

Installations- Dokumentation

OctoGate
EINFACH. SICHER. GESCHÜTZT. -

Version 1.2 FINAL

OctoGate - Technische Dokumentation

OctoGate IT Security Systems GmbH
Friedrich-List-Str. 42
33100 Paderborn

Tel.: +49 5251 18040 0
E-Mail: info@octogate.de
Web: www.octogate.de

Verantwortlicher für den Inhalt: Frank Menne

Versionshistorie

Datum	Person	Version	Kommentar
22.09.2016	Jan Wagner	1.0	Initial-Dokument
23.09.2016	Thorsten Seidel	1.1	Revision und Kontrolle
21.02.2017	Jan Wagner	1.2	Überarbeitung

Inhalt

1	Packungsinhalt	4
2	Inbetriebnahme / Verkabelung	5

1 Packungsinhalt

OctoGate Access Point AC-1000

Im Lieferumfang sind enthalten:

- 1 x OctoGate Access Point AC-1000
- 1 x Befestigung für Wand- oder Deckenmontage
- 1 x Schaltnetzteil zur Stromversorgung via PoE („PoE Injector“ – falls kein PoE-fähiger Switch zur Verfügung steht)
INPUT: 100-240V~50/60Hz; OUTPUT: 48V -0,5A
- 1 x Strom-Anschlusskabel für PoE-Injector, zweipolig
- 1 x CAT 5e LAN-Kabel
- 1 x Satz Schrauben und Dübel zur Befestigung



2 Inbetriebnahme/Verkabelung

Im ersten Schritt gilt es den AC-1000 in das Netzwerk einzubinden.

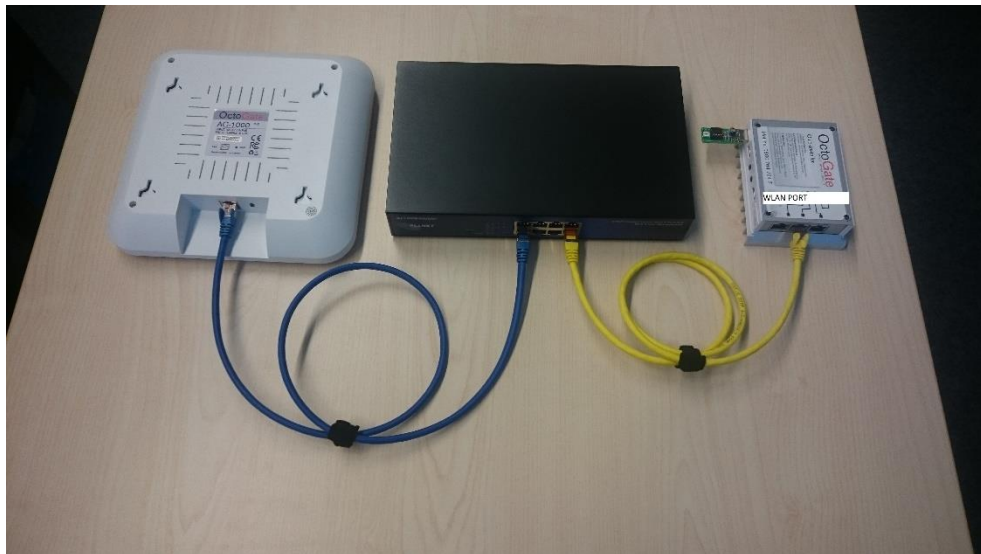
Möglichkeit 1: über einen PoE-fähigen Switch



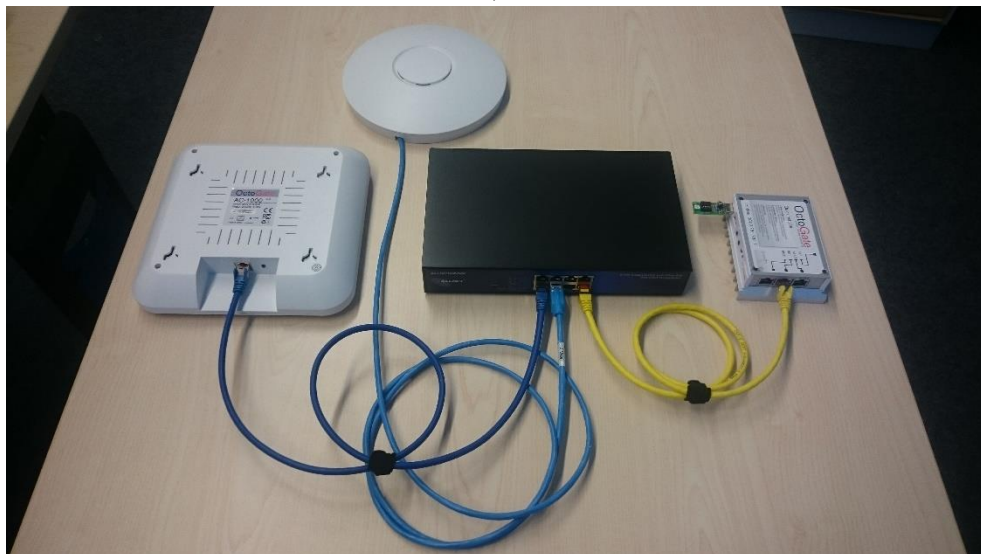
Möglichkeit 2: über den mitgelieferten PoE-Injector



Im zweiten Schritt wird der Switch mit dem WLAN-Port der OctoGate Firewall verbunden.

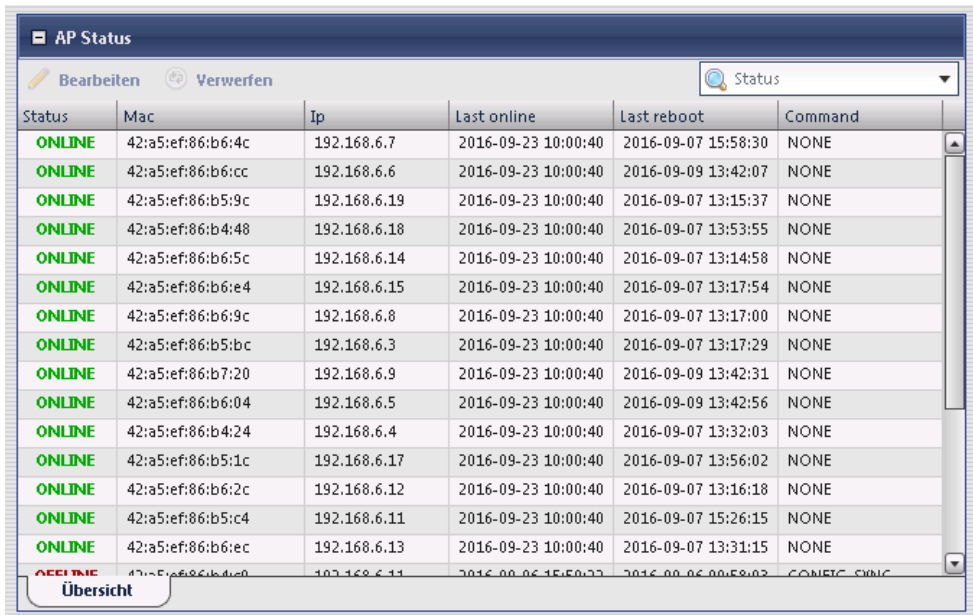


Je nach Anzahl der Access Points, den ersten Schritt wiederholen.



Sollte Ihre OctoGate Firewall noch nicht gestartet sein, holen Sie dies bitte zuerst nach. Ist diese betriebsbereit, schalten Sie die Access Points ein indem Sie den PoE-Switch einschalten oder das mitgelieferte Schaltnetzteil mit dem Stromnetz verbinden.

Danach beginnt die automatische Installation des AC-1000 durch die OctoGate Firewall. Die Geräte melden sich auf der WebGui:



The screenshot shows a web interface titled 'AP Status'. At the top, there are buttons for 'Bearbeiten' (Edit) and 'Verwerfen' (Cancel), and a search box labeled 'Status'. Below this is a table with the following columns: Status, Mac, Ip, Last online, Last reboot, and Command. All 15 rows in the table show a status of 'ONLINE' in green text. The 'Mac' addresses are in the format 42:a5:ef:86:b6:xx, and the 'Ip' addresses are in the format 192.168.6.xx. The 'Last online' and 'Last reboot' columns show timestamps from 2016-09-23 10:00:40 and 2016-09-07 15:58:30 respectively. The 'Command' column for all rows is 'NONE'. At the bottom left of the table, there is a button labeled 'Übersicht' (Overview).

Status	Mac	Ip	Last online	Last reboot	Command
ONLINE	42:a5:ef:86:b6:4c	192.168.6.7	2016-09-23 10:00:40	2016-09-07 15:58:30	NONE
ONLINE	42:a5:ef:86:b6:cc	192.168.6.6	2016-09-23 10:00:40	2016-09-09 13:42:07	NONE
ONLINE	42:a5:ef:86:b5:9c	192.168.6.19	2016-09-23 10:00:40	2016-09-07 13:15:37	NONE
ONLINE	42:a5:ef:86:b4:48	192.168.6.18	2016-09-23 10:00:40	2016-09-07 13:53:55	NONE
ONLINE	42:a5:ef:86:b6:5c	192.168.6.14	2016-09-23 10:00:40	2016-09-07 13:14:58	NONE
ONLINE	42:a5:ef:86:b6:e4	192.168.6.15	2016-09-23 10:00:40	2016-09-07 13:17:54	NONE
ONLINE	42:a5:ef:86:b6:9c	192.168.6.8	2016-09-23 10:00:40	2016-09-07 13:17:00	NONE
ONLINE	42:a5:ef:86:b5:bc	192.168.6.3	2016-09-23 10:00:40	2016-09-07 13:17:29	NONE
ONLINE	42:a5:ef:86:b7:20	192.168.6.9	2016-09-23 10:00:40	2016-09-09 13:42:31	NONE
ONLINE	42:a5:ef:86:b6:04	192.168.6.5	2016-09-23 10:00:40	2016-09-09 13:42:56	NONE
ONLINE	42:a5:ef:86:b4:24	192.168.6.4	2016-09-23 10:00:40	2016-09-07 13:32:03	NONE
ONLINE	42:a5:ef:86:b5:1c	192.168.6.17	2016-09-23 10:00:40	2016-09-07 13:56:02	NONE
ONLINE	42:a5:ef:86:b6:2c	192.168.6.12	2016-09-23 10:00:40	2016-09-07 13:16:18	NONE
ONLINE	42:a5:ef:86:b5:c4	192.168.6.11	2016-09-23 10:00:40	2016-09-07 15:26:15	NONE
ONLINE	42:a5:ef:86:b6:ec	192.168.6.13	2016-09-23 10:00:40	2016-09-07 13:31:15	NONE

3 Virtuelle Access Points

Nachdem sich die Geräte auf der WebGui der OctoGate Firewall gemeldet haben, strahlen sie drei vorkonfigurierte Netze aus. Diese SSID's können Sie unter dem Punkt „Wireless“ verwalten. Hier definieren Sie die Namen, wählen die Art der Authentifizierung oder treffen manuell eine Frequenzbandwahl.

The screenshot displays the 'AP Standard-Konfiguration' interface. It features two frequency band sections: '2.4GHz Band' and '5.0GHz Band', each with a 'Frequenz abschalten' checkbox. Below these are three WLAN configuration tabs: 'WLAN 1', 'WLAN 2', and 'WLAN 3'. The 'WLAN 3' tab is selected, showing a configuration form with the following fields: 'Versteckt / Unsichtbar' (checkbox), 'SSID' (text input containing 'GO-BYOD'), 'Authentifizierung' (dropdown menu set to 'WPA2-PSK'), and 'Passwort' (two masked text input fields). At the bottom right of the form are 'Verwerfen' and 'Speichern' buttons.

1.octo_guest

Gäste-Netz für Schüler oder schulfremde Geräte

Dieses WLAN-Netz ist offen konfiguriert. Ein neuer Gast bekommt zunächst eine Anmeldeseite und muss sein Gerät einmalig mit einem individuellen Voucher authentifizieren. Sie können in der WebGui unter dem Punkt „OctoGate Guest“ Zugangscodes mit einer bestimmten Dauer erstellen.

Übersicht
Datensatz bearbeiten.

Code : AITHAI

Beschreibung : Max Müller

Start : 2016-09-21 11:21:25

Ende : 2017-07-28 11:21:25

Stunden : 7440,00

OK Abbrechen

Das Gäste-Netz wird in der Praxis meistens für schülereigene Geräte verwendet. Die Schülerdaten werden im Vorfeld erfasst und die Dauer des Vouchers wird auf die Schulzeitdauer des Schülers begrenzt. Bei Verstößen gegen die Schul-AGBs ist es möglich, im „Vieraugen-Prinzip“ den Schuldigen zu identifizieren.

2.octo_lehrer

Lehrer-Netz für private Geräte der Lehrer

In diesem Netz wird der Zugang, wie gewohnt, über ein Passwort gewährt (WPA2). Das Passwort muss bei der Konfiguration definiert werden, es gibt kein voreingestelltes (default) Passwort. Ein zufällig generiertes wird bei der Installation der OctoGate Firewall erstellt. Sie können dieses verwenden, müssen es aber nicht.

3.octo_seg

Schuleigene Geräte-Netz (SEG) für schuleigene Geräte

Das SEG-Netz dient den schuleigenen Geräten, welche die Schule den Schülern zum Arbeiten zur Verfügung stellt. Hier empfiehlt sich der Einsatz der Radius Authentifizierung per x509 Zertifikat. Mit diesem ist es den Schülern unmöglich, das WLAN Passwort des Gerätes auszulesen.