

Authentifizierung am http Proxy

Domänenfremde Geräte

OctoGate
EINFACH. SICHER. GESCHÜTZT. -

Version 1.4

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
8.12.2016	Felix Wischke	1.0	Initial-Dokument
14.01.2017	Felix Wischke	1.1	Mobile Geräte im Detail
31.01.2017	Felix Wischke	1.2	Windows im Detail
01.02.2017	Felix Wischke	1.3	Proxy Autokonfiguration
23.02.2017	Jan Wagner	1.4	Überarbeitung

Inhalt

1	Authentifizierung am Proxy.....	4
	SPNEGO	4
	NTLMSSP	4
	Digest	5
	Basic.....	5
1.1	Authentifizierung domänenfremder Geräte.....	6
2	Authentifizierung in Windows	7
	Internet Explorer 11	7
	Chrome.....	9
	Firefox	12
3	Android.....	15
	WLAN Einstellungen.....	15
	Chrome Mobile	16
	Firefox Mobile	17
4	iOS Safari	20
5	Proxy Autokonfiguration	21

1 Authentifizierung am Proxy

Der Proxy-Server der OctoGate operiert als konventioneller HTTP/HTTPS-Proxy auf der Adresse octo.octo:8080 oder alternativ als transparenter Proxy.

Eine Authentifizierung ist nur möglich, wenn ein Client explizit weiß, dass er mit einem Proxy verbunden ist. Im Falle eines transparenten Proxys kann ein Client nicht feststellen, dass ein Proxy eine Authentifizierung anfordert. Deswegen kann in diesem Fall nur über Kriterien wie die IP-Adresse des Clients autorisiert werden (in der OctoGate ein sog. MixedMode User).

Eine Authentifizierung ist Bestandteil des HTTP-Protokolls (<https://tools.ietf.org/html/rfc7235>). Dafür wird der HTTP-Code ,407 – Proxy Authentication Required‘ verwendet. Folgend im HTTP-Header schickt der Proxy die unterstützten Mechanismen zur Authentifizierung mit.

Die zurzeit gängigen Verfahren sind SPNEGO, NTLMSSP, Digest und Basic.

SPNEGO

SPNEGO ist ein Mechanismus zum Aushandeln eines Authentifizierungsverfahrens. Das gängige Verfahren ist hier das Kerberos Protokoll, welches allerdings ein gültiges Ticket vom Kerberos-Server benötigt. Kerberos setzt deshalb voraus, dass der Client zuerst Mitglied der Domäne ist. Wenn Kerberos nicht ausgehandelt werden kann, wird stattdessen NTLMSSP benutzt.

NTLMSSP

NTLMSSP ist das NT Lan Manager Security Support Provider Verfahren. Dieses funktioniert mittels der Verarbeitung des NT-Passworthashes des Clients. Der Client antwortet auf eine Challenge des Domänencontrollers. Die richtige Beantwortung der Challenge beweist die Kenntnis des Passworts, ohne dass das Passwort im Klartext übertragen werden muss. Innerhalb des NTLMSSP können

verschiedene Protokollversionen ausgehandelt werden: LM, NTLM und NTLMv2.

Digest

Digest ist als Verfahren dem NTLMSSP ähnlich, die Verarbeitung des Passworthashes ist allerdings flexibel gehalten. In den meisten Fällen ist deshalb Kenntnis des Passworts auf der Proxyseite erforderlich.

Basic

Basic ist das älteste Verfahren zur Authentifizierung. Das Passwort wird im Base64-Verfahren encodiert und dann übertragen. Es bietet deshalb keinen weiteren Schutz des Passworts.

1.1 Authentifizierung domänenfremder Geräte

Bei einer Active-Directory-Domäne scheidet Digest als Verfahren aus, da die Passwörter der Clients nur als NT-Hash auf dem Domänencontroller verfügbar sind. Da die Geräte nicht zur Domäne gehören scheidet ebenfalls SPNEGO aus. Als Verfahren zur Authentifizierung bleibt deshalb nur NTLMSSP übrig. Basic kann durch den Proxy zu NTLM umgesetzt werden, indem der Proxy mit den Klartext-Credentials den NT-Passworthash ausrechnet. Diese zwei Verfahren werden deshalb vom OctoGate-Proxy advertiert.

Der Proxy selber leitet Authentifizierungsanfragen nur an den Domänencontroller weiter, dazu muss die OctoGate aber Mitglied der Domäne sein.

Eine Mitgliedschaft des Clientgeräts ist nicht zwingend notwendig, der Benutzer eines Clientgerätes muss allerdings durch Authentifizierung beweisen, dass er gültige Credentials für die Domäne besitzt.

Damit ein Client sich erfolgreich authentifizieren kann, muss er zuerst ein Verfahren auswählen. Dabei fangen alle Clients automatisch mit größerer Sicherheit an. NTLMSSP kommt also immer vor Basic, NTLMv2 wird vor NTLM und LM gewählt.

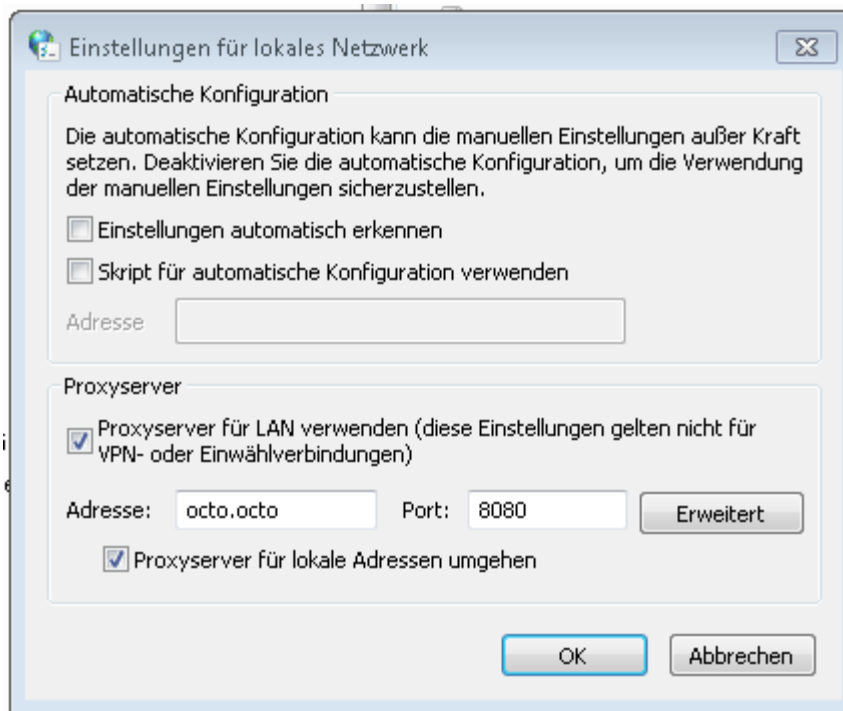
Auf die ausgehandelte Protokoll-Version hat der Proxy keinen Einfluss. Ältere NTLM-Versionen können im Domänencontroller per Policy deaktiviert werden, was aber die Authentifizierung von Geräten verhindert, die Probleme mit NTLMv2 haben.

Damit der Client den Proxy auch findet, muss er über den Nameserver den Namen octo.octo auflösen können. Ist die OctoGate nicht der Nameserver, muss in Ihrem Nameserver ein entsprechender Eintrag hinterlegt werden.

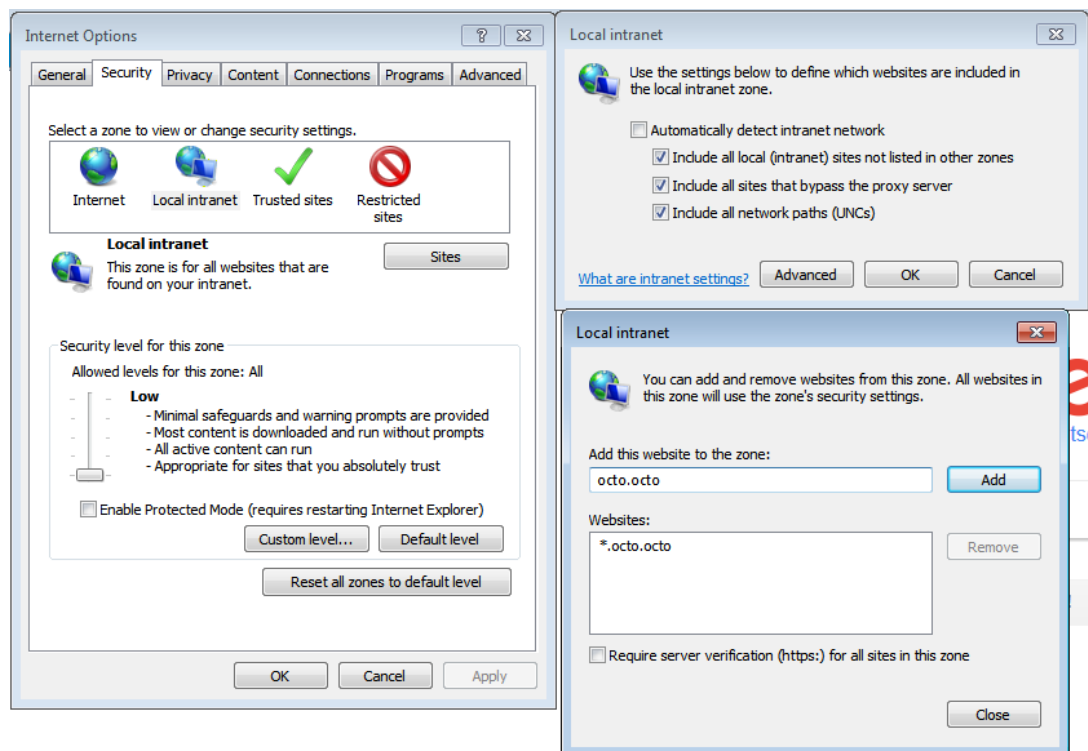
2 Authentifizierung in Windows

Internet Explorer 11

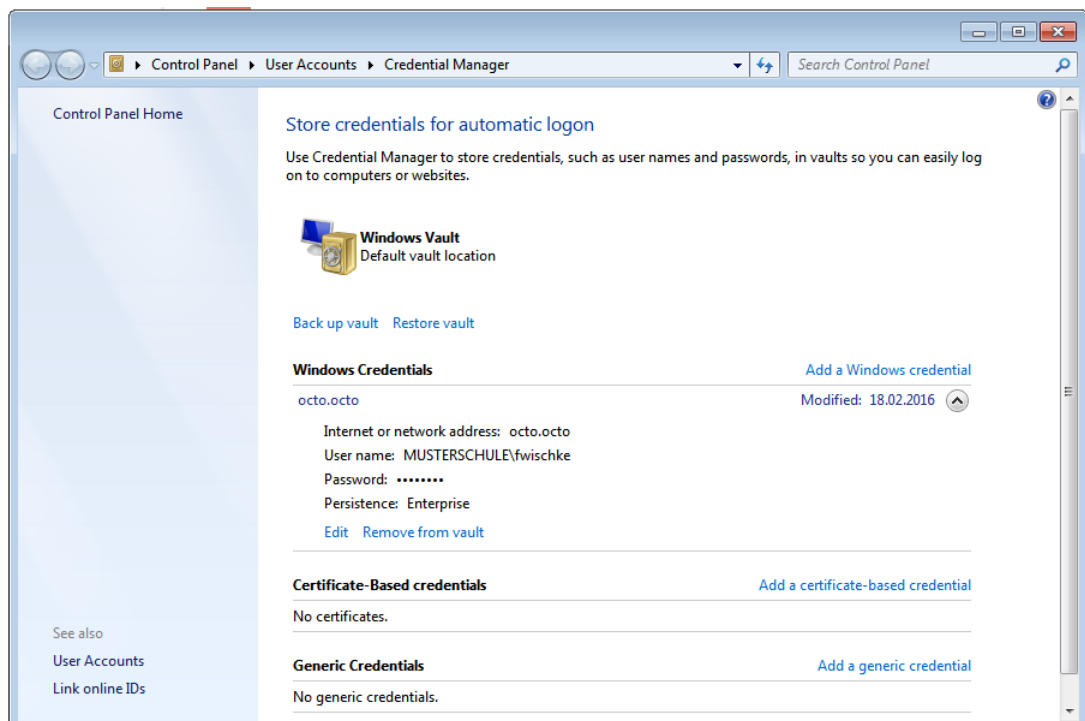
Der Internet Explorer benutzt die systemweiten Proxyeinstellungen. Diese sind über die Internetoptionen zu erreichen. Hier muss octo.octo mit dem Port 8080 hinterlegt werden.



Damit das System erlaubt, dass am Proxy authentifiziert wird, muss octo.octo in der Intranetzone liegen. Sollte dies nicht automatisch erkannt werden, muss dieser Eintrag manuell zur Intranetzone hinzugefügt, und gegebenenfalls die Sicherheitseinstellungen angepasst, werden.

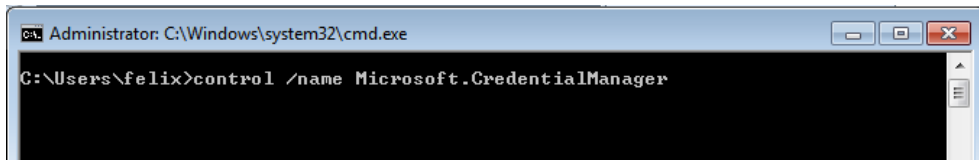


Als letztes müssen noch Credentials für octo.octo hinterlegt werden. Dies geht über den systeminternen Credential Manager.



Der Username „musterschule\fwischke“ ist in dem Format „Domäne\User“ gehalten. Dies ist nicht immer zwingend notwendig, aber auf jeden Fall eindeutig.

Der Credential Manager ist über die Startmenüsuche zu erreichen. Er kann aber in jedem aktuellem Windows über folgende Kommandozeile aufgerufen werden:



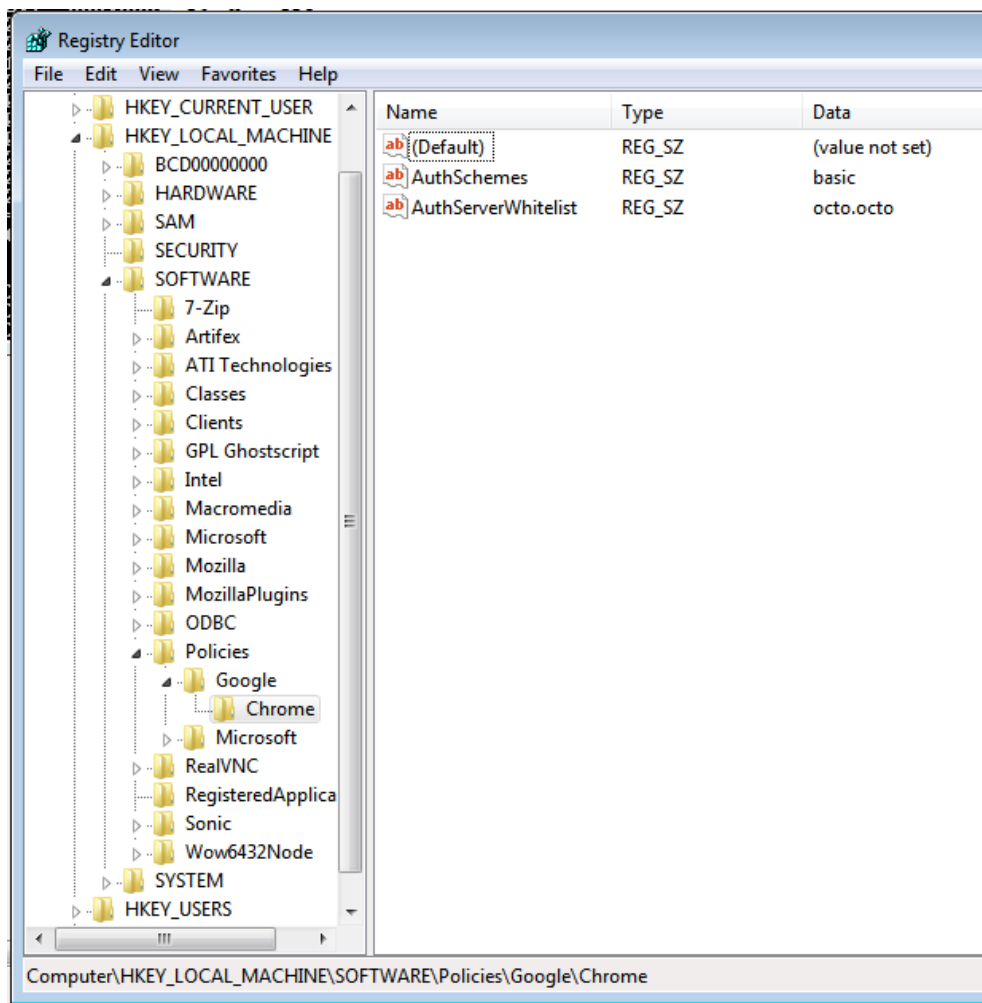
Chrome

Chrome benutzt die systemweiten Proxyeinstellungen. Die Konfiguration unterscheidet sich in dieser Hinsicht nicht vom Internetexplorer. Allerdings wird Chrome octo.octo nicht als Intranetseite ansehen. Dazu als Quelle <https://dev.chromium.org/developers/design-documents/http-authentication>.

Insbesondere der Abschnitt: "In Windows only, if the AuthServer-Whitelist setting is not specified, the permitted list consists of those servers in the Local Machine or Local Intranet security zone (for example, when the host in the URL includes a"."character it is outside the Local Intranet security zone), which is the behavior present in IE. Treating servers that bypass proxies as being in the intranet zone is not currently supported."

Dies führt dazu, dass im Chrome zulässige Authentifizierungsserver per Policy mitgeteilt werden müssen. Ebenfalls funktioniert das gesamte NTLM-Protokoll nicht zuverlässig, wenn das Gerät nicht in der Domäne ist. Für einen reibungslosen Betrieb muss es deshalb durch eine weitere Policy deaktiviert werden.

Das Setzen der Policy ist zur Zeit nur über Registryeinträge möglich. Die dementsprechenden Direktiven über die Kommandozeile werden in Windows zurzeit ignoriert.



Die Registryeinträge werden im Detail hier erläutert:

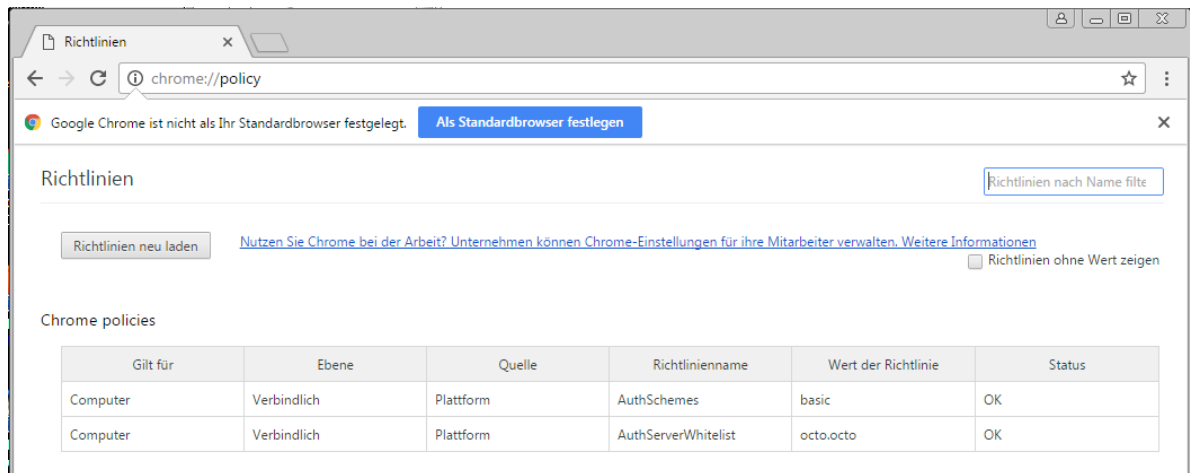
<https://dev.chromium.org/administrators/policy-list-3#AuthServerWhitelist>

<https://dev.chromium.org/administrators/policy-list-3#AuthSchemes>

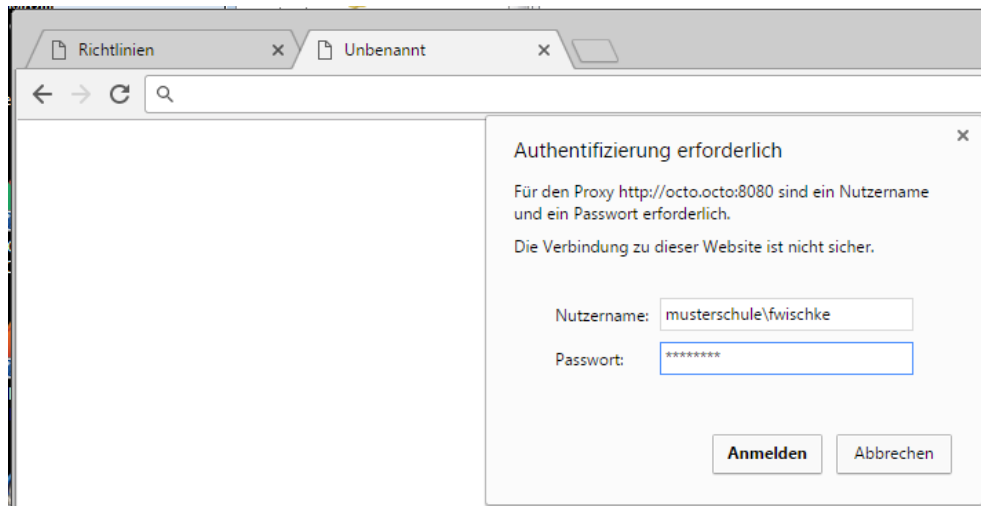
Der Eintrag AuthSchemes darf nur den Wert basic enthalten, sonst versucht Chrome bei jedem Request wieder NTLM auszuhandeln und scheitert subsequent.

AuthServerWhitelist muss auf octo.octo (oder die korrespondierende IP-Adresse) gesetzt werden. Nur dann werden Authentifizierungsaufforderungen auch beantwortet.

Dass die Policies gesetzt sind, kann über die eingebaute Seite `chrome://policy` verifiziert werden.

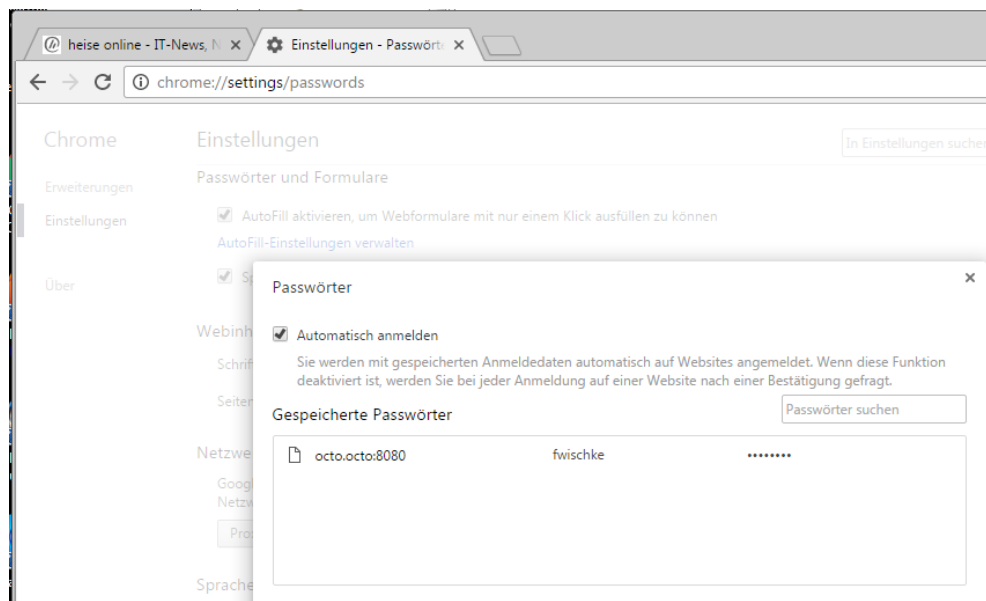


Chrome wird beim Starten nach Credentials fragen, selbst wenn im Windows Credential Manager bereits ein Login hinterlegt ist.



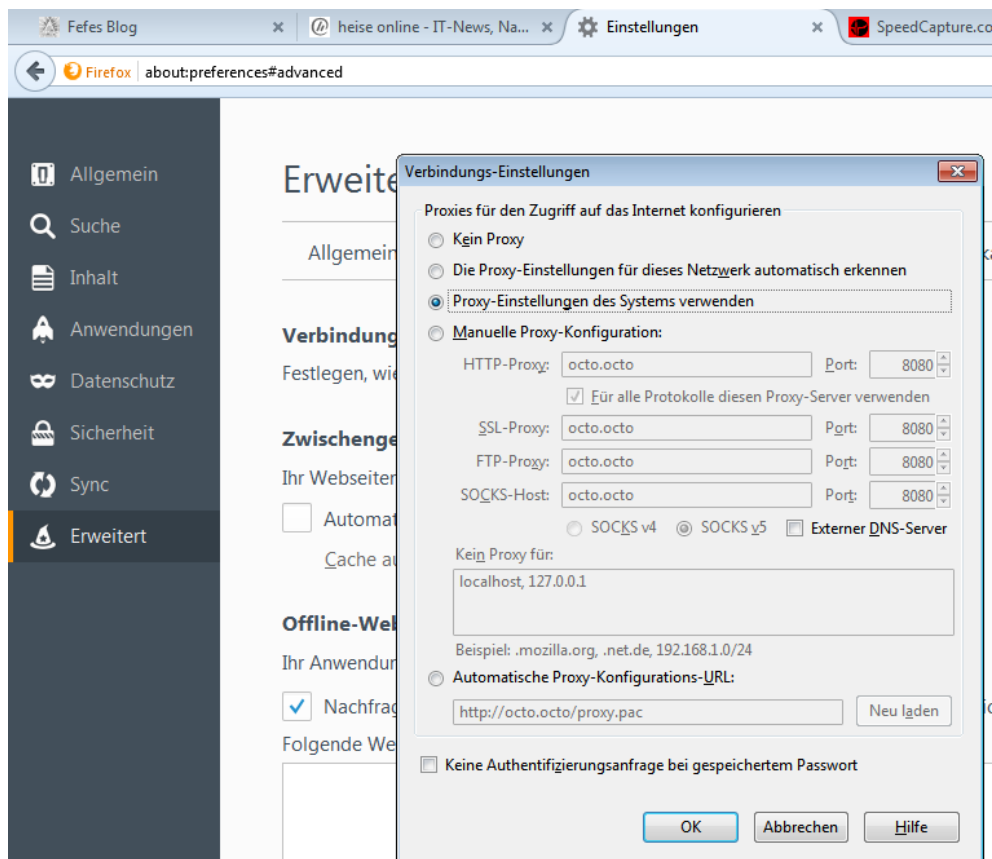
Nach erfolgreicher Anmeldung möchte Chrome die Credentials speichern. Sollten die Credentials nicht gespeichert werden, sind sie nur für die laufende Session hinterlegt.

Der Chrome Password Manager ist über die URL `chrome://settings/passwords` erreichbar. Sollten die Credentials in der Domäne ungültig werden, können sie hier gelöscht werden.



Firefox

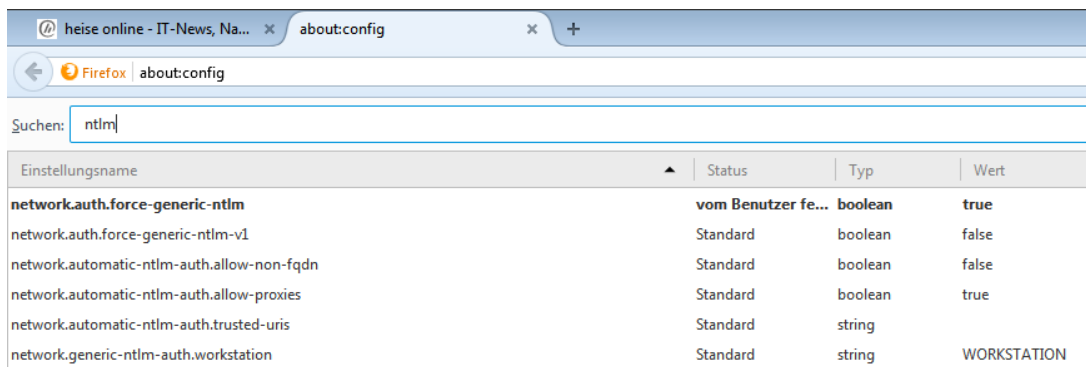
Im Gegensatz zu Chrome und Internetexplorer hat Firefox eigene Proxyeinstellungen, kann aber die Einstellungen des Systems übernehmen.



Alternativ kann manuell octo.octo:8080 als Proxy eingetragen werden. Der Proxy tunnelt das Socks-Protokoll nicht, nur anonymes, passives FTP.

Mit Firefox funktioniert NTLMv2 nicht. Die Policies bieten allerdings die Möglichkeit, stattdessen generisches NTLM zu verwenden. Dies ist dem Basic-Verfahren gegenüber zu bevorzugen.

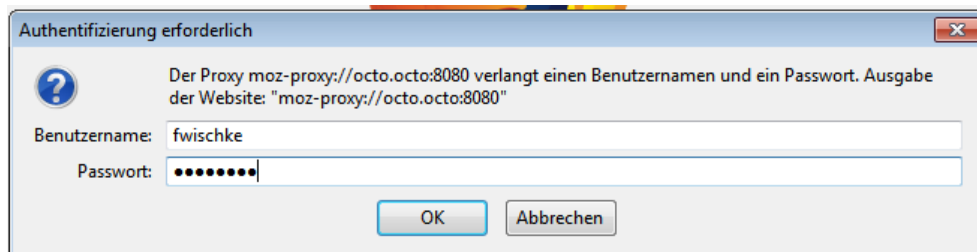
Um NTLM zu erzwingen, muss in den Firefox-Einstellungen `about:config` die Policy `,network.auth.force-generic-ntlm'` auf `,true'` gesetzt werden.



The screenshot shows the Firefox 'about:config' page with the search bar containing 'ntlm'. A table of settings is displayed below the search bar.

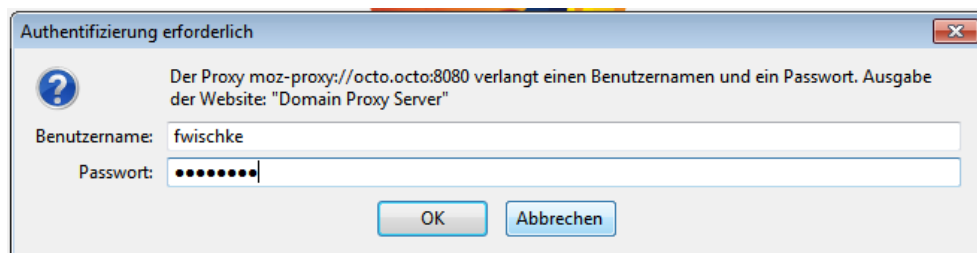
Einstellungsname	Status	Typ	Wert
network.auth.force-generic-ntlm	vom Benutzer fe...	boolean	true
network.auth.force-generic-ntlm-v1	Standard	boolean	false
network.automatic-ntlm-auth.allow-non-fqdn	Standard	boolean	false
network.automatic-ntlm-auth.allow-proxies	Standard	boolean	true
network.automatic-ntlm-auth.trusted-uris	Standard	string	
network.generic-ntlm-auth.workstation	Standard	string	WORKSTATION

Danach muss Firefox neu gestartet werden. Beim nächsten Aufruf einer Website kann authentifiziert werden.



Danach wird Firefox danach fragen, die Credentials zu speichern. Wie bei Chrome sind die Credentials sonst nur für die laufende Session gültig.

Sollte in der Domäne das generische NTLM Verfahren nicht erlaubt sein, kann hier ‚Abbrechen‘ selektiert werden. Danach erscheint ein subtil verschiedenes Authentifizierungsfenster:

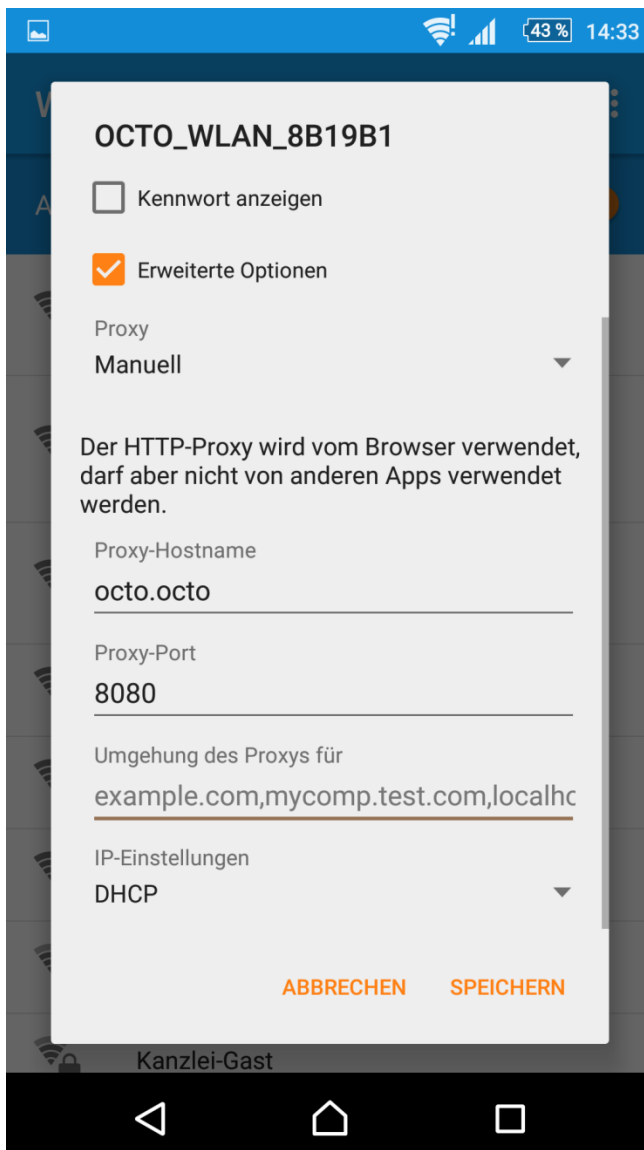


In diesem Fall übersetzt der OctoGate-Proxy das Authentifizierungsverfahren Basic zu NTLM für den Client.

3 Android

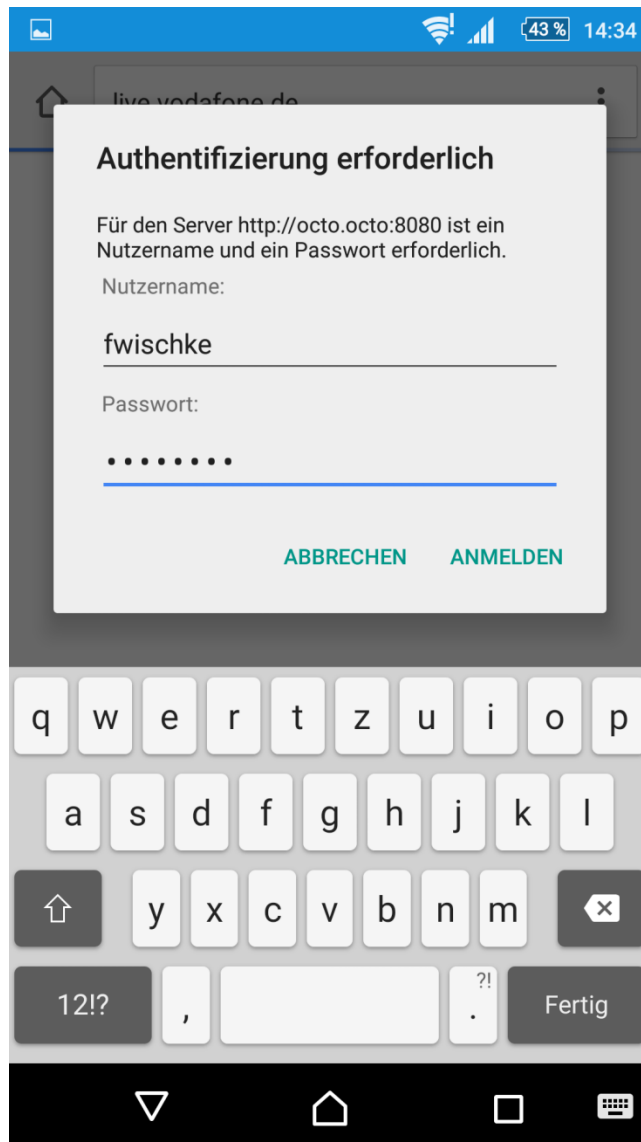
WLAN Einstellungen

Das Einrichten des Proxys passiert bei Android ausnahmslos pro WLAN-Profil. Durch längeres Selektieren des Profils lässt sich ein Kontextmenü öffnen. Dort müssen die erweiterten Einstellungen ausgewählt werden.

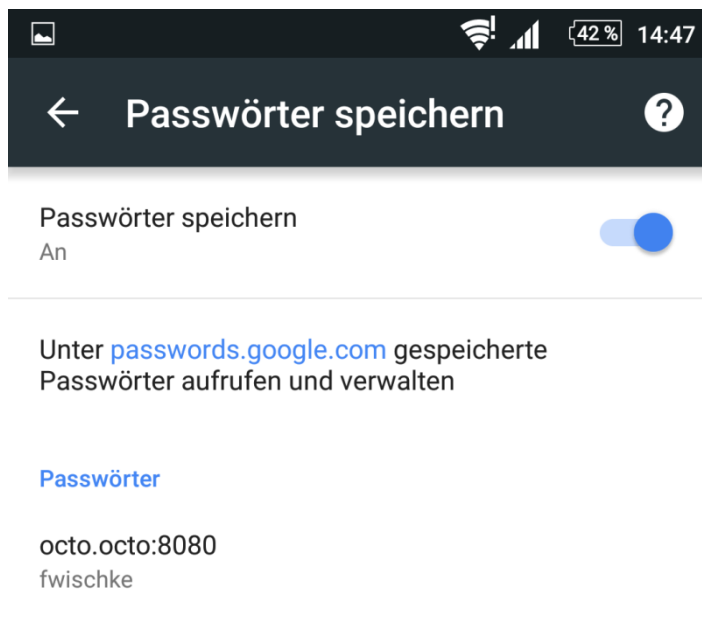


Chrome Mobile

Chrome erkennt automatisch, dass Credentials zur Authentifizierung benötigt werden. Es gibt nichts weiter zu beachten.

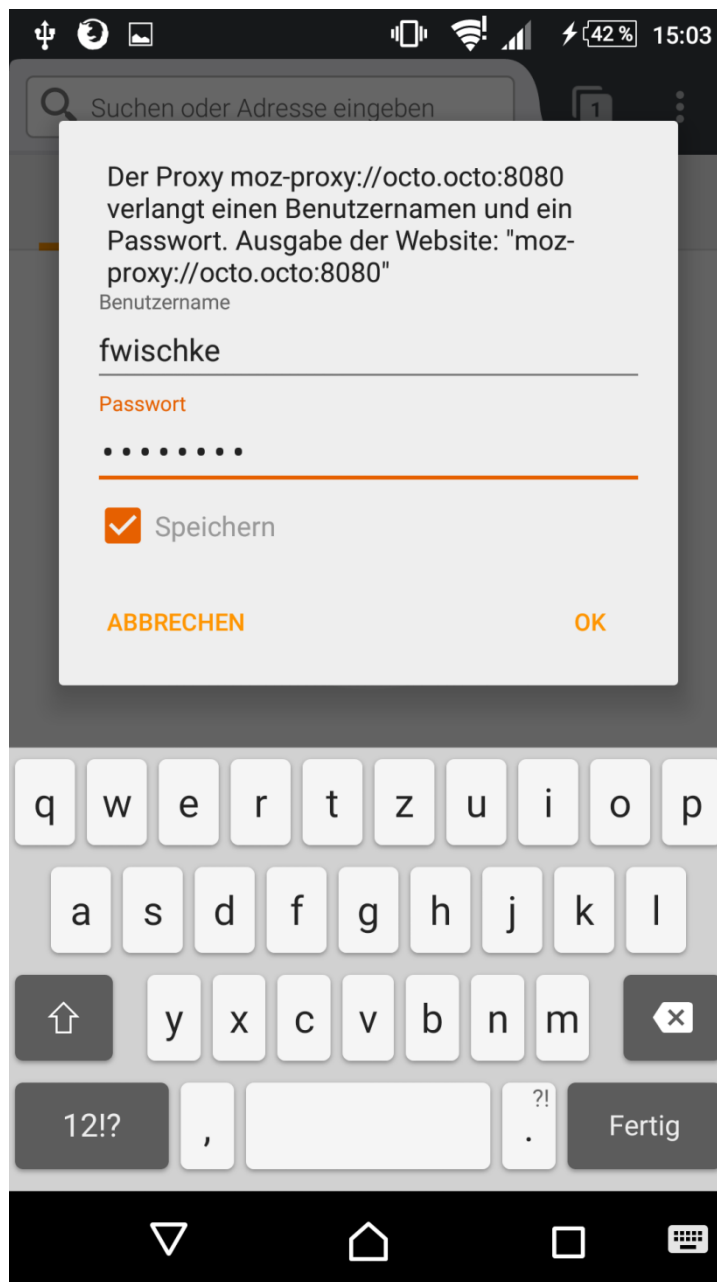


Chrome wird danach fragen, ob die Credentials gespeichert werden sollen. Sie werden danach pro Session einmal verifiziert. Trotzdem existiert ein Credential Manager.

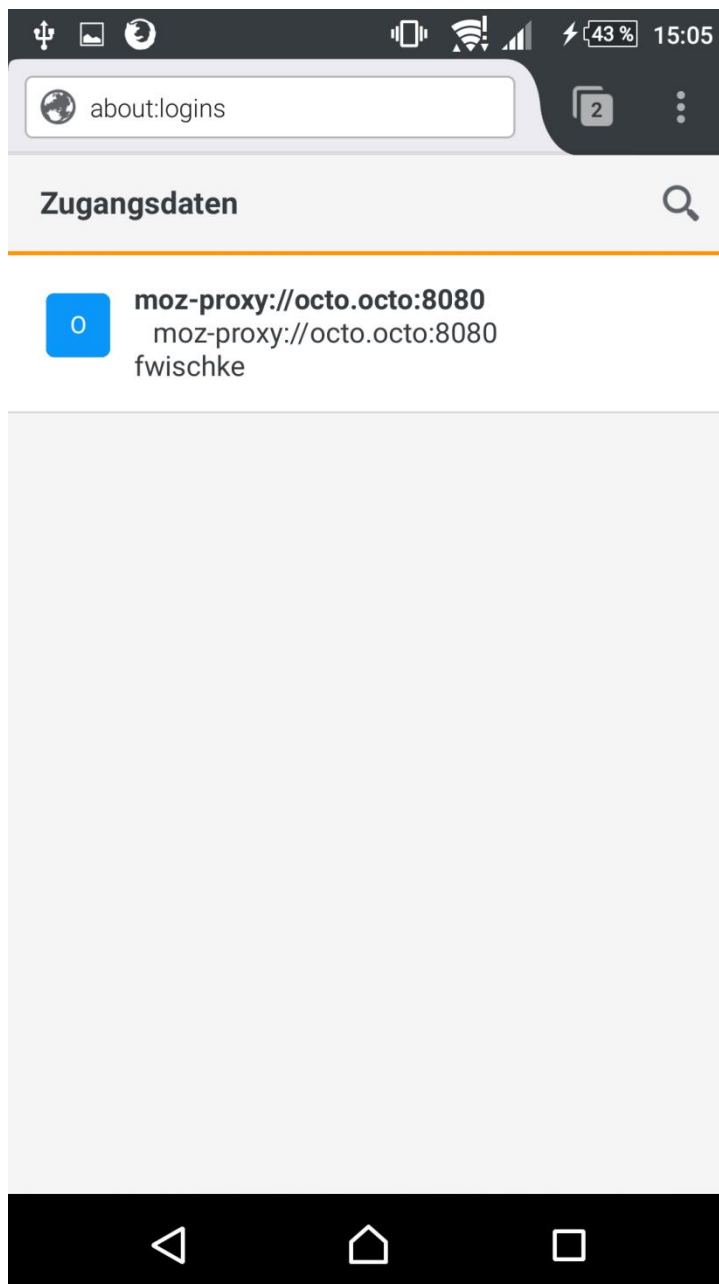


Firefox Mobile

Wie Chrome Mobile benötigt Firefox Mobile keine weiteren Einstellungen.

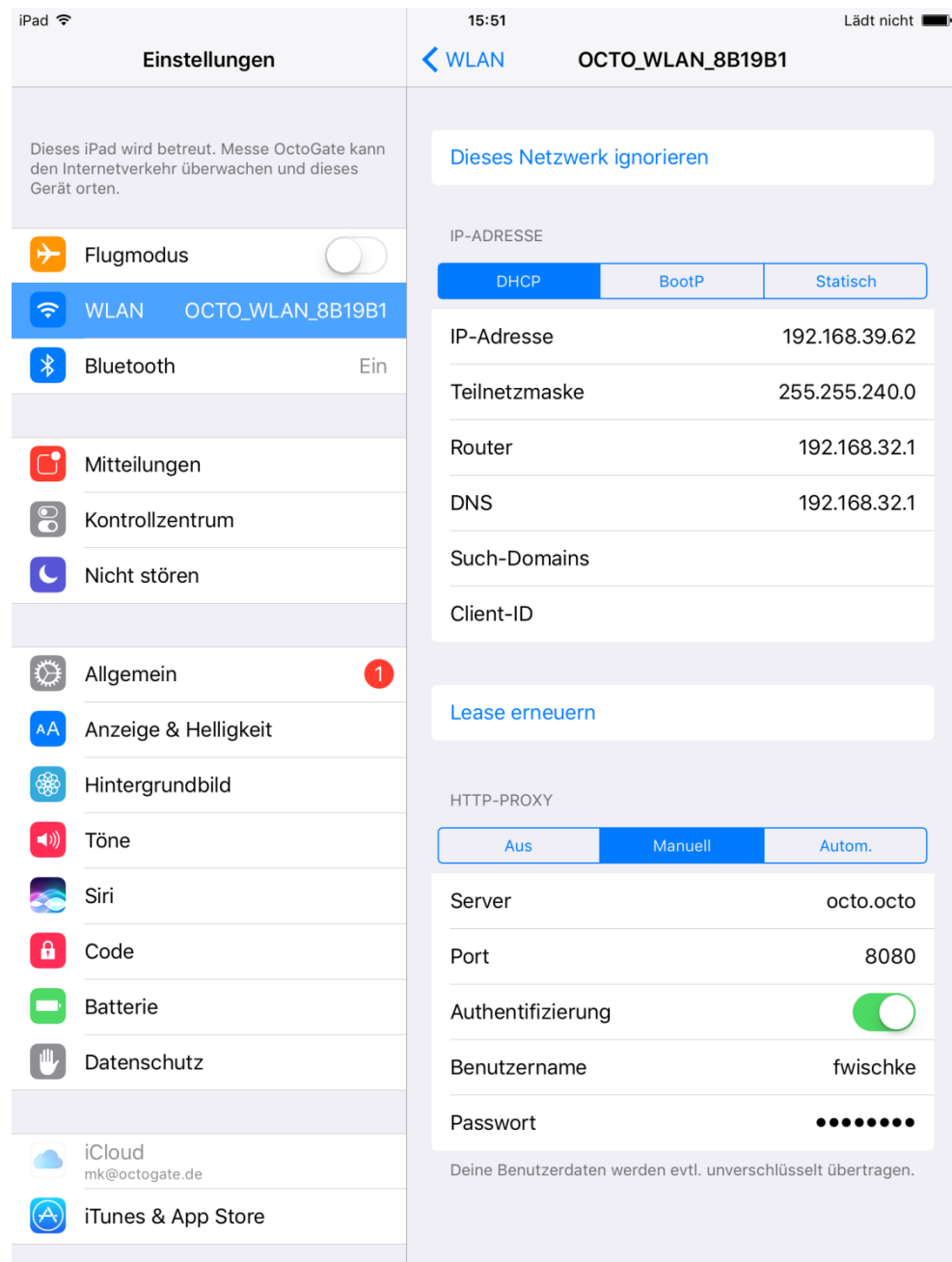


Es bietet ebenfalls das Speichern der Credentials an und verfügt über einen Credential Manager.



4 iOS Safari

Bei iOS findet die gesamte Proxykonfiguration über das WLAN-Profil statt. Es sind im Safari keine weiteren Einstellungen notwendig.



5 Proxy Autokonfiguration

Proxy Autokonfiguration dient dazu, das Verhalten des Clients gegenüber dem Proxy genauer zu definieren. Dabei kann mitgeteilt werden, für welche URLs überhaupt ein Proxy benutzt werden soll und welche direkt geladen werden sollen. Ferner ist es möglich für unterschiedliche Protokolle unterschiedliche Proxys zu definieren. Z.B. kann für RSYNC/FTP/Socks ein anderer Proxy benutzt werden als für http.

Die OctoGate unterstützt Proxy-Autokonfiguration über die URL `http://octo.octo/proxy.pac`

Dafür muss allerdings am zugehörigen Netzwerkinterface der Port TCP:80 geöffnet sein. Der Inhalt der Proxy.pac beschränkt sich darauf, die Intranetzone der Domäne `*.domain.name` vom Proxy auszunehmen.

Die automatische Erkennung des Proxys über WPAD wird nicht unterstützt.