

## Kurzanleitung „Wake On LAN Gateway“ zum Aufwecken ausgeschalteter Rechner

Mit Hilfe des WOLGateway ist es möglich einen Rechner, der sich im internen Netzwerk befindet, über die Ferne einzuschalten. Dies kann dann sinnvoll sein, wenn man sich z.B. über VPN einwählt und auf seinen Rechner per Remote Desktop Verbindung zugreifen möchte, dieser aber nicht eingeschaltet ist. Im Umkehrschluss spart dies auch Strom, da man den Rechner nicht ständig eingeschaltet lassen muss, wenn man später entfernt darauf zugreifen möchte.

Als technische Voraussetzung muss der aufzuweckende Rechner noch am Strom und kabelgebundenen Netzwerk angeschlossen sein, sowie WakeOnLAN unterstützen. Sollte das Aufwecken daher nicht auf Anhieb funktionieren, am besten an den Administrator wenden. Dieser kann prüfen, ob das Feature im UEFI/BIOS des Rechners aktiviert ist (es lautet im UEFI mitunter: *Erweitert, Advanced Power Management (APM), Aufwecken über PCIe* und in vielen BIOS: *Power Management, Wake On LAN, Enabled*).

## Verfahren

Es gibt zwei Verfahren, die man anwenden kann.

Bei **Verfahren 1** installiert man sich eine Client-Anwendung, die sich bei Bedarf starten lässt und die Adresse eines oder mehrerer Zielrechner in den Einstellungen speichert. Aufwecken erfolgt dann z.B. per einfachem Doppelklick auf ein Icon auf dem Desktop.

Beispiel Installations-URL: <http://servername/WOL/Install/>  
(Internet Explorer verwenden)

Bei **Verfahren 2** muss man überhaupt nichts auf seinem Rechner installieren, sondern ruft lediglich eine spezielle Internetseite im Browser (wie dem Internet Explorer) auf, z.B.:

<http://servername/WOL/service.svc/rest/SendMagicPacketTo/00-50-56-C0-00-01>

Wobei die letzten Zahlen die physikalische MAC-Adresse des Zielrechners symbolisieren, der aufzuwecken ist.

Übersicht der Verfahren:

Art	URL
<b>Verfahren 1: Lokal installierte Client-Anwendung</b>	
Benutzung	per installierter Client-Anwendung
Installation	<a href="http://servername/WOL/Install/">http://servername/WOL/Install/</a>
Installation**	<a href="https://servername/WOL/Install/">https://servername/WOL/Install/</a>
<b>Verfahren 2: Aufwecken per Browser</b>	
http	<a href="http://servername/WOL/service.svc/rest/SendMagicPacketTo/...">http://servername/WOL/service.svc/rest/SendMagicPacketTo/...</a>
https*	<a href="https://servername/WOL/service.svc/rest/SendMagicPacketTo/...">https://servername/WOL/service.svc/rest/SendMagicPacketTo/...</a>

\* Bei selbst generiertem SSL-Zertifikat sind Zertifikatsfehler im Browser zu ignorieren

\*\* Bei selbst generiertem SSL-Zertifikat nur möglich, wenn dieses als vertrauenswürdig im Internet Explorer importiert wird

## Anleitung Verfahren 1: Lokal installierte Client-Anwendung

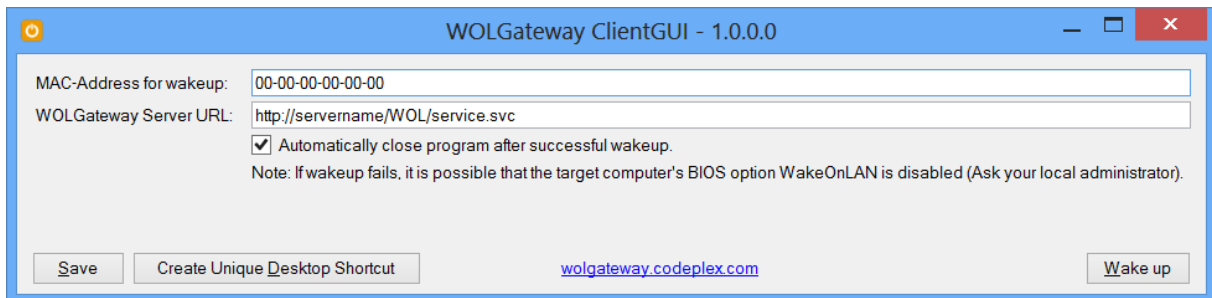
1. Installation der Client-Anwendung (auf dem Rechner, der später andere aufwecken soll).  
Auf dem Rechner der geweckt werden soll, muss nichts installiert werden!

Folgende URL über den Internet Explorer ansteuern (Beispiel setzt voraus, dass das WOLGateway.IISModul auf dem Server innerhalb der WebSite „WOL“ installiert wurde):

<http://servername/WOL/Install/>



2. Nach erfolgreicher Installation startet die Anwendung automatisch.

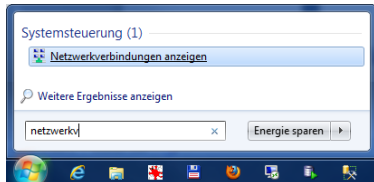


3. Im ersten Feld ist dann die physikalische MAC-Adresse der Netzwerkkarte des Zielrechners einzutragen, der aufgeweckt werden soll (also nicht die des Rechners, auf dem man das Programm soeben installiert hat). Das Feld URL ist im Allgemeinen nicht abzuändern.

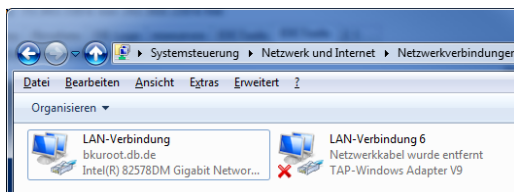
4. Sofern man die physikalische MAC-Adresse des Zielrechners noch nicht ermittelt hat, lässt sich diese über folgenden Weg herausfinden:

**Achtung: Schritt 4 ist nur auf dem Zielrechner (der aufgeweckt werden soll) auszuführen!**

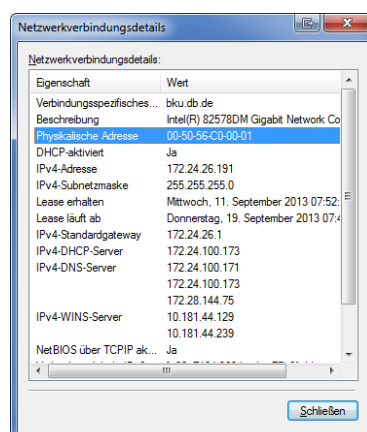
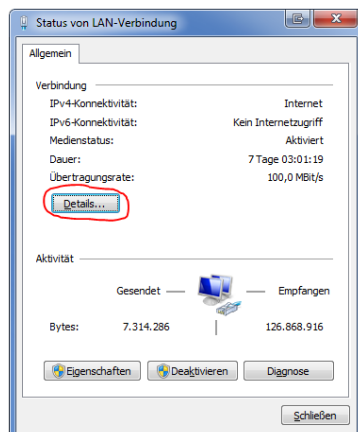
Windows-Startknopf bzw. Windows-Taste (⊞) drücken, dann **Netzwerk** in das Suchfeld eintippen. Dann wird **Netzwerkverbindungen anzeigen** angeboten. Dies anklicken.



Im anschließend geöffneten Fenster sieht man alle Netzwerkverbindungen, die dieser Rechner besitzt. Sollte der Rechner mehrere Verbindungen haben, ist nur diejenige wichtig, die auch wirklich verbunden ist (alle, die ein rotes X mit „Netzwerkabel wurde entfernt“ stehen haben, kann man ignorieren). Und es muss eine kabelgebundene Verbindung sein, kein WLAN, etc.



Jetzt auf die Verbindung einen Doppelclick ausführen, um deren Status-Fenster aufzurufen. Dann auf Details klicken.



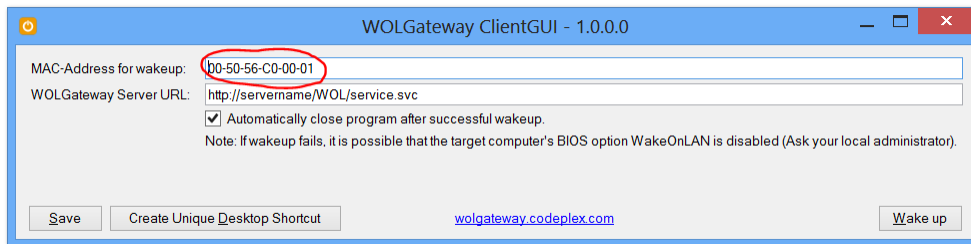
Im Detailfenster findet man anschließend die physikalische MAC-Adresse der Netzwerkkarte dieses Rechners.

**Tip:** Eine andere Möglichkeit zur Ermittlung der physikalischen MAC-Adressen besteht darin, die Eingabeaufforderung zu starten und sich per Kommando

**ipconfig /all**

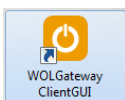
unter anderem die physikalischen MAC-Adressen aller Netzwerkkarten des PCs anzeigen zu lassen.

5. Und genau diese „Physikalische Adresse“ ist auf dem anderen Rechner (auf dem man zuvor schon die WOLGateway-Anwendung installiert hat) einzutragen. Also z.B. wie folgt:

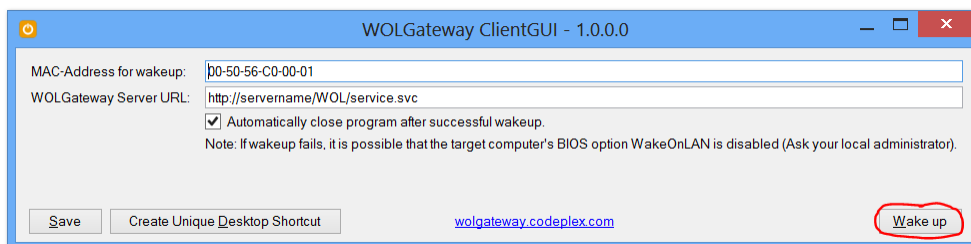


6. Abschließend Speichern über den **Save** Knopf.

Ab jetzt lässt sich die Anwendung verwenden. Hierfür liegt auf dem Desktop eine Verknüpfung:



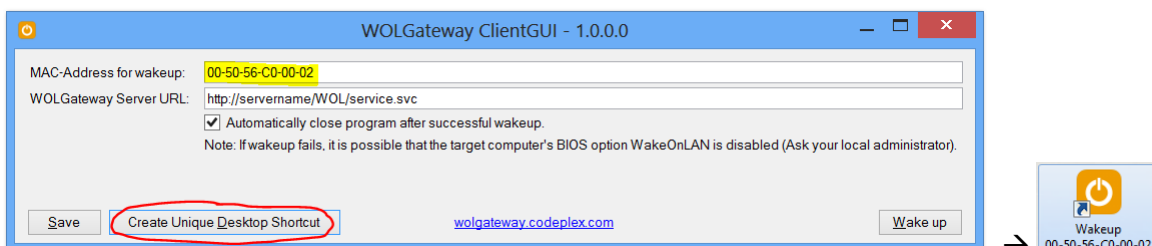
Wenn man jetzt testweise den Zielrechner herunterfährt und auf dem anderen Rechner die Anwendung startet und anschließend auf **Wake up** klickt, wird über den internen Server ein so genanntes „Magic Packet“ gesendet, welches den Zielrechner aufweckt (sofern dieser die oben genannten technischen Voraussetzungen erfüllt).



Die Anwendung schließt sich im Erfolgsfall automatisch (Standardverhalten).  
Nur im Fehlerfall bleibt die Anwendung offen und zeigt die Fehlermeldung an.

Sofern man die Anwendung auch nach dem Aufwecken offen halten möchte, um z.B. weitere MAC-Adressen einzugeben und andere Rechner aufzuwecken, kann man den Haken bei **Automatically Close** herausnehmen und diese Einstellung bei Bedarf per **Save** speichern.

**Tipp:** Über den zusätzlichen Knopf „Create Unique Desktop Shortcut“ lässt sich ein Schnellziel auf den Desktop anlegen. Bei dessen Start wird automatisch der eingetragene Rechner geweckt und die Anwendung schließt sich wieder. Das funktioniert für eine beliebige Anzahl von Rechnern (jeder Rechner bekommt eine eigene Desktop-Verknüpfung mit der MAC-Adresse des aufzuweckenden Rechners, die man natürlich nach Anlegen beliebig umbenennen kann).



## Anleitung Verfahren 2: Aufwecken per Browser

Hierfür muss lediglich eine Internetseite aus dem Browser angesteuert werden. Hier beispielhaft mit dem Internet Explorer. Aufruf erfolgt über folgende Adresse (Beispiel setzt voraus, dass das WOLGateway.IISModul auf dem Server innerhalb der WebSite „WOL“ installiert wurde).

<http://servername/WOL/service.svc/rest/SendMagicPacketTo/00-00-00-00-00-00>

Wobei die letzten Zahlen die MAC-Adresse des Zielrechners symbolisieren, der aufzuwecken ist, konkret für das Beispiel aus Verfahren 1 wäre das dann:

<http://servername/WOL/service.svc/rest/SendMagicPacketTo/00-50-56-C0-00-01>

Wie man die MAC-Adresse des Zielrechners ermittelt, steht im Detail in Kapitel 4 (des ersten Verfahrens).

Wenn abschließend die Meldung:

`<string xmlns="http://schemas.microsoft.com/2003/10/Serialization/">Magic packet sent...</string>`

im Browser erscheint wurde erfolgreich über ein Datenpaket gesendet, welches den Zielrechner aufweckt (sofern dieser die oben genannten technischen Voraussetzungen erfüllt).

**Tipp:** Man kann einfache Desktop-Verknüpfungen (Shortcuts) erstellen oder alternativ Verknüpfungen/Lesezeichen anlegen, die dann den ein oder anderen Rechner aufwecken.

**Tipp für technisch Versierte:** Zusätzlich zur unverschlüsselten http-Adresse besteht auch die Möglichkeit einen SSL-Endpoint (https) zur Verfügung zu stellen. Es ist dabei darauf zu achten, dass man entweder mit einem seitens Trustcenter ausgestellten „echten“ Zertifikat arbeitet. Oder alternativ das (z.B. selbst generierte) Zertifikat dem Internet Explorer als vertrauenswürdiges Stammzertifikat „anlernt“. Dann lässt sich die Client-Anwendung aus Verfahren 1 im Bedarfsfall auch per https-URL installieren: <https://servername/WOL/Install/> - was sonst auf Grund von Einschränkungen im ClickOnce Deployment fehlschlagen würde.

Anders als ClickOnce kann die installierbare Client-Anwendung nach erfolgreicher Installation sowohl mit „echten“ vertrauenswürdigen Zertifikaten, als auch mit selbst generierten SSL-Zertifikaten umgehen. Es gibt hierfür eigens den Schalter „IgnoreServerCertificateValidation“ in den Project Settings der ClientGUI, welcher die Validierung des SSL-Zertifikats im Bedarfsfall immer positiv quittiert.