# Authentifizierung am http Proxy

Domänenfremde Geräte



Version 1.4

#### **OctoGate - Technische Dokumentation**

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

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

Verantwortlicher für den Inhalt: Frank Menne

Version	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

Authentifizierung am Proxy	4
SPNEGO	4
NTI MSSP	Δ
Digest	∓ 5
	5 5
Dasic	
Authentifizierung domänenfremder Geräte	6
Authentifizierung in Windows	7
Internet Explorer 11	7
Chrome	g
Firefoy	12
	12
Android	15
WI AN Finstellungen	15
Chrome Mobile	16
Firefox Mobile	10
	17
iOS Safari	20
	20
Proxy Autokonfiguration	21
	Autnentifizierung am Proxy

-

### **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.

😢 Einstellun	gen für lokales Netz	werk			X
Automatisc	he Konfiguration				
Die automa setzen. De der manuel	atische Konfiguration k aktivieren Sie die auto Ilen Einstellungen sich(	ann die n matische erzustelle	nanuellen Einstellu : Konfiguration, ui :n.	ungen außer K m die Verwend	raft lung
📃 Einstellu	ungen automatisch erk	ennen			
🔲 Skript fo	ür automatische Konfi	guration	verwenden		
Adresse					
Proxyserve	er				
✓ Proxyse VPN- oc	erver für LAN verwend Ier Einwählverbindung	den (dies) jen)	e Einstellungen ge	elten nicht für	
Adresse:	octo.octo	Port:	8080	Erweitert	
📝 Pro:	xyserver für lokale Ad	ressen u	ngehen		
			ОК	Abbrech	nen

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.

Internet Options	Local intranet 🖾
General Security Privacy Content Connections Programs Advanced	Use the settings below to define which websites are included in the local intranet zone.
Select a zone to view or change security settings.	Automatically detect intranet network
	$\overline{\mathbb{V}}$ Include all local (intranet) sites not listed in other zones
Internet Local intranet Trusted sites Restricted	Include all sites that bypass the proxy server
sites	Include all network paths (UNCs)
Local intranet         Sites           This zone is for all websites that are found on your intranet.         Sites	What are intranet settings? Advanced OK Cancel
	Local intranet
Security level for this zone Allowed levels for this zone: All  Low  Minimal safeguards and warning prompts are provided Most content is downloaded and run without prompts	You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
- All active content can run - Appropriate for sites that you absolutely trust	Add this website to the zone:
	octo.octo Add
Enable Protected Mode (requires restarting Internet Explorer)	Websites:
Custom level Default level	*.octo.octo Remove
Reset all zones to default level	
OK Cancel Apply	Require server verification (https:) for all sites in this zone
	Close

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/designdocuments/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.

) Richtlinien	×				
→ C O chrome://policy					
Google Chrome ist nicht als Ihr Standardbrowser festgelegt. Als Standardbrowser festlegen					
ichtlinien					Richtlinien nach Name filte
Richtlinien neu laden	Nutzen Sie Chrome bei der Arl	beit? Unternehmen können Chr	ome-Einstellungen für ihre N	fitarbeiter verwalten. Weitere In	formationen Richtlinien ohne Wert zeige
Richtlinien neu laden hrome policies Gilt für	Nutzen Sie Chrome bei der Art	beit? Unternehmen können Chr Quelle	ome-Einstellungen für ihre N Richtlinienname	litarbeiter verwalten. Weitere In Wert der Richtlinie	formationen Richtlinien ohne Wert zeige Status
Richtlinien neu laden hrome policies Gilt für Computer	Nutzen Sie Chrome bei der Art	beit? Unternehmen können Chr Quelle Plattform	ome-Einstellungen für ihre M Richtlinienname AuthSchemes	litarbeiter verwalten. Weitere In Wert der Richtlinie basic	formationen Richtlinien ohne Wert zeige Status OK

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

Richtlinien X	×
$\leftarrow \rightarrow$ C $\bigcirc$	
	Authentifizierung erforderlich Für den Proxy http://octo.octo:8080 sind ein Nutzername und ein Passwort erforderlich.
	Die Verbindung zu dieser Website ist nicht sicher. Nutzername: musterschule\fwischke Passwort: *******
	<b>Anmelden</b> Abbrechen

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.

eise online - Γ	T-News, N 🗙	🔹 Einstellungen - Passwörte 🗙			
$\epsilon \rightarrow \mathbf{C}$ (0 $\epsilon$	chrome:// <b>setti</b>	ngs/passwords			
	Einstell				
	Passwört	er und Formulare			
Einstellungen	AutoFil	toFill aktivieren, um Webformulare r Il-Einstellungen verwalten	nit nur einem Klick ausfüllen zu k	önnen	
	✓ Sp	Passwörter			×
	Webinh	<ul> <li>Automatisch anmelden</li> </ul>			
	Schrif	Sie werden mit gespeicherten deaktiviert ist, werden Sie bei	Anmeldedaten automatisch auf jeder Anmeldung auf einer Web:	Websites angemeldet. Wenn diese Funktion site nach einer Bestätigung gefragt.	
	Seiter	Gespeicherte Passwörter		Passwörter suchen	
	Netzwe	🗅 octo.octo:8080	fwischke		
	Googi Netzv				
	Pro				
	Sprache				

#### Firefox

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

Electric Street	nces#advanced				
<ul><li>Allgemein</li><li>Q Suche</li></ul>	Erweite	/erbindungs-Einstellur Proxies für den Zug ⊙ K <u>e</u> in Proxy	ngen riff auf das Internet konfigurieren –		
Inhalt	Allgemein	<ul> <li>Die Proxy-Einstellung</li> <li>Proxy-Einstellung</li> </ul>	ellungen für dieses Netz <u>w</u> erk autom ngen des Systems verwenden	natisch erker	nnen
Anwendungen	Verbindung	Manuelle Proxy	-Konfiguration:		
😎 Datenschutz	Festlegen, wie	HTTP-Proxy:	octo.octo √ <u>F</u> ür alle Protokolle diesen Prox	<u>P</u> ort: y-Server ver	8080 👻 wenden
🗟 Sicherheit	Zwischenge	<u>S</u> SL-Proxy:	octo.octo	Port:	8080 🔹
	Ibr Wobsoitor	FTP-Pro <u>x</u> y:	octo.octo	Po <u>r</u> t:	8080 🔹
💭 Sync	In webseiter	SO <u>C</u> KS-Host:	octo.octo	Por <u>t</u> :	8080
🗴 Erweitert	Automat <u>C</u> ache au	Kei <u>n</u> Proxy für: localhost, 127.	○ SOC <u>K</u> S v4	Externer [	<u>)</u> NS-Server
	Offline-Wel Ihr Anwendur Vachfrag Folgende We	Beispiel: .mozil C Automatische F http://octo.oc	la.org, .net.de, 192.168.1.0/24 Proxy-Konfigurations- <u>U</u> RL: to/proxy.pac gierungsanfrage bei gespeichertem OK Abbr	Passwort	leu l <u>a</u> den <u>H</u> ilfe

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.

@ heise online - IT-News, Na × about:config × +			
E Firefox about:config			
Suchen: ntlm			
Einstellungsname	Status	Тур	Wert
network.auth.force-generic-ntlm	vom Benutzer fe	boolean	true
network.auth.force-generic-ntlm network.auth.force-generic-ntlm-v1	vom Benutzer fe Standard	boolean boolean	<b>true</b> false
network.auth.force-generic-ntlm network.auth.force-generic-ntlm-v1 network.automatic-ntlm-auth.allow-non-fqdn	vom Benutzer fe Standard Standard	<b>boolean</b> boolean boolean	<b>true</b> false false
network.auth.force-generic-ntlm network.auth.force-generic-ntlm-v1 network.automatic-ntlm-auth.allow-non-fqdn network.automatic-ntlm-auth.allow-proxies	vom Benutzer fe Standard Standard Standard	<b>boolean</b> boolean boolean boolean	<b>true</b> false false true
network.auth.force-generic-ntlm network.auth.force-generic-ntlm-v1 network.automatic-ntlm-auth.allow-non-fqdn network.automatic-ntlm-auth.allow-proxies network.automatic-ntlm-auth.trusted-uris	vom Benutzer fe Standard Standard Standard Standard	boolean boolean boolean boolean string	<b>true</b> false false true

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

Authentifizierung	erforderlich
?	Der Proxy moz-proxy://octo.octo:8080 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "moz-proxy://octo.octo:8080"
Benutzername:	fwischke
Passwort:	••••••
	OK Abbrechen

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:

Authentifizierung	erforderlich
?	Der Proxy moz-proxy://octo.octo:8080 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "Domain Proxy Server"
Benutzername:	fwischke
Passwort:	••••••
	OK Abbrechen

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.

	🤿 📶 (43%) 14	:33
۷	OCTO WI AN 8B19B1	•
A	Kennwort anzeigen	
-	Erweiterte Optionen	
	Proxy Manuell	
line.	Der HTTP-Proxy wird vom Browser verwendet, darf aber nicht von anderen Apps verwendet werden.	
-	Proxy-Hostname	
, e	octo.octo	
M.	Proxy-Port 8080	
I.	Umgehung des Proxys für	
	example.com,mycomp.test.com,localhc	
11-	IP-Einstellungen DHCP	
111-	ABBRECHEN SPEICHERN	
	G Kanzlei-Gast	
	$\checkmark$ $\bigcirc$ $\Box$	

#### **Chrome Mobile**

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

■		
live vodefone de		
Authentifizierung erforderlich		
Für den Server http://octo.octo:8080 ist ein Nutzername und ein Passwort erforderlich.		
fwischke		
Passwort:		
ABBRECHEN ANMELDEN		
qwertzuiop		
asdfghjkl		
12!? ,		

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.

	:03			
Q Suchen oder Adresse eingeben				
Der Proxy moz-proxy://octo.octo:8080 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "moz- proxy://octo.octo:8080" Benutzername				
fwischke				
Passwort				
·····				
Speichern				
ABBRECHEN OK				
q w e r t z u i o	р			
asdfghjkl				
<pre></pre>				
12!? , Fertig				
	<b></b>			

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.

iPad ᅙ	15:51	Lädt nicht 🗖
Einstellungen	<b>&lt;</b> WLAN OCTO_WLAN_8B19B1	
Dieses iPad wird betreut. Messe OctoGate kann den Internetverkehr überwachen und dieses Gerät orten.	Dieses Netzwerk ignorieren	
Flugmodus	IP-ADRESSE	
ᅙ WLAN OCTO_WLAN_8B19B1	DHCP BootP	Statisch
Bluetooth Ein	Teilnetzmaske	255.255.240.0
Mitteilungen	Router	192.168.32.1
Rontrollzentrum	DNS	192.168.32.1
Vicht stören	Such-Domains	
	Client-ID	
Allgemein 1		
AA Anzeige & Helligkeit	Lease erneuern	
Hintergrundbild	HTTP-PROXY	
(I) Töne	Aus Manuell	Autom.
Siri	Server	octo.octo
6 Code	Port	8080
Batterie	Authentifizierung	
Datenschutz	Benutzername	fwischke
(a) iClaud	Passwort	••••••
mk@octogate.de	Deine Benutzerdaten werden evtl. unverschlüsselt übertragen.	
iTunes & App Store		

# **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.