

Subnet- / Portscanner & Wake on LAN Tool



Volker Steitz

Scannt Netzwerksegmente, Ports und startet Systeme

STEITZ® IT-Solutions

www.vs-net.com

01.11.2011

Inhalt

Subnetscanner & „Wake On LAN“ Tool.....	2
Vorbereitende Maßnahmen - Firewall Konfigurieren.....	3
Erster Programmstart	5
Netzwerksegment scannen	6
Portscan	13
Netzwerkinfo	14
Abschließende Maßnahmen - Firewall Konfigurieren.....	16

Subnetscanner & „Wake On LAN“ Tool

Damit Wake on LAN funktioniert, müssen einige Grundbedingungen erfüllt sein.

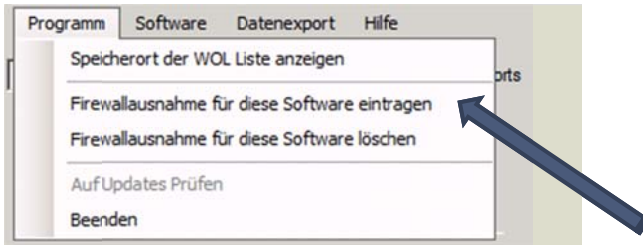
Allgemein muss die Voraussetzung gegeben sein, dass die Netzwerkkarte über den Standby-Stromzweig des Netzteils weiterhin mit Strom versorgt wird, während der Computer ausgeschaltet ist.

Dies ist bei fast allen Systemen, die nicht älter als vier Jahre sind, fast immer der Fall.

Weiterhin müssen Sie im BIOS Ihres Systems WoL aktivieren. Hierzu müssen sowohl die Hauptplatine als auch die Netzwerkkarte im BIOS APM (Advanced Power Management) oder das Advanced Configuration and Power Interface (ACPI) unterstützen.

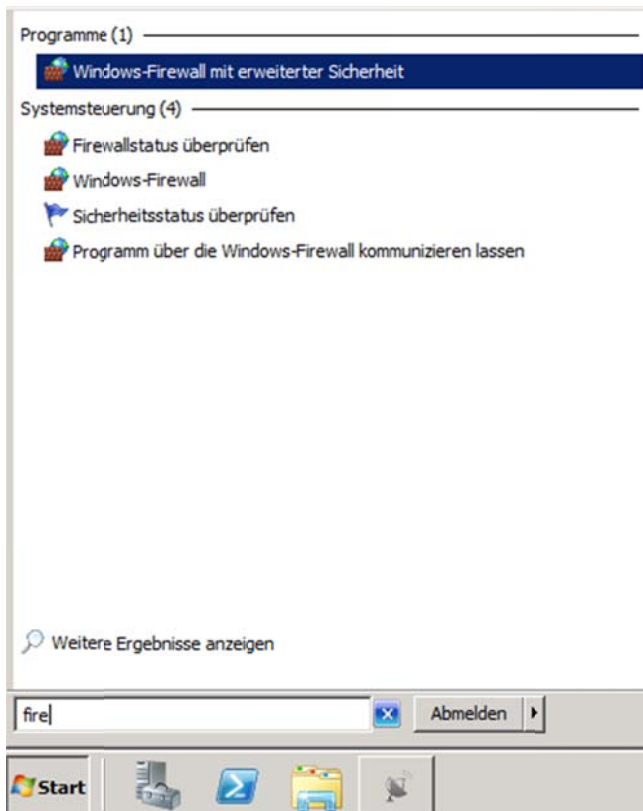
Vorbereitende Maßnahmen - Firewall Konfigurieren

Wenn Sie Windows 7 oder Windows Server 2008 einsetzen, sollten Sie - bevor Sie mit dieser Software arbeiten – eine Ausnahme in Ihren Firewall Regeln eintragen. Bitte verwenden Sie hierzu aus dem Menu Programm den Menüpunkt „FIREWALLAUSNAHME FÜR DIESE SOFTWARE EINTRAGEN“.

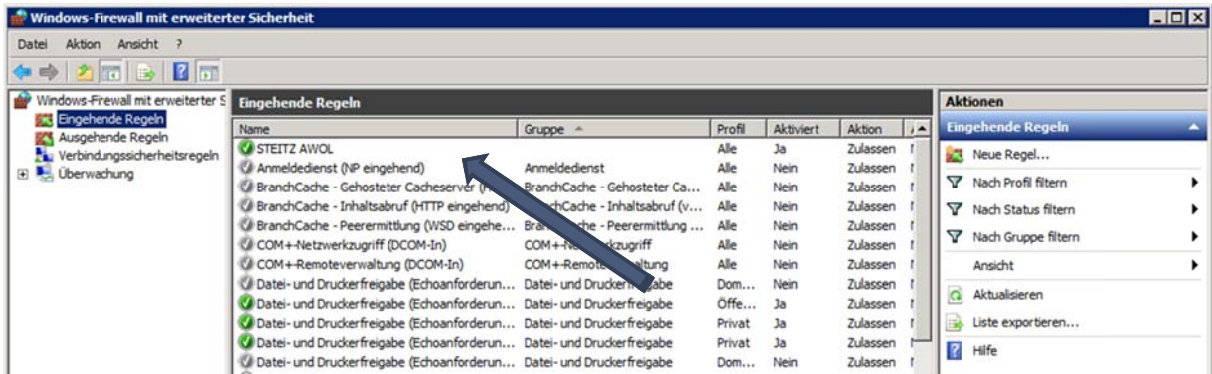


Kontrolle des Eintrages

Bitte Starten Sie das Konfigurationsprogramm für die Windows Firewall mit erweiterter Sicherheit

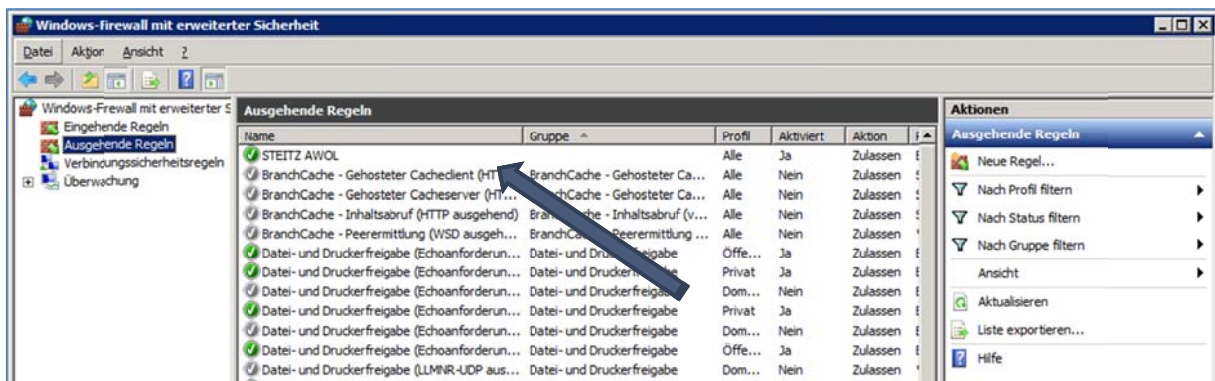


Bitte führen Sie auf „Eingehende Regeln“ einen Doppelklick aus



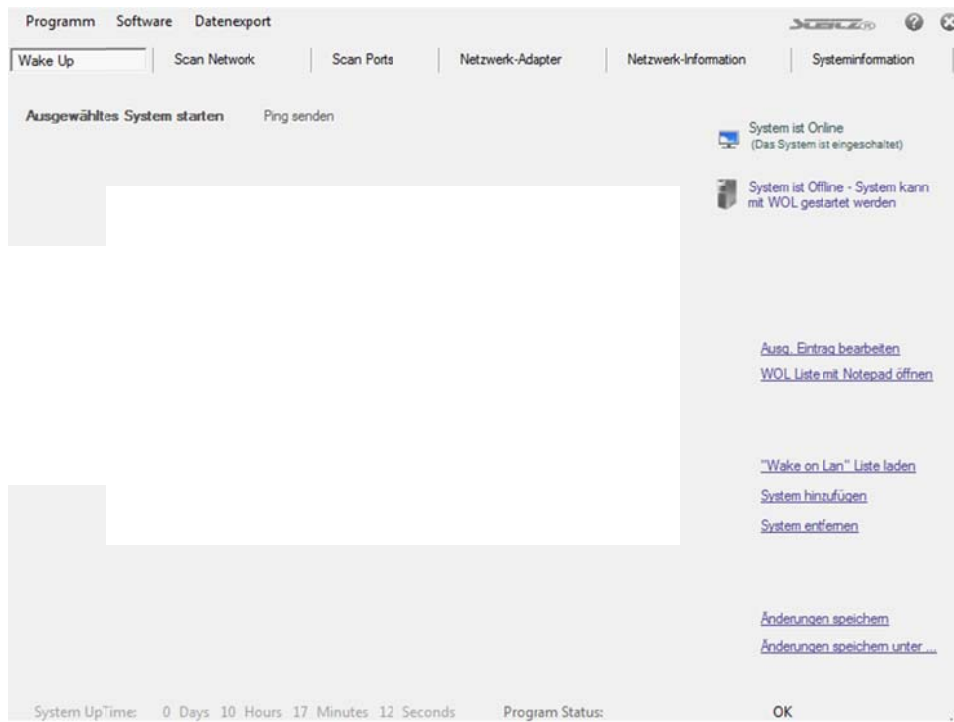
Es muss nun der o.g. Eintrag vorhanden sein

Bitte führen Sie auf „Ausgehende Regeln“ einen Doppelklick aus



Es muss nun der o.g. Eintrag vorhanden sein

Erster Programmstart



...Beim ersten

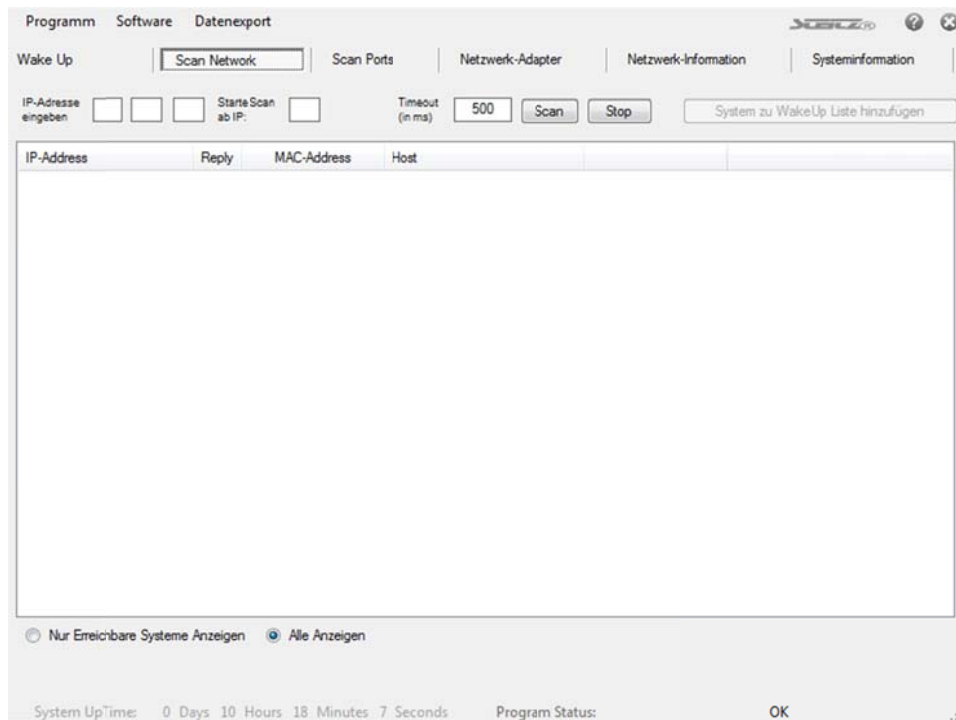
Programmstart sieht die Software wie im o.g. Bild aus.

Es ist noch keine Netzwerkliste hinterlegt.

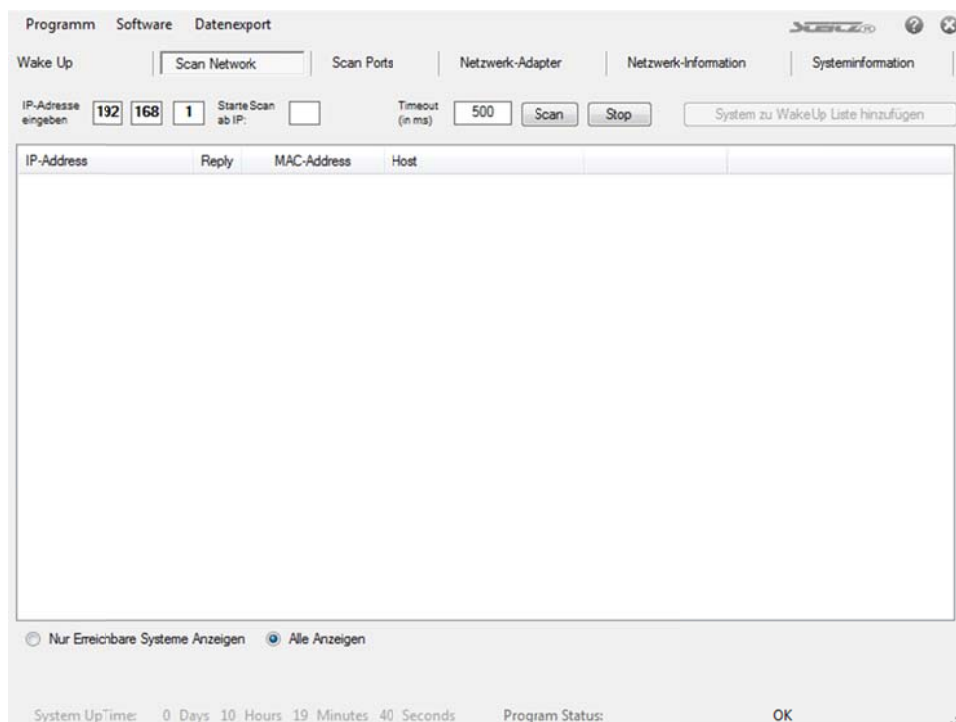
Bitte schalten Sie alle Systeme Ihres Netzwerkes ein und wechseln Sie auf die Registerkarte

SCAN NETWORK

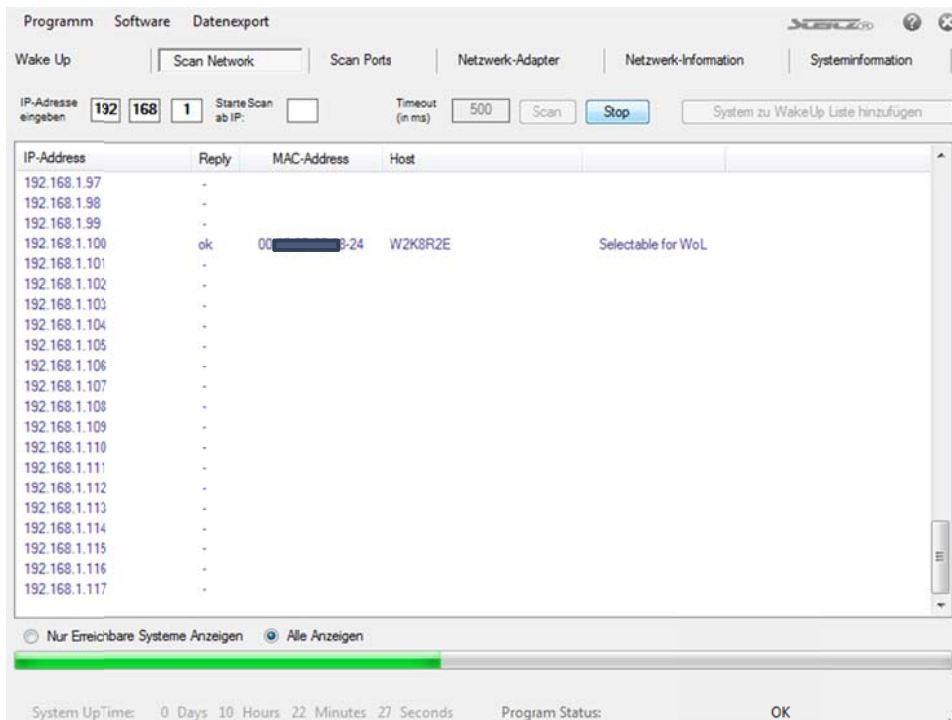
Netzwerksegment scannen



Bitte tragen Sie die ersten 3 Segmente Ihrer IP-Adresse ein z.B. 192.168.1



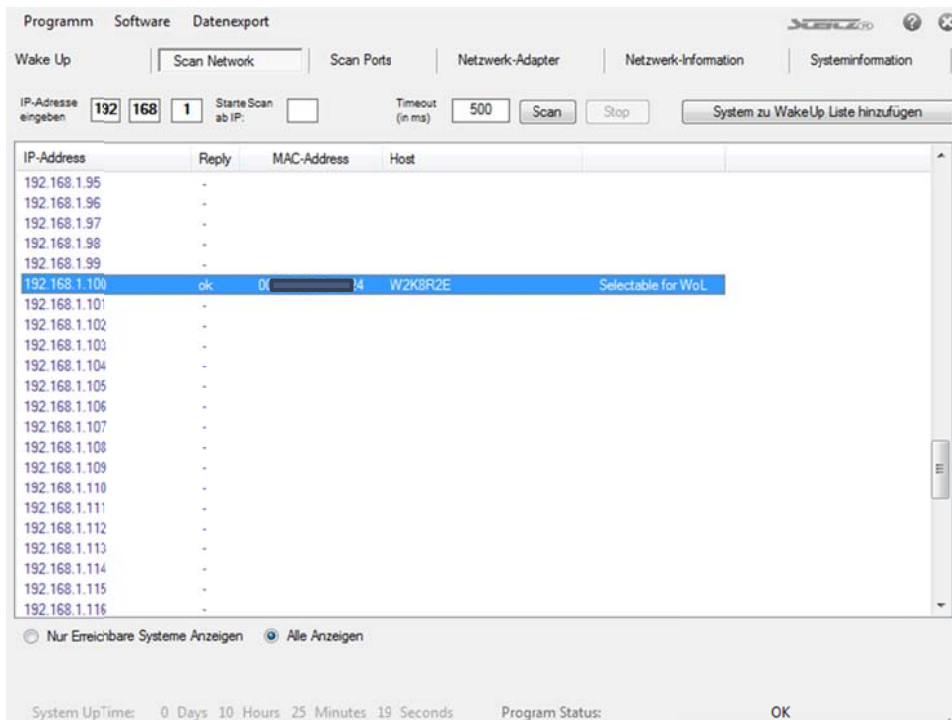
Wollen Sie alle Systeme von 1 – 254 scannen, drücken Sie bitte auf SCAN.
Andernfalls geben Sie noch die Start-IP ein und drücken anschließend auf SCAN



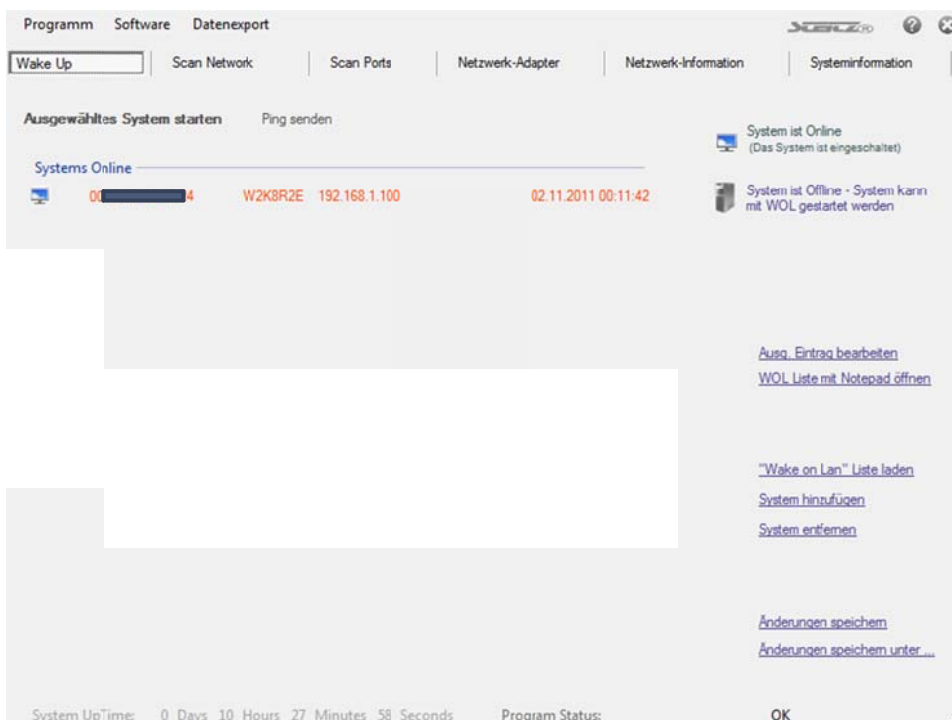
Die Software scannt das Subnet nach erreichbaren Systemen ab und listet sie entsprechend auf.

Arbeiten Sie mit einer Domäne oder verfügeben Sie über ein sauber konfigurierte DNS-Dienste, werden die Namen entsprechend aufgelöst.

Nach erfolgreichen Scan können Sie sich eine Liste der Wake On Lan Systeme erstellen. Bitte markieren Sie das in dieser Liste aufzunehmende System und drücken Sie entweder auf „System zu WakeUp-Liste hinzufügen“ oder führen Sie einen Doppelklick auf dem selektierten Eintrag aus.

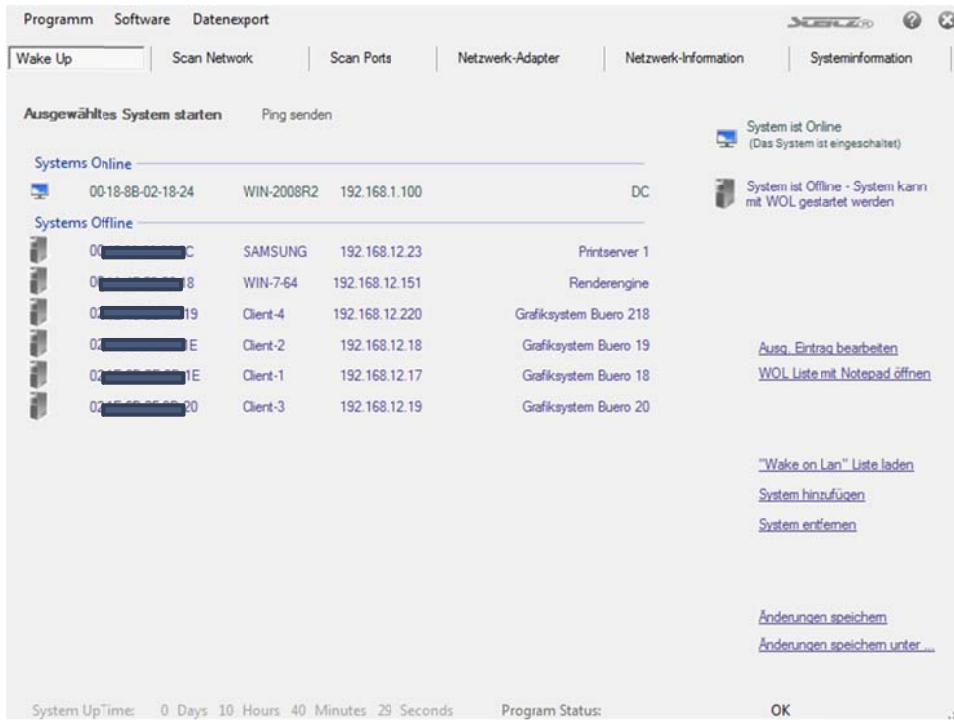


Wenn Sie nun auf die Registerkarte „Wake Up“ wechseln, sehen Sie, dass das System hinzugefügt wurde.



Wiederholen Sie diesen Vorgang für jedes System, welches Sie künftig über das Netzwerk „aufwecken“ wollen.

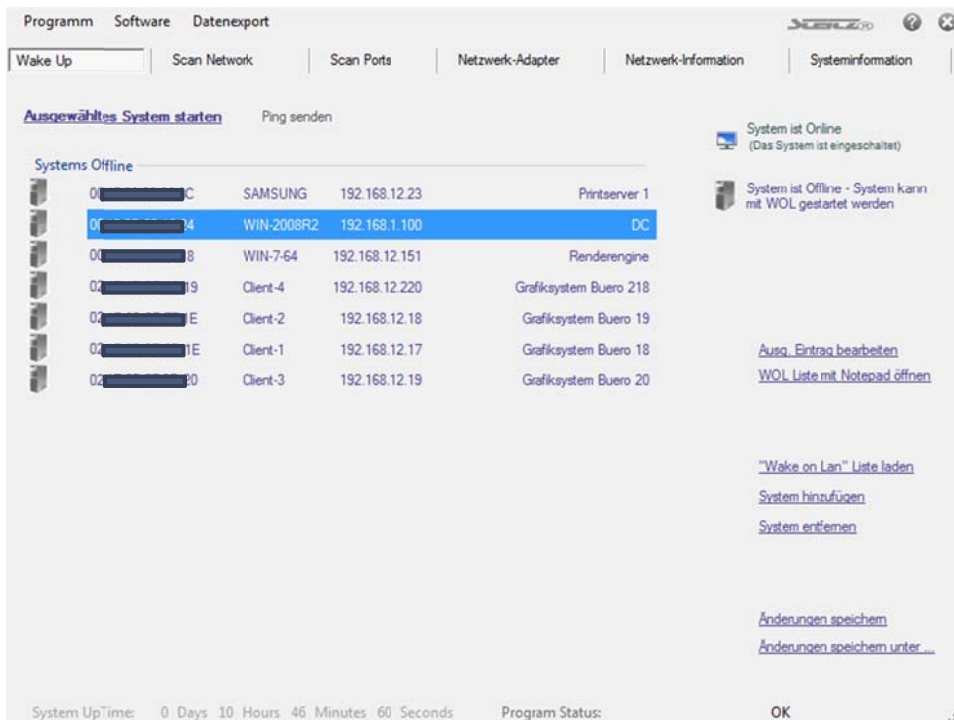
Ihre Liste könnte dann wie folgt aussehen



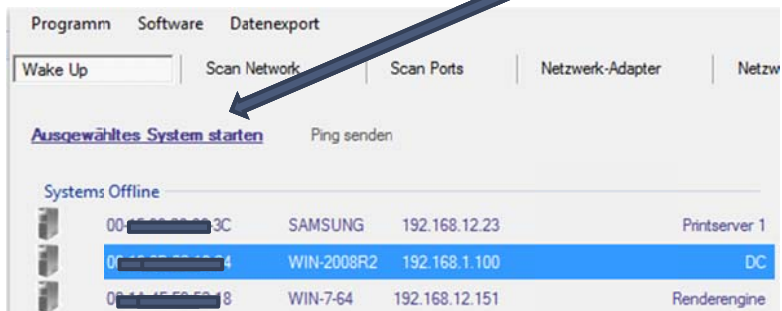
Dieses System ist online



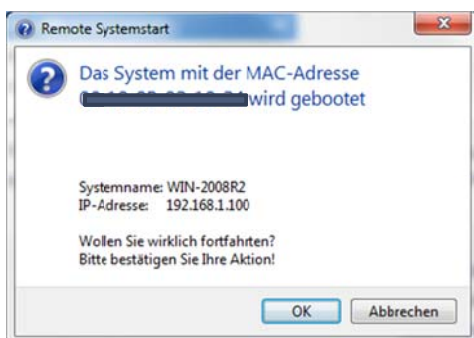
Dieses System ist offline - Sie können es mit dem Befehl



Wählen Sie ein System aus und drücken Sie auf „Ausgewähltes System starten“

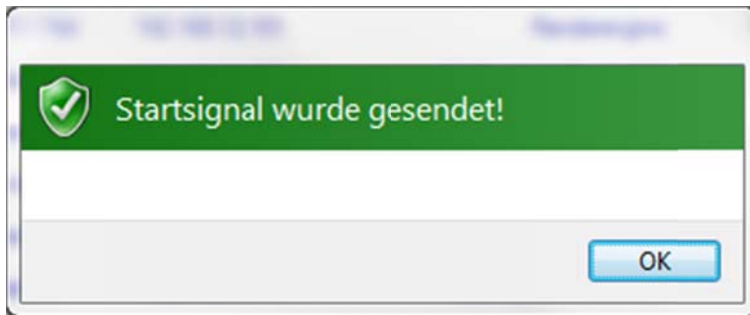


Sie erhalten die folgende Meldung

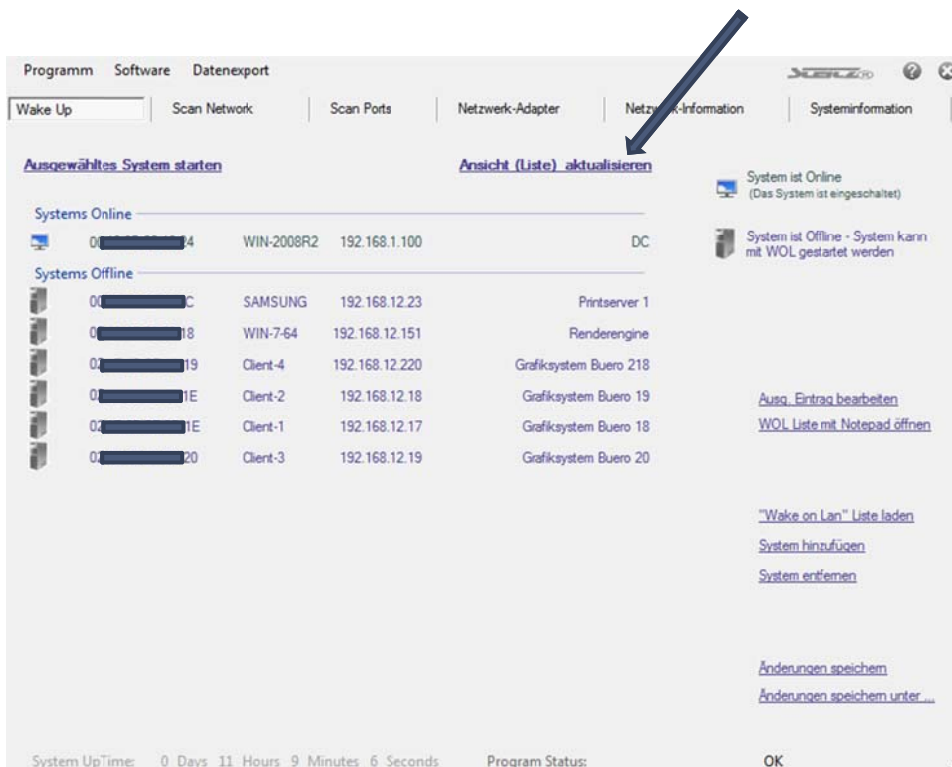


Bitte wählen Sie Ok oder Abbrechen

Sie erhalten anschliessend folgende Info



Wenn Sie nach einer kurzen Wartezeit (wie empfohlen dem System bis zu einer Minute Zeit zum Booten zu geben) auf den Link „Ansicht (Liste) aktualisieren“ drücken ...

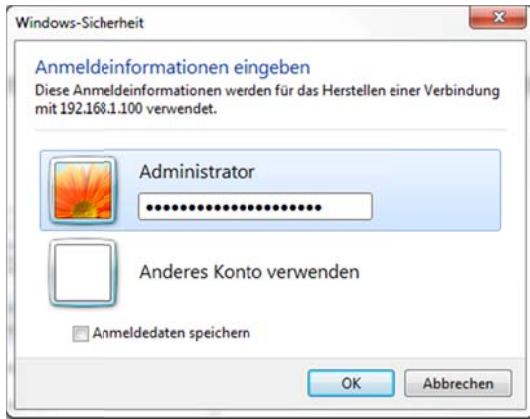


Sollte sich die Darstellung wie gezeigt geändert haben.

Das gestartete System ist nun unter der Rubrik „Systems Online“ eingetragen.

Sie haben nun die Möglichkeit, durch einen Rechtsklick mit dem ausgewählten System eine Remote-Desktop-Session zu initiieren





Bitte geben Sie Ihre Anmeldeinformationen ein und drücken Sie OK

Portscan

TCP connect Scan

Die Software verwendet die einfachste Scanmethode – TCP connect Scan.

Der Portscanner nutzt den connect Systemaufruf für den Portscan. Den eigentlichen Verbindungsaufbau übernimmt dann das Betriebssystem. Falls der Systemaufruf erfolgreich war, ist der Port offen. Die Verbindung wird dann sofort mit close wieder geschlossen. Konnte die Verbindung nicht aufgebaut werden, ist der Port geschlossen.

Spezielle Rechte sind nicht erforderlich.

Programm Software Datenexport

Wake Up | Scan Network | **Scan Ports** | Netzwerk-Adapter | Netzwerk-Information | Systeminformation

Host: 192.168.1.1 Start Port: 60 End Port: 100 Display only Open Ports Display Service Description [Scan Ports] [Cancel]

Status Portscan: Port Scanner [100%]

Host	Port	State	Service
192.168.1.1	67	Closed	Bootstrap Protocol Server
192.168.1.1	62	Closed	ACA Services
192.168.1.1	63	Closed	whois
192.168.1.1	66	Closed	Oracle SQL*NET
192.168.1.1	64	Closed	Communications Integrator (CI)
192.168.1.1	61	Closed	NI MAIL
192.168.1.1	60	Closed	Unassigned
192.168.1.1	65	Closed	TACACS-Database Service
192.168.1.1	68	Closed	Bootstrap Protocol Client
192.168.1.1	69	Closed	Trivial File Transfer
192.168.1.1	80	Open	World Wide Web HTTP
192.168.1.1	70	Closed	Gopher
192.168.1.1	71	Closed	Remote Job Service
192.168.1.1	73	Closed	Remote Job Service
192.168.1.1	72	Closed	Remote Job Service
192.168.1.1	74	Closed	Remote Job Service
192.168.1.1	81	Closed	HOSTS2 Name Server
192.168.1.1	79	Closed	Finger
192.168.1.1	77	Closed	any private RJE service
192.168.1.1	75	Closed	any private dial out service
192.168.1.1	76	Closed	Distributed External Object Store

System UpTime: 0 Days 10 Hours 6 Minutes 40 Seconds Program Status: OK

Netzwerkinfo

The screenshot shows the 'Netzwerkinfo' application window with the 'Netzwerk-Information' tab selected. The window displays details for the selected network interface 'LAN-Verbindung 2'.

Network Interfaces:

- LAN-Verbindung 2
 - MAC Address: [REDACTED]
 - IP-Address: 192.168.1.142
 - Type: Ethernet
 - Operational Status: Up
 - Speed: 100 MB/s
 - Receive Only: False
 - Support Multicast: True
 - Support IPv4: True
 - Support IPv6: True
 - Id: { [REDACTED] }
- VMware Network Adapter VMnet1
- VMware Network Adapter VMnet8
- Loopback Pseudo-Interface 1
- isatap.{F41D422B-83F3-48FB-A905-CC9EA751C45C}
- LAN-Verbindung* 2
- isatap.{8B7171EE-FC7E-404C-BD76-147993A0D4D6}
- isatap.{63A6C882-1F14-46DD-9E38-1AC8BDC4FC5C}

IPv4 Statistics:

- BytesReceived: 02,34 GB
- BytesSent: 01,85 GB
- IncomingPacketsDiscarded: 0
- IncomingPacketsWithErrors: 0
- IncomingUnknownProtocolPackets: 0
- NonUnicastPacketsReceived: 0
- NonUnicastPacketsReceived: 25.798
- NonUnicastPacketsSent: 5.623
- OutgoingPacketsDiscarded: 0
- OutgoingPacketsWithErrors: 0
- OutputQueueLength: 0
- UnicastPacketsReceived: 28.668.678
- UnicastPacketsSent: 50.760.708

IP Properties:

- DnsSuffix: None
- IsDnsEnabled: False
- IsDynamicDnsEnabled: True
- Anycast Addresses
- DhcpServer Addresses
- Dns Addresses
- Gateway Addresses
- Multicast Addresses
- Unicast Addresses
- WinsServers Addresses
- IPv4 Interface Properties
- IPv6 Interface Properties

At the bottom of the window, there is a checkbox for 'Show Loopback Infos' (checked), 'Manage' and 'Refresh' buttons, and a status bar showing 'System UpTime: 0 Days 9 Hours 59 Minutes 12 Seconds' and 'Program Status: OK'.

Programm Software Datenexport SERVO

Wake Up | Scan Network | Scan Ports | **Netzwerk-Adapter** | Netzwerk-Information | Systeminformation

Network Availability: **Mindestens ein Netzwerkadapter ist verfügbar.**

Interfaces: **Broadcom NetXtreme-Gigabit-Ethernet #2**

DNS Suffix: **Speed: 100 MB**

Supports Multicast: **True Bytes Sent: 1.935.758 KB**

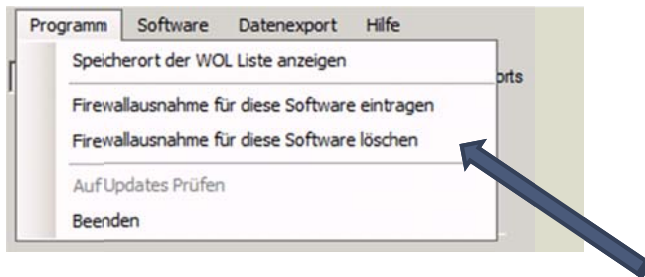
Operational Status: **Up Bytes Received: 2.450.309 KB**

Address	Type
fe80::91f:4aa4:93f5:c029%14	Unicast
192.168.1.142	Unicast
ff01::1%14	Multicast
ff02::1%14	Multicast
ff02::c%14	Multicast
ff02::1:3%14	Multicast
ff02::1:fff5:c029%14	Multicast
224.0.0.1	Multicast
224.0.0.251	Multicast
224.0.0.252	Multicast
239.255.255.250	Multicast
████████████████████	Gateway
████████████████████	DHCP Server
████████████████████	DNS Server

System UpTime: 0 Days 9 Hours 58 Minutes 46 Seconds Program Status: OK

Abschließende Maßnahmen - Firewall Konfigurieren

Haben Sie bei Windows 7 oder Windows Server 2008 eine Firewallausnahem eingetragen und wollen Sie dies wieder entfernen, verwenden Sie hierzu aus dem Menu Programm den Menupunkt „FIREWALLAUSNAHME FÜR DIESE SOFTWARE LÖSCHEN“.



Die ein- und ausgehenden Regeln werden gelöscht.