A1 Web Security Installationshilfe

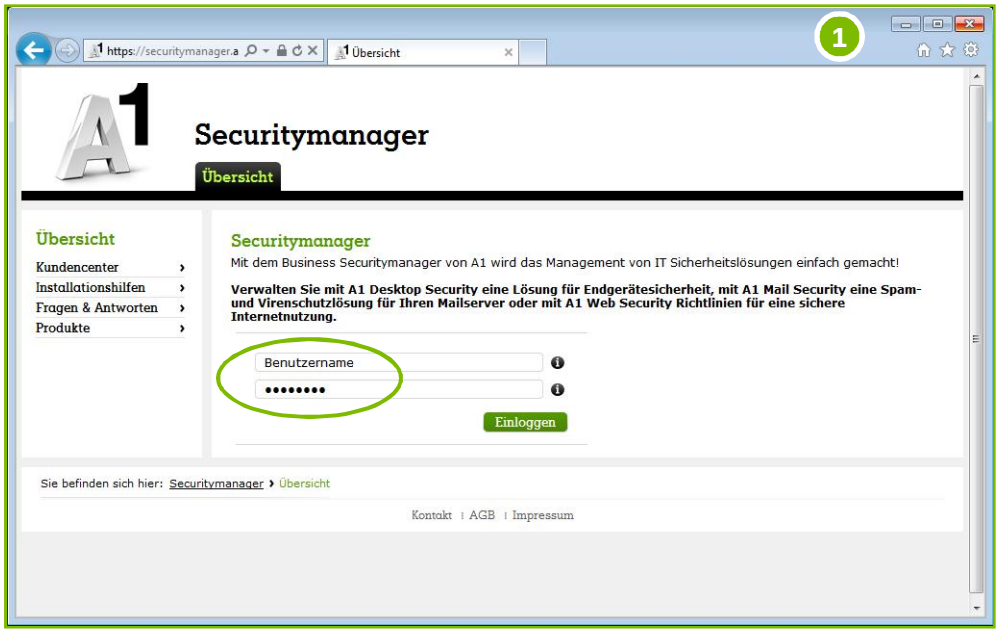
Proxykonfiguration im Securitymanager

Administration der Filterregeln.

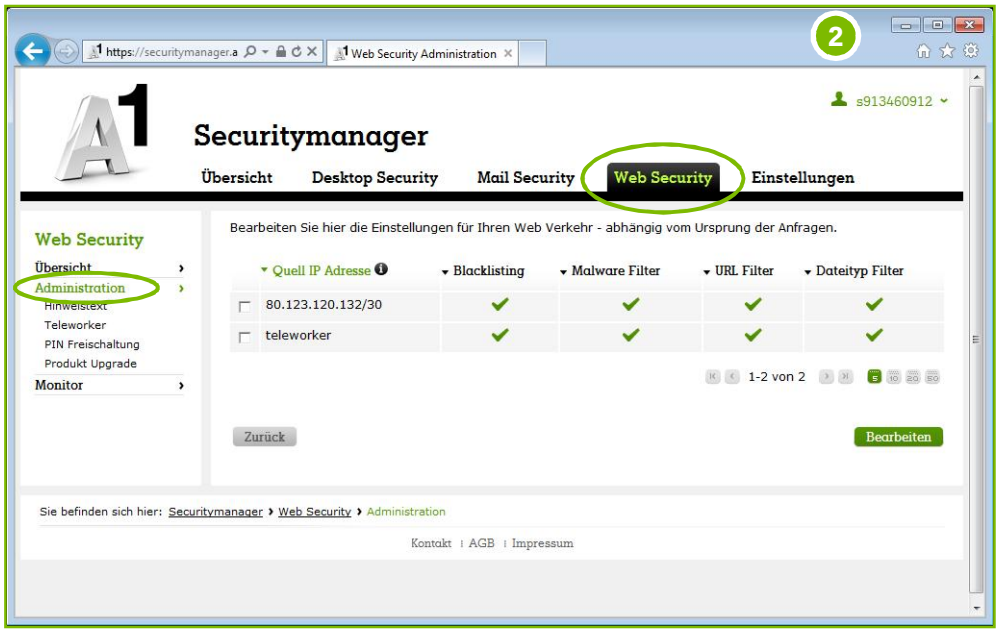
Verwalten Sie Ihre Filtereinstellungen im Securitymanager unter https://securitymanager.a1.net

1. **Loggen Sie sich im Securitymanager ein.**

   Benutzername und Passwort entnehmen Sie bitte dem Serviceübersichts-datenblatt Ihres Business Internet Anschlusses.



2. **Wählen Sie den Menüpunkt „Web Security“ und anschließend „Administration“. Hier finden Sie eine Überblickstabelle mit Ihren Filterregeln: Ein Regelwerk für die IP Adresse(n) Ihres A1 Business Internet Anschlusses fürs Büro und ein separates Teleworker-Regelwerk, falls Sie A1 Web Security von unterwegs aus nutzen.**



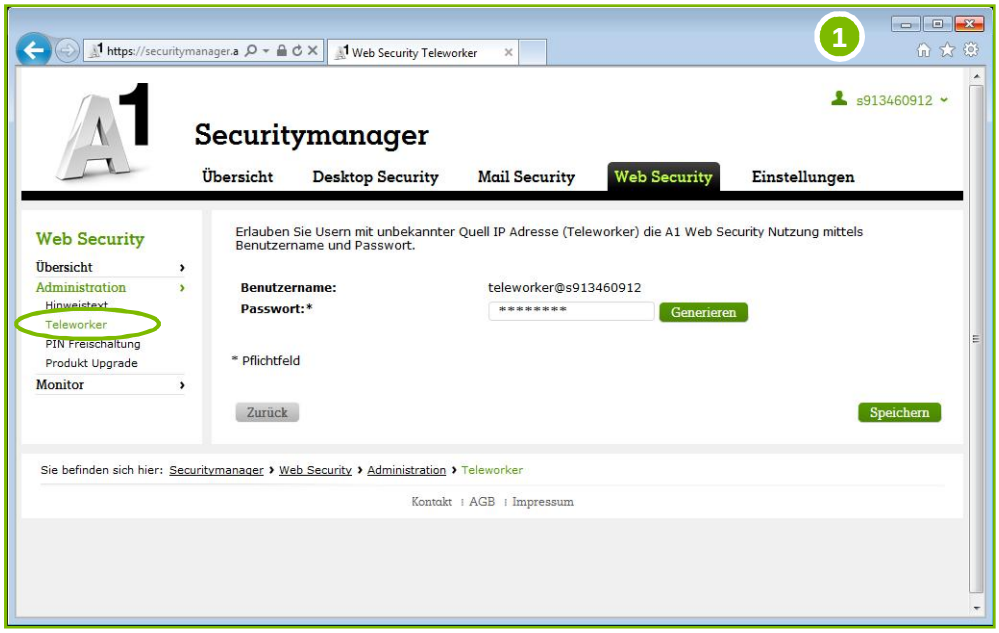
Hinweis: Die Authentifizierung der Benutzer am Proxyserver secureproxy.a1.net erfolgt automatisch über die IP Adresse Ihres Internet Anschlusses. Für die Verwendung des Proxys von unterwegs aus (Regelwerk „Teleworker“) ist eine Authentifizierung mit Benutzername und Passwort erforderlich.

Konfiguration für Teleworker.

Legen Sie ein Passwort fest, damit Sie A1 Web Security auch unterwegs oder von zu Hause aus nutzen können.

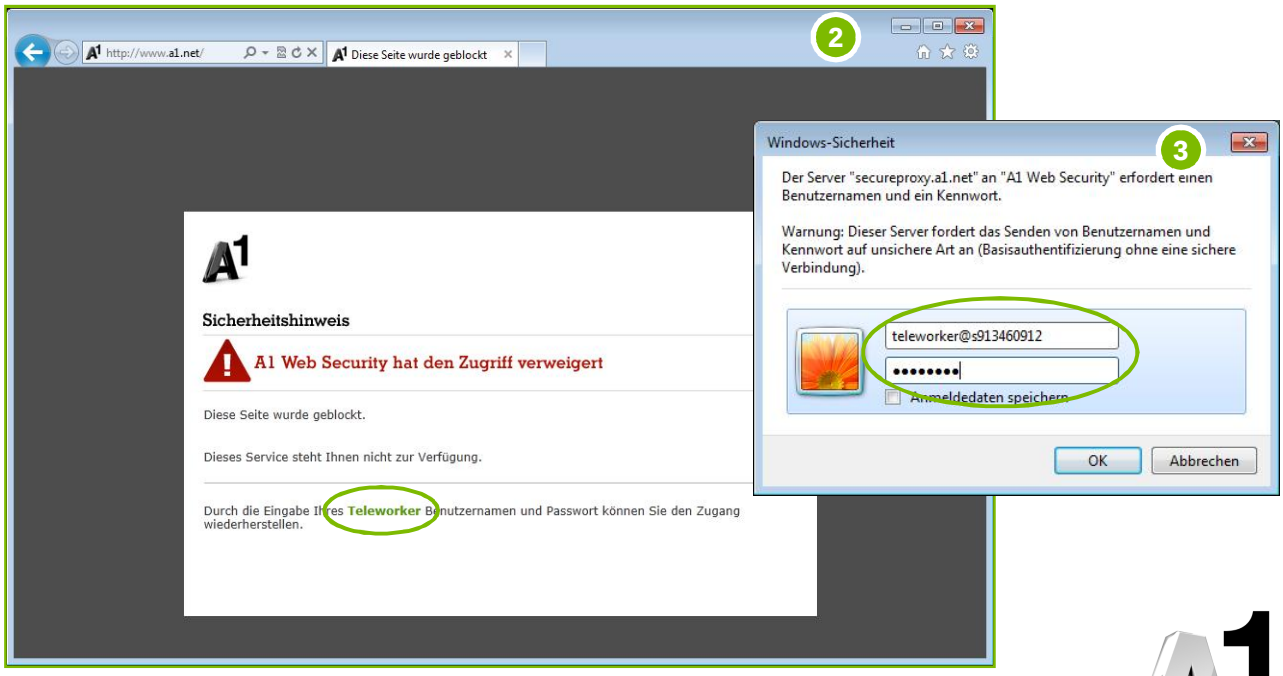
1. **Auf der Seite „Teleworker“ können Sie ein Passwort selber wählen oder generieren lassen.**

   Der zugehörige Benutzername ist vorgegeben.



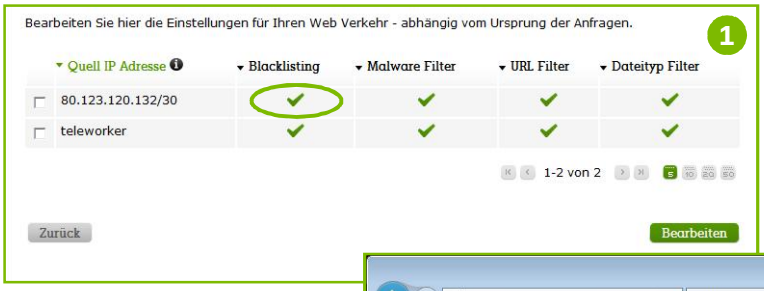
2. **Benutzer die im Web Browser den Proxyserver secureproxy.a1.net verwenden und A1 Web Security von unterwegs aus nutzen, erhalten beim Aufruf einer beliebigen Internetseite einen Sicherheitshinweis. Mit Klick auf „Teleworker“ erfolgt die Authentifizierung am Proxyserver.**

3. **Nach erfolgreicher Eingabe von Benutzername und Passwort wird der Zugang zum Internet hergestellt und die Nutzungsrichtlinie „Teleworker“ angewendet.**

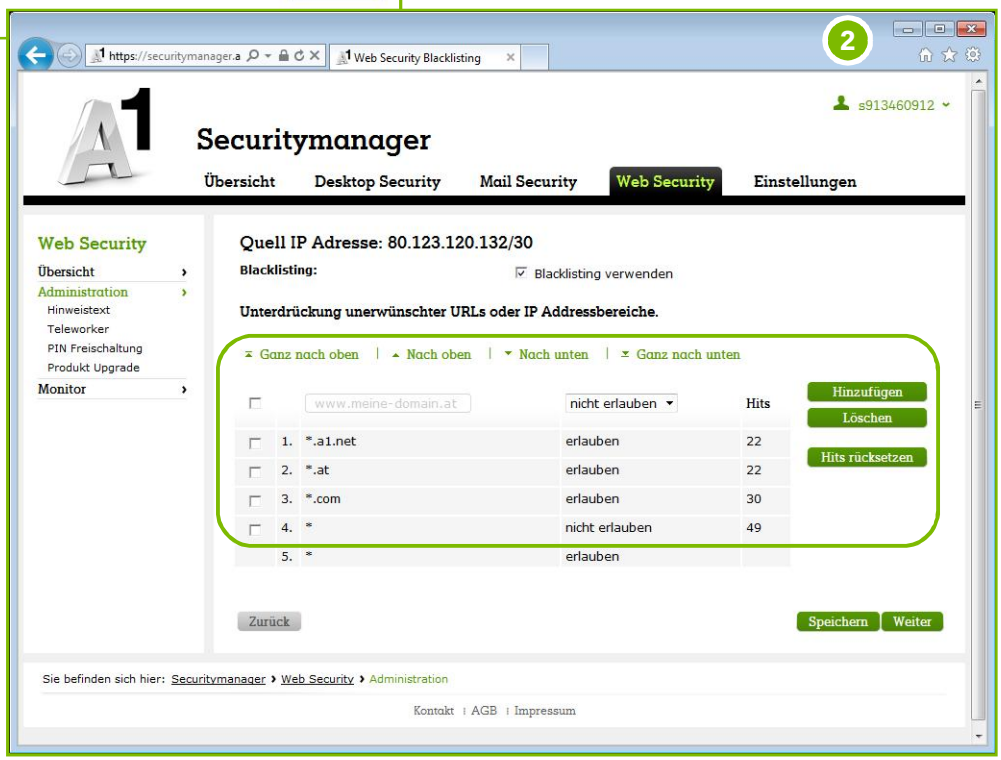


Blacklisting.

Stoppen Sie den Zugriff auf bestimmte Internetseiten und konfigurieren Sie Ausnahme-Regeln (Whitelisting).



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



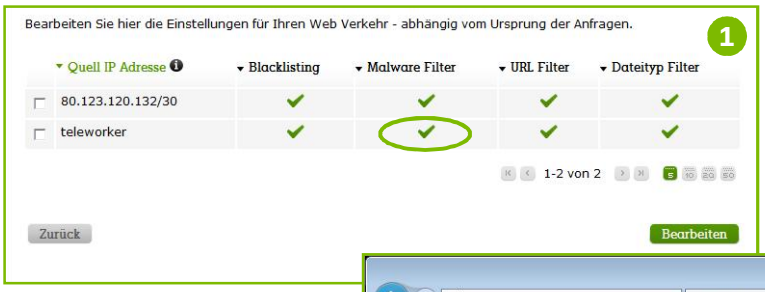
2. **Auf der Detailseite können Sie individuelle Filterregeln hinzufügen, sortieren bzw. umreihen und löschen. Das Filter-Regelwerk wird sequentiell abgearbeitet, Beginn mit der ersten Regel (top-down). Trifft eine Regel zu, so wird die Aktion ausgeführt und die darunter liegenden Regeln nicht weiter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

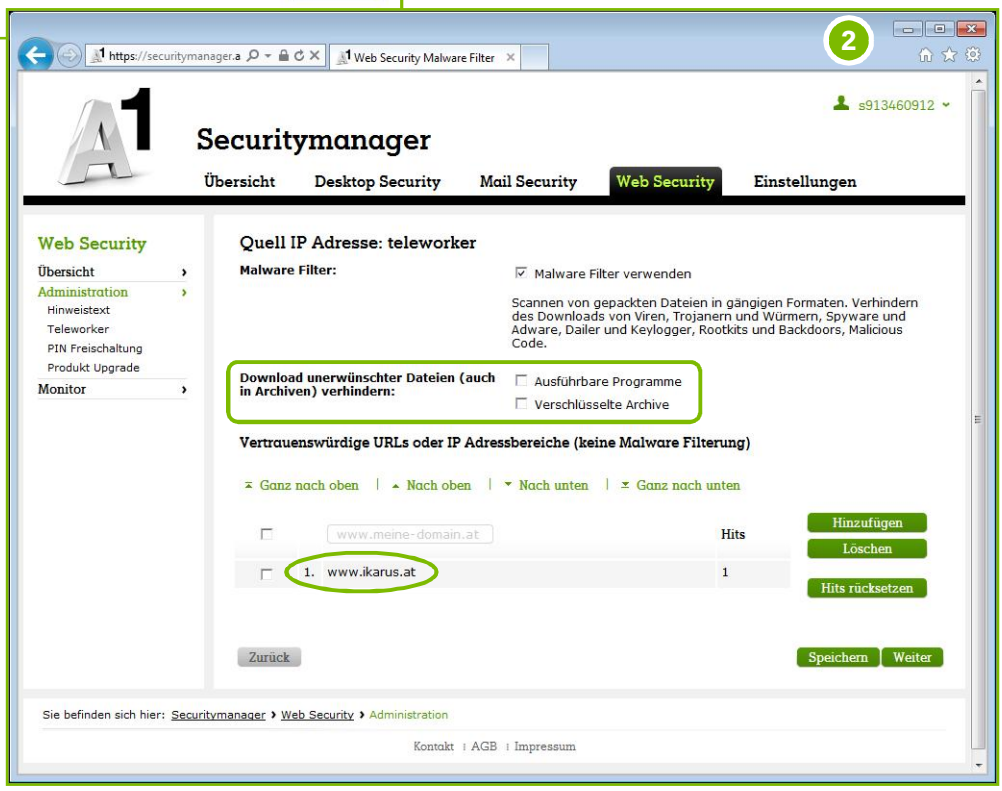
   Im gezeigten Beispiel ist der Aufruf von .at und .com Internetseiten für die Benutzer erlaubt. Alle anderen, mit Ausnahme von a1.net Webseiten, sind für die Benutzer gesperrt.

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

Malware Filter.

Verhindern Sie den Download von Schädlingen wie Viren, Trojaner & Co. auf Ihre Internet Arbeitsplätze.





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

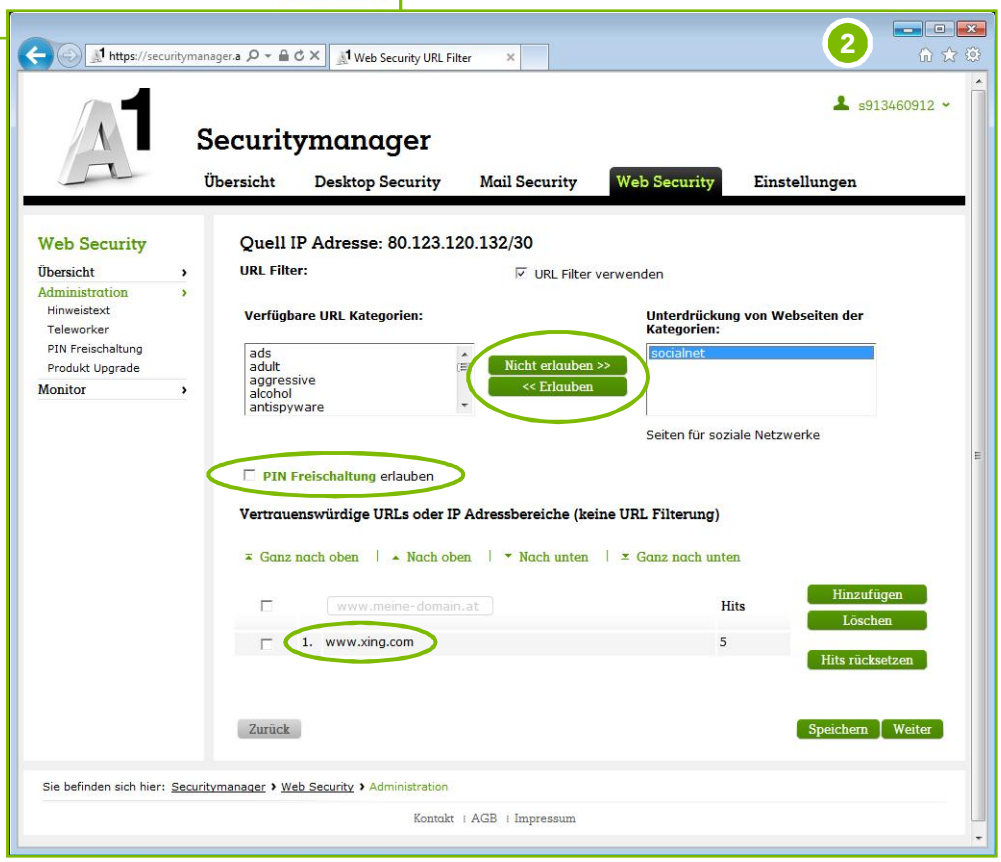
2. **Auf der Detailseite haben Sie die Möglichkeit einzustellen, ob auch der Download potentiell gefährlicher Dateien wie ausführbare Programme oder verschlüsselte Archivdateien geblockt werden sollen.**

   Weiters können Sie Ausnahme-Regeln hinzufügen. Im gezeigten Beispiel wird www.ikarus.at vertraut und diese Internetseite nicht auf Schadsoftware untersucht. Sie können somit Testviren von dieser Seite herunterladen.

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

URL Filter.

Unterbinden Sie den Aufruf von Webseiten, sortiert nach unterschiedlichen Themen und Interessen.



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

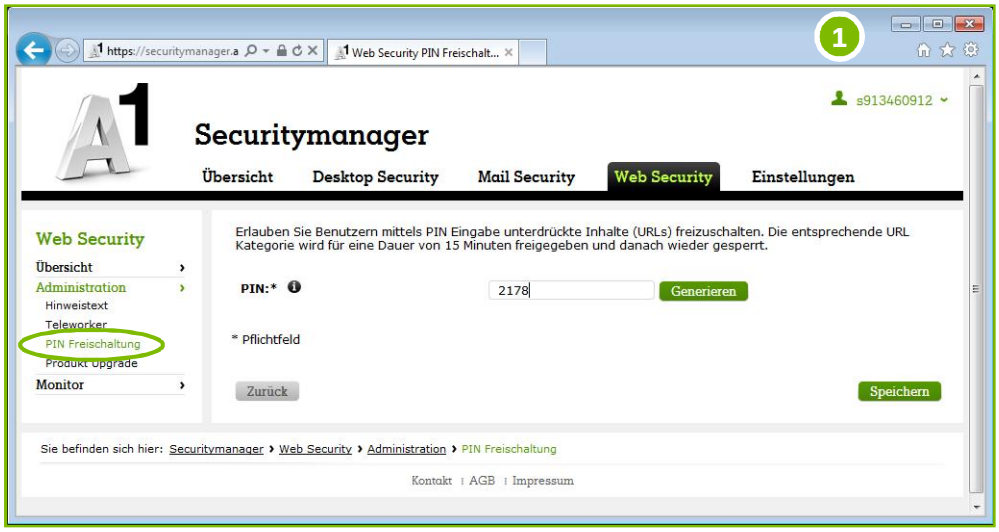
2. **Auf der URL Filter-Detailseite finden Sie Kategorien von Internetseiten. Wählen Sie jene Kategorien aus, die Sie für Ihre Benutzer „Erlauben“ oder „Nicht erlauben“ möchten. Im Beispiel werden Socialnetwork-Seiten (Facebook, Twitter, usw.) gesperrt. Der Zugriff auf Xing wird mit einer Ausnahme-Regel gestattet.**

   Mit der Funktion „PIN Freischaltung“ geben Sie Ihren Internet Benutzern die Möglichkeit auf zunächst gesperrte Webseiten (im Beispiel Socialnetwork-Seiten) nach Eingabe eines PINs zuzugreifen.

PIN Freischaltung verwenden.

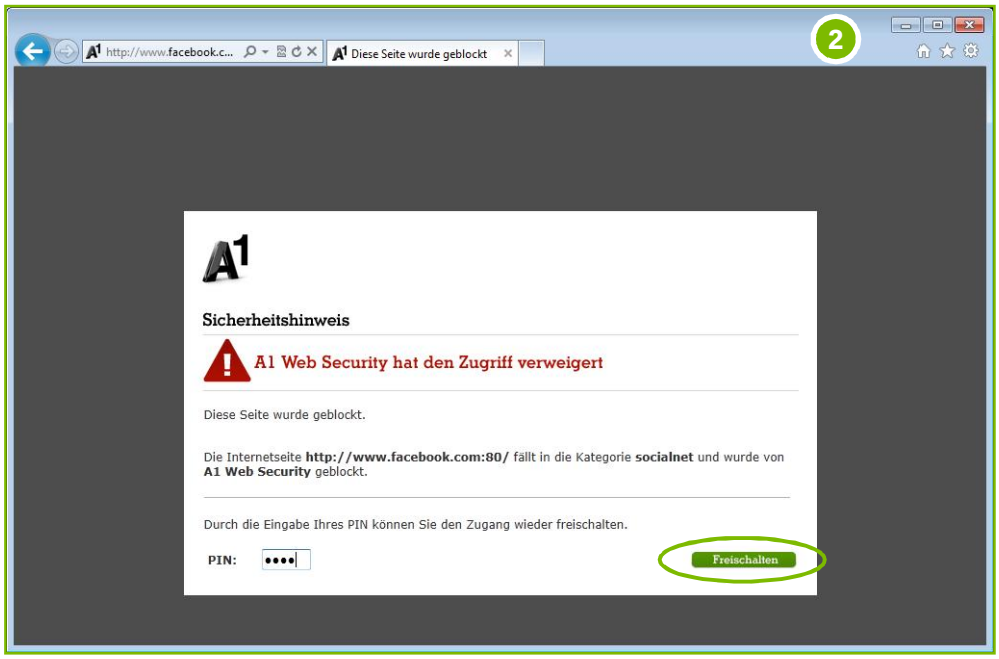
Legen Sie einen vierstelligen PIN fest, damit einzelne Benutzer geblockte Internetseiten entsperren können.

1. **Auf der Seite „PIN Freischaltung“ können Sie einen PIN selber wählen oder automatisch generieren lassen.**



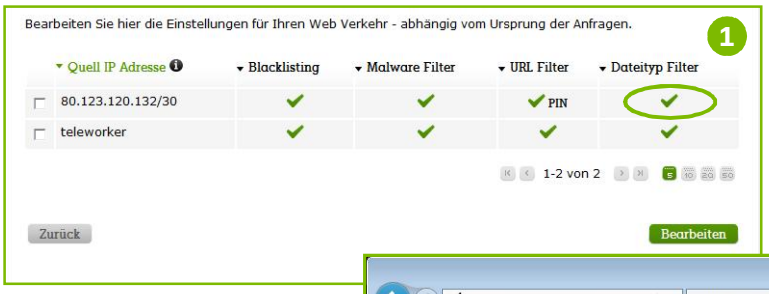
2. **Benutzer die diesen vierstelligen PIN kennen, haben die Möglichkeit gesperrte URL Kategorien (im Beispiel Socialnetwork-Seiten) mit dem Button „Freischalten“ für eine Dauer von 15 Minuten zu entsperren.**

   Nach Ablauf der Zeit wird die entsprechende URL Kategorie für Ihren Business Internet Anschluss wieder gesperrt und der PIN muss vom Benutzer gegebenenfalls erneut eingetippt werden.

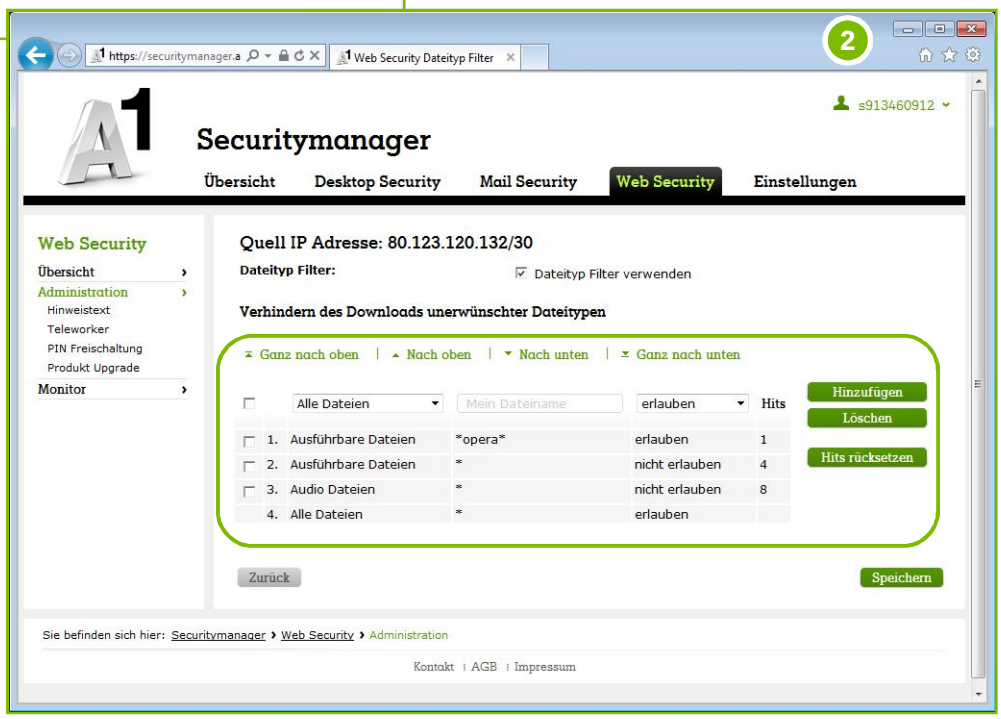


Dateityp Filter.

Stoppen Sie den Download unerwünschter Dateien und konfigurieren Sie Ausnahme-Regeln (Whitelisting).



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



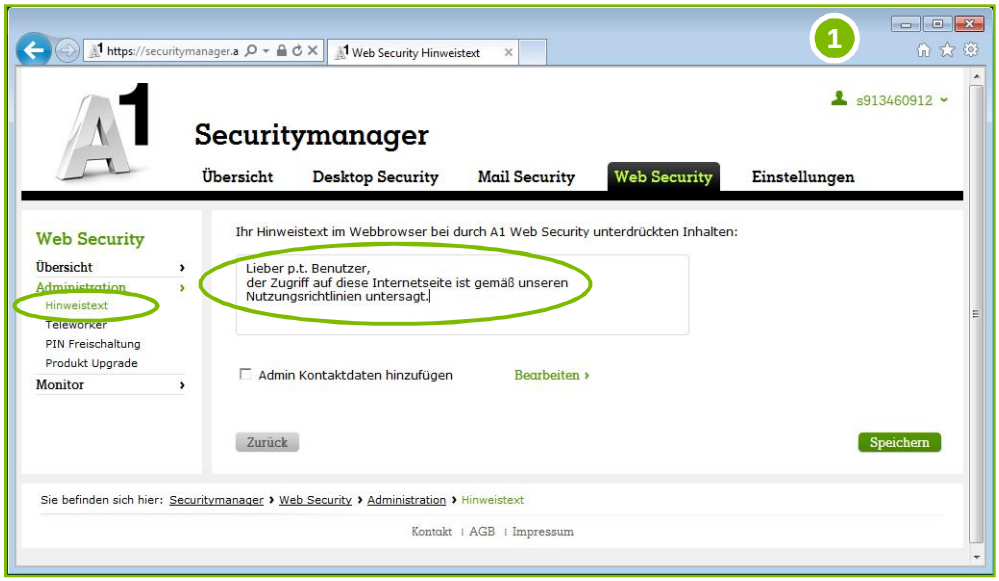
2. **Auf der Detailseite können Sie individuelle Filterregeln hinzufügen, sortieren oder löschen. Das Filter-Regelwerk wird sequentiell abgearbeitet, Beginn mit der ersten Regel (top-down). Trifft eine Regel zu, so wird die Aktion ausgeführt und die darunter liegenden Regeln nicht weiter überprüft (fire-and-forget).**

   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).

Hinweistext an die Benutzer.

Formulieren Sie eine individuelle Nachricht welche die Benutzer bei gesperrten Internetseiten sehen.

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



2. **Beim ansurfen von gesperrten Webseiten erhalten die Benutzer den A1 Web Security Sicherheitshinweis ergänzt um Ihren persönlichen Hinweistext.**