

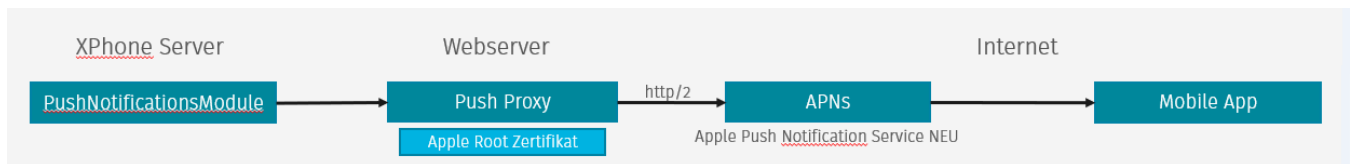
Push Notifications

Stand 16.05.2023

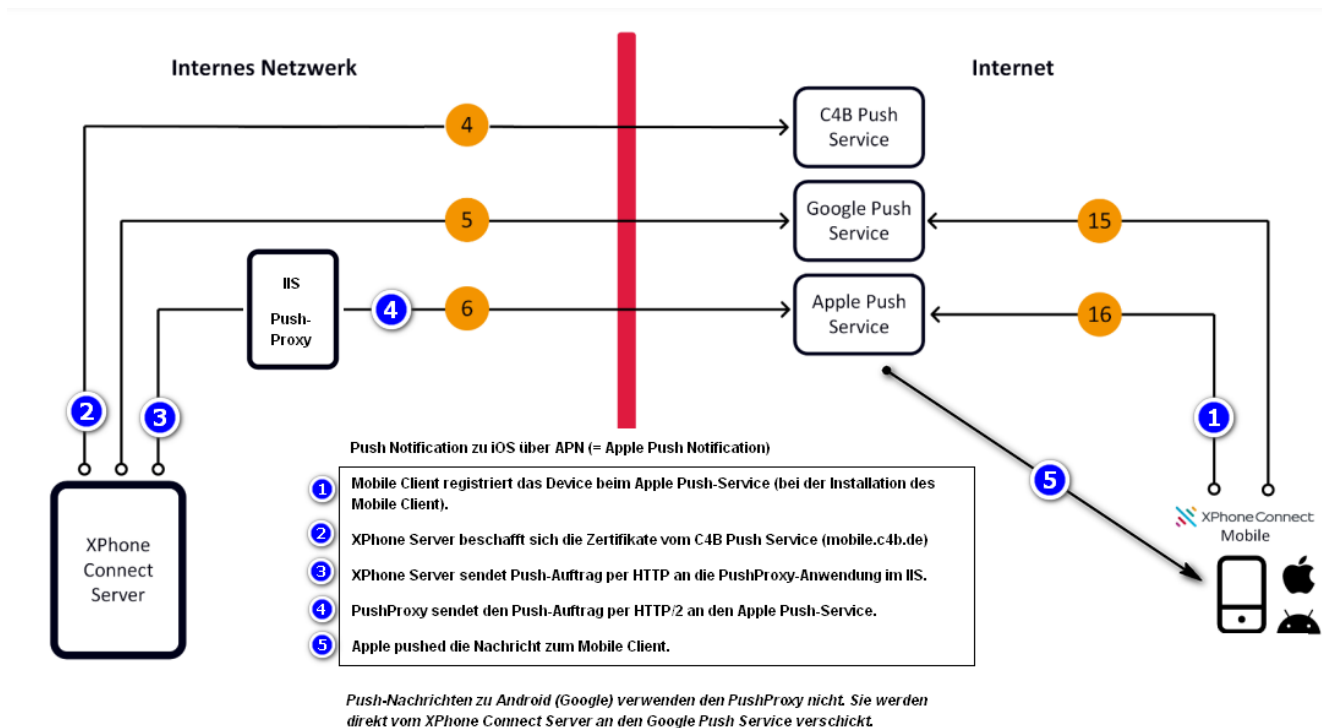
- Übersicht
 - Blockdiagramm "Apple Push Notifications" (APN)
 - Ablauf im Detail
- Dokumentation
 - Port-Übersicht und Firewall Einstellungen
 - Apple Push Services (PDF als Beilage zur V8)
 - Relevante Links in die Server-Doku
- Konfiguration
 - Step 0 - DNS und Proxy-Server und HTTP Verben (PUT, DELETE, ...)
 - Step 1 - Installation auf dem IIS des XPhone Connect Servers
 - Step 2 - Zugriff des XPhone Server Dienstes auf die Web-Anwendung "PushProxy"
 - Step 3 - Zugriff auf <https://mobile.c4b.de/pushconfig>
 - Step 4 - Zugriff der Web-Anwendung "PushProxy" auf die Push-Services von Google und Apple
 - Step 5 - Funktionstest

Übersicht

Blockdiagramm "Apple Push Notifications" (APN)



Ablauf im Detail



Legende zu den gelben Punkten:

4	XPhone Connect Server	C4B Push Service	443	TCP	https
5	XPhone Connect Server	Google Push Service	443	TCP	https
6	XPhone Connect Server	Apple Push Service	443 (2197)	TCP	https
15	XPhone Connect Mobile	Google Push Service	5228 5229 5230	TCP	https
16	XPhone Connect Mobile	Apple Push Service	5223	TCP	https

Dokumentation

Port-Übersicht und Firewall Einstellungen

<https://www.c4b.com/c4b-media/docs/whitepaper/c4b-portuebersicht.pdf>

[FirewalleinstellungenMobile.pdf](#)

Apple Push Services (PDF als Beilage zur V8)

[XPhone Connect - Mobile - Apple Push Service.pdf](#)

Relevante Links in die Server-Doku

<https://help.c4b.com/xphone-connect-9/doc/de/admin/config/feat/mobile.html#push-benachrichtigungen>

<https://help.c4b.com/xphone-connect-9/doc/de/admin/start/sys-req/infstrctr.html#inst-mobile-push>

Konfiguration

Step 0 - DNS und Proxy-Server und HTTP Verben (PUT, DELETE, ...)

DNS. Überprüfen Sie, ob der XPhone Server alle benötigten Servernamen im öffentlichen DNS auflösen kann. Wenn z.B. die Servernamen "mobile.c4b.de" oder "api.push.apple.com" nicht in IP Adressen aufgelöst werden können, können keine Push-Nachrichten zugestellt werden.

Sie können das z.B. mit dem Kommando "nslookup" überprüfen. Es darf **nicht** zu einem Timeout kommen, wie in diesem Fehler-Beispiel:

```
C:\Users\svc_xphone>nslookup api.push.apple.com
DNS request timed out.
    timeout was 2 seconds.
Server:    Unknown
Address: 192.168.1.40

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out

C:\Users\svc_xphone>
```

Proxy-Server. Welche Proxy-Einstellungen gelten auf dem XPhone Server? Konfigurieren Sie ggf. einen Proxy-Server in der XPhone Administration und aktivieren Sie diese Einstellung auch für den Push-Dienst.

Umgekehrt kann es ebenso sein, dass für den XPhone Server eine explizite Ausnahme im konfiguriert ist, so dass er den Proxy umgehen darf. In diesem Fall kann es notwendig sein, dass die automatische Proxy-Erkennung in Windows dauerhaft abgeschaltet wird:

Proxy

Automatic proxy setup

Use a proxy server for Ethernet or WiFi connections. These settings don't apply to VPN connections.

Automatically detect settings

☐ Off

Use setup script

☐ Off

Spezielle HTTP Verben (PUT, DELETE, ...). Es gibt Reverse Proxies oder (Web Application-)Firewalls, die nicht alle HTTP Verben zulassen. Normalerweise sind GET und POST erlaubt.

Unsere Mobile Anwendung verwendet jedoch auch PUT und DELETE, insbesondere zum Schreiben des für Push-Nachrichten notwendigen **DeviceTokens** ! Kann dieser Token nicht in die XPhone Datenbank geschrieben werden, werden niemals Push-Nachrichten an das Mobile Device gesendet (klar - der XPhone Server wüsste ja gar nicht, an welches Ziel).

Die Mobile Anwendung erkennt die gesperrten HTTP Verben u.U. nicht einmal als Fehler. Grund: der Reverse Proxy bzw. die WAF returniert ein "200 OK" an den Client.

PUT https://.../xphoneconnect/mobile Send

Params Authorization Headers (9) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL JSON Beautify

Body Cookies (2) Headers (5) Test Results

200 OK 10 ms 389 B Save as Example

Pretty Raw Preview Visualize HTML

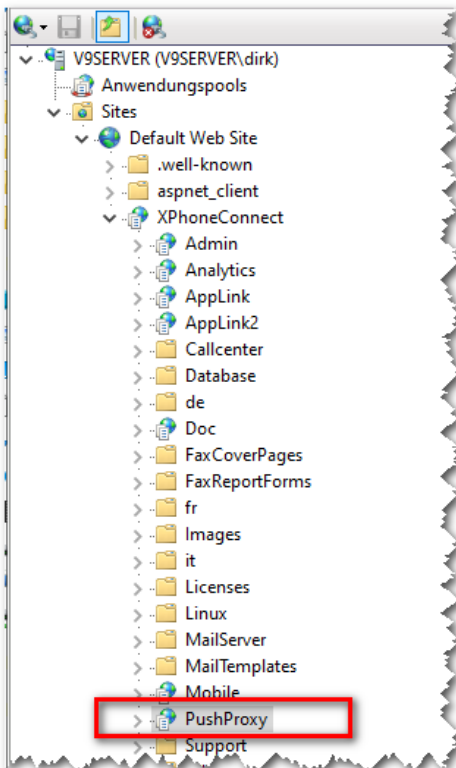
```
1 <html>
2
3 <head>
4   <title>Request Rejected</title>
5 </head>
6
7 <body>The requested URL was rejected. Please consult with your
8 administrator.<br><br>Your support ID is: 15266715296673062801<br><br><a href='javascript:history.
9   back();'>[Go
10   Back]</a></body>
11 </html>
```

Gesperrte HTTP Verben können mit einem Dummy PUT Request überprüft werden.

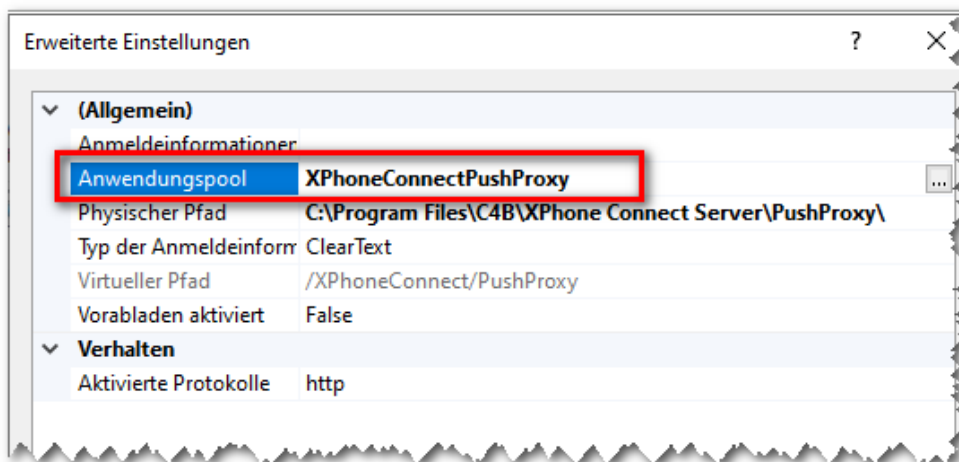
Wenn es Zweifel gibt, ob die DeviceTokens korrekt in der XPhone Datenbank hinterlegt wurden, hilft ein Blick in diese Tabelle: **[XPDATA].[dbo].[EfUserPushNotificationDevices]**

Step 1 - Installation auf dem IIS des XPhone Connect Servers

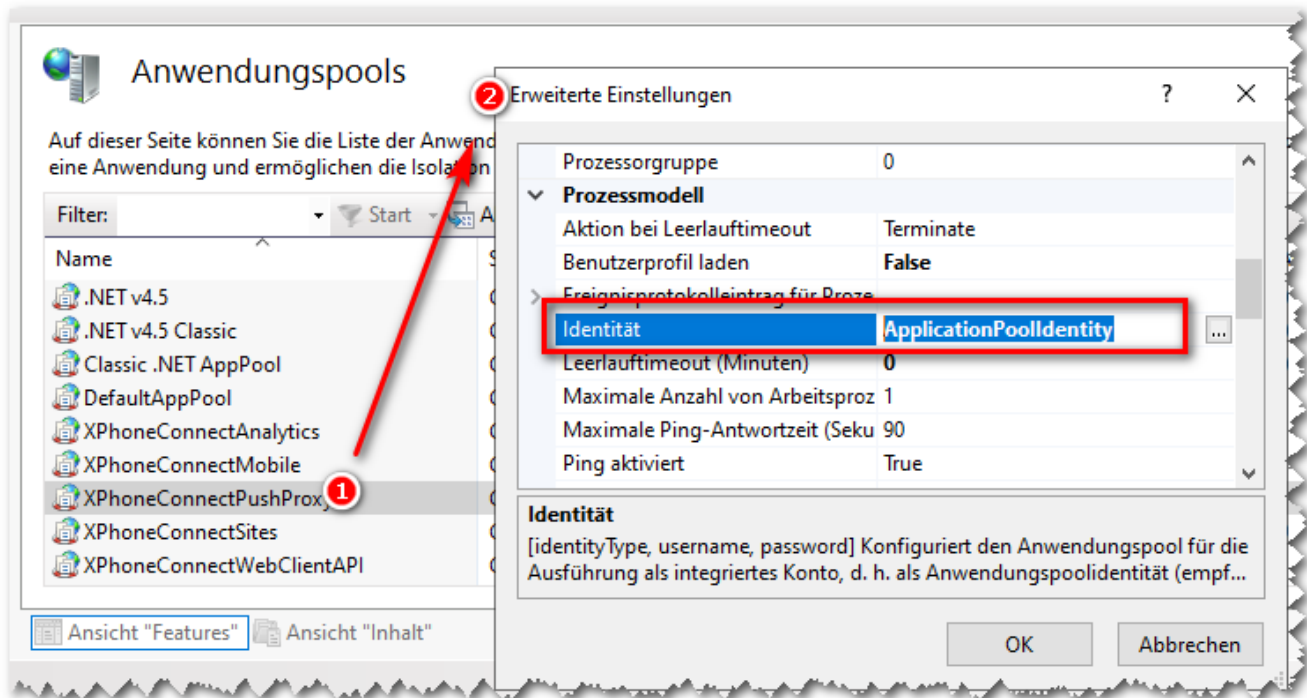
Auf dem IIS des XPhone Servers (nicht etwa auf einem ausgelagerten IIS) muss die Web-Anwendung "IIS\Sites\Default Web Site\XPhoneConnect\PushProxy" installiert sein.



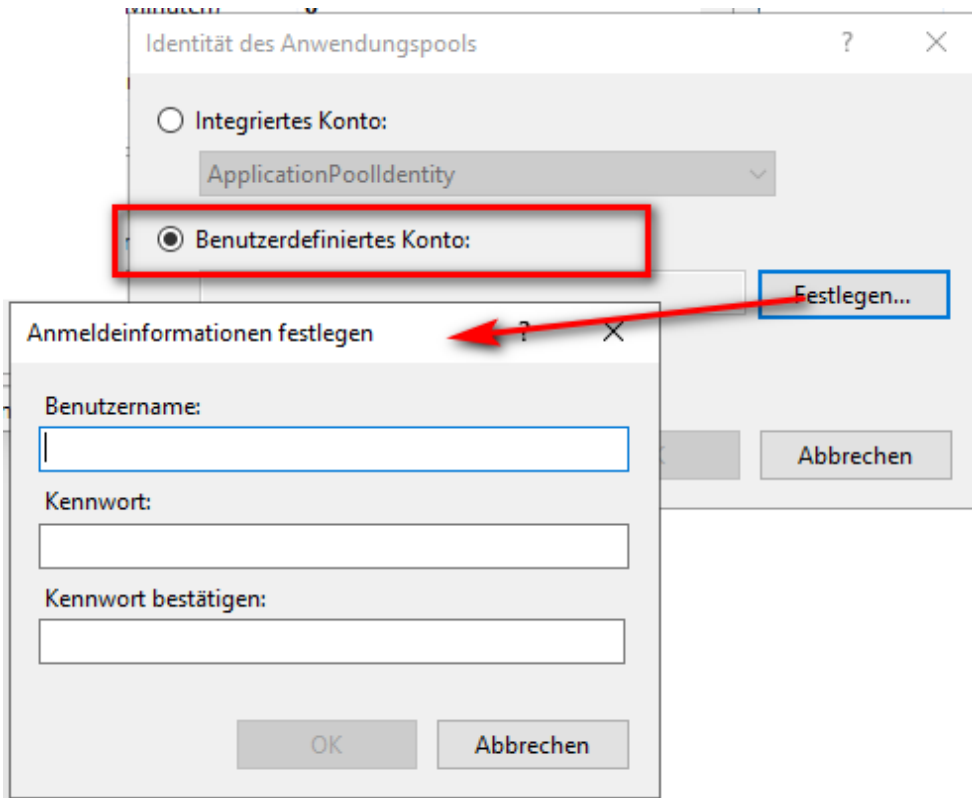
Die Web-Anwendung "PushProxy" muss unter dem Application-Pool "XPhoneConnectPushProxy" laufen (rechte Maustaste Erweiterte Einstellungen):



Der Anwendungs-Pool "XPhoneConnectPushProxy" läuft standardmäßig unter der Identität "ApplicationPoolIdentity":



Je nachdem, welche **Berechtigungen** für die Firewall oder evtl. für einen Proxy-Server im Unternehmen benötigt werden, um die beteiligten Dienste im Internet zu erreichen, muss die Identität des Anwendungs-Pools umgestellt werden, z.B. auf einen berechtigten Domänen-User. Dazu klickt man auf die drei Punkte (neben dem roten Rahmen) und gelangt in einen Dialog zum Eintragen der neuen Identität. In der Regel wird man ein "Benutzerdefiniertes Konto:" wählen und die Anmeldeinformationen über den Button "Festlegen:" definieren:



WICHTIG: Dieser Account braucht ebenfalls **Schreibrechte** auf dem Verzeichnis "C:\Program Files\C4B\XPhone Connect Server\PushProxy"!

Warum? Weil der PushProxy dort im Filesystem die Zertifikate ablegen muss, die er sich von "mobile.c4b.de" beschafft hat:

» Lokaler Datenträger (C:) » Programme » C4B » XPhone Connect Server » PushProxy

Name	Änderungsdatum	Typ	Größe
apns.p12	23.12.2022 12:29	Privater Informati...	4 KB
appsettings.json	02.12.2022 12:16	JSON-Datei	1 KB
appsettings.json.install	30.11.2022 21:52	INSTALL-Datei	1 KB
avs.p12	23.12.2022 12:29	Privater Informati...	4 KB
Newtonsoft.Json.dll	02.05.2022 15:35	Anwendungswe...	652 KB

Step 2 - Zugriff des XPhone Server Dienstes auf die Web-Anwendung "PushProxy"

Dieser - lokale - HTTP-Zugriff (Port 80) sollte eigentlich immer funktionieren. Tja, sollte - es gibt Ausnahmen!

Im Auslieferungszustand versucht der XPhone Server den PushProxy auf dieser URL zu erreichen:

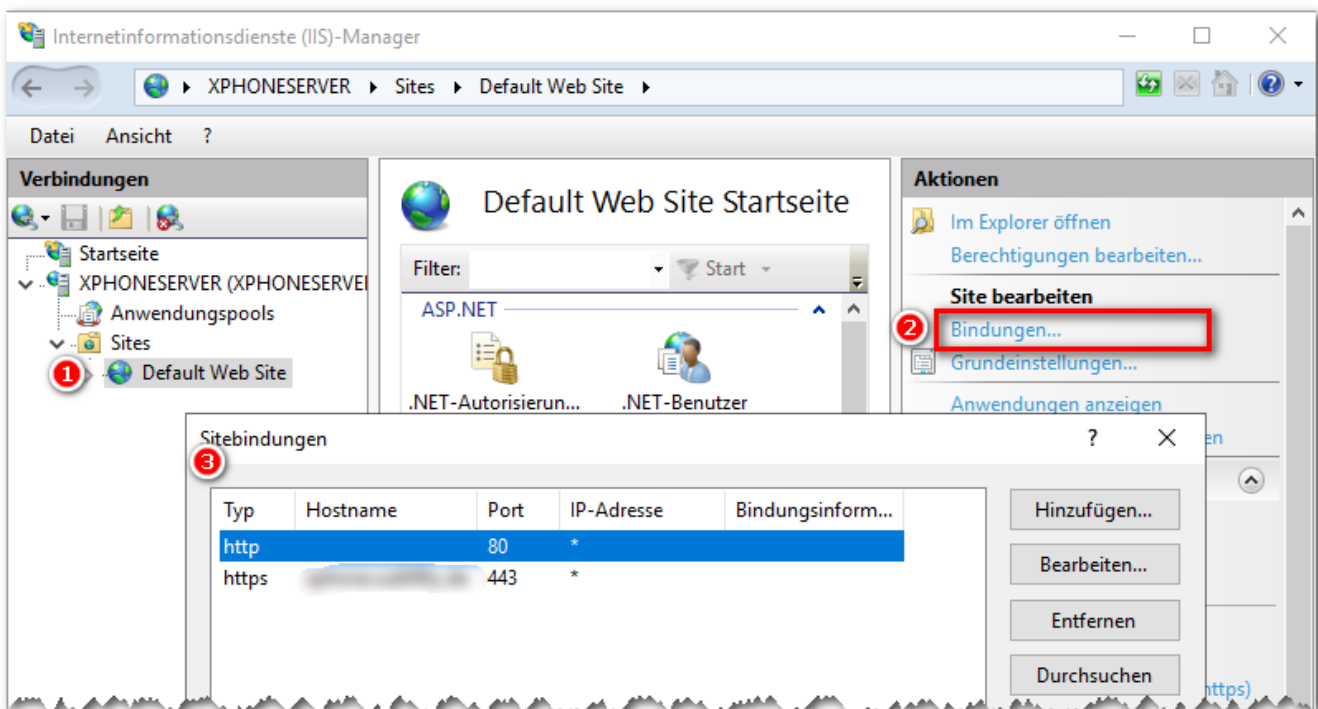
```
http://localhost/XPhoneConnect/PushProxy/
```

Man kann die Erreichbarkeit des PushProxy-Dienstes mit Hilfe eines **"healthcheck"** überprüfen. Dazu gibt im Browser, der auf dem XPhone Server Rechner geöffnet ist, diese URL ein:

```
http://localhost/XPhoneConnect/PushProxy/healthcheck
```

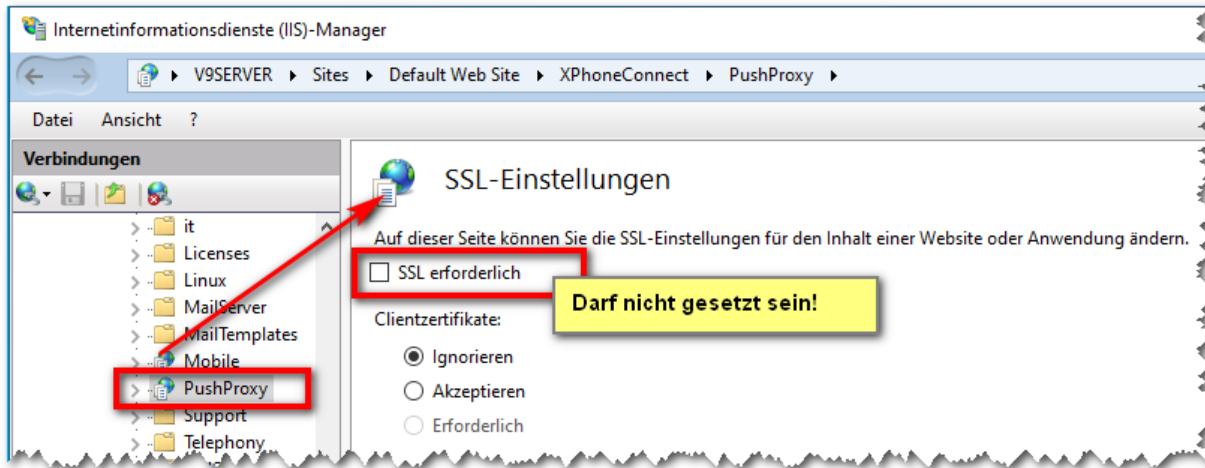
Als Ergebnis sollte man eine weiße Seite und eine HTTP Response 200 erhalten. Wenn das nicht der Fall ist, helfen die folgenden ACHTUNG Hinweise weiter.

Ein guter Einstiegspunkt in die Analyse sind die im IIS eingestellten "Bindungen" für die Default Webseite:



Im obigen Beispiel sind keine Einschränkungen bzgl. Hostname oder IP-Adresse für Port 80 eingestellt. Das ist auch der Default. Je nachdem, welche Einstellungen in Ihrem System vorhanden sind, kann es leicht sein, dass man mit "localhost" nicht auf dem IIS kommt! In solchen Fällen helfen die folgenden ACHTUNG Hinweise weiter!

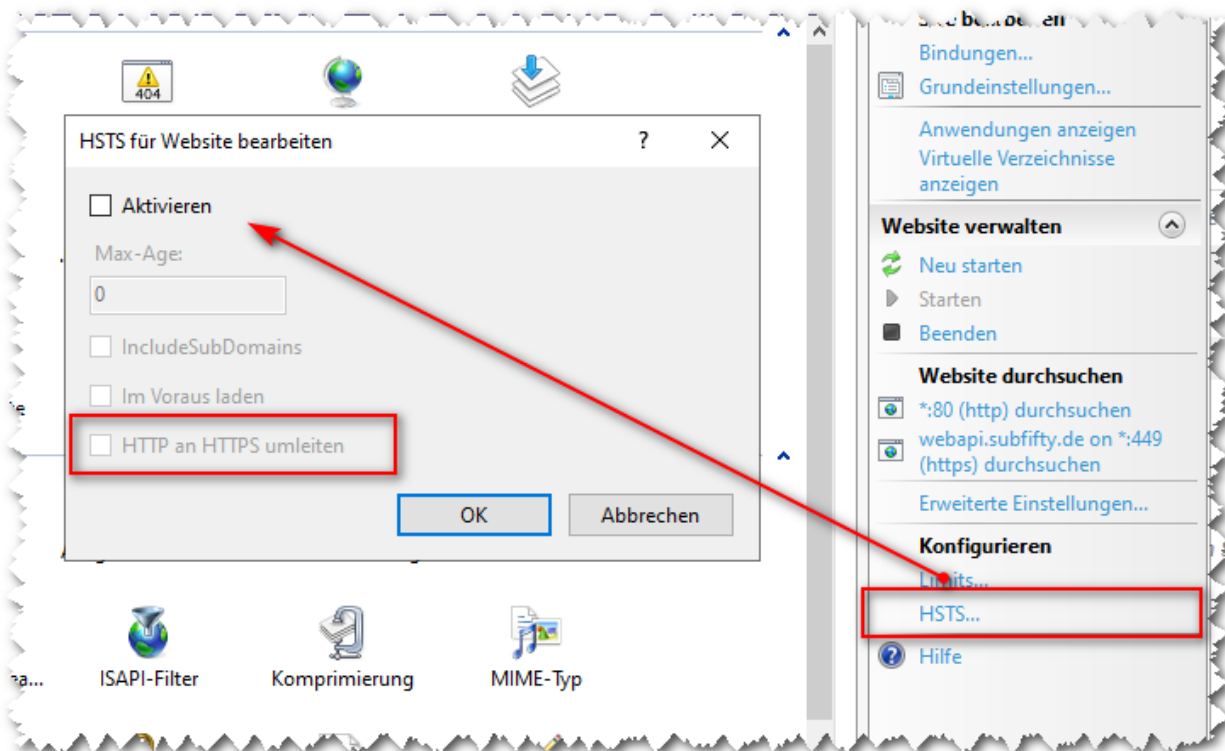
ACHTUNG (1): Es gibt offenbar Kunden, die auch für den lokalen Zugriff auf den IIS (also auf "localhost") immer **SSL erzwingen!!!** In diesem Fall kann der XPhone Server den PushProxy nicht auf Port 80 erreichen! Abhilfe: man erlaubt im IIS für den PushProxy auch den Zugriff über HTTP (Port 80). Das hat im speziellen Supportfall geholfen.



Bei der Analyse haben die **Eventlogs für das PushProxyModule geholfen (DebugHigh)**. Dort steht dann drin, dass HTTP nicht erlaubt ist, weil HTTPS zwingend erforderlich ist.

ACHTUNG (2): Manche Kunden stellen im IIS ein (auch auf dem IIS, der auf dem XPhone Server läuft), dass **jeder HTTP Request automatisch auf HTTPS umgeleitet** wird.

Dann ist HSTS aktiviert und der Haken bei "HTTP an HTTPS umleiten" gesetzt:



(Der Punkt 'HSTS...' ist in der rechten Menüleiste zu finden, wenn im IIS die 'Default Web Site' markiert ist).

Damit kommt unser Push-Mechanismus für Apple nicht ohne weiteres klar. Der XPhone Server sucht den PushProxy standardmäßig auf "<http://localhost/xphoneconnect/pushproxy/>". Durch die erzwungene Umleitung auf HTTPS erreicht er ihn dort jetzt nicht mehr!

Jetzt muss in der Datei **atlas.xml** die korrekte URL für den PushProxy eingetragen werden. Man fügt der schon vorhandenen Sektion **<PushNotificationSettings>** das neue Attribut **proxyBaseAddress** hinzu und trägt dort die passende URL für den PushProxy ein:

```
<PushNotificationSettings
proxyBaseAddress="https://servername_not_localhost/xphoneconnect/pushproxy"
... />
```

ACHTUNG (3): In einem Fall war es so, dass **weder URL "http://localhost/..." noch die URL "http://127.0.0.1/..." auf dem IIS des XPhone Servers erreichbar** waren!! Der XPhone Server lief auf einem ausgelagerten Rechenzentrum. Genaue Ursachen wurden nicht erforscht. Abhilfe: genau wie im vorigen ACHTUNG (2): Eintrag in der atlas.xml die lokale IP Adresse (ungleich localhost und ungleich 127.0.0.1) setzen.

ACHTUNG (4): In manchen IIS Installationen ist das Feature **"IP- und Domäneneinschränkungen"** aktiviert:

Serverrollen auswählen

ZIELSERVER
V9Server

Vorbereitung

Installationstyp

Serverauswahl

Serverrollen

Features

Bestätigung

Ergebnisse

Wählen Sie mindestens eine Rolle aus, die auf dem ausgewählten Server installiert werden soll.

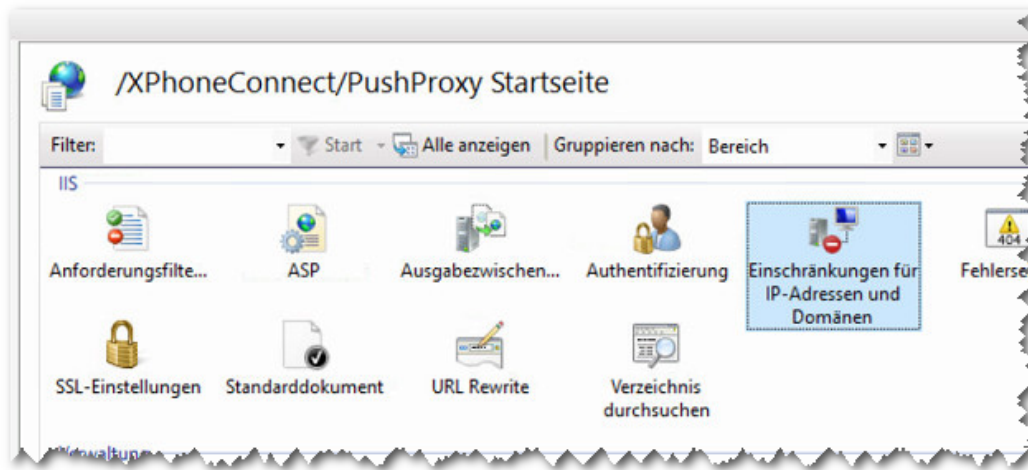
Rollen

- ☐ volumenaktivierungsdienste
- ☒ Webserver (IIS) (22 von 43 installiert)
 - ☒ Webserver (19 von 34 installiert)
 - ☒ Allgemeine HTTP-Features (4 von 6 installiert)
 - ☒ Leistung (Installiert)
 - ☒ Sicherheit (3 von 9 installiert)
 - ☒ Anforderungsfilterung (Installiert)
 - ☐ Authentifizierung über Clientzertifikate
 - ☐ Authentifizierung über IIS-Clientzertifikate
 - ☐ Digestauthentifizierung
 - ☐ **IP- und Domäneneinschränkungen**
 - ☒ Standardauthentifizierung (Installiert)
 - ☐ Unterstützung zentraler SSL-Zertifikate
 - ☐ URL-Autorisierung
 - ☒ Windows-Authentifizierung (Installiert)
 - ☒ Systemzustand und Diagnose (2 von 6 installiert)
 - ☒ Anwendungsentwicklung (8 von 11 installiert)
 - ☐ FTP-Server
 - ☒ Verwaltungsprogramme (3 von 7 installiert)

Beschreibung

Mit 'IP- und Domäneneinschränkungen' können Sie Inhalt basierend auf der IP-Quelladresse oder dem Quelldomännennamen der Anforderung zulassen oder verweigern. Anstatt den Zugriff auf Inhalte mit Gruppen, Rollen oder NTFS-Dateisystemberechtigungen zu steuern, können Sie bestimmte IP-Adressen oder Domännennamen festlegen.

Achten Sie in diesem Fall darauf, dass der XPhone Server Dienst auf die Web-Anwendung "PushProxy" ausreichend Zugriffsberechtigungen hat. Es müssen also i.d.R. alle lokalen IP-Adressen erlaubt sein!

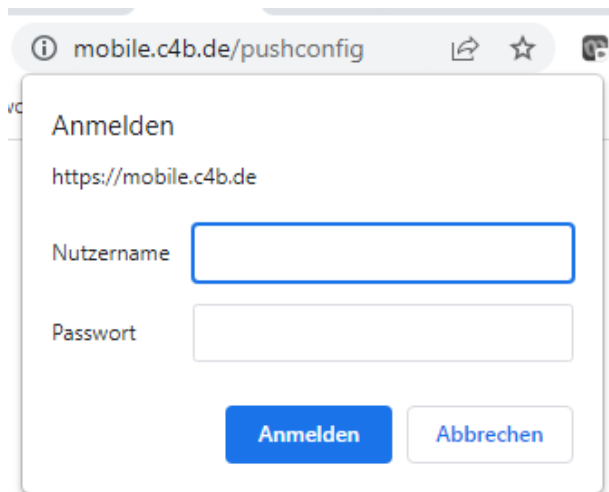


Ist das Feature installiert aber nicht konfiguriert, kann es sich wie eine Art Blacklist verhalten und ebenfalls den Zugriff auf die localhost-Adresse sperren. Ein Indiz für diesen Fall ist, dass die reguläre XPhone Connect Administrationsoberfläche nicht über localhost aufrufbar ist. Hier hilft es, das Feature einfach wieder zu deinstallieren. Aber: Vorher klären, ob das Feature absichtlich und für einen bestimmten Grund installiert wurde und falls dem so ist, sollten stattdessen die Zugriffsberechtigungen geprüft werden.

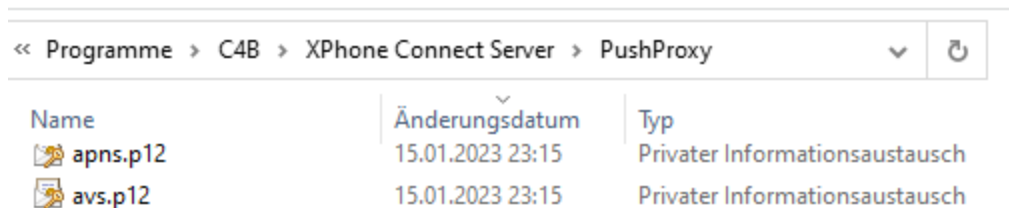
Step 3 - Zugriff auf <https://mobile.c4b.de/pushconfig>

Der Dienste-Account des XPhone Connect Servers muss auf die URL <https://mobile.c4b.de/pushconfig> zugreifen können. Dazu muss Port 443 ausgehend in der Firewall geöffnet sein.

Der Aufruf dieser URL muss diese Anmeldemaske anzeigen. Damit ist die Erreichbarkeit gegeben. Man muss sich nicht anmelden können (die Credentials sind "geheim").



Der PushProxy holt sich von dort die Zugriffs-Tokens für die Anmeldung am Apple Push Service. Diese Tokens speichert er lokal im Verzeichnis "C:\Program Files\C4B\XPhone Connect Server\PushProxy" ab. **Dazu benötigt er Schreibrechte** auf diesem Verzeichnis!



Die Berechtigungen müssen dem technischen Windows-User "IIS APPPOOL\XPhoneConnectPushProxy" vergeben werden:

Man nehme den rot umrandeten Wert, und zwar alles innerhalb der eckigen Klammern (ohne die Klammern). Auf diese Weise kann man sich eine "echte" Push-Notification an sein iPhone schicken.

Step 5 - Funktionstest

XPhone Connect Mobile App auf einem Smartphone (Android, iOS) einrichten und mit einem XPhone User Account verbinden ("Mobile User").

In der Mobile App werden die Push-Benachrichtigungen aktiviert (Hamburger-Menü Einstellungen Push-Benachrichtigungen).

Dieser Mobile User muss jetzt alle XPhone Connect Desktop Clients und seine Mobile Anwendung auf dem Smartphone beenden. Hinweis: so lange noch ein Desktop-Client läuft, werden keine Push-Nachrichten verschickt!

Szenario 1: ein anderer XPhone User schickt eine IM-Nachricht an den Mobile User. Der Mobile User muss in kurzer Zeit eine Push-Nachricht darüber empfangen.

Szenario 2: Der Mobile User stellt als aktives Gerät seine Office Leitung ein. Jetzt wird er von einem anderen XPhone User oder von einem externen Teilnehmer auf seiner Office-Nummer angerufen. Kurze Zeit später sollte er eine Push-Nachricht über einen verpassten Anruf erhalten.