

A1 Gäste WLAN Anleitung

Einstellungen im Securitymanager
Anschluss eigene WLAN Access-Points

Version 1.1



INHALT

1. Einstieg Security Manager	Seite 3
2. Landing Page anpassen	Seite 4
3. Kategorien von Internetseiten blocken	Seite 8
4. Malware Filter	Seite 9
5. Blacklisting	Seite 10
6. Dateityp Filter	Seite 11
7. Hinweistext für Gäste	Seite 12
8. Anschluss eigene WLAN Access-Points	Seite 13



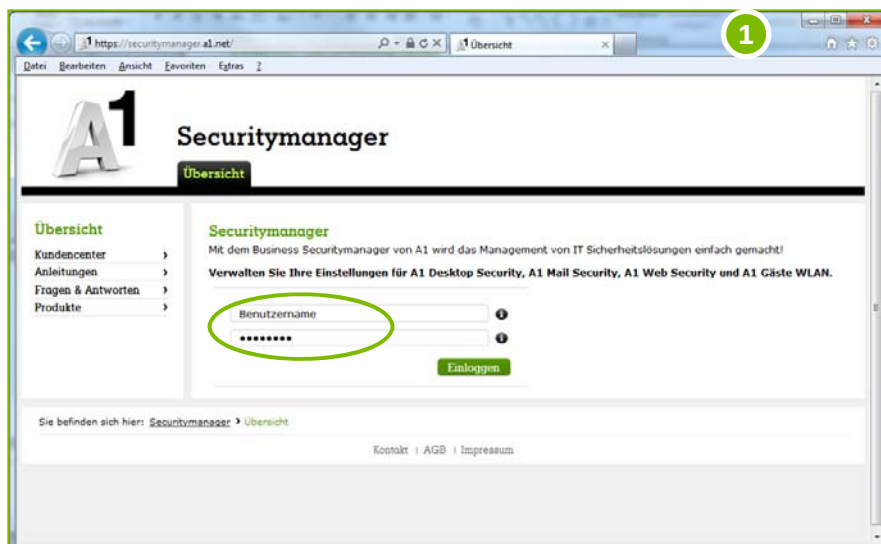
1. Einstieg in den Securitymanager

1. Loggen Sie sich im Securitymanager unter

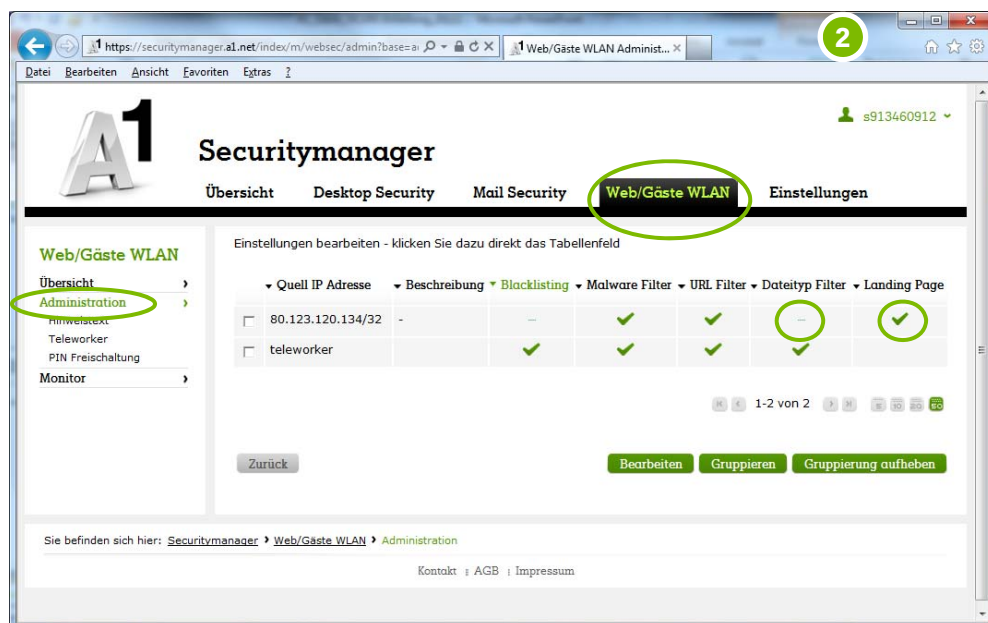
<https://securitymanager.a1.net>

ein.

Benutzername und Passwort entnehmen Sie bitte dem Serviceübersichtsdatenblatt Ihres Business Internet Anschlusses.



2. Wählen Sie den Menüpunkt „Web/Gäste WLAN“ und anschließend „Administration“ aus. Hier finden Sie einen Überblick über Ihre Filtereinstellungen. Wenn Sie die „Landing Page“ (= Startseite für Ihre Gäste) anpassen wollen, können Sie diese ebenfalls über den Überblick aufrufen.



Hinweis: Um die Landing Page anzupassen oder die Filtereinstellungen zu ändern klicken Sie bitte direkt auf die Symbole

in der Übersichtstabelle. Das  bedeutet dass die Filterregel aktiv ist – bei  ist die Regel nicht aktiv.



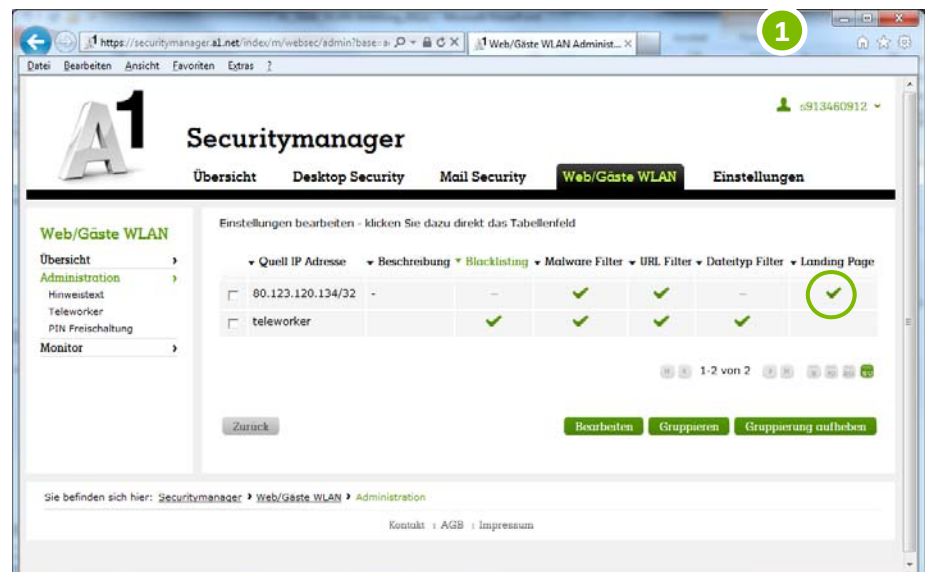
Landing Page anpassen

2. Landing Page anpassen

1. Klicken Sie in der Übersichtstabelle im Menüpunkt „Administration“ auf das

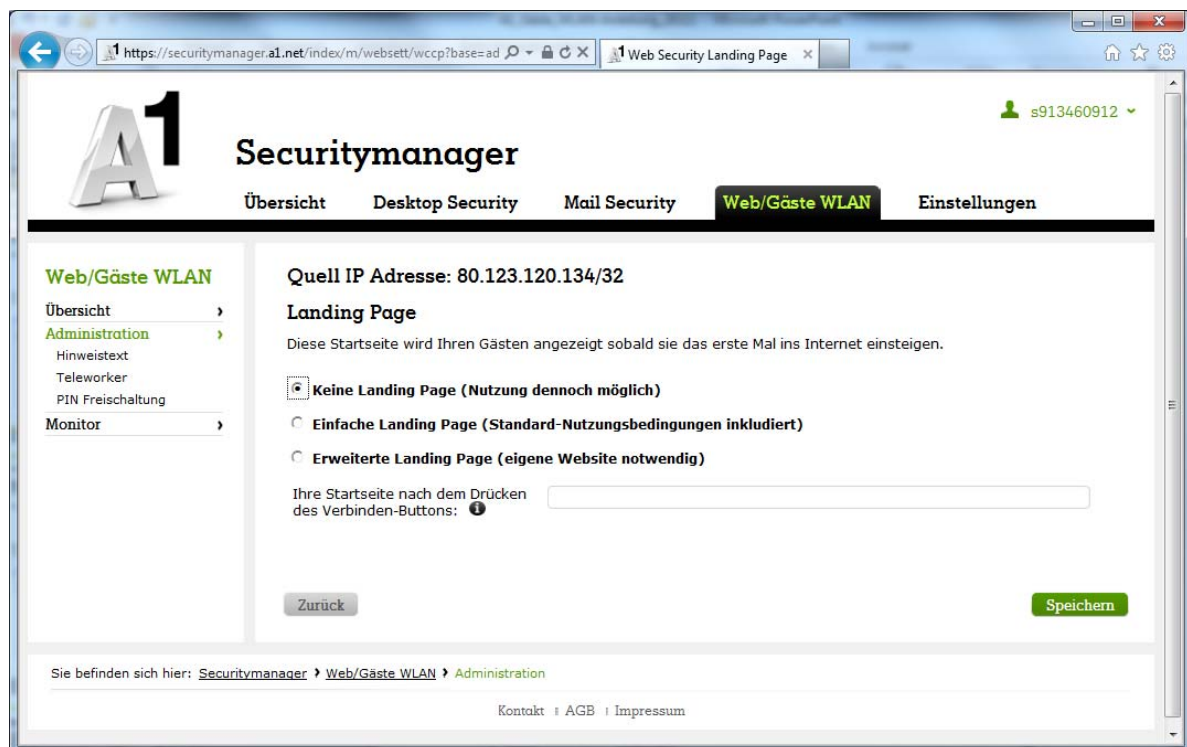


unter „Landing Page“



2. Wählen Sie auf der folgenden Seite zwischen folgenden Varianten aus:

Keine Landing Page: Im Internet surfen ohne Anzeige der Startseite und ohne die Nutzungsbedingungen zu akzeptieren.



Landing Page anpassen

Einfache Landing Page: Sobald Ihr Gast eine beliebige Webseite aufruft, geht eine Startseite mit den Nutzungsbedingungen auf. Erst nachdem er diese akzeptiert hat kann er im Internet surfen.

Die Startseite ist mit einem „Standard-Logo“ und „Standard-Nutzungsbedingungen“ vorausgefüllt die individuell angepasst werden können.



Logo und Nutzungsbedingungen anpassen

Die Datei mit Ihrem Logo soll folgende Voraussetzungen erfüllen:

Format: JPG oder JPN

Seitenverhältnis: 3,5:1 (bei einem anderen Seitenverhältnis wird automatisch auf diesen Wert skaliert)

min. Größe: 350 x 100 Pixel (Empfehlung)

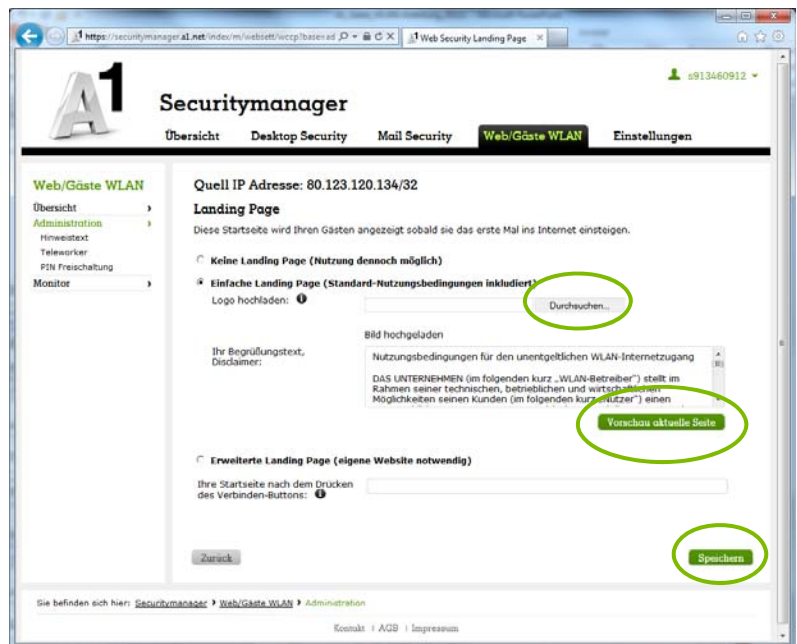
max. Größe: 655 x 187 Pixel

max. Dateigröße: 512kB



Landing Page anpassen

- Klicken Sie auf „Durchsuchen“ um die Datei mit Ihrem Logo auszuwählen.
- Passen Sie die Nutzungsbedingungen an oder kopieren Sie Ihren eigenen Text in das Eingabefeld.
- Klicken Sie auf „Speichern“ um die Änderungen zu übernehmen.
- Mit „Vorschau aktuelle Seite“ wird eine Voransicht der Landing Page angezeigt.



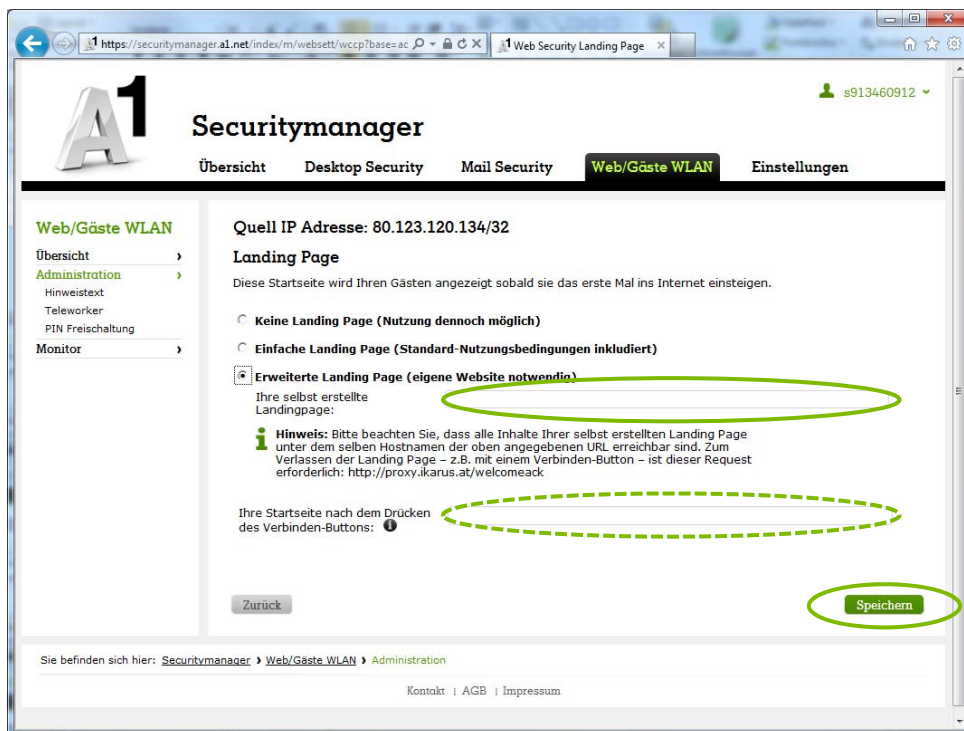
Tipp: Wenn sie den vorgegebenen Text verwenden möchten brauchen Sie nur „DAS UNTERNEHMEN“ durch Ihren Firmennamen ersetzen.

Nutzungsbedingungen für den unentgeltlichen WLAN-Internetzugang

DAS UNTERNEHMEN (im folgenden kurz „WLAN-Betreiber“) stellt im Rahmen seiner technischen, betrieblichen und wirtschaftlichen



Erweiterte Landing Page



Gestalten Sie Ihre eigene Landing-Page für Ihre Gäste auf einem externen Webspace (z.B. „A1 Webspace Business“ – ist bei Ihrem Business Internet von A1 inkludiert). Erst nachdem der Gast auf Ihrer Webseite eine Aktion gesetzt hat (z.B. auf „Verbinden“ geklickt hat) kann er im Internet surfen.

- Wichtig dabei ist dass beim Verlassen der Landing Page - z.B. mit einem Verbinden-Button - ein Request auf

<http://proxy.ikarus.at/welcomeack>

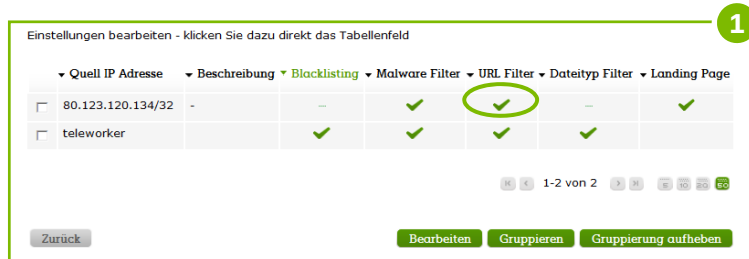
ausgelöst wird.

- Tragen Sie die Adresse Ihrer selbst erstellten Landing Page ein. Bitte beachten Sie, dass alle Inhalte Ihrer Landing Page unter dem angegebenen Hostnamen erreichbar sind (z.B. unter <http://www.firma.at>).
- Optional können Sie auch eine Startseite angeben, die angezeigt wird, sobald Sie den „Verbinde-Button“ drücken.
- Klicken Sie auf „Speichern“ um die Änderungen zu übernehmen

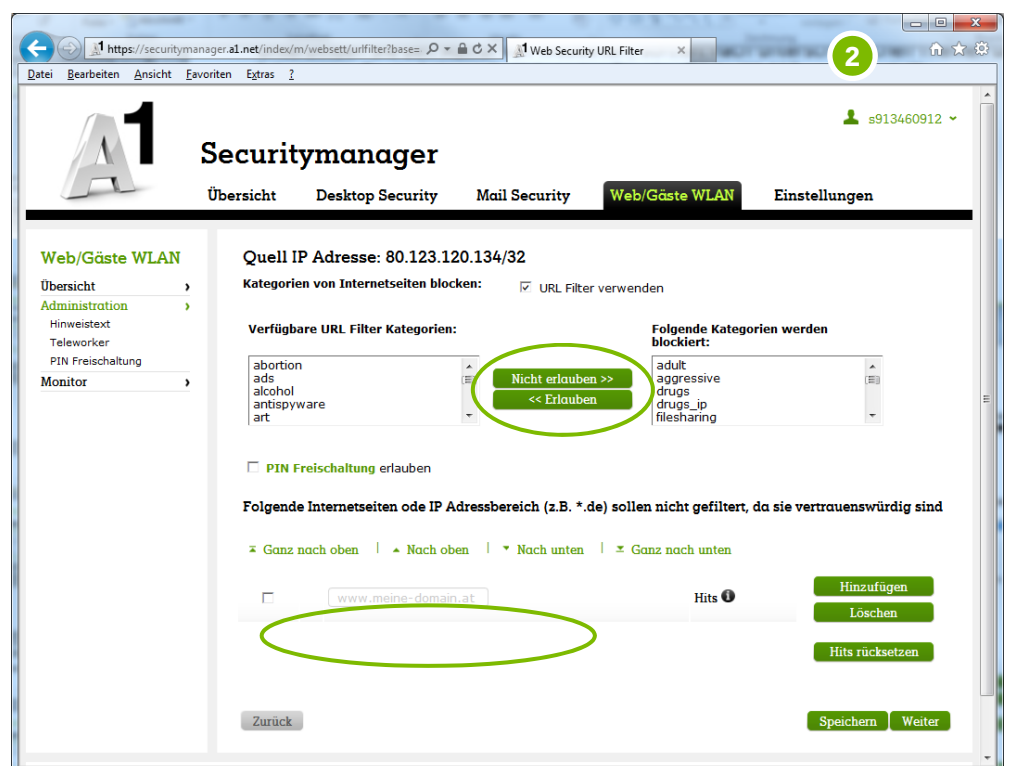
Kategorien von Internetseiten blocken

3. Kategorien von Internetseiten blocken

Unterbinden Sie den Aufruf von Webseiten, sortiert nach unterschiedlichen Themen und Interessen. Sinnvolle Kategorien für ein „Gäste WLAN“ sind bereits voreingestellt.



1. Klicken Sie in der Überblickstabelle Ihrer Filterregeln auf die Zelle für den URL Filter, um die Detailseite für dieses Filtermodul zu öffnen.



2. Auf der URL Filter-Detailseite finden Sie Kategorien von Internetseiten. Wählen Sie jene Kategorien aus, die Sie für Ihre Benutzer „Erlauben“ oder „Nicht erlauben“ möchten.

Sollen bestimmte Websites nicht gefiltert werden, so geben Sie diese bitte unter „Folgende Internetseiten oder IP Adressbereiche sollen nicht gefiltert werden [...]“ an.

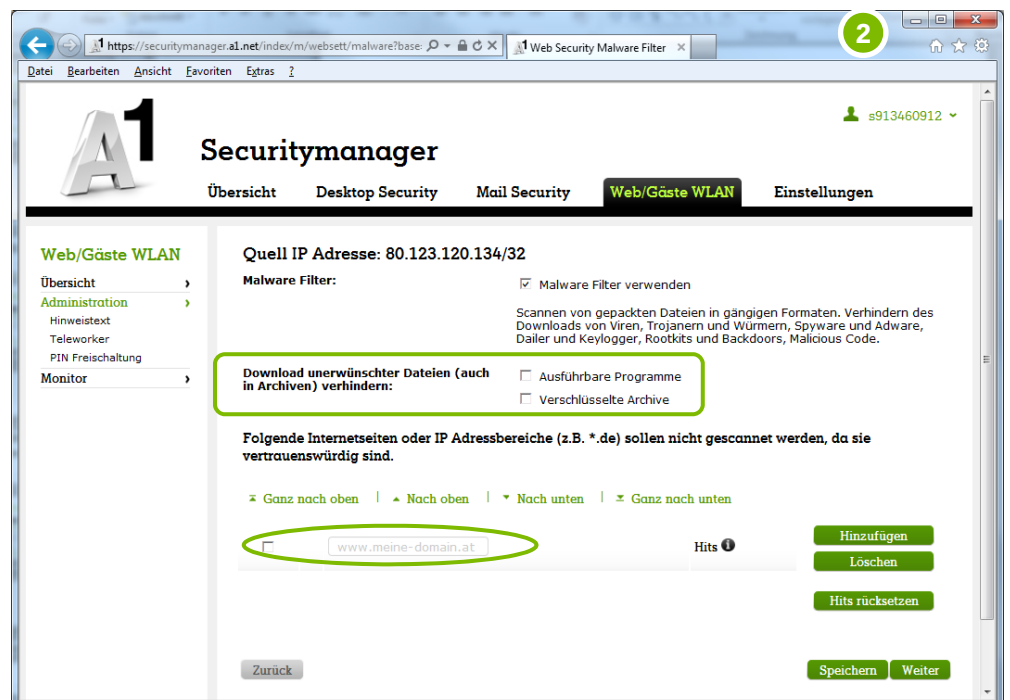


4. Malware Filter

Schützen Sie Ihre Gäste vor Viren, Trojanern & Co. Dieser Filter ist standardmäßig eingeschaltet.



1. Klicken Sie in der Überblickstabelle Ihrer Filterregeln auf die Zelle für den Malware Filter, um die entsprechende Detailseite für diesen Filter zu öffnen.



2. Auf der Detailseite haben Sie die Möglichkeit einzustellen, ob auch der Download potentiell gefährlicher Dateien wie ausführbare Programme oder verschlüsselte Archivdateien geblockt werden sollen.

Weiters können Sie Ausnahme-Regeln hinzufügen

Tipp: In den Eingabefeldern für Ihre individuellen Filterregeln sind nicht nur URLs bzw. Domainnamen zulässig, sondern auch IP Adressbereiche in CIDR-Notation wie z.B. 80.123.120.132/30.



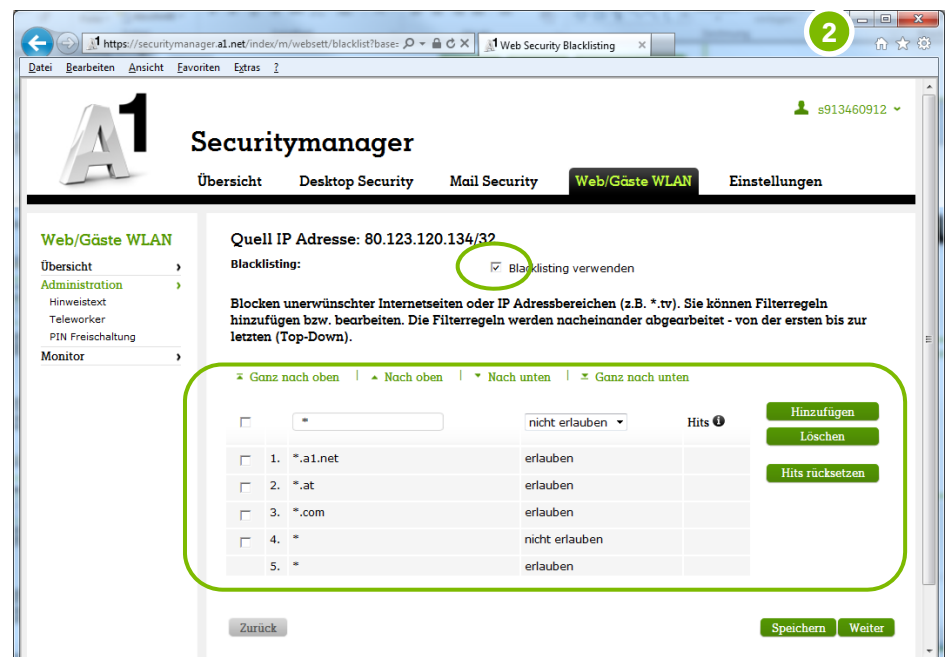
5. Blacklisting

Verhindern Sie den Zugriff auf bestimmte Internetseiten und konfigurieren Sie Ausnahme-Regeln (Whitelisting). Diesen Filter können Sie zusätzlich aktivieren.



1. Klicken Sie in der Überblickstabelle Ihrer Filterregeln auf die Zelle fürs Blacklisting, um die entsprechende Detailseite für diesen Filter zu öffnen.

2. Setzen Sie ein Häkchen bei „Blacklisting verwenden“



3. Auf der Detailseite können Sie individuelle Filterregeln hinzufügen, sortieren bzw. umreihen und löschen. Das Filter-Regelwerk wird sequentiell abgearbeitet, beginnend mit der ersten Regel (top-down). Trifft eine Regel zu, so wird die Aktion ausgeführt und die darunter liegenden Regeln nicht weiter überprüft (fire-and-forget).

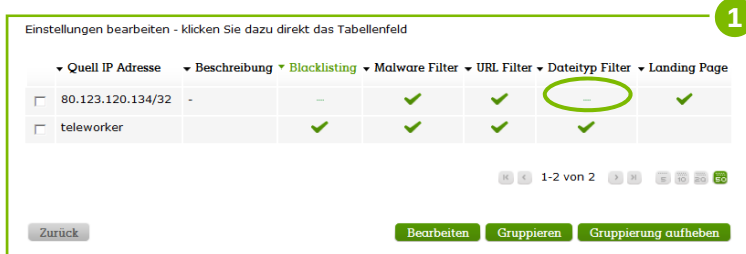
Im gezeigten Beispiel ist der Aufruf von .at, .com und a1.net Internetseiten für Gäste erlaubt. Alle anderen sind gesperrt.

Hinweis: Die Spalte „Hits“ zählt mit, wie oft eine bestimmte Filterregel tatsächlich ausgeführt wurde.



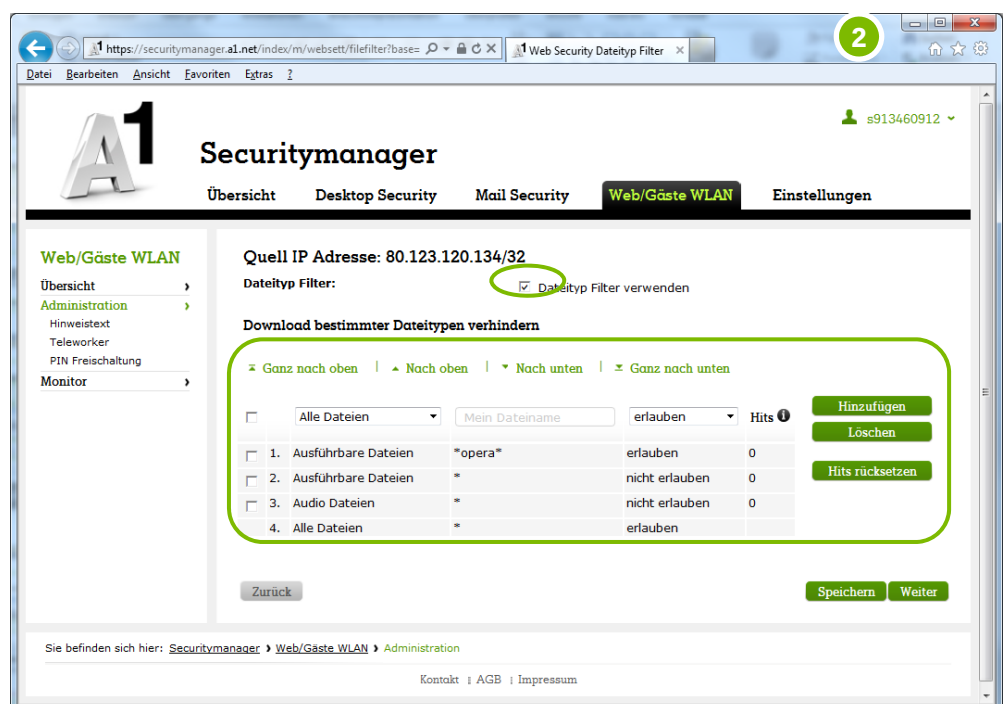
6. Dateityp Filter

Verhindern Sie den Download unerwünschter Dateien und konfigurieren Sie Ausnahme-Regeln (Whitelisting). Diesen Filter können Sie zusätzlich aktivieren.



1. Klicken Sie in der Überblickstabelle Ihrer Filterregeln auf die Zelle für den Dateityp Filter, um die entsprechende Detailseite zu öffnen.

2. Setzen Sie ein Häkchen bei „Dateityp Filter verwenden“



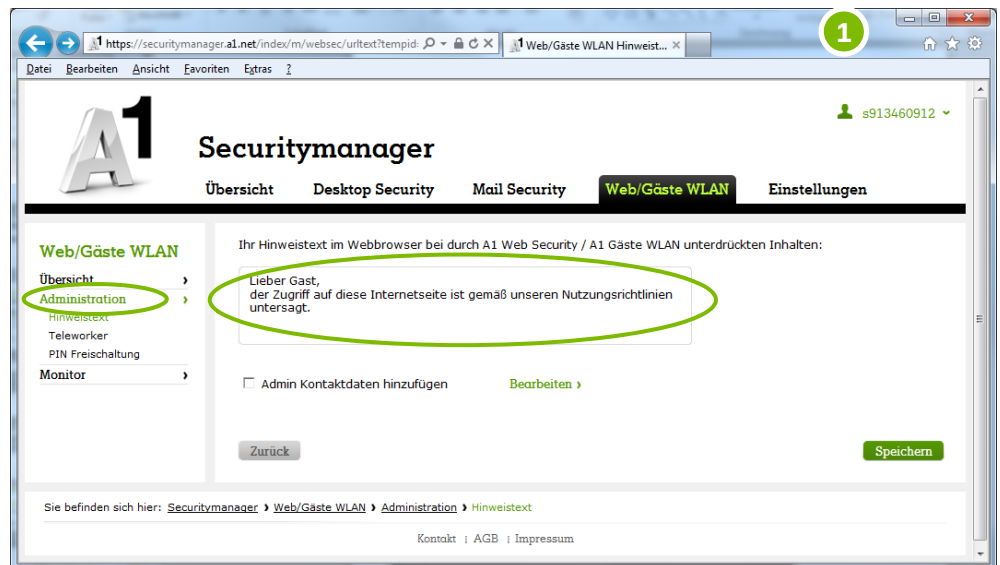
3. Auf der Detailseite können Sie individuelle Filterregeln hinzufügen, sortieren oder löschen. Das Filter-Regelwerk wird sequentiell abgearbeitet, beginnend mit der ersten Regel (top-down). Trifft eine Regel zu, so wird die Aktion ausgeführt und die darunter liegenden Regeln nicht weiter überprüft (fire-and-forget).

Im gezeigten Beispiel ist der Download von Musikdateien und ausführbaren Programmen nicht erlaubt. Mit einer Ausnahme-Regel wird festgelegt, dass z.B. exe Dateien mit „opera“ im Dateinamen heruntergeladen werden dürfen. Die letzte Regel (im Beispiel die Nummer 4) legt fest, was mit Dateien passiert, die im Filter-Regelwerk nicht explizit behandelt werden (clean-up).

7. Hinweistext für Gäste

Formulieren Sie eine individuelle Nachricht, die Ihre Gäste bei gesperrten Internetseiten sehen.

1. Im Menü „Administration“ unter „Hinweistext“ können Sie Ihren Text eingeben und speichern.



2. Wenn Ihr Gast eine gesperrte Webseite öffnen will, erhält er einen Sicherheitshinweis, ergänzt um Ihren persönlichen Hinweistext.

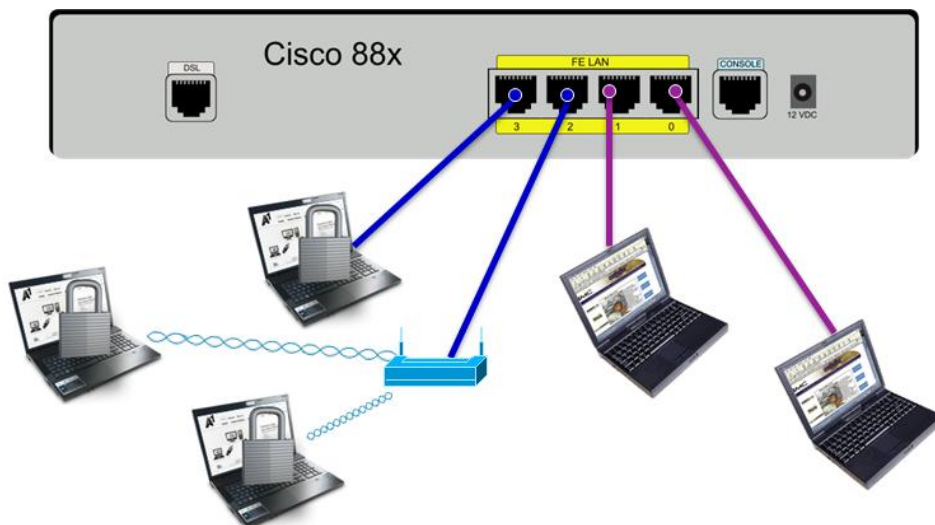


8. Anschluss eigene WLAN Access-Points

Mit der Aktivierung von „A1 Gäste WLAN“ für Ihren „A1 Breitband Pro Business“ Anschluss wurde auch die Beschaltung der Ethernet-Ports am Router von A1 angepasst.

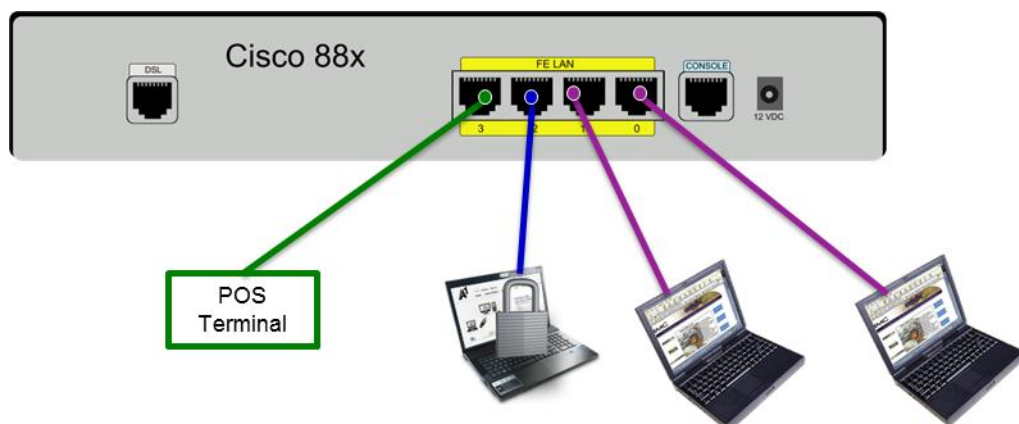
Mit welchen Ports Sie Ihre WLAN Access-Points verbinden, hängt von den genutzten Services ab. Webtraffic von den „A1 Gäste WLAN“ Ports wird automatisch an das zentrale „A1 Gäste WLAN“ Service bei A1 weitergeleitet.

Variante 1: Internet + „A1 Gäste WLAN“



Internet: Port 0,1
A1 Gäste WLAN: Port 2,3 ⇒ WLAN Access-Points

Variante 2: Internet + „A1 Gäste WLAN“ + Bankomat (POS)

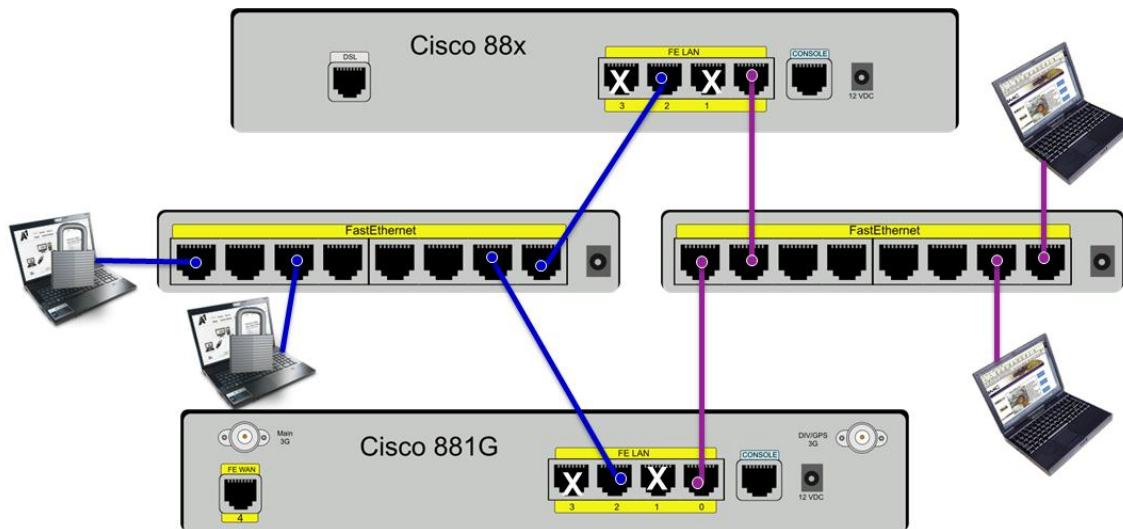


Internet: Port 0,1
A1 Gäste WLAN: Port 2 ⇒ WLAN Access-Points
Bankomat: Port 3



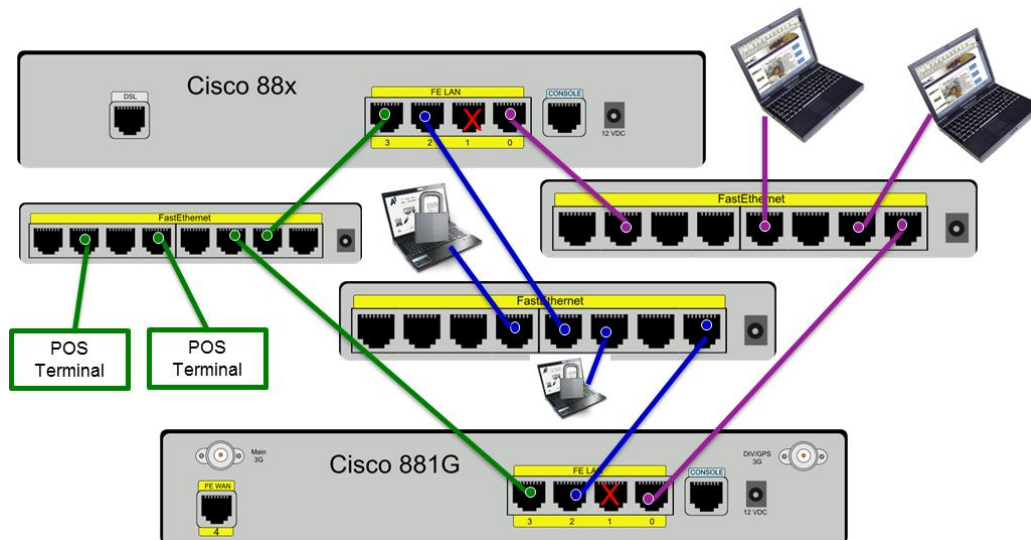
Anschluss WLAN Access-Points

Variante 3: Internet + „A1 Gäste WLAN“ mit Backup Mobile



Internet: Port 0 ⇒ Switch
A1 Gäste WLAN: Port 2 ⇒ Switch ⇒ WLAN Access-Points

Variante 4: Internet + „A1 Gäste WLAN“ + Bankomat (POS) mit Backup Mobile



Internet: Port 0 ⇒ Switch
A1 Gäste WLAN: Port 2 ⇒ Switch ⇒ WLAN Access-Points
Bankomat: Port 3 ⇒ Switch

Einstellungen eigene WLAN Access-Points

Der A1-Router ist für das Gäste-WLAN als DHCP-Server (Adressbereich 10.1.1.0/24) konfiguriert.

Empfohlene Einstellungen WLAN Access-Points:

- DHCP-Client
- SSID: [Ihr Firmenname] Gäste-WLAN
- Verschlüsselung:
 - Einstieg für Gäste nur mit Passwort:
Modus: WPA2
WLAN-Netzwerkschlüssel: [Passwort für Ihre Gäste]
 - Einstieg für Gäste ohne Passwort: keine
Achtung erhöhtes Sicherheitsrisiko durch unverschlüsselte
WLAN-Verbindung
- WLAN-Geräte dürfen NICHT untereinander kommunizieren

Wenn Sie Ihre WLAN Access-Points sowohl für Ihr Firmen-WLAN als auch für das Gäste-WLAN einsetzen wollen wird die Verwendung von VLANs und WLAN Access Points mit mehreren logischen WLANs („Multi SSID“) empfohlen.