersicht (Overview):** A sidebar menu on the left with options: Status (selected), Administration, WAN, Webfilter, Firewall, Netzwerk, VPN / Remote, E-Mail, and OctoScan.
- Kunde (Customer):**
 - Firmenname: HSM
 - Geschäftsführer
 - Technik
 - Adresse
- OctoGate:**
 - Modell: 20-r
 - OctoGate Version: 8.4.0
 - WebGUI Version: OctoGate WebGUI 4.00
 - Letztes System Update: 31.01.2011 18:21:26
 - Letzte Viren Signatur: 25.03.2011 13:20:07
- Vorfälle (Incidents):**
 - Firewall: 0
 - IPs: 0
 - Anti-Virus: 0
 - Anti-Spam: 0
 - Web-Filter: 0
- Hardware:**
 - Betriebszeit: 3 Tage 2h 52m 25s
 - Temperatur: - °C
 - Aktive Interfaces: 1
 - CPU: 15% (represented by a progress bar)
 - RAM: 76% (represented by a progress bar)
 - HDD: 65% (represented by a progress bar)
- Netzwerk (Network):**
 - Verbindung (Connection):**
 - Typ: Statische IP
 - IP: 212.8.209.186
 - Gateway: 212.8.209.178
 - Netmask: 255.255.255.240
 - DNS: 212.8.216.41, 212.8.216.42
 - Hostname: vosadooc.ozone.octogate.de
 - Traffic (Up / Down):**

Interface	Up (kBps)	Down (kBps)
INT	0.00	0.00
DMZ	0.00	0.00
WLAN	1.26	0.39
EXT	0.00	0.00
VPN-Server	0.00	0.00
- Dienste (Services):**
 - Virenschanner (Active)
 - Proxy (Active)
 - Proxy ADS (Inactive)
 - Proxy Virenschanner (Active)
 - Samba-Freigabe (Inactive)
 - Spamfilter (Active)
 - VPN-Server (Active)
 - DHCP-Server (Inactive)
 - Octo-Virenschanner-Server (Active)
 - Lokales Mail-Relay (Active)

5.4 Administration

In der Kategorie *Administration* nehmen Sie Einstellungen hinsichtlich der Module, Benutzerrollen bzw. -rechte sowie Wartungseinstellungen vor.

5.4.1 Module

Unter dem Menüpunkt Module finden Sie alle für Ihre OctoGate freigeschalteten Module. Freigeschaltete Module können Sie hier gezielt aktivieren oder deaktivieren.



Name	Beschreibung	Service	Aktiv
Firewall	Port Firewall	alle	<input checked="" type="checkbox"/>
Guest Management	Gastzugänge verwalten	alle	<input checked="" type="checkbox"/>
Mail Relay	Mail-Relay mit Spamfilter und Virenschanner	smtp	<input checked="" type="checkbox"/>
Spamfilter	Proxybasierter Spamfilter mit Virenschanner	pop3/smtp	<input checked="" type="checkbox"/>
User Management	Benutzersteuerung für den Web-Proxy	http/https/ftp	<input checked="" type="checkbox"/>
VPN-Server	VPN-Server für Token und Zertifikat	vpn	<input checked="" type="checkbox"/>
Virenschanner Server	Server für die OctoScan-Clients	Octoscan	<input checked="" type="checkbox"/>
Webfilter	Proxybasierter Webfilter mit Virenschanner	http/https/ftp	<input checked="" type="checkbox"/>

Wenn Sie ein Modul aktivieren oder deaktivieren möchten, wählen Sie das entsprechende Modul aus der Tabelle aus und klicken Sie oben links auf Bearbeiten. Im folgenden Dialog können Sie die Aktivierung einstellen, indem Sie die Checkbox an- oder abwählen. Bestätigen Sie Ihre Einstellungen mit Klick auf OK.

5.4.2 Benutzer

Sie können hier Benutzer für die Administration anlegen und mit unterschiedlichen Rollen versehen. Die Benutzerrollen bestimmen, auf welche Funktionen der WebGUI ein Benutzer Zugriff erhält. Wenn Ihre OctoGate über das optionale User-Management verfügt, können Sie in der Rubrik Webfilter den hier angelegten Benutzern zusätzlich Webfilterprofile zuordnen (siehe Kapitel 5.7.4).

Folgende Benutzerrollen stehen zur Verfügung:

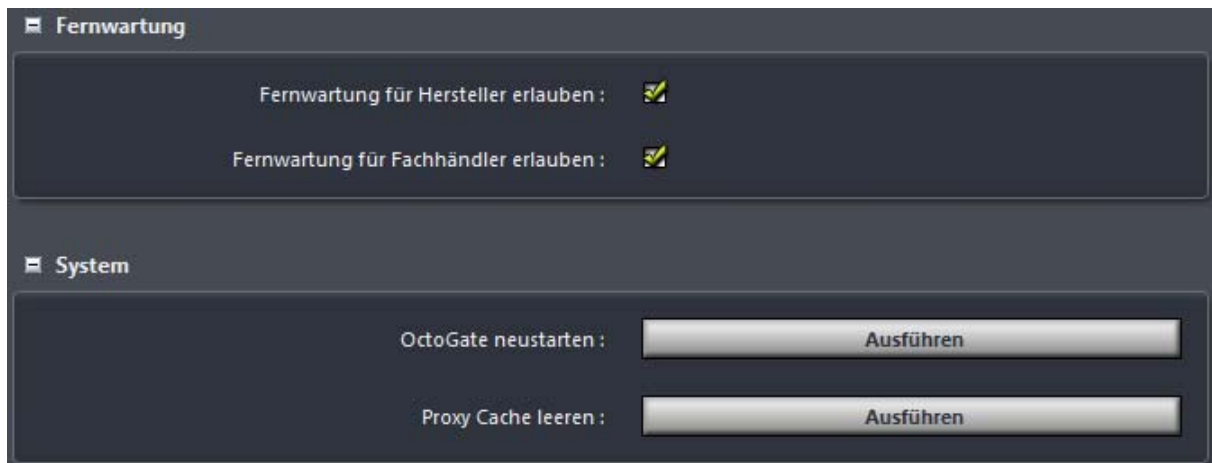
Benutzerrolle	Bedeutung
Allgemeine Statistiken	Der Benutzer hat ausschließlich Zugriff auf allgemeine Statusinformationen
Basis	Der Benutzer hat Zugriff auf die Benutzerverwaltung und Wartungs-

	einstellungen
Firewall	Der Benutzer hat Vollzugriff auf die Rubrik <i>Firewall</i>
Gruppenadministration	Der Benutzer hat Zugriff auf die Gruppenadministration des Webfilters
Logfiles	Der Benutzer hat Zugriff auf von der OctoGate geloggte Informationen
Mail	Der Benutzer hat Vollzugriff auf die Rubrik <i>E-Mail</i>
Module	Der Benutzer hat Zugriff auf die Verwaltung der freigeschalteten Module
Netzwerk	Der Benutzer hat Vollzugriff auf die Rubrik <i>Netzwerk</i>
OctoScan	Der Benutzer hat Vollzugriff auf die Rubrik <i>OctoScan</i>
Spam	Der Benutzer hat Zugriff auf die Konfiguration des Spamfilters
Spam-User	
VPN	Der Benutzer hat Vollzugriff auf die Rubrik <i>VPN</i>
WAN	Der Benutzer hat Vollzugriff auf die Rubrik <i>WAN</i>
Webfilter	Der Benutzer hat Vollzugriff auf die Rubrik <i>Webfilter</i>

Benutzerrollen können beliebig miteinander kombiniert werden.

5.4.3 Wartung & Dienste

Sie können hier in jedem Unterbereich durch einen Klick auf die Schaltflächen bzw. durch Setzen eines Hakens die entsprechenden Funktionen auslösen bzw. ein-/ausschalten:



- **Fernwartung für Hersteller erlauben**
Wenn Sie keinen Zugriff auf Ihre OctoGate durch den OctoGate Support wünschen, können Sie die Fernwartung hier ausschalten.
- **OctoGate-Partner-Fernwartung**
Ihr OctoGate-Partner (Fachhändler) kann über eine VPN-Verbindung für Wartungszwecke auf Ihre OctoGate zugreifen. Wenn Sie diese Möglichkeit unterbinden möchten, können Sie diese Funktion hier ausschalten und bei Bedarf wieder einschalten.
- **OctoGate neustarten**
Hier können Sie über die Schaltfläche *System neustarten* einen Neustart Ihrer OctoGate durchführen (z.B. wenn der Support Sie nach Einspielung von Updates dazu auffordert).
- **Proxy-Cache leeren**
Leeren Sie durch Druck auf den Button den Cache ihres Proxys. Dies ist dann sinnvoll, wenn Sie Internetseiten aufrufen, die Sie nicht aus dem Cache des Proxys laden möchten.

5.5 WAN

Unter der Rubrik WAN finden Sie Einstellungsmöglichkeiten und Informationen zur Außenanbindung der OctoGate.

5.5.1 Verbindung

Hier finden Sie alle Daten zur Internetverbindung Ihrer OctoGate. Sie finden hier die IP Adresse der OctoGate nach außen, die verwendeten DNS-Adressen und den eindeutigen Namen Ihrer OctoGate. Der Name der OctoGate setzt sich nach folgendem Muster zusammen:

abcdefgh.ozone.octogate.de

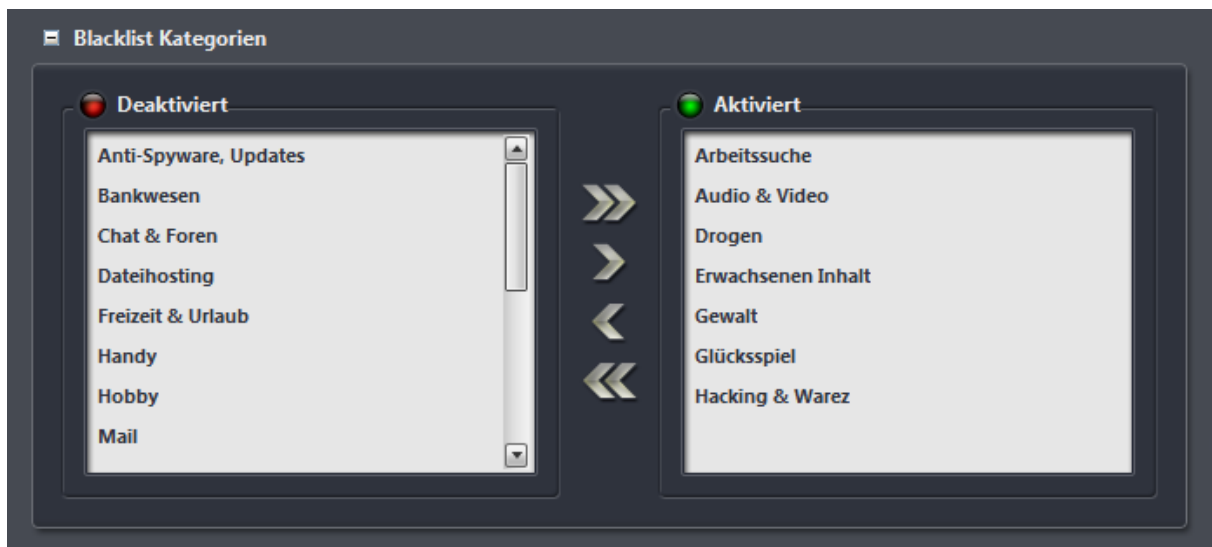
Der Name besteht immer aus acht Buchstaben. Evtl. Supportanfragen können Sie beschleunigen, wenn Sie diesen achtstelligen Namen bereithalten.

5.6 Webfilter (ohne aktiviertes User-Management)

Unter der Rubrik Webfilter können Sie die Einstellungen für den Contentfilter vornehmen. Die OctoGate verfügt über eine integrierte Datenbank mit ca. 60 Mio. verzeichneten URLs. Diese sind in 25 themenbezogenen Kategorien zusammengefasst und lassen sich gezielt für den Internetzugriff sperren.

5.6.1 Content-Filter

Definieren Sie hier auf Basis der Blacklist Kategorien und frei definierbaren Black- und Whitelisten die zulässigen bzw. gesperrten Webseiten und -inhalte.

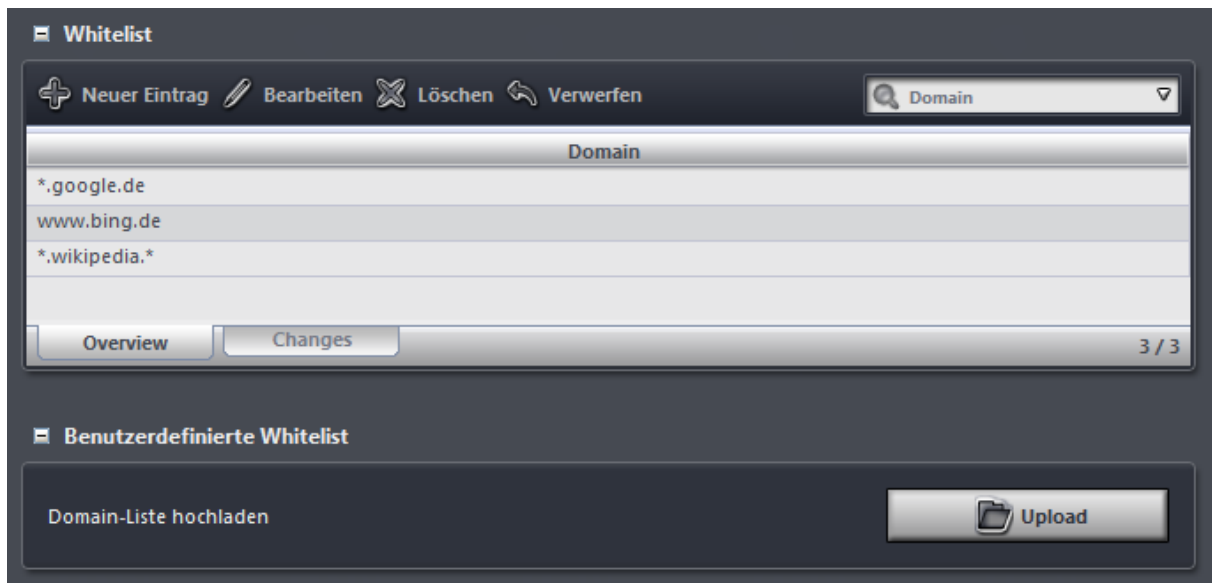


Wählen Sie im linken Feld die Kategorien aus, die Sie sperren (aktivieren) möchten, indem Sie diese anklicken und durch Klick auf den einfachen Pfeil in die „Aktiviert“-Liste verschieben. Wenn Sie mehrere Kategorien sperren möchten, halten Sie die Strg-Taste Ihrer Tastatur gedrückt, während Sie die gewünschten Kategorien auswählen. Aktivieren Sie die Mehrfachauswahl ebenfalls, indem Sie auf den einfachen Pfeil nach rechts klicken. Sie können auch in einem Schritt alle vorhandenen Kategorien aktivieren, indem Sie auf den Doppelpfeil nach rechts klicken.

Bereits aktivierte Kategorien können Sie wieder entsperren, indem Sie die gewünschten Einträge nach gleichem Muster wie oben beschrieben vom rechts nach links setzen.

Anmerkung: Auf die Kategorisierung einzelner Internetadressen haben wir keinen Einfluss. Sollten unerwartet Seiten geblockt werden, empfehlen wir die gezielte Freigabe mithilfe der *Whitelist*-Funktion (siehe unten)

Sie können Internetadressen gezielt freigeben, so dass diese auch erreichbar sind, wenn diese Adresse in einer gesperrten Kategorie gelistet ist. So können Sie beispielsweise die Kategorie *Suchmaschinen* sperren und Google gezielt freigeben, wenn Sie ausschließlich Google freigeben möchten.



Klicken Sie auf *Neuer Eintrag*, um einen neuen Whitelist-Eintrag vorzunehmen. Tragen sie im folgenden Dialog die freizugebende Domain nach folgendem Muster ein:

www.google.de: Ausschließlich diese Domain ist freigegeben. Subdomains wie *maps.google.de* werden gesperrt.

**.google.de*: Alle Subdomains sind zulässig wie *maps.google.de*, *translate.google.de* usw.

.google.: Alle Subdomains und Top-Level-Domains sind zulässig, wie z.B. *translate.google.com*, *maps.google.at* usw.

www.google.de: Nur diese Kombination aus Sub- und Top-Level-Domain ist zulässig. Andere Kombinationen werden gesperrt.

google.de: Es wird nur diese URL gesperrt. Wenn jedoch automatisch auf www.google.de umgeleitet wird, funktioniert der Aufruf dennoch. Daher sollten immer vollständige URLs angegeben werden.

Wollen Sie eine selbst definierte Liste von Domains blocken, so können Sie diese in einer Textdatei (.txt), getrennt durch einen Zeilenumbruch, ablegen und unter *Domain-Liste hochladen* als Datei in Ihre Liste geblockter Seiten importieren.

Anmerkung: Eine bestehende Liste von Domains wird durch die Aktion „Domain-Liste hochladen“ überschrieben!

Wenn Sie bestimmte Domains gezielt sperren möchten, dann pflegen Sie diese in der Tabelle *Blacklist*. Hier gelten die gleichen Konventionen wie für die *Whitelist* (s.o.).

5.6.2 Pausen-Filter

Über den Pausenfilter können Sie gezielt für zu definierende Zeiträume von der Standardkonfiguration abweichende Filtereinstellungen vornehmen. Wählen Sie hierzu im Navigationsmenü den Eintrag

Webfilter -> Pausen-Filter. Für die Anlage eines neuen Pausenfilters klicken Sie auf *Neuer Eintrag*. Es können beliebig viele Pausenfilter definiert werden.

The screenshot shows the 'Pausen-Filter' configuration dialog. The dialog is titled 'Pausen-Filter' and has a subtitle 'Zeitlich beschränkter globaler Filter für alle Benutzer'. It contains several input fields: 'Filter-Name' (a text box with a red border), 'von' and 'bis' (time selection controls), 'Tage' (a dropdown menu set to 'Täglich'), and 'Beschreibung' (a text area). There is also a checked 'Aktiv' checkbox. At the bottom, there are three buttons: 'Abbrechen', 'Zurück', and 'Weiter'. In the background, a table with columns 'FilterName', 'von', 'bis', 'Tage', 'Beschreibung', and 'Aktiv' is visible, along with a toolbar with icons for 'Neuer Eintrag', 'Bearbeiten', 'Löschen', and 'Verwerfen'.

Geben Sie im folgenden Dialog einen Namen für den neuen Pausenfilter (Pflichtfeld) an und definieren Sie die Start- (von:) und Endzeit (bis:) sowie die Tage, an denen der Pausenfilter gültig sein soll (Alle/Mo-Fr/Sa-So). Die Beschreibung ist optional. Anschließend klicken Sie auf Weiter, um in den folgenden Dialogen die Filtereinstellungen nach Kategorien sowie Black- und Whitelist vorzunehmen.

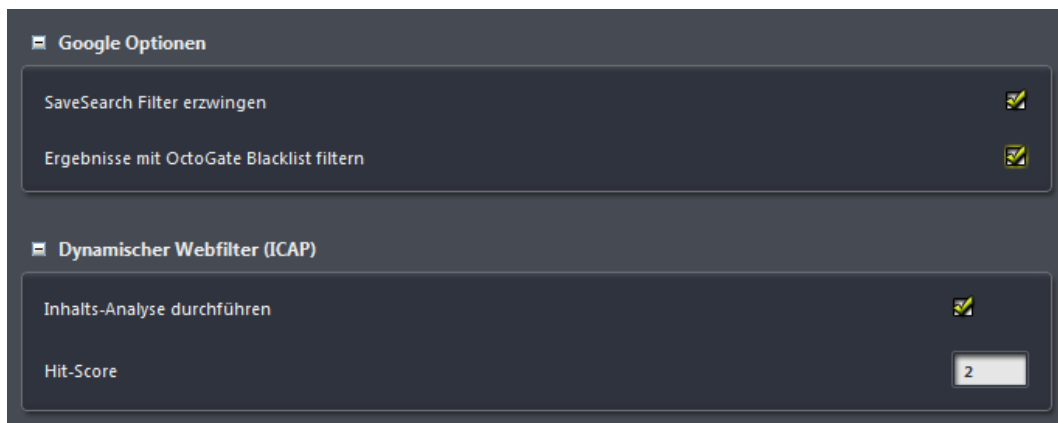
5.7 Webfilter (Aktiviertes User-Management)

Mit dem freigeschalteten und aktivierten Modul User-Management (siehe Abschnitt 5.4.1) können Sie benutzerindividuelle Webfilterprofile einrichten und vieles mehr. Mit aktiviertem User-Management steht Ihnen neben dem URL-Filter außerdem auch ein dynamischer Inhaltsfilter zur Verfügung, der Inhalte auf Basis einer Schlagwortliste analysieren und ggf. filtern kann.

! **Anmerkung:** Für den Internetzugriff ist die Verwendung der OctoGate als Proxy Voraussetzung (siehe 10.2).

5.7.1 Allgemein

Hier konfigurieren Sie die allgemeinen, d.h. die für alle Profile gültigen Einstellungen. Sie können definieren, ob Google-Suchergebnisse zusätzlich gefiltert werden sollen. Aktivieren Sie *SaveSearch Filter* erzwingen, um die Ergebnisse immer, d.h. unabhängig von den benutzerseitig vorgenommenen Google-Sucheinstellungen, mit dem Google-eigenen Filter *Safesearch* zu filtern. Aktivieren Sie Ergebnisse mit *OctoGate Blacklist* filtern, wenn die Suchergebnisse zusätzlich durch die globale Blacklist gefiltert werden sollen. Wenn Sie die Google-Optionen deaktivieren werden alle Suchergebnisse angezeigt. Erst bei Aufruf eines der angezeigten Ergebnisse werden Inhalte in Abhängigkeit von den Profileinstellungen ggf. gesperrt.



Weiterhin können Sie im unteren Dialogfeld die dynamische Inhaltsanalyse aktivieren. In diesem Falle werden alle aufgerufenen Internetinhalte über einen so genannten ICAP-Server (*Internet Content Adaption Protocol*), der die aufgerufenen Inhalte auf die Vorkommen bestimmter Schlagwörter hin untersucht. Der Hit-Score gibt dabei an, wie restriktiv die Inhalts-Analyse vorgehen soll. Jedes Schlagwort hat einen Score von 1 bis 9 (siehe 5.7.9). Je niedriger Sie also hier den Score wählen, desto weniger Schlagwörter müssen auf einer Internetseite vorhanden sein, um den Zugriff auf diese Seite zu sperren, da die Sperrung durch die Inhalts-Analyse dann veranlasst wird, wenn der Hit-Score erreicht oder überschritten wird. Wählen Sie beispielsweise einen Hit-Score von 9, so sind z.B. neun Schlagwörter mit Score 1 oder ein Schlagwort mit Score 4 in Verbindung mit einem Schlagwort mit Score 5 nötig, um eine Sperrung zu veranlassen.

5.7.2 Active Directory

Wenn Sie einen eigenen Microsoft Verzeichnisdienst (Active Directory) in Ihrem Netz betreiben, so können Sie die Benutzer, die im Verzeichnisdienst angelegt sind, in das OctoGate Usermanagement übernehmen. In diesem Menüpunkt aktivieren Sie die Synchronisation mit Active Directory, die nach Angabe der Verbindungsdaten zum Verzeichnisserver von der OctoGate in Intervallen automatisch durchgeführt wird.

Alle Felder in diesem Konfigurationsdialog sind Pflichtfelder. Aktivieren Sie Funktion, indem Sie die Checkbox *Aktiv* anhaken. Geben Sie Ihren Domänennamen, den Namen sowie die IP-Adresse des Verzeichnisseservers an. Schließlich wird noch das Administrator-Login für den Verzeichnisserver benötigt.

Aktivieren Sie die Checkbox Single Sign-on, wenn Benutzer die OctoGate an der Domäne angemeldete Benutzer automatisch erkennen soll. In diesem Falle ist kein separates Login am Browser für den Internetzugang erforderlich.

! | Wenn Sie diese Einstellung aktivieren, ist ein Zugriff von Benutzern, die nicht in der Domäne verzeichnet sind, nicht möglich.

Die Zuordnung der Benutzer zu Filterprofilen erfolgt über Active Directory-Sicherheitsgruppen. Legen Sie im Verzeichnis Sicherheitsgruppen mit dem Namen *Octo_Name* (Das Präfix *Octo_* muss einem beliebigen Namen vorangestellt sein) und fügen Sie diesen Sicherheitsgruppen die gewünschten Benutzer hinzu. Die OctoGate wird dann automatisch gemäß diesen Namen Filterprofile anlegen, die unter dem Menüpunkt *Filter-Profil* (s. 5.7.4) bearbeitet werden können.

! | Dieser Menüpunkt steht ausschließlich dem registrierten Administrator zur Verfügung und kann keinem zusätzlichen User über Sicherheitsrollen zur Verfügung gestellt werden.

Alle Objekte (Benutzer, Filterprofile), die mit dem Active Directory-Verzeichnis synchronisiert wurden, werden als „importiert“ gekennzeichnet. Änderungen an diesen Objekten in der WebGUI sind möglich. Sie können diesem Benutzer ebenfalls Sicherheitsrollen zuweisen, um diesem Benutzer Rechte für die Konfiguration einzelner Bereiche zu geben (s. 5.4.2).

5.7.3 Benutzer-Verwaltung

Unter diesem Menüpunkt verwalten Sie die Benutzer, die Zugriff auf das Internet erhalten dürfen. Legen Sie einen neuen Benutzer an, indem Sie auf *Neuer Eintrag* klicken.

Benutzer - Stammdaten

Die markierten Pflichtfelder müssen ausgefüllt werden.

Benutzername * :

Profil :

Vorname :

Nachname :

E-Mail * :

Passwort * :

Adresse :

Telefon :

IP-Netz :

Subnetz :

Bit Dezimal

Mixed Mode : Internetzugriff aus diesem Netz ohne Login erlauben

Gruppe :

Importiert : aus Active Directory importiert

Füllen Sie mindestens alle rot markierten Pflichtfelder aus und weisen Sie dem Benutzer ein eingerichtetes Profil zu (siehe Abschnitt 5.7.4). (Standardmäßig ist das Profil *Standard* zugewiesen, welches Sie unter *Filter-Profile* bearbeiten können). Optional können Sie den Benutzer auf eine IP-Adresse oder einen IP-Adressbereich einschränken. Geben Sie hierzu unter IP-Netz die Adresse ein und eine passende Subnetzmaske. Soll es sich um eine einzige IP-Adresse handeln und nicht um einen Adressbereich, geben Sie als Subnetzmaske „32“ (Bit) bzw. „255.255.255.255“ (Dezimal) ein. Wenn Sie den *Mixed Mode* aktivieren, ist für den Zugriff aus dem angegebenen Netz kein Login nötig. Wenn Sie die IP-Adresse auf 0.0.0.0 belassen und den Mixed Mode aktivieren, so gilt der Mixed Mode für alle Clients, unabhängig davon, in welchem internen Netz sie sich befinden. Ein explizites Login ist dann erst über eine Sperrseite möglich, die bei Aufruf einer gesperrten URL angezeigt wird:

Zugriff nicht erlaubt!

Login

Die von Ihnen aufgerufene URL wurde durch die OctoGate-Firewall geblockt.
Sollte dieses nicht erwünscht sein, wenden Sie sich bitte an den Support.

Telefon: +49 800 764 764 7
E-Mail: support@octogate.de

Geblockte URL:

www.google.de/

Status:

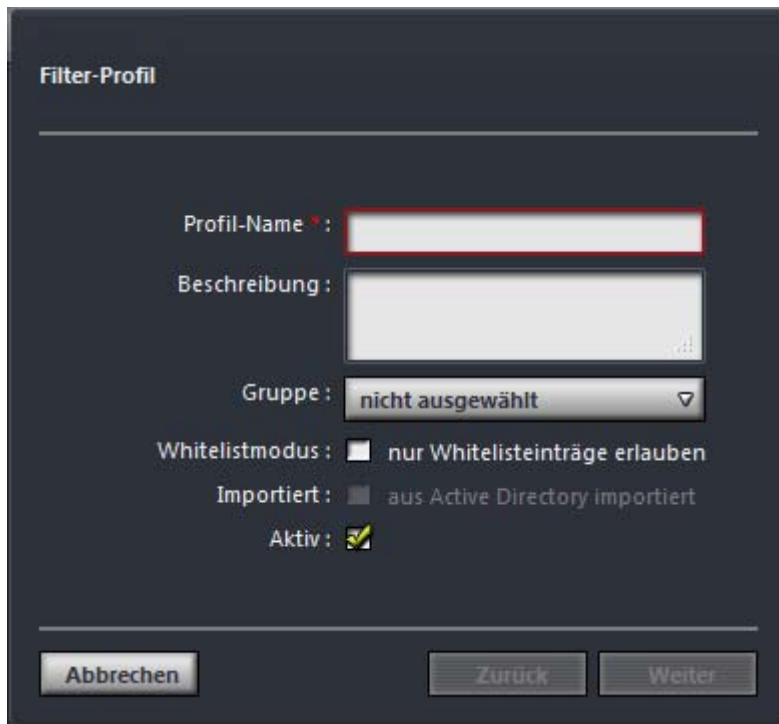
Parameter	Wert
Quell-IP	10.124.89.9
Benutzername	Admin
Kategorie	
Globale Blacklist	-
Filter-Profil Blacklist	-

Für die Richtigkeit und exakte Kategorisierung der Blacklisten übernehmen wir keine Gewähr!

! **Anmerkung:** Im Mixed Mode ist für die Authentifizierung kein expliziter Proxy im Browser-Eintrag notwendig. Jedoch muss die OctoGate als Proxy explizit eingetragen werden, wenn ein Login über die Sperrseite erfolgen soll (siehe Abschnitt 10.2).

5.7.4 Filter-Profile

Hier legen Sie Filterprofile an, die Sie den Benutzern zuordnen können. Jedes Profil enthält eigene Zuweisungen von erlaubten/gesperrten Inhaltskategorien sowie eigene Black- und Whitelist-Einstellungen. Legen Sie ein neues Profil an, indem Sie auf *Neuer Eintrag* klicken. Im folgenden Dialog geben Sie einen Profilnamen an. Der Profilname wird in der Konfiguration von Benutzern zur Auswahl angezeigt, daher sollte ein möglichst sprechender Name gewählt werden.



Filter-Profil

Profil-Name * :

Beschreibung :

Gruppe :

Whitelistmodus : nur Whitelisteinträge erlauben

Importiert : aus Active Directory importiert

Aktiv :

Die Beschreibung ist optional. Wenn Sie möchten, dass dieses Profil ausschließlich URLs zulässt, die in der Whitelist dieses Profils gepflegt sind, aktivieren Sie das Kontrollkästchen *Whitelist-Modus*. Damit dieses Profil bei der Anlage neuer Benutzer auswählbar ist, muss das Kontrollkästchen *Aktiv* aktiviert sein. Zusätzlich können Sie das Profil optional einer Gruppe zuordnen, wenn Sie einzelnen Benutzern Bearbeitungsrechte für dieses Profil einräumen möchten (vgl. 5.7.5). Anschließend klicken Sie auf *Weiter*. In den folgenden Dialogen weisen Sie die zu sperrenden Kategorien zu und legen die Black- und Whitelists für dieses Profil an (vgl. 5.6.1). Bestätigen Sie im letzten Schritt des Dialogs mit *Fertigstellen*. Bevor Sie ein neu erstelltes Profil verwenden können, müssen Sie die vorgenommenen Änderungen speichern. Ein entsprechender Hinweis weist Sie nach Fertigstellung eines Profils darauf hin.

5.7.5 Gruppen

Eine Gruppe ist eine Einheit für die Administration des Webfilters, die Benutzer und Profile zusammenfasst, für die sich beschränkte Administrationsrechte einräumen lassen. So kann ein Benutzer, der der Gruppe x zugeordnet wurde, sich mit seinem Login direkt an der WebGUI anmelden und erhält dann Zugriff auf alle Elemente (Benutzer, Filter-Profile), die der Gruppe x zugeordnet sind. Die Berechtigung, die ein Benutzer für eine Gruppe besitzt, wird in der Benutzerverwaltung der Rubrik Webfilter (s. 5.7.3) eingestellt. Für die Anlage einer neuen Gruppe klicken Sie auf *Neuer Eintrag* und geben Sie im folgenden Dialog den Namen der neuen Gruppe an und optional eine E-Mail-Adresse, die mit dieser Gruppe assoziiert sein soll. Weitere Angaben sind für die Anlage nicht notwendig. Klicken Sie anschließend auf *OK*. Bevor Sie eine neu erstellte Gruppe verwenden können, müssen Sie die vorgenommenen Änderungen speichern. Ein entsprechender Hinweis weist Sie nach Fertigstellung einer Gruppe darauf hin.

5.7.6 Globale Whitelist

Die Globale Whitelist gilt profilübergreifend und gibt gezielt URLs frei, die durch URL-Kategorien in Filterprofilen gesperrt sind. Die individuelle Blacklist eines Filterprofils wiederum überschreibt die in der Globalen Whitelist freigegebenen URLs. Sie können einzelne URLs der Liste über *Neuer Eintrag* hinzufügen, oder eigene Listen im ASCII-Format (eine URL pro Zeile) hochladen. Der Eintrag der URLs erfolgt wie in Abschnitt 5.6.1 erläutert.

5.7.7 Globale Blacklist

Die Globale Blacklist gilt profilübergreifend und sperrt gezielt URLs. Die individuelle Blacklist eines Filterprofils wiederum überschreibt die in der Globalen Blacklist gesperrten URLs. Sie können einzelne URLs der Liste über *Neuer Eintrag* hinzufügen, oder eigene Listen im ASCII-Format (eine URL pro Zeile) hochladen. Der Eintrag der URLs erfolgt wie in Abschnitt 5.6.1 erläutert.

5.7.8 Whitelist ohne Login

URLs, die Sie in dieser Liste pflegen, sind von allen PCs hinter der OctoGate auch ohne Benutzerlogin erreichbar. So kann beispielsweise das firmeneigene Intranet global freigegeben werden, ohne dass ein Login notwendig ist. Alle hier gepflegten URLs sind auch nach Login eines Benutzers erreichbar. Der Eintrag der URLs erfolgt wie in Abschnitt 5.6.1 erläutert.

5.7.9 Inhaltsfilter Badwords

Hier pflegen Sie die Schlagwörter, auf deren Basis die inhaltliche Analyse des Webfilters arbeiten soll. Die OctoGate bringt bereits eine umfangreiche Liste an pornographischen und gewaltverherrlichenden Schlagwörtern mit. Jedes Schlagwort ist mit einer *Score* versehen, die die Gewichtung eines Wortes widerspiegelt. Je höher die Score, desto eher wird der Fund dieses Wortes auf einer Webseite dazu führen, dass die Seite für den Zugriff gesperrt wird. Durch *Bearbeiten* einzelner Datensätze kann die Score angepasst werden. Neue Schlagwörter tragen sie mit Klick auf *Neuer Eintrag* ein oder laden Sie vordefinierte Listen mit Schlagwörtern hoch, die wie folgt aufgebaut sein müssen:

```
Schlagwort1; [Score]
Schlagwort2; [Score]
...
```

Hochgeladene Listen werden in die bestehenden Einträge integriert.

Entscheidend für die Schärfe der Inhaltsanalyse ist neben der individuellen Gewichtung der Schlagwörter die Angabe des Schwellenwertes (*Hit-Score*) – s. Abschnitt 5.7.1.

5.7.10 Pausen-Filter

Mit dem Pausenfilter ist es möglich, für begrenzte Zeitfenster veränderte Filtereinstellungen zu definieren. In diesen Zeitfenstern gelten die vorgenommenen Filtereinstellungen global für alle

Benutzer. Es können beliebig viele Zeitfenster mit jeweils unterschiedlichen Einstellungen eingerichtet werden. Für die Anlage eines neuen Pausenfilters klicken Sie auf *Neuer Eintrag*.



Pausen-Filter
Zeitlich beschränkter globaler Filter für alle Benutzer

Filter-Name : früh

von : 09 : 00

bis : 09 : 15

Tage : Mo-Fr

Beschreibung :

Aktiv :

Abbrechen Zurück Weiter

Im Dialog geben Sie einen Namen für den Pausen-Filter an und definieren Start- und Endzeit der Gültigkeit. Sie können außerdem festlegen, dass der Filter *täglich*, *Mo-Fr* oder *Sa-So* gültig ist. Die Angabe einer Beschreibung ist optional. Bereits eingerichtete Pausenfilter können durch Entfernen des Häkchens des Kontrollkästchens *Aktiv* temporär deaktiviert werden. Klicken Sie anschließend auf *Weiter* und nehmen Sie in den folgenden Schritten die gewünschten Filtereinstellungen (Kategorien, Black- und Whitelist) vor. Die Änderungen werden nach Fertigstellung in die Speicherliste aufgenommen und werden nach Speicherung aktiv.

5.8 Firewall

Unter der Rubrik Firewall Ports freischalten, Portweiterleitungen einrichten und Source-NAT sowie Destination-NAT konfigurieren.

5.8.1 Portfreischaltungen

Hier schalten Sie für das von Ihnen gewünschte OctoGate-Interface Ports frei. Sie können Ports für die Kommunikation nach draußen freischalten oder gezielt Ports für die Kommunikation innerhalb der internen Netze freigeben. Klicken Sie für die Anlage einer neuen Portfreischaltung auf *Neuer Eintrag*.

Geben Sie eine Beschreibung an, anhand derer Sie die Einstellungen später identifizieren können (optional). Geben Sie die Portnummer bzw. die Portrange an, die Sie freigeben möchte und wählen Sie aus der Dropdown-Liste das zugehörige Protokoll:

TCP: beschränkt die Portfreigabe auf das Protokoll TCP

UDP: beschränkt die Portfreigabe auf das Protokoll UDP

ICMP: beschränkt die Portfreigabe auf das Protokoll ICMP

ALL: die Portfreigabe gilt für alle Protokolle

Mit der Dropdown-Box *Int IN* geben Sie das eingehende Interface an (ALL (Regel gilt für alle Interfaces), INT, DMZ, WLAN, EXT) und optional die Herkunfts-IP-Adresse (Quell-IP). Wenn Sie 0.0.0.0 als Quell-IP angeben, gilt diese Regel für alle Quell-IP-Adressen.

Mit der Dropdown-Box *Int OUT* geben Sie das ausgehende Interface an (ALL (Regel gilt für alle Interfaces), INT, DMZ, WLAN, EXT) und optional die Ziel-IP-Adresse (Ziel-IP). Wenn Sie 0.0.0.0 als Ziel-IP angeben, gilt diese Regel für alle Ziel-IP-Adressen.

Bestätigen Sie die Regel mit *OK*.

Der folgenden Tabelle können Sie einige typische Portbelegungen entnehmen:

Port-Nr.	Dienst	Beschreibung
7	Echo	Zurücksenden empfangener Dateien
20	FTP-Data	Dateitransfer (Datentransfer vom Server zum Client)
21	FTP	Dateitransfer (Initiierung, Senden von Steuerbefehlen)
22	SSH	Secure Shell
23	Telnet	Terminalemulation

25	SMTP, ESMTP	E-Mail-Versand
37	TCP, UDP	Datenaustausch Zeitprotokoll
53	DNS	Auflösung von Domainnamen in IP-Adressen
67	UDP	DHCP Server
68	UDP	DHCP Client
70	Gopher	Internet-Informationdienst
80	HTTP	Webserver
110	POP3	Client-Zugriff für E-Mail-Server
123	UDP	NTP Zeitprotokoll
143	IMAP	E-Mail-Zugriff (auf dem Mailserver)
220	IMAP3	E-Mail-Zugriff
443	HTTPS	sicherer Webserver
465	SMTPS	SMTP über SSL
520	RIP	Routing-Protokoll
531	IRC	Chat-System
587	TCP	Alternativer E-Mail-Versand
993	IMAPs	SSL-verschlüsselter IMAP
1194	UDP	OpenVPN
1433	ms-sql-s	MS DB-Server
1494	DATEV	Steuer- und Finanzbuchhaltungssoftware
1521	oraclesrv	Oracle DB-Server
1723	TCP	Verbindungsaufbau PPTP
3128	Squid	Proxyserver
3306	MySQL	Zugriff auf MySQL-Datenbanken
3389	RDP	Windows Remotedesktopzugriff, Windows Terminal Services
4000	ICQ	Instant Messaging
5432	PostgreSQL	OpenSource DBMS
5900	vnc-server	Virtual Network Computing
6667	IRC	Chat-System
8080	Proxy	Internetzugriff

5.8.2 Portweiterleitungen

Portweiterleitungen richten Sie ein, um auf einem bestimmten Port eingehenden Datenverkehr an eine bestimmte Zieladresse im internen Netz weiterzuleiten. Hierbei kann außerdem an einen anderen Port weitergeleitet werden. Klicken Sie für die Anlage einer neuen Portweiterleitung auf *Neuer Eintrag*.

Portweiterleitungen

Neuer Eintrag.

Beschreibung:

Protokoll:

Int IN:

Quell-IP:

Quell-Port:

Ziel-IP:

Ziel-Port:

Geben Sie eine Beschreibung an, anhand derer Sie die Einstellungen später identifizieren können (optional). Wählen Sie aus der Dropdown-Liste das zugehörige Protokoll:

TCP: beschränkt die Portfreigabe auf das Protokoll TCP

UDP: beschränkt die Portfreigabe auf das Protokoll UDP

ICMP: beschränkt die Portfreigabe auf das Protokoll ICMP

ALL: die Portfreigabe gilt für alle Protokolle

Mit der Dropdown-Box *Int IN* geben Sie das eingehende Interface an (ALL (Regel gilt für alle Interfaces), INT, DMZ, WLAN, EXT) und optional die Herkunfts-IP-Adresse (Quell-IP). Wenn Sie 0.0.0.0 als Quell-IP angeben, gilt diese Regel für alle Quell-IP-Adressen. Der Quell-Port bezeichnet den Port des Herkunftsrechners. Lassen Sie das Feld frei, wenn Sie Datenpakete aller Ports weiterleiten möchten.

Geben Sie die Ziel-IP-Adresse (Ziel-IP), sowie den Ziel-Port an, auf die umgeleitet werden soll. Wenn Sie 0.0.0.0 als Ziel-IP angeben, gilt diese Regel für alle Ziel-IP-Adressen.

Bestätigen Sie die Regel mit *OK*.

5.8.3 NAT

Jedes Datenpaket, das von einer internen Quelle ins Internet geht, wird automatisch mit der externen IP-Adresse der OctoGate maskiert. Hierfür ist also die Angabe expliziter Masquerading-Regeln nicht erforderlich. Es gibt aber Fälle, in denen die Angabe expliziter Regeln notwendig ist, insbesondere wenn dynamische Adressen verwendet werden.

Klicken Sie für die Anlage einer neuen Regel auf *Neuer Eintrag*.



Masquerade

Neuer Eintrag.

Beschreibung :

Protokoll :

Int OUT :

Quell-IP :

Ziel-IP :

Ziel-Port :

Geben Sie eine Beschreibung für Ihre Regel an, wählen Sie das Protokoll, für das diese Regel gelten soll und geben Sie das ausgehende Interface (*Int OUT*), mit dessen IP-Adresse die Datenpakete maskiert werden sollen. Als Bedingung für diese Regel können eine Quell-IP (0.0.0.0 = alle) und eine Ziel-IP (0.0.0.0 = alle) sowie ein Ziel-Port angegeben werden.

Verwenden Sie SNAT (Source NAT), um die Quell-IP eines Clients durch eine neue IP-Adresse zu ersetzen. Für die Anlage einer neuen SNAT-Regel klicken Sie auf *Neuer Eintrag*.

SNAT

Neuer Eintrag,

Beschreibung :

Protokoll :

Int OUT :

Quell-IP :

Quell-Port :

Ziel-IP :

Ziel-Port :

Quell-IP Neu :

Quell-Port Neu :

Geben Sie eine Beschreibung für die neue SNAT Regel an und bestimmen Sie das Protokoll sowie das Interface, für die diese Regel gelten soll. Geben Sie die Quell-IP/den Quell-Port, die durch eine neue Quell-IP/einen neuen Quell-Port ersetzt werden sollen. Geben Sie optional als Bedingung für diese Regel eine Ziel-IP/einen Ziel-Port an, für den diese Regel gelten soll.

5.9 Netzwerk

5.9.1 IP-Adressen

Hier können Sie die IP-Konfiguration der verschiedenen Netzwerk-Interfaces Ihrer OctoGate vornehmen. Sie können jedem Interface beliebig viele IP-Adressen zuordnen. Das Interface ist unter allen konfigurierten IP-Adressen erreichbar. Klicken Sie auf *Neuer Eintrag*:

IP-Konfiguration
Neuer Eintrag.

Name :

IP-Adresse :

Interface :

Subnetz :

Bit Dezimal

Geben Sie einen Namen für den neuen Eintrag an. Wählen Sie das zu konfigurierende Interface aus der Dropdown-Liste und geben Sie IP-Adresse für das Interface an. Geben Sie außerdem die zugehörige Subnetzmaske an (Bit- oder Dezimalschreibweise).

5.9.2 DHCP

Hier können Sie die automatische Vergabe von IP-Adressen an angeschlossene Clients für jedes Interface konfigurieren.

Klicken Sie unter *DHCP-Server* auf *Neuer Eintrag*, um DHCP an einem Interface zu aktivieren:

DHCP Server
Neuer Eintrag.

Interface :

DHCP Von :

DHCP Bis :

Lease Time * :

Wählen Sie zunächst aus der Dropdownliste das gewünschte Interface aus und geben Sie den gewünschten Adressbereich mit Start- und Endadresse des Vergabebereichs an. Im Pflichtfeld *Lease Time* geben Sie die Dauer der Zuordnung einer IP zu einem Client in Stunden an.

Verbindet sich nun ein Client in dem Netz, für das Sie DHCP aktiviert haben, erscheint dieser Client in der Tabelle *DHCP Clients*.

DHCP Server

Neuer Eintrag | Bearbeiten | Löschen | Verwerfen

Interface

Interface	DHCPVon	DHCPBis	LeaseTime
WLAN	192.168.111.100	192.168.111.150	48

Overview

DHCP Clients

Neuer Eintrag | Bearbeiten | Löschen | Verwerfen

Hostname

Hostname	Statisch	IPAdresse	MACAdresse	Lease
HP	<input type="checkbox"/>	192.168.111.124	64:31:50:84:25:12	23.06. 14:15

Overview

Die Spalte *Lease* zeigt den Zeitpunkt des Ablaufs der Adresszuordnung zu einem Client. Bestimmt wird dieser Zeitpunkt durch die *Lease Time* des zugehörigen Netzes. Wenn Sie eine vergebene IP-Adresse an einen Client dauerhaft an diesen Client binden wollen, so markieren Sie den Client und klicken auf *Bearbeiten* (bzw. führen einen Doppelklick auf dem Eintrag aus):

DHCP Clients

Datensatz bearbeiten.

Hostname:

Statisch *:

IP-Adresse:

MAC-Adresse:

Lease:

OK

Setzen Sie das Häkchen im Feld *Statisch*, um die aktuell zugeordnete Adresse dauerhaft zu vergeben.

5.9.3 Routing

Konfigurieren Sie hier Routen in ein anzugebendes Zielnetz. Legen Sie statische Routen an, indem sie in der Tabelle *Statisch* auf *Neuer Eintrag* klicken:

The screenshot shows a dialog box titled 'Statisch' with the subtitle 'Neuer Eintrag.'. It contains the following fields and controls:

- Name:** A text input field.
- Ziel:** An IP address input field with four segments, each containing the number '0'.
- Subnetz:** A dropdown menu showing '24'.
- Bit / Dezimal:** Two radio buttons, with 'Bit' selected.
- Gateway:** An IP address input field with four segments, each containing the number '0'.
- Buttons:** 'OK' and 'Abbrechen' at the bottom.

Geben Sie einen Namen für die Route an und die IP-Adresse mit Subnetzmaske des Zielnetzes sowie den Gateway, über den das Zielnetz erreichbar ist.

Sie können auch Routen für eingerichtete VPN-Clients anlegen. Klicken Sie hierfür in der Tabelle *VPN* auf *Neuer Eintrag*:

The screenshot shows a dialog box titled 'VPN' with the subtitle 'Neuer Eintrag.'. It contains the following fields and controls:

- Beschreibung:** A text input field.
- Client:** A dropdown menu showing 'ettest'.
- IP:** An IP address input field with four segments, each containing the number '0'.
- Subnetz:** A dropdown menu showing '24'.
- Bit / Dezimal:** Two radio buttons, with 'Bit' selected.
- Methode:** A dropdown menu showing 'Client-Route'.
- Buttons:** 'OK' and 'Abbrechen' at the bottom.

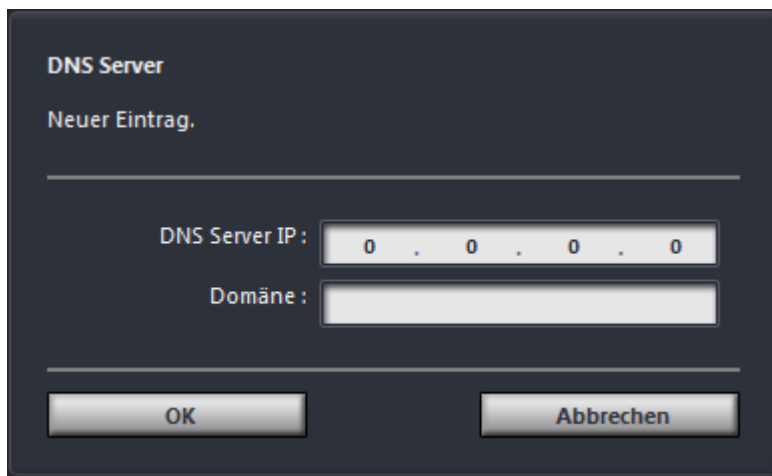
Geben Sie eine Beschreibung für die VPN-Route an und wählen Sie aus der Dropdownliste einen eingerichteten VPN-Client, für den Sie eine Route einrichten möchten. Weiterhin geben Sie den IP-

Adressbereich des Quellnetzes (Methode: Remote-Netz) bzw. des Zielnetzes (Methode: Client-Route) ein (IP und Subnetzmaskemaske) und wählen die Methode:

- Client-Route: Der ausgewählte VPN-Client erhält Zugriff auf den angegebenen IP-Adressbereich.
- Remote-Netz: Ein Remotenetz erhält über den ausgewählten VPN-Client Zugriff auf den angegebenen IP-Adressbereich.

5.9.4 DNS

Sie können mehrere DNS-Server anlegen. Klicken Sie dafür auf *Neuer Eintrag*:



DNS Server
Neuer Eintrag.

DNS Server IP : 0 . 0 . 0 . 0

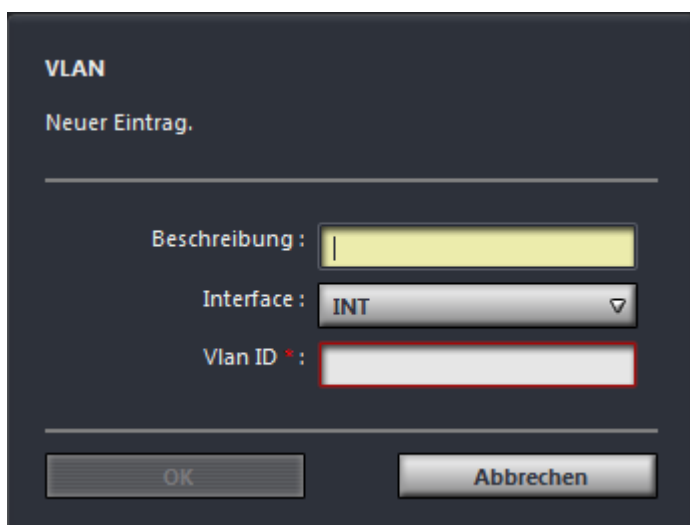
Domäne :

OK Abbrechen

Tragen Sie die IP-Adresse des DNS-Servers ein und geben Sie optional eine Domäne an, wenn Anfragen aus einer Domäne von diesem DNS-Server beantwortet werden sollen.

5.9.5 VLAN

Die OctoGate unterstützt mehrere virtuelle Netzwerke, die einem physischen Interface zugeordnet sind. Klicken Sie auf *Neuer Eintrag*, um ein neues, virtuelles LAN-Interface zu erstellen:



VLAN
Neuer Eintrag.

Beschreibung : |

Interface : INT ▾

Vlan ID * : |

OK Abbrechen

Geben Sie eine Beschreibung an und wählen Sie das Interface, an dem Sie das VLAN einrichten möchten. Schließlich müssen Sie eine ID vergeben (1-9999), anhand derer Sie dieses VLAN-Interface in allen Konfigurationsdialogen identifizieren können. Wenn Sie beispielsweise am Interface INT ein VLAN mit der ID 1 einrichten, finden Sie dieses VLAN Interface in den Dialogen wieder unter der Bezeichnung „VLAN_INT0001“.

5.10 VPN/Remote

In dieser Rubrik konfigurieren Sie unterschiedliche Wege des Fernzugriffs. Der Fernzugriff kann einerseits über gesicherte VPN-Tunnel erfolgen oder durch eine Benutzer-Authentifizierung, die von der OctoGate bei Zugriff von außen zwischengeschaltet wird.

5.10.1 OctoVPN-Clients

Folgende **Einstellungen** können Sie für jeden in der Tabelle aufgeführten **VPN-Client** vornehmen:

! **Anmerkung:** Sämtliche Änderungen, die Sie für einen VPN-Client vornehmen, müssen Sie mit einem Klick auf den Button *speichern* bestätigen. Sollte eine VPN-Verbindung des Clients, für den Änderungen vorgenommen wurden, bestehen, wird diese automatisch getrennt. Eine erneute Einwahl wird erforderlich.

- **Aktiv:** Sie können die Einwahl eines VPN Clients vorübergehend deaktivieren. Dieser kann zu jedem Zeitpunkt wieder aktiviert werden.
- **Passwort:** Vergeben Sie ein Passwort, welches für den Verbindungsaufbau gefordert werden soll.
- **Default Route:** Mit dieser Option leiten Sie den gesamten Internet-Traffic des VPN-Clients über die OctoGate. In diesem Falle wird auch der Datenverkehr des entfernten VPN-Users durch die Sicherheitsfunktionen der OctoGate geschützt. Es empfiehlt sich hier den VPN-Client auf dem entfernten Endgerät als Dienst zu konfigurieren. Nähere Informationen hierzu erhalten Sie in Kapitel 8.
- **Push DNS:** Sie können hier weiterhin für jeden VPN-Schlüssel festlegen, dass die OctoGate an diesen VPN-Client ihren DNS-Server vergibt. Dies ist sinnvoll um dem VPN-Client Adressen aus dem internen Netz bekannt zu machen (Beispiel: octo.octo). Diese Option ist automatisch aktiviert, wenn *Default Route* gewählt ist.
- **INT/DMZ/WLAN:** Wählen Sie die Ethernet-Ports, an denen die Netze angeschlossen sind, für die der VPN-Client Zugriff erhalten soll.
- **Fremdrouten:** Sie können unter Netzwerk/Routen (s. 5.9.3) VPN Routen konfigurieren. Damit die dort eingerichteten Routen gültig werden, muss hier die Option *Fremdrouten* aktiviert sein.
- **Name/Telefon/...:** Sie können Stammdaten des Benutzers für die Identifizierung eines VPN Clients hinterlegen. Diese Angaben sind optional.

Wenn Sie einen VPN-Client dauerhaft entfernen möchten, markieren Sie den zu löschenden VPN-Client und wählen Sie die Option *Löschen* aus der Titelleiste der Übersichtstabelle. Dabei ist zu beachten, dass der Name eines gelöschten Clients nicht erneut vergeben werden kann.

Weitere **VPN-Clients** können Sie über den Button „VPN Client erstellen“ **hinzufügen**; sollte die maximale Anzahl VPN-Clients bereits erreicht sein, nehmen Sie bitte Kontakt mit dem OctoGate-Support auf. Im folgenden Dialog geben Sie einen Namen für den Client ein.



The image shows a web-based dialog box for creating a new VPN client. The title bar indicates 'VPN-Client erstellen (Noch 17 verfügbar)'. The dialog contains several input fields for user information: Clientname, Tokenseriennummer, Benutzer, E-Mail, Telefon, Stadt, and Beschreibung. A 'VPN-Client generieren' button is positioned at the bottom right of the form.

Aus Gründen der Übersichtlichkeit empfiehlt sich hier der Name des VPN-Users. Wenn Sie einen VPN-Client mit Token-Sicherung erstellen, nehmen Sie den Tokenwerfer zur Hand und geben Sie die Seriennummer, die Sie auf der Rückseite des Tokenwerfers finden, in das Feld *Tokenseriennummer* ein. Der Tokenwerfer ist nun an die Verwendung mit diesem VPN-Client gekoppelt. Weitere Informationen zur Einrichtung finden Sie in Kapitel 8.

Es wird Ihnen in der Titelleiste dieses Dialogs angezeigt, wie viele VPN-Clients noch zur Verfügung stehen. Sollten Sie einen VPN Client benötigen, Ihnen aber kein VPN-Client mehr zur Verfügung stehen, wenden Sie sich bitte an Ihren OctoGate-Partner.

! **Anmerkung:** Es kann sein, dass Ihr VPN-Client-Name abgelehnt wird. Das kann daran liegen, dass in der Vergangenheit bereits einmal ein VPN-Client dieses Namens existierte und gelöscht wurde.

Es stehen Ihnen folgende **Downloads** zur Verfügung:

- *Download EXE:* Wählen Sie die ausführbare Installationsdatei, wenn der VPN-Client unter Windows (für Windows Betriebssysteme ab Version 2000) installiert werden soll. Die Installationsroutine prüft das Vorhandensein der VPN-Software, installiert diese gegebenenfalls und fügt den entsprechenden *VPN-Schlüssel* hinzu.

- Download ZIP: Wählen Sie das ZIP-Archiv, wenn Sie den VPN-Schlüssel für nicht-Windows-Systeme benötigen. Der Schlüssel ist kompatibel mit OpenVPN unter Linux oder der OpenVPN-Umsetzung „Tunnelblick“ für MacOS X.

5.10.2 Fernzugriff

Fernzugriffe werden für jeden Benutzer explizit konfiguriert. Wird versucht, mit dem Browser einen bestimmten Dienst (z.B. ein Webmail-Portal) hinter der OctoGate zu erreichen, wird auf eine Login-Seite zwangsumgeleitet, über die der Zugreifende sich mit seinen in der OctoGate hinterlegten Benutzerdaten zunächst anmelden muss. Die Benutzerdaten legen Sie – auch ohne aktiviertes Usermanagement – unter dem Menüpunkt Administration/Benutzer (s. Kapitel 5.4.2) an. Nach erfolgreicher Anmeldung wird der zugehörige Datenport für die Dauer der Kommunikation geöffnet und der Zugriff auf eine interne Ziel-IP gewährt. Dies bietet den Vorteil, dass die Ressource nur mit erfolgreicher Authentifizierung aus dem Internet erreichbar ist.

Klicken Sie oberhalb der Tabelle auf Neuer Eintrag, um einen Fernzugriff zu konfigurieren:



Geben Sie eine Beschreibung an (z.B. den Namen der Ressource, auf die zugegriffen werden soll) und wählen Sie einen Benutzer aus, der auf diese Ressource zugreifen darf. Soll der Zugriff nur von einer bestimmten Quell-IP zulässig sein, so geben Sie diese explizit im Feld Quell-IP an, andernfalls lassen Sie den Eintrag 0.0.0.0 unverändert. In dem Feld Ziel-IP geben Sie die IP-Adresse der Ressource an, auf die zugegriffen werden soll. Wenn Sie den Eintrag bei 0.0.0.0 belassen, ist Zugriff auf alle IP-Adressen der internen Netze möglich. Sie müssen jedoch einen Port angeben, über den der Zugriff von außen erfolgt. Bestätigen Sie Ihre Eingaben mit **OK**.

Fernzugriff

Geben Sie Ihre Zugangsdaten ein.

Benutzer:

Passwort:

Status:

Anmeldung erforderlich

Wird versucht, von außen auf den konfigurierten Port (im Beispiel Port 443) zuzugreifen, erscheint im Browser obige Login-Maske. Die Freischaltung des Ports erfolgt nur, wenn an dieser Stelle gültige Anmeldedaten eingegeben werden.

5.10.3 Mail-Relay

Wenn Sie das optionale Modul „Mail-Relay“ aktiviert haben (siehe 5.4.1) können Sie hier festlegen, für welche Mail-Domain die OctoGate zuständig sein soll:

- Geben Sie Ihre Mail-Domain beispielsweise in der Form *meine-firma.de* ein, wenn ihre Mailadressen von der Form *name@meine-firma.de* sind.
- Geben Sie optional die IP Ihres Mailservers an, an den die OctoGate alle eingehenden Mails weiterleiten soll.
- Wenn Sie das IP-Feld freilassen, fungiert die OctoGate für diese Domain selbst als Mailserver. In dem Fall müssen Sie die OctoGate als Mailserver in Ihrem *Mailprogramm* konfigurieren:

Eingehender Mailserver: octo.octo

Ausgehender Mailserver: octo.octo

Protokoll: Wahlweise IMAP oder POP3

Durch mehrfache Einträge können Sie mehrere Domains von der OctoGate verwalten lassen.

Unter *Mail-Forwarder* geben Sie die Zugangsdaten zu Ihrem Mail-Provider ein. Diese Informationen werden benötigt, um zu verschickende E-Mails an den Postausgangsserver beim Provider weiterzuleiten. „Speichern“ nach der Eintragung nicht vergessen!

5.11 OctoScan

In der *Übersicht* sehen Sie statistische Informationen über registrierte Clients sowie eine tabellarische Übersicht über alle derzeit laufenden Workstations und ihre jeweiligen Hostnamen. Sie können den Einträgen in der Tabelle die derzeit laufende OctoScan-Version sowie den jeweiligen Status einsehen. Das angegebene Datum bezieht sich auf die Anmeldung des Clients.

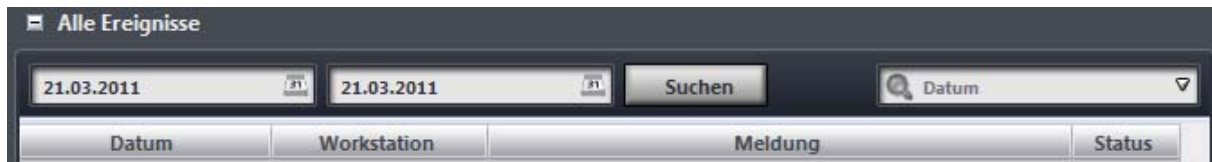
Unter *Einstellungen* können Sie globale Einstellungen vornehmen, die für alle Clients gelten (*Global*). Alternativ können Sie aus der Tabelle einzelne Workstations auswählen und für diese individuelle Konfigurationen vornehmen. Hierfür wählen Sie eine Workstation aus der Tabelle aus und klicken im Tabellenkopf auf *Bearbeiten*. Im folgenden Dialog müssen Sie die Option Globale Konfiguration überschreiben durch Setzen eines Hakens aktivieren, um individuelle Einstellungen vornehmen zu können.

Die im Folgenden beschriebenen Einstellungsoptionen gelten sowohl für die globale als auch für die individuelle Konfiguration:

- *Remote-Konfiguration aktivieren*: Aktivieren Sie diese Option um die clientseitige Konfiguration (s. Kapitel 2) zu deaktivieren und die Konfiguration ausschließlich remote vorzunehmen.
- *USB-Medien verweigern*: Aktivieren Sie diese Option, wenn Sie externe USB-Medien an den Clients nicht zulassen möchten.
- *Client verteilt Virendefinitionen*: Wenn ein bzw. alle Clients in der Lage sein sollen, aktuelle Virensignaturen untereinander auszutauschen, aktivieren Sie diese Option.
- *Suchmodus*: Legen Sie fest, bei welcher Aktion (Lesen/Ausführen/Schreiben) OctoScan auf Dateien zugreifen soll. Wählen Sie die Aktion *Lesen* für höchste Sicherheit.
- *Reaktion auf Fund*: Legen Sie hier fest, wie sich OctoScan bei einem Virenfund verhalten soll (Dialog anzeigen/in Quarantäne verschieben/Löschen).
- *Client-Stand verwenden*: Legen Sie hier fest, welche Programmversion bei einem automatischen Upgrade verwendet werden soll (Normal/Beta). Wenn Sie *Beta* wählen, werden auch Beta-Versionen als Upgrade installiert.
- *Log-Level*: Legen Sie hier fest, mit welchem Detail-Level Informationen in den Log-Dateien mitgeloggt werden sollen. *Debug* entspricht einem hohen Detailgrad, *Info* entspricht einem niedrigen Detailgrad.
- *Vom Scanvorgang ausschließen – Verzeichnisse/Dateiendungen*: Hier können Sie Verzeichnisse und Dateiendungen angeben, die vom Scanner ausgeschlossen werden sollen.
- *Automatischer Scandurchlauf*: Geben Sie hier die Parameter für einen automatischen Scandurchlauf an. Sie können optional den Scandurchlauf auf einzelne Verzeichnisse einschränken sowie das Startdatum, Uhrzeit und Intervall (ab Startdatum) in Tagen angeben.

Nach Eingabe aller Daten klicken Sie auf *Speichern*. Klicken Sie auf *Verwerfen*, wenn Sie vorgenommene Änderungen zurücksetzen möchten.

Weiterhin haben sie Zugriff auf unterschiedliche Logs, in denen Sie alle Ereignisse in chronologischer Reihenfolge in einer Tabelle aufgeführt sehen. Sie können im Tabellenkopf die Anzeige auf einen bestimmten Zeitraum einschränken, indem Sie das Start- und Enddatum des gewünschten Zeitfensters angeben und auf *Suchen* klicken.



Sie können die Listen auch filtern, indem Sie im Suchfeld rechts im Tabellenkopf zunächst den Spaltennamen auswählen und anschließend den Suchbegriff, nach dem gefiltert werden soll, eingeben. Sie können sich auf diese Weise beispielsweise alle Ereignisse eines bestimmten Hostnamens anzeigen lassen.

Folgende Logs stehen Ihnen zur Verfügung:

- Alle Ereignisse: Hier sehen Sie alle Informationen zusammengefasst, die die Workstations gemeldet haben.
- Virenfunde: Hier sehen Sie alle Virenfunde, die von den Workstations gemeldet wurden.
- Virendefinitionen: Hier entnehmen Sie wann welche Workstation das letzte Mal mit neuen Virendefinitionen versorgt wurde.
- Clients: Wählen Sie im Tabellenkopf den Zeitraum in Tagen, in dem sich bis zum aktuellen Zeitpunkt Clients nicht mehr gemeldet haben.

5.12 OctoGuest

OctoGate Guest ermöglicht es, zeitlich limitierte Zugangscodes zu generieren, die den Zugang zum Internet über die OctoGate für eine definierte Dauer ermöglichen. Dies ist beispielsweise in Hotels sinnvoll, wenn Gästen der Zugang zum Internet gewährt werden soll.

Die Anmeldung erfolgt in einem eigenen physikalischen Netz. Wenn aus diesem Netz eine Anforderung kommt, wird auf ein Login-Portal der OctoGate zwangsumgeleitet. Idealerweise wird ein Gästernetz in Kombination mit einem WLAN-Accesspoint betrieben, der an dem für das Gästernetz konfigurierten LAN-Port der OctoGate angeschlossen wird.

5.12.1 Einstellungen

Wählen Sie unter *Einstellungen* das Interface, an dem das Gästernetz betrieben werden soll. Aktivieren Sie die Option *Transparenter Proxy*, wenn der Datenverkehr transparent gefiltert werden soll.



Wenn Sie den transparenten Proxy aktivieren, müssen Sie folgende Punkte - je nach Ausstattung Ihrer OctoGate beachten:

- Wenn Sie über das Modul Usermanagement verfügen und dieses aktiviert haben sollten Sie einen User anlegen, der im Mixed Mode-Modus arbeitet und über den IP-Adressbereich des Gästernetz identifiziert wird.

Beispiel: Das Gästernetz vergibt IP Adressen im Bereich 192.168.3.xxx (DHCP-Konfiguration siehe Abschnitt 5.9.2). Sie legen daher einen User mit folgenden Daten an (siehe Abschnitt 5.7.3):

- Benutzername: beliebig
 - Profil: Weisen Sie das Profil zu, dessen Einstellungen für alle Gäste gelten sollen
 - E-Mail: beliebig
 - Passwort: beliebig
 - IP-Netz: 192.168.3.0
 - Subnetz: 24 Bit bzw. 255.255.255.0
 - Mixed Mode aktiviert
- Wenn Sie den Contentfilter ohne aktiviertes Usermanagement einsetzen, so gelten die Einstellungen des Contentfilters sowohl für das interne Netz als auch für Gästernetz

Im Gästernetz sind grundsätzlich alle Ports offen, um Gäste, die über das Gästernetz ins Internet gehen in ihrem Nutzungsverhalten nicht eingeschränkt werden. So werden beispielsweise VPN-Verbindungen oder die Nutzung von Chat- und Kommunikationsprogrammen nicht beeinträchtigt.

5.12.2 Zugangscodes

Generieren Sie hier Zugangscodes mit von Ihnen gewählter Gültigkeitsdauer:



The screenshot shows a web interface titled "Codes Generieren". It features three input fields for configuration: "Gültigkeit (Tage:Stunden:Minuten)" with values 1, 00, and 00; "Anzahl Codes" with the value 10; and a "Codes generieren" button.

Geben Sie die Gültigkeit in Tag/Stunden/Minuten an, tragen Sie die Anzahl zu generierenden Zugangscodes ein und klicken Sie auf *Codes generieren*. Es folgt unmittelbar ein Speichern-Unter-Dialog, der es Ihnen erlaubt, die soeben generierten Codes als CSV-Datei abzuspeichern. Diese Datei dient dazu, die Codes ausdrucken und verfügbar machen zu können.

Alle bisher generierten Zugangscodes werden in der Übersichtstabelle angezeigt. Die gesamte Liste können Sie jederzeit ins CSV-Format exportieren und abspeichern, indem Sie im unteren Tabellenrand auf *Export* klicken.

Gastzugang

Geben Sie hier Ihren Zugangscode ein.

Code:

Ihre IP: 10.12.12.12

Status:

Freischaltung erforderlich

Wird versucht, über das Gästernetz auf das Internet zuzugreifen, wird auf obige Login-Maske umgeleitet. Hier muss nun ein gültiger Zugangscode eingegeben werden. Daraufhin ist die in der Makse angezeigte IP-Adresse für die Gültigkeitsdauer des Zugangscode freigegeben. Der Inhaber des Zugangscode kann jedoch sein Endgerät wechseln. In diesem Falle wird die Login-Maske erneut angezeigt und der Benutzer kann seinen Zugangscode erneut eingeben. Der Zugangscode wird nicht an die IP-Adresse gekoppelt. Innerhalb der Gültigkeitsdauer kann der Zugangscode mit beliebigen Endgeräten genutzt werden.

6 Berichte / Reporter

Um auf die Statistiken und Auswertungen des OctoGate Reporting-Systems zugreifen zu können, ist ein spezielles *Reporter-Passwort* notwendig, um die Administration der OctoGate und den Zugriff auf datenschutzrechtlich relevante Daten zu trennen. Das Passwort erhalten Sie über den OctoGate Support.

6.1 Zugriff auf Reports

Melden Sie sich über die GUI mit folgenden Benutzerdaten an:

Benutzername: reporter

Kennwort: *Reporter-Passwort* (wenden Sie sich für dieses Passwort an den OctoGate-Support)

Das folgende Menü der WebGUI erlaubt ausschließlich Zugriff auf die Berichte:

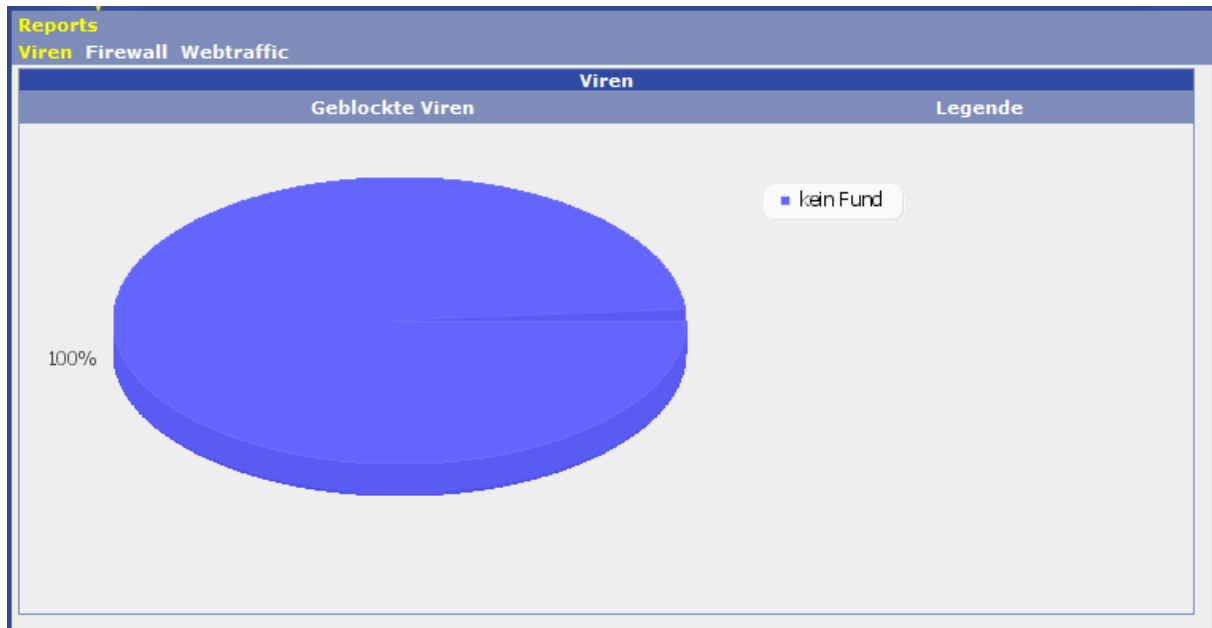


Sie werden nach Klick auf Berichte auf ein separates Fenster umgeleitet, das die Statistikfunktionen der OctoGate unter einer eigenen Oberfläche anzeigt. Beachten Sie gegebenenfalls, dass Ihr Browser für diesen Vorgang Popup-Fenster zulässt.

Das OctoGate-Reporting bietet Ihnen Zugriff auf drei Bereiche: Viren, Firewall und Webtraffic, die in den folgenden Abschnitten näher erläutert werden.

6.1.1 Viren

Dieser Menüpunkt bietet Ihnen eine Übersicht über die von Ihrer OctoGate geblockten Viren, Trojaner etc., die Ihrem System ohne Schutz Schaden zugefügt hätten.

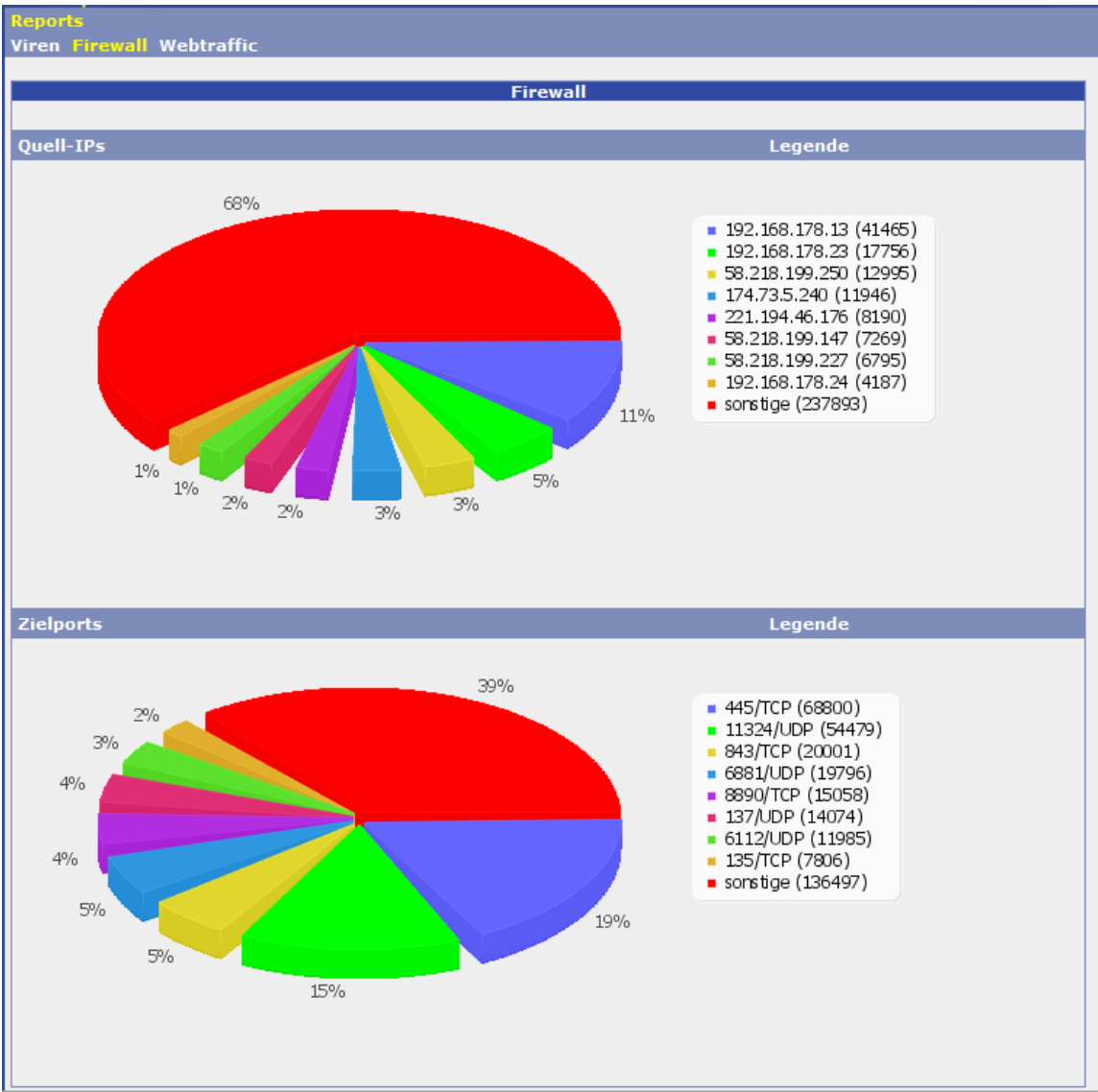


6.1.2 Firewall

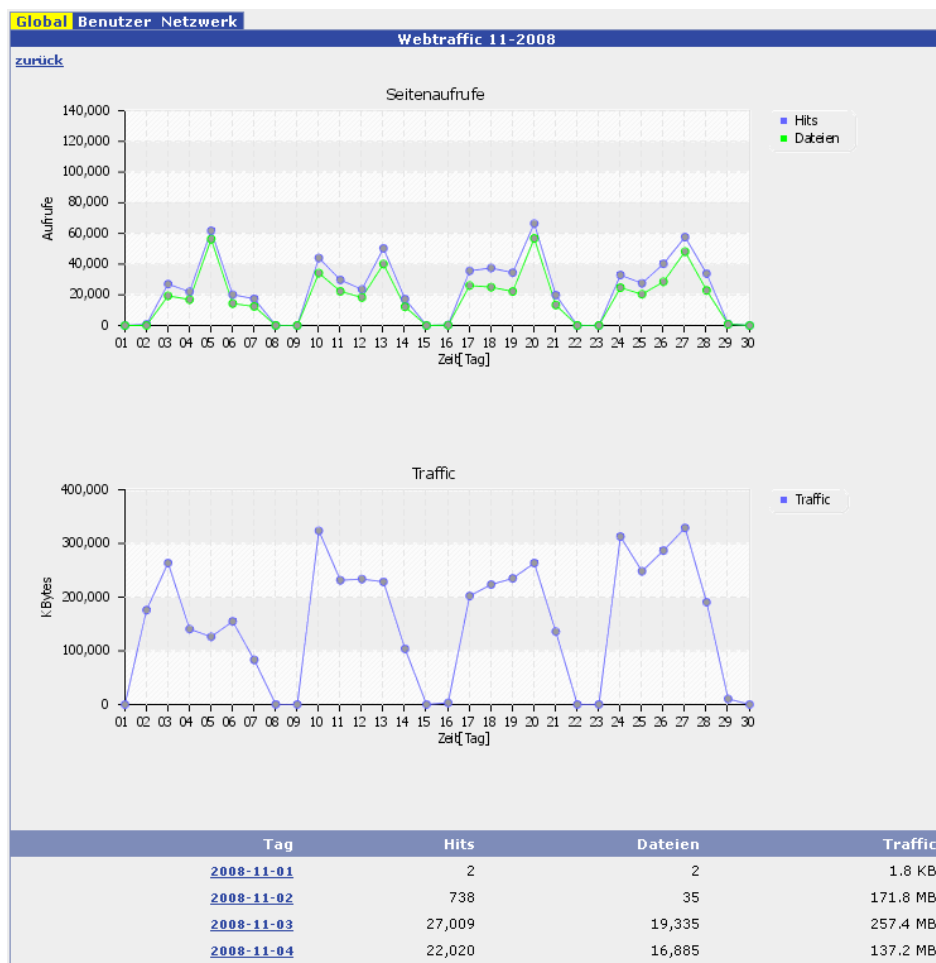
Hier erhalten Sie eine Übersicht über geblockte Angriffe und unerlaubte Verbindungsversuche.

Im oberen Bereich der Seite sehen Sie eine Übersicht über die geblockten Angriffe in Form eines Kreisdiagramms, das Ihnen die absolute Anzahl an Verbindungsversuchen anzeigt. Auf der rechten Seite sind die im Kreisdiagramm verwendeten Farben den zugehörigen IP-Adressen zugeordnet.

Im unteren Teil der Seite sehen Sie die geblockten Hosts nach Portnummern in Form eines Kreisdiagramms, das Ihnen die absolute Anzahl an Verbindungsversuchen anzeigt. Auf der rechten Seite sind die im Kreisdiagramm verwendeten Farben den zugehörigen Portnummern zugeordnet.



6.1.3 Webtraffic



Die Grafiken zeigen nun den Verlauf über die Tage des angezeigten Monats. Details zu den einzelnen Tagen können Sie wiederum einsehen, indem Sie einen Tag aus der unteren Liste auswählen.

Klicken Sie oben links auf *zurück*, um zur Ausgangsansicht zurückzukehren.

Sowohl in der Wochendetailansicht als auch in der Tagesdetailansicht sehen Sie eine Übersicht über die in dem jeweiligen Zeitraum am häufigsten aufgerufenen Internetseiten und die am häufigsten zurückgegebenen Antwortcodes:

URL	Hits	Traffic
http://80.237.225.168	102,806	34.7 MB
http://push.teleboerse.de	54,731	56.6 MB
http://www.n-tv.de	22,939	172 MB
http://suchen.mobile.de	20,430	23.8 MB
http://images.gmx.net	10,566	5 MB
http://www.paderline.com	10,160	87.7 MB
http://www.schwackenet.de	9,787	34.9 MB
http://www.mobile.de	8,538	7.5 MB
http://static.gmx.net	8,508	4.8 MB
http://ad.de.doubleclick.net	8,392	8.7 MB
http://www.google-analytics.com	8,359	4.7 MB
http://de.buvvip.com	8,266	105.8 MB
http://www.teleboerse.de	6,821	1.7 MB
http://portal.gmx.net	6,604	17.3 MB
http://de.mq40.mail.yahoo.com	6,512	32.2 MB
http://www.t-online.de	5,821	25.5 MB
http://kurse.teleboerse.de	5,629	27.4 MB
http://www.sport1.de	5,486	40.3 MB
http://www.awq-leasing.de	5,184	17.4 MB
http://pics.ebaystatic.com	4,987	25.6 MB

Antwort Code	Hits	Traffic
OK (200)	8,318	3.9 GB
No Content (204)	52	556.3 KB
Partial Content (206)	30	282.3 MB
Moved Permanently (301)	370	1.8 MB
Moved Temporarily (302)	1,475	17.9 MB
See Other (303)	9	30.3 KB
Not Modified (304)	1,645	45.4 MB
Bad Request (400)	7	9.7 KB
Unauthorized (401)	12	23.5 KB
Forbidden (403)	30	92.7 KB
Not Found (404)	604	13.4 MB
Proxy Authentication Required (407)	679	5.8 MB
Gone (410)	8	31.3 KB
Internal Server Error (500)	11	372.6 KB
Bad Gateway (502)	33	2.8 MB
Service Unavailable (503)	76	250.1 KB
Gateway Timeout (504)	11	52.3 KB
Unbekannter Fehler	147	37.3 KB

6.1.3.1 Benutzer

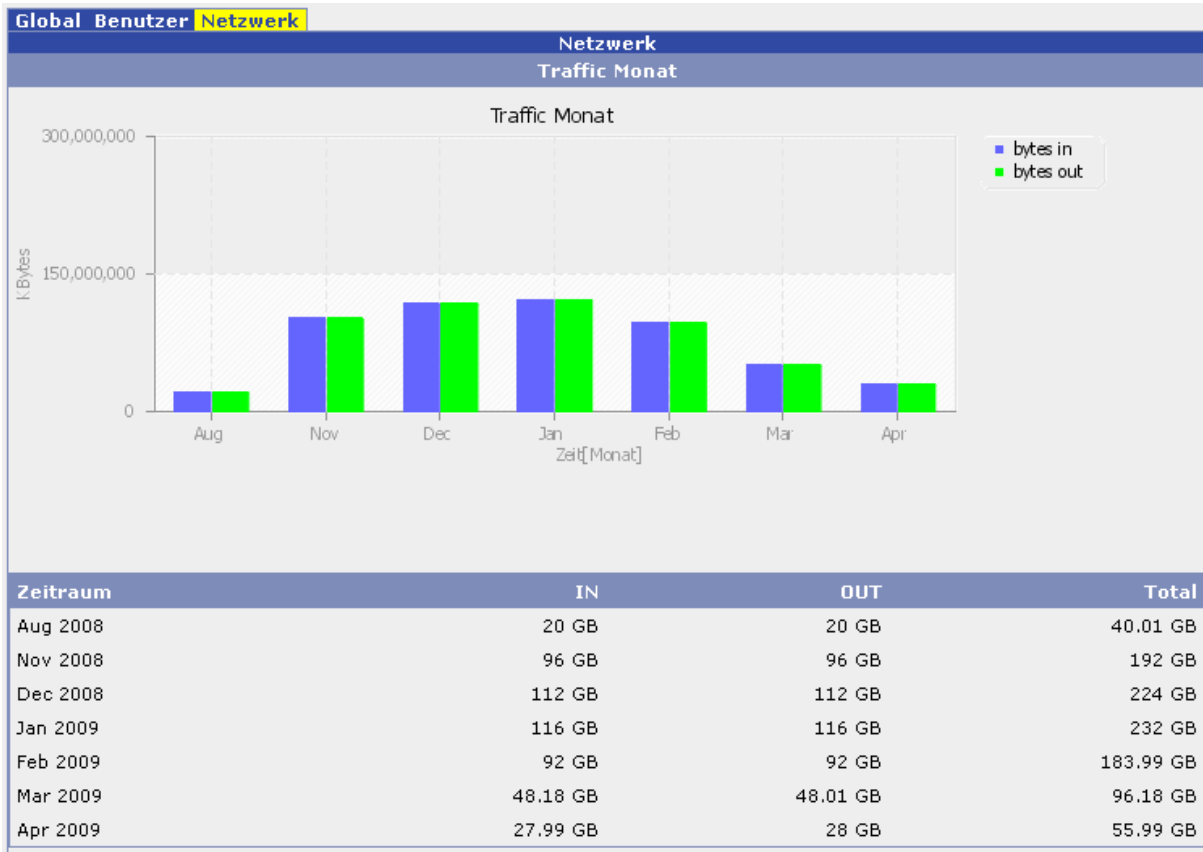
Klicken Sie auf den Reiter Benutzer, um für jeden eingerichteten Benutzer (wenn User-Management eingerichtet ist) bzw. für jede IP-Adresse der angeschlossenen PCs eine detaillierte Auswertung über besuchte Seiten zu erhalten.

Wählen Sie aus den Dropdown-Feldern den Benutzer/die IP-Adresse sowie den gewünschten Stichtag aus, um für diesen Tag detaillierte Informationen über den durch diesen User/Arbeitsplatz verursachten Internet-Traffic zu erhalten.

6.1.3.2 Netzwerk

Unter dem Reiter *Netzwerk* erhalten Sie eine Übersicht über den gesamten ein- und ausgehenden Datenverkehr, unabhängig über welches Protokoll der Datenverkehr stattgefunden hat.

Die Daten werden Ihnen grafisch aufbereitet sowohl Monat-, Tag-, als auch Stunden-basiert präsentiert. Die folgende Abbildung zeigt Ihnen beispielhaft die monatsbasierte Darstellung.



7 Der OctoGate RemoteSupport

Bei dem *OctoGate RemoteSupport*-Client handelt es sich um ein kleines Softwaretool auf Basis des *Teamviewer-Clients*, das es dem OctoGate-Support ermöglicht, eine Fernwartung direkt auf Ihrem PC durchzuführen. Sollten Sie also Hilfe durch den OctoGate-Support beispielsweise bei der korrekten Konfiguration Ihres PCs benötigen, verwenden Sie den OctoGate RemoteSupport-Client, um diese Hilfestellung vorzubereiten.

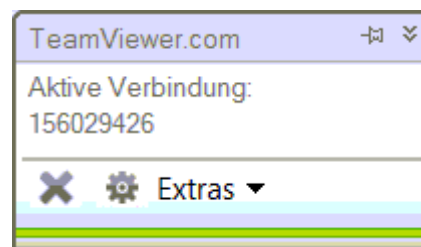
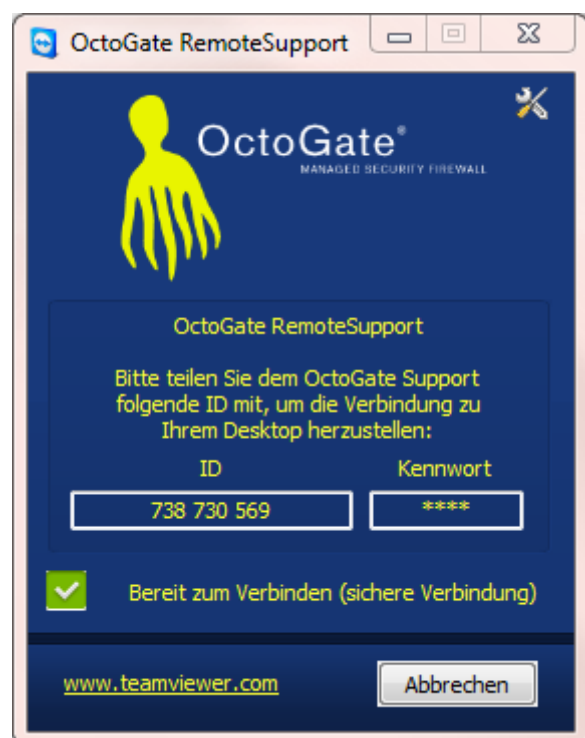
Laden Sie sich den OctoGate RemoteSupport-Client über den Link *Downloads* in der Titelleiste der WebGUI herunter. Eine Installation ist nicht erforderlich.

Starten Sie den Client, indem Sie auf die heruntergeladene Datei doppelklicken; Sie sehen den hier abgebildeten Sitzungs-Dialog.

Rufen Sie den OctoGate Support an und beschreiben Sie Ihr Problem.

Teilen Sie dem Support die gezeigte ID Ihrer Sitzung mit, damit dieser eine Verbindung zu Ihrem Desktop herstellen kann. Nach Verbindung mit Ihrem Desktop erhält der OctoGate-Support Zugriff auf Ihren Rechner und ist in der Lage, Ihren Rechner fernzusteuern.

Um die Verbindung zu beenden, schließen Sie die Verbindung, indem Sie in dem kleinen Steuerfenster auf das Kreuz zum Schließen der Verbindung klicken.



8 Der VPN-Client

Eine VPN-Verbindung ermöglicht Ihnen eine sichere Verbindung von außen über einen so genannten Tunnel durch das Internet zu Ihrem Netzwerk. Hierfür müssen Sie die VPN-Client Software samt VPN-Schlüssel auf Ihrem Endgerät installieren.

Die Client Software ist verfügbar für alle aktuellen Windows Versionen, inkl. der 64-Bit Versionen von Windows XP, Vista und 2003 Server. Darüber hinaus sind VPN-Clients auch für Linux und Unix, MacOS sowie Windows Mobile verfügbar, so dass Sie auch eine Vielzahl von PDAs und SmartPhones für den Aufbau von VPN-Verbindungen verwenden können.

Die **Verbindung** lässt sich zusätzlich **durch einen Token** und/oder ein Passwort (siehe unten) **absichern**, um ein Maximum an Sicherheit zu gewährleisten, da ohne Passwort bzw. ohne Token ein Verbindungsaufbau unmöglich ist. Die Absicherung mittels Token ist optional und benötigt für die Einwahl einen Tokenwerfer ähnlich dem hier abgebildeten:



Betätigen des Knopfes links vom Display des Tokenwerfers generiert eine achtstellige Nummer – den so genannten Token - der für die Authentifizierung bei jeder Verbindungsherstellung einzugeben ist. Für jeden Verbindungsaufbau wird eine neue Nummer generiert.

Alternativ oder zusätzlich lässt sich eine **VPN-Verbindung** auch **mit einem Passwort sichern**. Die Einrichtung eines Passworts ist für jeden VPN-Schlüssel möglich. Wünschen Sie die Absicherung über ein Passwort, wenden Sie sich bitte an den OctoGate-Support. Dieser wird den VPN-Server auf Ihrer OctoGate entsprechend konfigurieren, so dass für jeden von Ihnen erstellten VPN-Client ein Passwort automatisch generiert wird.

Einrichtung

8.1.1 Windows-Betriebssysteme

Die OctoGate VPN-Clients laufen unter allen Windows Versionen ab Windows 2000. Bitte beachten Sie, dass für die Installation des VPN-Clients Administratorrechte erforderlich sind.

Download und Erstellung eines VPN-Clients nimmt der Administrator-User vor (siehe Kapitel 5.10).

8.1.1.1 VPN-Client installieren

Für die Einrichtung eines VPN-Clients unter Windows NT, 2000, XP und Vista erhalten Sie von Ihrem Administrator eine ausführbare Datei. Ausführen dieser Datei startet den VPN-Client-Installer mit der Frage, ob Sie den VPN-Key importieren möchten.

Sollten Sie bereits einen OctoGate VPN-Key auf Ihrem System installiert haben, wird dieser Key Ihrer bestehenden Installation hinzugefügt, andernfalls wird der Client komplett neu auf Ihrem System eingerichtet.



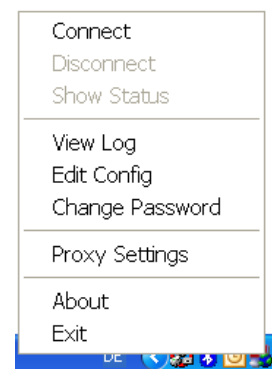
OctoVPN-Max_Mustermann-installer.exe



8.1.1.2 Manueller Verbindungsaufbau

Der VPN-Client integriert sich im Windows System-Tray (Fußzeile Ihres Desktop), von wo aus Sie eine **Verbindung** bequem **manuell starten** und stoppen können. Ein Rechtsklick auf „OpenVPN GUI“ öffnet das abgebildete Menü und ein Klick auf „Connect“ baut die VPN-Verbindung auf.

Sollte es sich um einen VPN-Client mit Token-Authentifizierung handeln, ist für den erfolgreichen Verbindungsaufbau die Eingabe von Logindaten notwendig.



In dem Fall geben Sie als *Username* den Namen des VPN-Clients an (vgl. Übersicht in Kapitel 5.10). Das *Passwort* setzt sich zusammen aus dem automatisch generierten 4-stelligen Passwort (einsehbar in der VPN-Client-Übersicht, siehe Kapitel 5.10) und der 8-stelligen Nummernfolge, die vom Tokenwerfer generiert wird.

8.1.1.3 Automatischer Verbindungsaufbau

Alternativ zu dem manuellen Verbindungsaufbau lässt sich der VPN-Client auch als Windows-Systemdienst starten. Dieser stellt mit Hochfahren des Systems automatisch eine gesicherte VPN-Verbindung zur OctoGate her. Es müssen jedoch einige Voraussetzungen für den automatischen Verbindungsaufbau über den Systemdienst erfüllt sein:

- Der Benutzer muss Administrator-Rechte besitzen
- Es darf nur ein VPN-Schlüssel installiert sein (keine Auswahl möglich)
- Der VPN-Schlüssel darf nicht mit einem Passwort oder Token gesichert sein, da der Systemdienst keine Benutzereingaben entgegennehmen kann

Sollte einer der genannten Punkte bei Ihnen nicht erfüllt sein, müssen Sie die Verbindung wie oben beschrieben manuell herstellen.

8.1.1.4 Aktivierung des Systemdienstes

Der Systemdienst wird mit dem VPN-Client installiert, muss jedoch manuell aktiviert werden:

- Öffnen Sie die Windows „Systemsteuerung“ und gehen Sie über „Verwaltung→Dienste“ (bzw. „Leistung+Wartung→Verwaltung“) zur Liste der auf Ihrem System installierten Systemdienste.
- Wählen Sie den Dienst „OpenVPN Service“, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen Sie „Eigenschaften“.
- In diesem Dialog wählen Sie Starttyp: „Automatisch“. Bestätigen Sie Ihre Änderungen mit OK.

Von nun an wird die VPN-Verbindung automatisch gestartet.

8.1.2 Windows Mobile

Für mobile Endgeräte wie PDAs und SmartPhones, die auf *Windows Mobile* basieren, können Sie über den OctoGate-Support spezielle VPN-Clients beziehen, die speziell auf die Version Ihres mobilen Endgeräts zugeschnitten sind.

8.1.3 Linux, MacOS X

Für alle weiteren Betriebssysteme stehen Ihnen VPN-Clients im Rahmen des OpenVPN-Projekts im Internet zur Verfügung, die Sie in Verbindung mit den VPN-Schlüsseln, die der Administrator-User über die WebGUI der OctoGate separat als komprimierte Datei herunterladen kann (siehe Kapitel 5.10), genutzt werden können.

Selbstverständlich steht Ihnen der OctoGate-Support bei Fragen und für Hilfestellung zur Verfügung.

9 OctoScan Client

Nach Installation verbirgt sich der OctoScan Client im System Tray von Windows. Ein Doppelklick auf das Symbol holt die Benutzeroberfläche des OctoScan Clients in den Vordergrund.

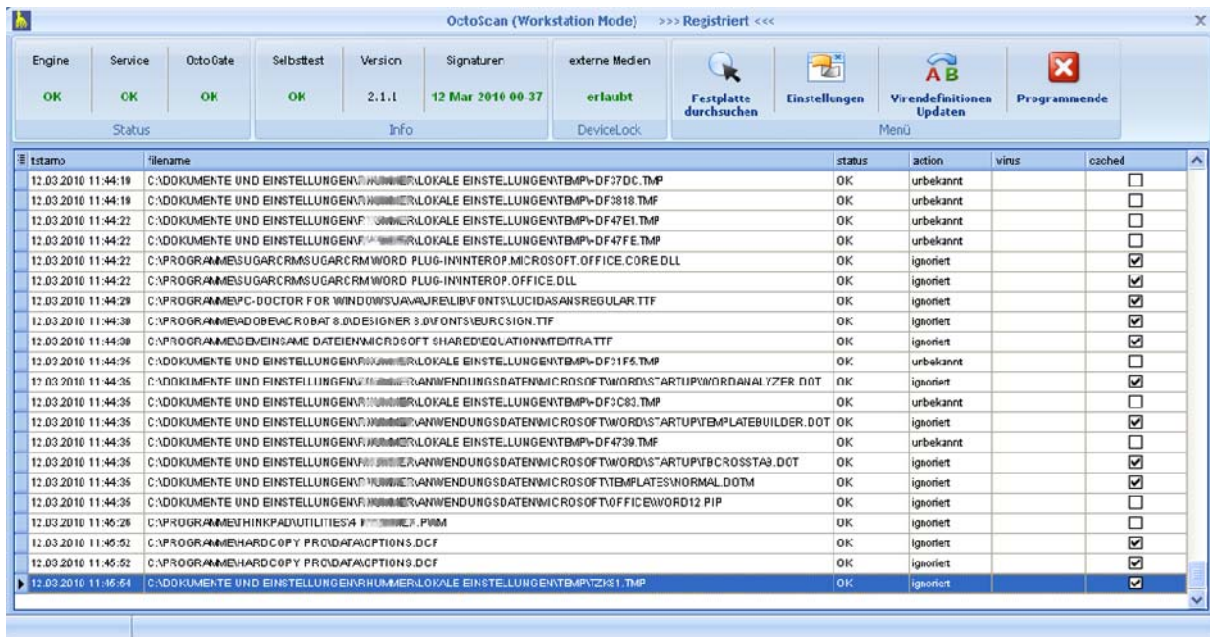


Abbildung 1: OctoScan - Hauptfenster mit Live-Log

Über diese Oberfläche kann der Benutzer folgende Funktionen direkt über den Client aufrufen:

- *Festplatte durchsuchen*: Im folgenden Dialog kann ein beliebiges Laufwerk oder Verzeichnis (oder Netzlaufwerk) für einen manuellen Virensuchlauf ausgewählt werden. Dieser Suchlauf kann jederzeit durch einen Klick auf *Festplattenscan abbrechen* unterbrochen werden.
- *Einstellungen*: Sofern der Administrator dies zulässt, können direkt am Client Konfigurationseinstellungen vorgenommen werden. Werden die Einstellungen ausschließlich Remote vorgenommen

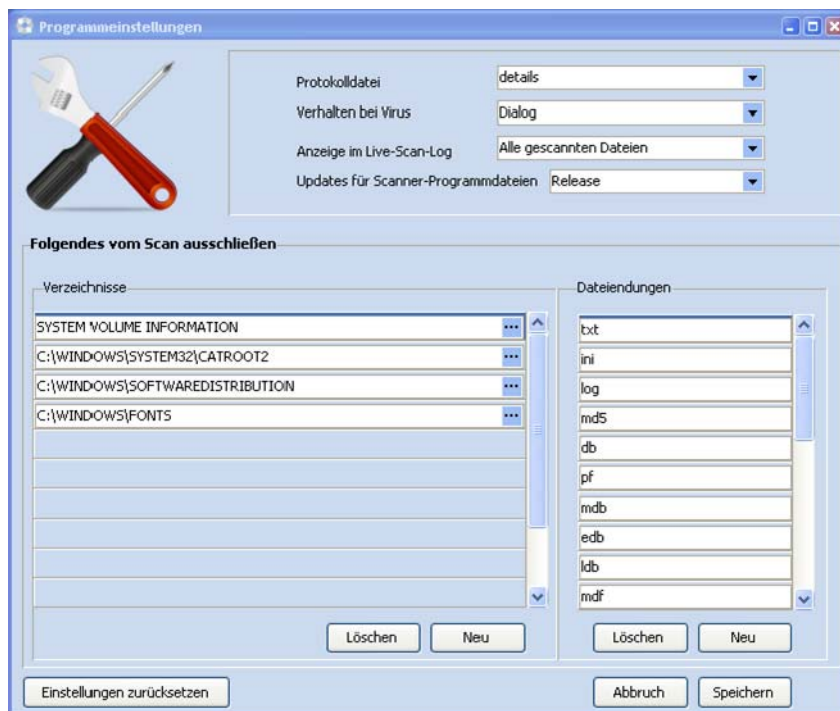


Abbildung 2: OctoScan - Programmeinstellungen

Folgende Einstellungen können über diesen Dialog vorgenommen werden:

- *Verhalten bei Virus*: Hier kann definiert werden, wie OctoScan bei einem Virenfund vorgehen soll: *Dialog* (Standard) zeigt bei Fund einen Auswahldialog, in dem der Benutzer über das weitere Vorgehen entscheiden kann. Außerdem stehen die Auswahlmöglichkeiten Löschen (löscht die kritische Datei automatisch), Blockieren (Blockiert die Datei) oder Quarantäne (Verschiebt die kritische Datei in den Quarantänebereich) zur Verfügung.
- *Anzeige im Live-Scan-Log*: Diese Einstellung bestimmt, welche Aktionen im Live-Log des Hauptfensters angezeigt werden. *Alle gescannten Dateien* zeigt sämtliche Dateien an, die gescannt werden, *Nur Virusmeldungen* zeigt ausschließlich erkannte Viren an.
- *Updates für Scanner-Programmdateien*: Diese Einstellung bestimmt, wie mit Upgrades der Programmdateien verfahren wird: *Release*: lediglich Release-Versionen werden installiert, *Testing* (Beta-Versionen): Neben den Releaseversionen werde auch Zwischenversionen (Beta-Versionen) installiert, die noch nicht als Releaseversion freigegeben wurden, *Kein Update*: Es werden keine Programm-Upgrades installiert.
- *Verzeichnisse/Dateiendungen*: Hier können Verzeichnisse oder Dateiendungen eingetragen werden, die vom Hintergrundscan ausgeschlossen werden sollen. Sie können Verzeichnisse oder Dateiendungen auch direkt aus dem Live-Log heraus vom Scanvorgang ausschließen, indem Sie mit der rechten Maustaste im Live-Log des Hauptfensters auf einen Eintrag klicken und diese dann im Kontextmenü die entsprechende Option wählen.

- *Virendefinitionen updaten*: Über diesen Button kann ein manuelles Update der Virensignaturen gestartet werden. OctoScan prüft regelmäßig im Hintergrund, ob neue Virensignaturen verfügbar sind.
- *Programmende*: Beendet die Konfigurationsoberfläche. OctoScan läuft als Dienst im Hintergrund weiter, so dass der Virenschutz weiterhin gewährleistet ist. Ein Neustart der Oberfläche kann jederzeit über das Windows-Startmenü vorgenommen werden.

Im OctoScan-Hauptfenster können Sie sich mit den Tastenkombinationen Strg+F6 bis Strg+F8 weitere Logs anzeigen lassen. Mit der Tastenkombination Strg+F5 gelangen Sie wieder zum Live-Log.

10 Fehlersuche

Hier finden Sie zu einigen Fehlerquellen Erste-Hilfe-Vorschläge, die sie bequem selber durchführen können, bevor Sie sich an Ihren OctoGate Support wenden.

10.1 E-Mail Versand

Wenn Sie beim Versuch, eine E-Mail zu versenden, wiederholt eine Fehlermeldung erhalten, kann das an fehlerhaft eingestellten Server-Zeitlimits liegen. Führen Sie bitte die für Ihren E-Mail-Client angegebenen Schritte durch.

10.1.1 Microsoft Outlook Express

- Wählen Sie im Menü "Extras" den Eintrag "Konten" aus
- Aktivieren Sie den Reiter „E-Mail“ und markieren Sie Ihr E-Mail Konto
- Klicken Sie auf „Eigenschaften“
- Stellen Sie im Reiter „Erweitert“ die Option „Zeitlimit des Servers“ auf die maximale Höhe ein
- Klicken Sie auf „Übernehmen“ und bestätigen Sie dann mit dem OK-Button
- Dann betätigen Sie im Fenster „Internetkonten“ den Button „Schließen“

10.1.2 Microsoft Office Outlook

- Wählen Sie im Menü "Extras" den Eintrag "E-Mail-Konten..." aus
- Wählen Sie dann die Option „Vorhandene E-Mail-Konten anzeigen oder bearbeiten“ und klicken Sie auf den Button „Weiter“
- Markieren Sie Ihr E-Mail-Konto und klicken Sie auf „Ändern“
- Klicken Sie den Button „Weitere Einstellungen..." an
- Stellen Sie den Schieber „Servertimeout“ auf maximale Höhe
- Bestätigen Sie mit dem OK-Button
- Zum Abschluss der Einstellungen klicken Sie in dem Fenster „E-Mail-Konten“ unten rechts auf den Button „Weiter“ und bestätigen mit einem Klick auf den Button „Fertigstellen“

10.1.3 Mozilla Thunderbird

Der *Mozilla Thunderbird* benötigt die genannten Einstellungen nicht. Sollten Sie trotzdem Schwierigkeiten haben, Mails zu versenden, kontaktieren Sie bitte unseren Support.

10.2 Webzugang / Proxykonfiguration

Wenn Sie das User-Management nutzen muss jeder Benutzer in seinem Web-Browser die OctoGate als Proxy eintragen, da sonst die Zuordnung der Profile nicht angewandt werden kann und kein Internetzugang möglich ist (Ausnahme: Zugriff im *Mixed-Mode*, siehe Abschnitt 5.4.2).

- Nach Eintragung des Proxy werden Sie beim ersten Webzugriff aufgefordert, sich mit einem Login und einem Passwort dem Proxy gegenüber zu identifizieren. (vgl. Kapitel 5.7.3).
- Zur Nutzung sicherer https-Verbindungen ist es ebenfalls notwendig, den Proxy im Browser einzutragen.

Im Folgenden wird dieser Vorgang für den *Internet Explorer* und den *Mozilla Firefox* erklärt².

10.2.1 Microsoft Internet Explorer

Im Regelfall sollte der Internet Explorer die Proxyeinstellungen automatisch von der OctoGate übernehmen. Sollten Sie dies überprüfen wollen, führen Sie folgende Schritte aus:

- Wählen Sie im Menü „Extras“ den Eintrag „Internet-Einstellungen“
- Wählen Sie den Reiter „Verbindungen“ aus
- Klicken Sie im Bereich „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“
- Im Fenster „Einstellungen für lokales Netzwerk“ haben Sie zwei Möglichkeiten:
 1. Aktivieren Sie im Bereich Proxyserver die Option „Proxyserver für LAN verwenden“ und tragen Sie den Hostnamen bzw. die IP-Adresse Ihrer OctoGate ein. Klicken Sie dann auf die Schaltfläche „Erweitert“ und aktivieren Sie die Option „Für alle Protokolle denselben Server verwenden“
 2. Markieren Sie die Checkbox „Automatisches Konfigurationsskript verwenden“ und tragen Sie in das Adressfeld die Adresse `http://octo.octo/proxy.pac` ein.
- Klicken Sie in diesem und dem darunter liegenden Fenster die Schaltfläche „Ok“ an

10.2.2 Mozilla Firefox

- Wählen Sie im Menü „Extras“ den Eintrag „Einstellungen...“
- Im Reiter „Erweitert“ die Schaltfläche „Verbindungs-Einstellungen“ anklicken
- Jetzt haben Sie zwei Möglichkeiten:
 1. Manuelle Proxy-Konfiguration auswählen und die IP-Adresse oder den Hostnamen der OctoGate eintragen und die Auswahl „Für alle Protokolle diesen Proxyserver verwenden“ markieren
 2. „Automatische Proxy-Konfigurations URL“ auswählen und in das Adressfeld die URL `http://octo.octo/proxy.pac` eintragen
- Klicken Sie in diesem und dem darunter liegenden Fenster die Schaltfläche „Ok“ an

² Versionen *Mozilla Firefox 3.5.5* und *Internet Explorer 8.0.6* bis auf minimale Abweichungen identische Vorgehensweise

10.3 FTP

Überprüfen Sie, ob in Ihrer Konfiguration der Port 21 freigeschaltet ist. Bei weiteren Problemen setzen Sie sich bitte mit unserem Support in Verbindung.

10.4 VoIP

Um VoIP zu nutzen, müssen Sie auf den jeweiligen Endgeräten Ihre OctoGate als Proxy eintragen. Wie Sie einen Proxy bei Ihrem Gerät eintragen entnehmen Sie bitte dem Handbuch des entsprechenden Gerätes.

10.5 Instant Messaging Services

Zur Nutzung von Instant Messaging Services (ICQ, AIM, Yahoo Messenger, etc.) müssen Sie in dem jeweiligen Messenger ebenfalls die OctoGate als Proxy eintragen.

10.6 VPN

Sie können zu Ihrer OctoGate ein zusätzliches Modul erwerben, das Ihnen ermöglicht, VPN-Verbindungen zu Ihrem Netz herzustellen. Bei etwaigen Problemen mit diesem Modul setzen Sie sich bitte mit unserem Support in Verbindung.

10.7 DNS

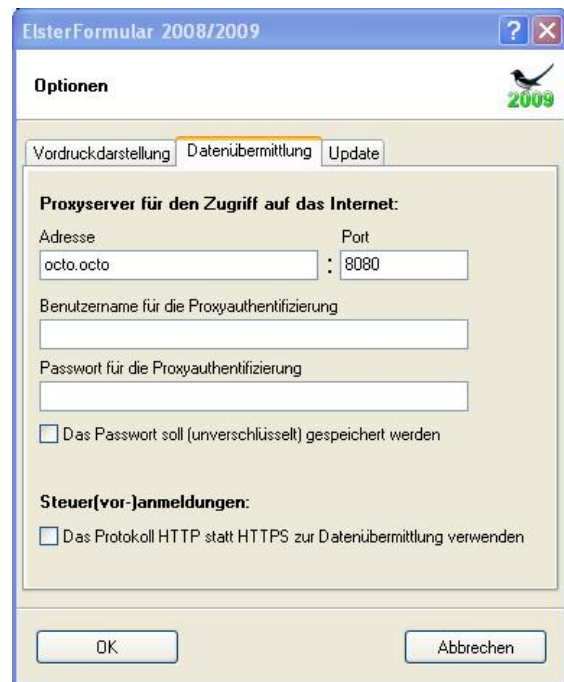
Tragen Sie bitte die OctoGate als Ihren DNS-Server ein (keine externen DNS-Server möglich).

10.8 Elster Steuersoftware

Zur Nutzung der Elster Steuersoftware („Elster-Formular“) tragen Sie bitte auch hier die OctoGate als Proxy ein. Dazu Öffnen Sie unter Menü *Extras* den Menüpunkt *Optionen / Einstellungen...*

Im folgenden Dialog (siehe Abbildung) wählen Sie den Reiter *Datenübermittlung* und geben als Adresse des Proxyservers „octo.octo“ und als Port „8080“ ein.

Sollten Sie sich als Benutzer gegenüber dem Proxy authentifizieren müssen (bei aktiviertem User-Management), so geben Sie Ihren OctoGate-Benutzernamen und Passwort entsprechend an, andernfalls lassen Sie die Felder leer. Bestätigen Sie zweimal mit OK.



Probleme kann es werden, wenn Sie die Elster-Steuersoftware aus einer eingebetteten Umgebung heraus bedienen.

10.9 Java Applets

Bei aktiviertem User-Management kann es vorkommen, dass Internetseiten, die Java-Applets enthalten, eine erneute Authentifizierung des Benutzers verlangen. Um dieses Problem zu umgehen, wechseln Sie in die „Systemsteuerung“ und klicken Sie doppelt auf *Java Plug-In* bzw. *Java*.

Je nach installierter Java-Version sehen Sie in einem *Java Control Panel* nun

- entweder einen Reiter *Browser*: Klicken Sie darauf und entfernen Sie das/die Häkchen vor dem/den von Ihnen verwendeten Browser(n).
- oder einen Reiter *Erweitert*: Klicken Sie darauf und öffnen in der erscheinenden Baumstruktur den Eintrag *Standard-Java für Browser* und deselektieren darin den/die von Ihnen verwendete Browser.

Nach einem Neustart Ihres Browsers sollte der Zugriff auf Java-Applets ohne erneute Authentifizierung funktionieren.

11 Anhang

11.1 Hinweise zum Datenschutz

Die OctoGate bietet Ihnen Informationen über alle ein- und ausgehenden Internetverbindungen Ihres Netzwerks an. Die Nutzung dieser Informationen ist abhängig von Ihrem Unternehmensstandort und durch die dort geltenden Datenschutzbestimmungen geregelt. Im Folgenden geben wir Ihnen einige grundlegende Informationen. Diese erheben keinen Anspruch auf Vollständigkeit, Aktualität oder Richtigkeit, sondern dienen Ihrer allgemeinen Information und nicht der Beratung im Falle eines aktuellen rechtlichen Anliegens. Das Geltend machen von Ansprüchen jeglicher Art ist ausgeschlossen. Nehmen Sie bitte die Beratung eines Rechtsanwaltes oder einer anderen qualifizierten Beratungsstelle in Anspruch.

11.1.1 Wissenswertes

Als Arbeitgeber sind Sie berechtigt, den Internetzugang auf geschäftsbezogene Vorgänge einzuschränken sowie die ein- und ausgehenden E-Mails zur Wahrung der Systemsicherheit auf Viren zu überprüfen. Insofern ist der Großteil des Funktionsumfangs Ihrer OctoGate nicht datenschutzrechtlich relevant.

Ihre OctoGate bietet Ihnen für nicht-administrative Zwecke den Benutzer ‚Reporter‘ an, dessen Passwort Ihrer Lieferung in einem versiegelten Umschlag beigelegt wurde. In der Reportersicht können Sie Verbindungsdaten benutzerbezogen abrufen. Da diese Daten den Benutzern Ihres Systems und damit ihren Mitarbeitern zugeordnet werden können, müssen Sie an dieser Stelle deren Rechte berücksichtigen.

Bei der betrieblichen Datenerfassung gilt das Gebot der Transparenz, d.h. Sie müssen Ihre Mitarbeiter darüber in Kenntnis setzen, welche ihrer Daten Sie zu welchem Zweck speichern. So ist z.B. das Speichern der Internetzugriffsdaten zur Kontrolle des Leistungs- und Arbeitsverhaltens Ihrer Mitarbeiter unzulässig.

Die übliche Vorgehensweise ist die Regelung solcher Maßnahmen über eine Betriebsvereinbarung. Sollte in Ihrem Unternehmen kein Betriebsrat existieren, so müssen Sie eine Vereinbarung mit jedem einzelnen Mitarbeiter treffen. Wichtig ist, dass die Speicherung personenbezogener Daten nur zum jeweils vereinbarten Zweck erlaubt ist.

Im konkreten Fall der OctoGate müssen Sie Ihre Mitarbeiter bzw. den Betriebsrat unterrichten, dass Sie die Möglichkeit haben, Ihr Surfverhalten im Detail nachzuvollziehen und vereinbaren, in welchen Fällen Sie von dieser Möglichkeit Gebrauch machen dürfen und werden.

„Grundsätzlich ist es schon aus Beweis Zwecken zu empfehlen, Verarbeitungszwecke schriftlich festzulegen. Verarbeiten Sie eine Vielzahl von gleich gearteten Datenkategorien, kann dies auch in der Verfahrensübersicht nach §4e/in der Verfahrensmeldung nach §4d geschehen. Voraussetzung hierfür ist allerdings, dass diese hinreichend konkret ausgestaltet ist.

„Hinreichend“ heißt: Anhand Ihrer Angaben muss eine kursorische Rechtmäßigkeitsprüfung möglich sein.“

(Quelle: „99+1 Beispiele und viele Tipps zum Bundesdatenschutzgesetz“, Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein)

Wenn Sie das Passwort des Benutzers ‚Reporter‘ versiegelt an einem sicheren Ort aufbewahren (z.B. ihn beim betrieblichen Datenschutzbeauftragten hinterlegen), kommt dies einer Sperrung der erhobenen Daten gleich, da sie auf diese Weise nicht eingesehen werden können.

11.2 Checklisten

11.2.1 Checkliste Datenschutz

- Verarbeiten Sie personenbezogene Daten in Ihrem Unternehmen?
- Sind gesetzliche Voraussetzungen an die Verarbeitung personenbezogener Daten geknüpft?
- Haftet der Unternehmer/Geschäftsführer für Verstöße gegen bestehende Datenschutzgesetze?
- Gibt es einen Datenschutzbeauftragten in Ihrem Unternehmen?
- Haben Sie Regelungen im Unternehmen, wie personenbezogene Daten verarbeitet werden dürfen?
- Existieren klare Regelungen wer personenbezogene Daten verarbeitet?
- Sind Ihre Mitarbeiter hinsichtlich der Erfordernisse des Bundesdatenschutzgesetzes geschult?
- Besitzen Sie schützenswerte Unternehmensdaten und haben Sie Regelungen getroffen, um diese vor Missbrauch zu schützen?
- Kennen die Führungskräfte in Ihrem Unternehmen Ihre Pflichten im Rahmen des Datenschutzes und darüber hinaus zum Schutz Ihrer elementaren Geschäftsdaten?
- Gibt es einen Zusammenhang zwischen Datenschutz und dem Image Ihres Unternehmens?

11.2.2 Checkliste IT-Sicherheit

- Gibt es Regelungen zur Datensicherheit in Ihrem Unternehmen?
- Gibt es Regelungen für die Nutzung der Benutzerpasswörter Ihrer Mitarbeiter?

- Sind Ihre Mitarbeiter mit den Verhaltensregeln für Passworte (Verbot der Weitergabe, Geheimhaltung,...) vertraut?
- Sind Ihre PC / Laptop / PDA gesichert, wenn der Raum verlassen wird, bzw. die Geräte unbeaufsichtigt sind?
- Werden regelmäßig (täglich) Updates für die Virenscanner (auch auf den Arbeitsplatz-PCs) durchgeführt?
- Werden regelmäßig Aktualisierungen Ihrer Betriebssysteme durchgeführt?
- Verschicken Sie alle Ihre Mails unverschlüsselt über das Internet?
- Ist die Nutzung der Systeme (z.B. Mail) Ihrer Mitarbeiter während einer Abwesenheit geregelt?
- Versuchen Sie regelmäßig, Daten aus Ihren Datensicherungen wiederherzustellen?
- Gibt es Notfallpläne, die den Geschäftsbetrieb bei einem Ausfall der IT sicherstellen?

12 Index

Active Directory	30
Administrator	21
AIM	<i>siehe Instant Messaging Services</i>
Anschlüsse OctoGate.....	12
Backup	20
Betriebsvereinbarung	71
Browsereinstellungen	68
Checklisten Datenschutz und IT-Sicherheit	72
Content-Filter.....	7
Datenschutz	71, 72
Datensperrung.....	72
Default Route	46
Device-Lock.....	7
DHCP	16
DMZ.....	12
DNS.....	18, 45, 69
Downloads	
VPN-Installer	47
Elster-Formular.....	70
E-Mail	
Fehler	67
E-Mail-Client	
Mozilla Thunderbird.....	67
Outlook	67
Outlook Express	67
Erster Zugriff.....	22
Fernwartung	26
HTTPS-Verbindungen	68
ICQ	<i>siehe Instant Messaging Services</i>
IMAP.....	49

Instant Messaging Services	69
ISDN-Verbindung	16
IT-Sicherheit	72
Java Applets	70
Konfiguration	
Netzwerk	16
OctoGate	14
USB-Stick	17
LC-Display	20
Lieferumfang	9
Login	22
Mail-Forwarder	49
Mail-Relay	8, 49
Managed Service	6
Mixed Mode	32, 52
Modem	16
Netzwerk	18
Anschlüsse	13
Konfiguration	16
OctoGate	
als Mailserver	49
als Proxy eintragen	68
Anschlüsse	10
booten	17
Ethernet-Anschlüsse	12
Herunterfahren	20
Konfiguration	14
Neustart	20
Remote Support	60
Passwort	
SMTP	49
Pausenfilter	28
POP3	49
Protokolle	

OctoGate	18
Webzugriff	68
Proxy	69
Reporter	54
Systemsicherheit	71
Tokenwerfer	61
URL-Liste	
hochladen	28
USB-Stick	9, 14
Usermanagement	52
Virenschanner	7
VPN	
Client	47
Report	57
Token- / Passwort-Sicherung	61
Webbrowser	68
WebGUI	
Login	22
Yahoo Messenger	<i>siehe</i> Instant Messaging Services
Zeitsynchronisation	18

www.octogate.de

