



Artikel zu IGEL OS

- [Überblick: Erste Schritte mit IGEL OS 11 \(see page 3\)](#)
- [Update und Upgrade \(see page 6\)](#)
- [BIOS Tools \(see page 216\)](#)
- [Citrix \(see page 219\)](#)
- [RDP \(see page 269\)](#)
- [VMware Horizon \(see page 286\)](#)
- [Evidian \(see page 295\)](#)
- [IBM iAccess \(see page 300\)](#)
- [Imprivata \(see page 314\)](#)
- [Microsoft Azure Virtual Desktop \(AVD\) \(see page 317\)](#)
- [SSH \(see page 325\)](#)
- [Amazon WorkSpaces mit dem HP Anyware PCoIP Client verwenden \(see page 329\)](#)
- [Konfiguration von Login Enterprise \(see page 338\)](#)
- [Nutanix \(see page 351\)](#)
- [Browser \(see page 353\)](#)
- [System \(see page 373\)](#)
- [Netzwerk \(see page 390\)](#)
- [Sicherheit \(see page 440\)](#)
- [Zertifikate \(see page 504\)](#)
- [Smartcard \(see page 539\)](#)
- [Desktop und Bildschirm \(see page 562\)](#)
- [Anpassung \(see page 588\)](#)
- [Geräte \(see page 677\)](#)
- [Drucker \(see page 801\)](#)
- [UD Pocket \(see page 812\)](#)
- [Sonstiges \(see page 824\)](#)



## Überblick: Erste Schritte mit IGEL OS 11

Der folgende Artikel bietet einen kurzen Überblick über die ersten Schritte mit einem IGEL Gerät oder einem Drittherstellergerät, das Sie in IGEL OS konvertieren möchten. Die Schritte sind grundsätzlich die gleichen, im Falle eines Drittherstellergeräts müssen Sie jedoch den IGEL OS Creator verwenden.

IGEL Gerät	Gerät eines Drittherstellers
<p><b>Schritt 1: UMS herunterladen und installieren</b></p> <ul style="list-style-type: none"> <li>• <a href="#">IGEL Downloadserver</a><sup>1</sup></li> <li>• Anleitung: Installation eines IGEL UMS Servers</li> <li>• <a href="#">Video (Windows)</a><sup>2</sup></li> <li>• <a href="#">Video (Linux)</a><sup>3</sup></li> </ul> <p><b>Schritt 2: IGEL OS 11 aktivieren</b></p> <p><b>mit dem Einrichtungsassistenten (kostenlose Testlizenz):</b></p> <ul style="list-style-type: none"> <li>• Anleitung: Einrichtungsassistent für IGEL OS, Abschnitt "Testlizenz anfordern". Siehe auch Eine Demo-Lizenz erhalten.</li> <li>• Video: <a href="#">Acquire a Demo License Including Workspace Edition and Enterprise Management Pack</a><sup>4</sup></li> </ul> <p><b>über UMS (gekaufte Lizenz):</b></p> <ul style="list-style-type: none"> <li>• Lizenzen mit der automatischen oder manuellen Lizenzbereitstellungsmethode bereitstellen</li> <li>• Video: <a href="#">Register an endpoint in the UMS and assign a license to it</a><sup>5</sup></li> </ul> <p><b>Schritt 3: Gerät konfigurieren</b></p> <p><b>über UMS:</b></p> <ul style="list-style-type: none"> <li>• Profil mit den notwendigen Einstellungen erstellen und es dem Gerät zuweisen. Siehe auch Profile.</li> <li>• Video: <a href="#">Configure an endpoint in the UMS using profiles</a><sup>6</sup></li> </ul> <p><b>ohne UMS:</b></p> <ul style="list-style-type: none"> <li>• IGEL Setup auf dem Gerät verwenden, um z.B. Benutzeroberfläche und Sitzungen zu konfigurieren</li> </ul>	<p><b>Schritt 1: UMS herunterladen und installieren</b></p> <ul style="list-style-type: none"> <li>• <a href="#">IGEL Downloadserver</a><sup>8</sup></li> <li>• Anleitung: Installation eines IGEL UMS Servers</li> <li>• <a href="#">Video (Windows)</a><sup>9</sup></li> <li>• <a href="#">Video (Linux)</a><sup>10</sup></li> </ul> <p><b>Schritt 2: IGEL OS 11 herunterladen</b></p> <ul style="list-style-type: none"> <li>• <a href="#">IGEL Downloadserver</a><sup>11</sup>, Bereich <b>OS 11 &gt; OS Creator</b></li> </ul> <p><b>Schritt 3: Gerät mit IGEL OS 11 konvertieren</b></p> <ul style="list-style-type: none"> <li>• IGEL OS Creator Referenzhandbuch</li> <li>• Video: <a href="#">Converting an x86-Endpoint Using the IGEL OS Creator</a><sup>12</sup></li> </ul> <p><b>Schritt 4: IGEL OS 11 aktivieren</b></p> <p><b>mit dem Einrichtungsassistenten (kostenlose Testlizenz):</b></p> <ul style="list-style-type: none"> <li>• Anleitung: Einrichtungsassistent für IGEL OS, Abschnitt "Testlizenz anfordern". Siehe auch Eine Demo-Lizenz erhalten.</li> <li>• Video: <a href="#">Acquire a Demo License Including Workspace Edition and Enterprise Management Pack</a><sup>13</sup></li> </ul> <p><b>über UMS (gekaufte Lizenz):</b></p> <ul style="list-style-type: none"> <li>• Lizenzen mit der automatischen oder manuellen Lizenzbereitstellungsmethode bereitstellen</li> <li>• Video: <a href="#">Register an endpoint in the UMS and assign a license to it</a><sup>14</sup></li> </ul>

5 <https://www.youtube.com/watch?v=01N-9b3P4wo>

6 <https://www.youtube.com/watch?v=Sc38mRv5Z1s>

8 <https://www.igel.com/software-downloads/workspace-edition/>

9 <https://www.youtube.com/watch?v=3YJnFiE7y5w>

10 [https://www.youtube.com/watch?v=p52CxtB\\_0ok](https://www.youtube.com/watch?v=p52CxtB_0ok)

11 <https://www.igel.com/software-downloads/workspace-edition/>

12 <https://www.youtube.com/watch?v=xVqcX6QTZ5g>

13 <https://www.youtube.com/watch?v=j31c8dzBMAg>

14 <https://www.youtube.com/watch?v=01N-9b3P4wo>


IGEL Gerät	Gerät eines Drittherstellers
<ul style="list-style-type: none"> <li>• Video: <a href="#">Configuring an Endpoint with IGEL OS 11</a><sup>7</sup></li> </ul>	<p><b>Schritt 5: Gerät konfigurieren</b></p> <p><b>über UMS:</b></p> <ul style="list-style-type: none"> <li>• Profil mit den notwendigen Einstellungen erstellen und es dem Gerät zuweisen. Siehe auch Profile.</li> <li>• Video: <a href="#">Configure an endpoint in the UMS using profiles</a><sup>15</sup></li> </ul> <p><b>ohne UMS:</b></p> <ul style="list-style-type: none"> <li>• IGEL Setup auf dem Gerät verwenden, um z.B. Benutzeroberfläche und Sitzungen zu konfigurieren</li> <li>• Video: <a href="#">Configuring an Endpoint with IGEL OS 11</a><sup>16</sup></li> </ul>

7 <https://www.youtube.com/watch?v=6WfLVgYBTHg>  
 15 <https://www.youtube.com/watch?v=Sc38mRv5Z1s>  
 16 <https://www.youtube.com/watch?v=6WfLVgYBTHg>


## Update und Upgrade

- [Upgrade from IGEL OS 11 to IGEL OS 12 \(see page 7\)](#)
- [Adapting IGEL OS 11.04 or Higher for Devices with Small Storage \(see page 8\)](#)
- [Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update \(see page 9\)](#)
- [Upgrade von IGEL OS 10 auf IGEL OS 11 \(see page 21\)](#)
- [Buddy Update einrichten \(see page 196\)](#)
- [Firmwareupdate \(see page 203\)](#)
- [IGEL OS mit einem USB-Gerät aktualisieren \(see page 207\)](#)
- [Firmware über die Linux-Konsole aktualisieren \(see page 209\)](#)
- [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher \(see page 212\)](#)
- [Error: "legacy ICG Root \(CA\) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG \(see page 213\)](#)
- [Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher \(see page 214\)](#)
- [Automatic Update Service \(see page 215\)](#)

## Upgrade from IGEL OS 11 to IGEL OS 12


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Adapting IGEL OS 11.04 or Higher for Devices with Small Storage


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## Upgrading UDC3 or UD Pocket from IGEL OS 10.06 to IGEL OS 11 via Universal Firmware Update

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Devices That Can Be Upgraded to IGEL OS 11

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Important! Consider This Before Upgrading

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Getting the UMS Ready

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Deploying the Licenses

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Creating the Universal Firmware Update

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Creating an Upgrade Profile


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Assigning the Upgrade Profile and the Universal Firmware Update to the Test Devices


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## Testing the Upgrade

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Unassigning the Upgrade Profile and the Universal Firmware Update

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Recovering the Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Upgrading All Devices

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Upgrade von IGEL OS 10 auf IGEL OS 11

- [UDC3-Geräte von IGEL OS 10 auf IGEL OS 11 upgraden \(see page 22\)](#)
- [IGEL Geräte von IGEL OS 10 nach IGEL OS 11 upgraden \(see page 121\)](#)

## UDC3-Geräte von IGEL OS 10 auf IGEL OS 11 upgraden

Dieses Dokument beschreibt, wie Sie eine beliebige Anzahl von Geräten (UDC3) von IGEL OS 10 auf IGEL OS 11 aktualisieren können.

Für das Upgrade auf IGEL OS 11 ist IGEL OS 10.05.800 oder höher erforderlich. Wenn Sie eine ältere Version von IGEL OS 10 haben, müssen Sie zuerst auf 10.05.800 oder höher aktualisieren.

Da mit IGEL OS 11 ein neues Lizenzmodell eingeführt wurde, muss für jedes Gerät eine Lizenz aus einem IGEL Workspace Edition Product Pack verfügbar sein. Wenn Sie über eine gültige Wartung für Ihre Geräte verfügen, können Sie Ihre vorhandenen UDC3- oder UD Pocket Product Packs in Workspace Edition (WE) Product Packs konvertieren; siehe [Lizenzen konvertieren für die Aktualisierung auf IGEL OS 11](#).

Die folgenden Methoden des Masseneinsatzes werden hier beschrieben:

- [Zero-Touch-Bereitstellung mit Universal Firmware Update \(see page 23\)](#): Massenumgrade von jeder Version von IGEL OS 10 auf IGEL OS 11 in einem Schritt mit Universal Firmware Update. Diese Methode kann sofort oder als geplanter Auftrag (Aufwachen oder Neustart) gestartet werden.
- [Zero-Touch-Bereitstellung mit Buddy Update \(see page 66\)](#): Massenumgrade von jeder Version von IGEL OS 10 auf IGEL OS 11 in einem Schritt mit zwei Geräten als Update Buddies. Diese Methode kann sofort oder als geplanter Auftrag (Aufwachen oder Neustart) gestartet werden.
- [Massenbereitstellung über eine geplante Aufgabe \(see page 101\)](#): Aktualisieren Sie Geräte, auf denen bereits IGEL OS 10.05.800 (oder höher) läuft, mit einem bestimmten geplanten Auftrag.

## Zero-Touch-Bereitstellung mit Universal Firmware Update

Diese Methode ist der bequemste Weg, um von IGEL OS 10 auf IGEL OS 11 zu aktualisieren. Das Verfahren verwendet die Funktion Universal Firmware Update der UMS (Universal Management Suite) und ein Profil.

Lesen Sie alle folgenden Kapitel aufmerksam und folgen Sie den Anweisungen.

1. [Geräte, die auf IGEL OS 11 hochgerüstet werden können \(see page 24\)](#)
2. [Wichtig! Berücksichtigen Sie dies vor dem Upgrade \(see page 40\)](#)
3. [Upgrade vorbereiten \(see page 42\)](#)
4. [Upgrade testen \(see page 47\)](#)
5. [Anforderungen überprüfen \(see page 51\)](#)
6. [Universal Firmware Updates erstellen \(see page 52\)](#)
7. [Profil erstellen \(see page 57\)](#)
8. [Lizenzen bereitstellen \(see page 61\)](#)
9. [Alles zusammensetzen \(see page 62\)](#)
10. [Upgrade durchführen \(see page 64\)](#)

Geräte, die auf IGEL OS 11 hochgerüstet werden können

✓ **Partnerlösungen für Peripheriegeräte**

Weitere unterstützte Hardware von IGEL Partnern, z.B. Headsets, finden Sie unter Partnerlösungen.

Grundvoraussetzungen

- CPU mit 64 Bit-Unterstützung
- CPU-Taktfrequenz:  $\geq 1$  GHz
- Arbeitsspeicher (RAM):  $\geq 2$  GB

- ⓘ Eine RAM-Größe von mehr als 2 GB wird empfohlen, wenn Sie das Folgende verwenden:
- Optimierungen für Unified Communications (verwendet eine clientseitige Media Engine)
  - Hochauflösende Grafikausgabe
  - Mehr als zwei Monitore

- ⓘ Bei Geräten mit 2 GB Arbeitsspeicher (RAM) und Shared Video Memory dürfen maximal 512 MB als Videospeicher verwendet werden.

- Speicher: Abhängig von der Release-Version von IGEL OS 11. Die Details sind unten aufgeführt:
  - Bis IGEL OS 11.03: Mindestens 2 GB;  $\geq 4$  GB empfohlen
  - Von IGEL OS 11.04 bis IGEL OS 11.07: Bei Verwendung des vollständigen Featuresets werden mindestens 2,4 GB an Speicherplatz benötigt. Eine Anleitung zur Reduktion des Featuresets finden Sie unter Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher.
  - Von IGEL OS 11.08 aufwärts: Bei Verwendung des vollständigen Featuresets werden mindestens 4 GB an Speicherplatz benötigt. Eine Anleitung zur Reduktion des Featuresets finden Sie unter Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher
- Kein VIA-Grafikadapter; diese werden von IGEL OS nicht mehr unterstützt.
- Legacy Bios und EFI/UEFI werden unterstützt.

Von OSC und UD Pocket mit IGEL OS 11 unterstützte Geräte

- ⚠ Die folgende Liste beinhaltet nur die Geräte, die **von IGEL getestet** werden (mit jeder Hauptversion von IGEL OS).  
Geräte, die nicht in dieser Liste enthalten sind, aber die Mindestanforderungen erfüllen, können ebenso als Kandidaten für eine Umstellung auf IGEL OS betrachtet werden. So ist von jedem x86-64-Gerät mit ausreichender Prozessorgeschwindigkeit und ausreichendem Arbeitsspeicher zu erwarten, dass es korrekt mit IGEL OS funktioniert. Im Rahmen einer IGEL OS Subscription oder aktiver Maintenance können Sie als Kunde davon ausgehen, dass Sie von IGEL die nötige Unterstützung erhalten. Dies gilt auch dann, wenn die entsprechenden Endgeräte nicht in der IGEL Knowledge Base oder anderswo aufgeführt sind (z. B. im IGEL Ready Showcase unter <https://www.igel.com/ready/showcase-categories/endpoints/>)."



Für Geräte, die hier oder im IGEL Ready-Showcase nicht aufgeführt sind, können Sie sich an den Hardwarehersteller wenden und ihn veranlassen, die Aufnahme dieser Geräte in das IGEL Ready-Programm zu beantragen.

Integrierte Treiber und unterstützte Peripheriegeräte werden in der [Datenbank für Drittanbieter-Hardware](#)<sup>17</sup> aufgelistet. Weitere Lösungen, die mit IGEL OS kompatibel sind, finden Sie unter Partnerlösungen.

**i** HP, Lenovo und LG Gerätemodelle sind ab Werk mit vorinstalliertem IGEL OS 11 erhältlich. Bitte wenden Sie sich an [IGEL Ready](#)<sup>18</sup>, um Informationen darüber zu erhalten, welche Gerätemodelle mit vorinstalliertem IGEL OS ausgeliefert werden.

**i** Für einige der hier aufgelisteten Geräte muss der Flash-Speicher auf  $\geq 2$  GB erweitert werden. Diese Geräte sind mit einem entsprechenden Hinweis versehen.

**i** Auf modernen Computern, wie z.B. auf Secured-Core-Rechnern (siehe <https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs>), kann es eine BIOS-Einstellung für Secure Boot geben, die die Verwendung des Microsoft Drittanbieterzertifikats für UEFI Secure Boot erlaubt. Die übliche Beschreibung einer solchen BIOS-Einstellung lautet "Allow Microsoft 3rd Party UEFI CA". Diese Einstellung muss aktiviert werden, da IGEL das Zertifikat eines Drittanbieters zur Unterstützung von UEFI Secure Boot verwendet. Wenn UEFI Secure Boot aktiviert ist, aber "Allow Microsoft 3rd Party UEFI CA" nicht aktiviert ist, können Sie IGEL OS Creator oder UD Pocket möglicherweise nicht starten. Wenn die Einstellung "Allow Microsoft 3rd Party UEFI CA" nach einer früheren Installation von IGEL OS deaktiviert wird, kann IGEL OS nicht gebootet werden. Informationen zur Aktivierung dieser Einstellung finden Sie unter Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot.

**i** Tasten mit [Fn] funktionieren möglicherweise auf einigen unterstützten und aufgelisteten Laptop-/Notebookmodellen nicht.

#### ADS-Tec

Name	Gerätekatgorie	Minimale Arbeitsspeicherröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
DVG-VMT9010	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9012	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

<sup>17</sup> <https://www.igel.de/linux-3rd-party-hardware-database/>

<sup>18</sup> <https://www.igel.com/technology-partners/>

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
DVG-VMT9015	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9112	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

#### Advantech

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L* (see page 38)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L* (see page 38)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

#### Advantech-DLoG

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
DLT-V6210	Industrie-PC/ Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrie-PC/ Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

#### Dell / Wyse

Name	Gerätekat egorie	Minimale Arbeitsspeich ergröße (RAM)	Festspeic her	Prozessor	Unterstützt ab IGEL OS Version	Hinweise
(AiO) 5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100	
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100	
5020	Thin Client	2 GB	8 GB	AMD G- Series SoC	11.02.140	
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100	
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100	
Latitude 5510	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100	Wake-on-LAN- Funktionalität wird nicht unterstützt.
Optiplex 3000	Thin Client	4 GB	32 GB	Intel Celeron N5105	11.08.200	

#### Dynabook

Name	Gerätekat egorie	Minimale Arbeitsspeich ergröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Portegé X20W-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portegé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

## Elo

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
(AiO) i2 Touch (15 und 22 Zoll)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

## Fujitsu

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Q957	Desktop-PC	8 GB	500 GB HDD	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

## HP

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version	WLAN-Chip	Hinweise
HP t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100		

Name	Geräteka tegorie	Minimale Arbeitsspei chergröße (RAM)	Festspei cher	Prozessor	Unterstütz t ab IGEL OS Version	WLAN-Chip	Hinweise
HP t430	Thin Client	2 GB	16 GB	Intel®Celeron®N4020	11.01.110	Intel AC9260	
HP t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100		
HP t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100		
HP t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100		
HP t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100		
HP t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	Intel AC9260  Realtek RTL8852AE	
HP t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	Intel AC926 0  Realtek RTL8852AE	
HP mt46	Mobile Thin Client	8 GB	32 GB	AMD Ryzen 3 PRO 4450U	11.07.100		Ohne Unterstützung für WWAN und Wake-on-LAN (beide Funktionen sind geplant)
HP Elite t655	Thin Client	4 GB / 8GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	Realtek RTL8852BE	

Name	Geräteka- tegorie	Minimale Arbeitsspei- chergröße (RAM)	Festspei- cher	Prozessor	Unterstütz- t ab IGEL OS Version	WLAN-Chip	Hinweise
HP Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Realtek RTL8852BE	Unterstützung für WWAN Intel XMM 7560 (ab 11.08.330)  Ohne Unterstützung für Wake-on- LAN (Funktion ist geplant)  Ohne Unterstützung für den integrierten Fingerabdrucks- ensor
				AMD Ryzen 5 5625U	11.08.330		
HP t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	Realtek RTL8852AE	
HP Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	Realtek RTL8852CE (Unterstützt ab 11.09.150)	
HP Pro mt440 G3	Mobile Thin Client	8 GB	128 GB	Intel Celeron 7305	11.08.440	Realtek RTL8852BE	Unterstützung für WWAN Intel XMM 7560 (ab 11.09.260)
HP Elite t755	Thin Client	8 GB	128 GB	AMD Ryzen Embedded V2546	11.09.260	Realtek RTL8852CE	Dieses Modell unterstützt keine USB-C Docking- Stationen

#### HP Dockingstationen

Name	Unterstützt ab IGEL OS Version	Hinweise
HP USB-C Dockingstation G5	11.08.230	
HP USB-C G5 Essential Dock	11.08.290	Wird nicht von HP t640 unterstützt

## Intel

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
NUC 5i5MYHE	Desktop-PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop-PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop-PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

## Lenovo

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
ThinkCentre M625q	Desktop-PC	4 GB	32 GB	AMD E2-9000e	Intel AC9260	11.04.100	
		8 GB	128 GB	AMD A4-9120e	QCA6174 802.11ac	11.04.100	
ThinkCentre M75n	Desktop PC	8 GB	256 GB	AMD Ryzen 3 Pro 3300 U	Intel AC9260	11.05.100	
ThinkCentre M70q	Desktop PC	16 GB	256 GB	Intel i5-10500t	Comet Lake PCH CNVi WiFi, Intel	11.05.100	

Name	Gerätekatgorie	Minimale Arbeitsspeichgröße (RAM)	Festspeicher	Prozessor	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
ThinkCentre M70q Gen 3	Desktop PC	16 GB	256 GB	Intel Core i5-12500T	Intel AX201	11.08.240	
ThinkCentre M75q Gen 2	Desktop PC	4 GB	256 GB	AMD Ryzen 5 PRO 5650U	Intel AX200	11.08.240	
K14 AMD Gen 1	Laptop/ Notebook	8 GB	256 GB	AMD Ryzen 5 PRO 5650U	Mediatek MT7921	11.08.240	
ThinkPad L14 Gen 1	Laptop/ Notebook	64 GB	1 TB	AMD Ryzen 7 Pro 4750U	Wi-Fi 6 AX200, Intel	11.05.100	
14w	Laptop/ Notebook	4 GB	64 GB	AMD A6-9220C	QCA6174 802.11ac	11.05.100	
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Quectel EM05-G 4G CAT4 LTE-Unterstützung ab 11.08.360
ThinkCentre Neo50q Gen 4	Thin Client	8 GB	256 GB	Intel Core i3-1215U	Wi-Fi 6 RTL8852 BE	11.08.240	
		4 GB	256 GB	Intel Celeron 7305	Wi-Fi 6 AX201		



Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
K14 Intel Gen 1	Laptop/ Notebook	16 GB	256 GB	Intel Core i5-1135G7	Intel AX210 WiFi / BT combo	11.08.290	
ThinkPad L14 Intel Gen 3	Laptop/ Notebook	16 GB	512 GB	Intel Core i5-1235U	Intel Wi-Fi 6 AX201 2x2 AX vPro	11.08.330	Quectel EM05-G 4G CAT4 LTE-Unterstützung ab 11.08.360
ThinkEdge SE10	Thin Client	8 GB	1 TB	Intel Atom x6425RE	MediaTek MT7921L EN	11.08.360	
			256 GB	Intel Atom x6214RE	Intel AX210	11.08.360	
ThinkPad L14 AMD Gen 4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852 CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L15 AMD Gen4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852 CE	11.08.440	Quectel EM05-G 4G CAT4

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeich er	Prozesso r	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
ThinkPad L14 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L15 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L13 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX201	11.09.210	Quectel EM05-G 4G CAT4 Kein integriertes LAN
ThinkPad L13 AMD Gen 4	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 3 PRO 7330U	AMD RZ616	11.09.210	Quectel EM05-G 4G CAT4 Kein integriertes LAN

#### Lenovo Dockingstationen

Name	Unterstützt ab IGEL OS Version
ThinkPad USB-C Hybrid Dock	11.07.100
IOBOX	11.07.100

Name	Unterstützt ab IGEL OS Version
Lenovo Universal USB-C Dock	11.08.440

## Lenovo USB-C-auf-Ethernet-Adapter

Name	Unterstützt ab IGEL OS Version	Unterstützt mit
USB-C-auf-Ethernet-Adapter	11.09.260	<ul style="list-style-type: none"> <li>• ThinkPad L13 Intel Gen4</li> <li>• ThinkPad L13 AMD Gen4</li> </ul>

## LG

Name	Gerätekatégorie	Minimale Arbeitsspeicherröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
24CK550* * (see page 39)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
24CK560* * (see page 39)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
38CK950	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
38CK900	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600N	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600W	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
34CN650	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
CQ600	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360
24CR670	All in One	4 GB	16 GB	Intel Celeron N5105	11.09.110
34CR650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210
27CQ650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210

#### LG Dockingstationen

Name	Unterstützt ab IGEL OS Version
LG USB Multi Port Hub	11.09.100

#### OnLogic

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
CL210G-10	Industrie-PC/ Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop-PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

#### Onyx Healthcare

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

**Pepperl+Fuchs**

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
BTC12N	Industrial Box Thin Client	4 GB	32 GB	Intel Apollo Lake N4200	11.09.100
BTC14N	Industrial Box Thin Client	4 GB	32 GB	AMD Ryzen Embedded V1202B	11.09.100

**Rein Medical**

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

**Secunet**

Name	Gerätekatégorie	Minimale Arbeitsspeichergröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

USB-Speichersticks, die als UD Pocket Hardware verwendet werden können

#### DIGITTRADE


Name	Speicherplatz	Unterstützt ab IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133


#### Transcend

Name
<a href="#">Powered by IGEL UD Pocket (see page 24)</a>
<a href="#">Powered by IGEL UD Pocket 2 (see page 24)</a>

Offiziell unterstützte virtuelle Umgebungen

- Getestet mit Ubuntu (64-Bit) und Standardeinstellungen

 Beachten Sie, dass die Verwendung eines UD Pockets auf einer virtuellen Maschine von IGEL **nicht** unterstützt wird.

 Für einige Features sind mehr als 2 GB RAM erforderlich. Beispiel: Wenn Sie Umgebungen mit zwei Monitoren verwenden, muss eine virtuelle Maschine über mindestens 8 GB RAM verfügen.

Name	Arbeitsspeicher (RAM)	Festspeicher	Typ	Unterstützt ab IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

\* Delock Adapter DP 1.2 zu DVI funktioniert nicht.


\*\* Wenn Sie an diesem Gerät einen zusätzlichen 4k-Bildschirm verwenden, ändern Sie bitte die BIOS-Einstellungen wie folgt:


1. Gehen Sie auf die Seite **Chipset**.
2. Setzen Sie **Integrated Graphics** auf "Force".
3. Setzen Sie **UMA Frame Buffer Size** auf "256M" oder höher.


Wenn Sie festgestellt haben, dass Ihre Geräte für ein Upgrade auf IGEL OS geeignet sind, beachten Sie [Wichtig! Berücksichtigen Sie dies vor dem Upgrade](#) (see page 40).


Wichtig! Berücksichtigen Sie dies vor dem Upgrade


Um sicherzustellen, dass Ihr Upgrade erfolgreich sein kann, überprüfen Sie die folgenden Warnungen und Hinweise; ein Warnsymbol zeigt an, dass irreversible Schäden an Ihren Geräten auftreten können.


 **Vorhandene Partitionen:** Jede vorhandene Partition auf dem Ziellaufwerk Ihres Geräts wird gelöscht. Das Installationsprogramm partitioniert das Zielgerät neu. Die Gesamtgröße der neu erstellten Partitionen wird basierend auf dem verfügbaren Festplattenspeicher berechnet. Der minimale Festplattenverbrauch beträgt 2 GB, der maximale 16 GB.

 **Kein Downgrade**  
Nach der Migration auf IGEL OS 11 können Sie Ihr IGEL OS 10 System nicht mehr wiederherstellen. Der Gerätespeicher wird mit einem neuen Partitionierungsschema vollständig überschrieben.

 **Funktionen (z. B. Clients)**  
IGEL OS 11 verfügt nicht über den kompletten Funktionsumfang von IGEL OS 10. Stellen Sie sicher, dass die aktuelle Version von IGEL OS 11 Ihren Anforderungen entspricht. Einzelheiten finden Sie in den entsprechenden Release-Informationen.

 **Eigene Partitionen**  
Der Inhalt von benutzerdefinierten Partitionen wird durch das Upgrade gelöscht. Stellen Sie sicher, dass Sie den Inhalt sichern und nach Abschluss des Upgrades wiederherstellen. Neben der Dysfunktionalität nach dem Upgrade können Anwendungen und Kerneltreiber in einer benutzerdefinierten Partition das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Wir empfehlen, benutzerdefinierte Partitionen beim Upgrade zu deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

 **Eigene Befehle**  
Die Persistenz von benutzerdefinierten Befehlen kann nicht garantiert werden. Neben der Dysfunktionalität nach dem Upgrade können benutzerdefinierte Befehle das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Im Allgemeinen müssen benutzerdefinierte Befehle für IGEL OS 11 angepasst werden. Wir empfehlen, dass Sie benutzerdefinierte Befehle beim Aktualisieren deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

 **Stromversorgung**  
Achten Sie darauf, dass das Gerät nicht mit Batterie betrieben wird, d. h. dass es während des gesamten Upgrade-Prozesses an eine Stromversorgung angeschlossen wird.

 **Netzwerk**



Alle Geräte müssen an ein WLAN oder LAN angeschlossen sein. LAN ist die empfohlene Option. Das Gerät wird nicht aktualisiert, wenn es mit OpenVPN, OpenConnect, Genucard, NCP VPN oder mobilem Breitband verbunden ist.

Wenn Sie alles Relevante berücksichtigt haben, fahren Sie fort mit [Upgrade vorbereiten](#) (see page 42).

### Upgrade vorbereiten

Dieser Abschnitt beschreibt die erforderlichen Vorbereitungen und Tests, bevor Produktivgeräte aktualisiert werden können. Die Prüfung sollte mit mindestens einem Gerät durchgeführt werden, das für Ihre Umgebung charakteristisch ist. Dieses Gerät sollte jede benutzerdefinierte Partition und jeden benutzerdefinierten Befehl enthalten, der möglicherweise in einem Ihrer Geräte vorhanden ist.

Um das Upgrade vorzubereiten, gehen Sie in folgenden Schritten vor:

1. [UMS vorbereiten](#) (see page 43)
2. [Setup einstellen](#) (see page 44)
3. [Lizenz bereitstellen](#) (see page 45)
4. [Update-Quelle konfigurieren](#) (see page 46)

### UMS vorbereiten

Um Ihre Geräte auf IGEL OS 11 aufzurüsten, benötigen Sie die entsprechende Version der UMS. Außerdem müssen die Geräte bei der UMS registriert sein, um ihre Lizenzen zu erhalten.


1. Wenn Sie dies noch nicht getan haben, aktualisieren Sie Ihre UMS auf Version 6.01.130 oder höher. Anweisungen finden Sie unter UMS Installation aktualisieren.
2. Stellen Sie sicher, dass Ihre Geräte an der UMS registriert sind. Weitere Informationen finden Sie im Kapitel Geräte am UMS Server registrieren des UMS Handbuchs.

Wenn die UMS bereit ist, fahren Sie mit [Setup anpassen \(see page 44\)](#) fort.

## Setup anpassen

Abhängig von den Funktionen, die jetzt verwendet werden oder in Zukunft verwendet werden, muss im Setup des Geräts ein bestimmter Parametersatz eingestellt werden.

1. Gehen Sie im Setup unter **System > Firmware Update > OS 11 Upgrade**.
2. Nehmen Sie die entsprechenden Einstellungen vor:
  - Aktivieren Sie **Upgrade auf OS 11**.

 Wenn das **Upgrade auf OS 11** aktiviert ist, sucht das Gerät nach einer Workspace Edition Lizenz und stoppt die Suche nach einer älteren UDC3- oder UD Pocket-Lizenz. Daher wird es in der UMS als nicht lizenziertes Gerät angezeigt, bis eine Workspace Edition Lizenz bereitgestellt wurde.

- Wenn Sie möchten, dass das Gerät das Upgrade sofort nach einem fehlgeschlagenen Versuch erneut durchführt, aktivieren Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist**. Das Gerät versucht das Upgrade 5 Mal erneut. Wenn der 5. Versuch fehlgeschlagen ist, wird eine Meldung im Fenster des Upgrade-Tools angezeigt.
  - Wenn Ihr Gerät über eine PowerTerm Lizenz verfügt und Sie auf IGEL OS 11 aktualisieren möchten, obwohl es PowerTerm nicht unterstützt, müssen Sie folgendes aktivieren **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist**.
  - Wählen Sie unter **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** die entsprechende Option:
    - Wenn Sie IGEL Cloud Gateway (ICG) oder Shared Workplace (SWP) oder eine benutzerdefinierte Partition verwenden und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn diese Funktionen weiterhin verwendet werden können, wählen Sie **Smart**. Wenn diese Option ausgewählt und eine dieser Funktionen aktiviert ist, wird das Upgrade nur durchgeführt, wenn das Gerät eine Lizenz von einem Enterprise Management Pack beziehen konnte.
    - Wenn Sie das Gerät zwingen möchten, eine Lizenz von einem Enterprise Management Pack abzurufen, und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn die Lizenz abgerufen werden kann, wählen Sie **Immer**.
    - Wenn Sie möchten, dass das Gerät auf IGEL OS 11 aktualisiert wird, ohne ein Enterprise Management Pack zu erhalten, ohne die möglicherweise aktivierten Funktionen zu berücksichtigen, wählen Sie **Niemals**.
  - Geben Sie unter **ZWartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** den Zeitraum an, in dem das Gerät in einem Massenbereitstellungsszenario auf eine Lizenz warten soll (siehe Zero-Touch-Bereitstellung mit Universal Firmware Update, Zero-Touch-Bereitstellung mit Buddy Update und [Massenbereitstellung über eine geplante Aufgabe](#) (see page 101)). Diese Einstellung verhindert, dass das Gerät das Upgrade zu einem ungünstigen Zeitpunkt startet, da die bereitgestellte Lizenz gerade installiert wird. Auf diese Weise verhindert die Einstellung ungewollte Unterbrechungen bei der Arbeit. Für ein Masseneinsatzszenario wird der Standardwert **10 Minuten** empfohlen.
3. Klicken Sie **Übernehmen**.

Wenn das Setup angepasst ist, fahren Sie mit [Lizenz bereitstellen](#) (see page 45) fort.

## Lizenz bereitstellen

Für ein Upgrade von IGEL OS 10 auf IGEL OS 11 benötigen Sie eine entsprechende Lizenz. Je nach Ihren Anforderungen werden eine oder mehrere dieser Lizenzen für jedes Gerät benötigt:

- Eine Workspace Edition-Lizenz für die Grundfunktionen. Weitere Informationen finden Sie unter Workspace Edition
- Wenn eines der folgenden Features verwendet wird, wird eine Enterprise Management Pack-Lizenz benötigt (siehe Enterprise Management Pack):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition, wenn IGEL OS 11.03.100 oder niedriger die Zielversion ist; mit IGEL OS 11.03.500 oder höher ist das Feature Custom Partition in der Workspace Edition enthalten.

Gehen Sie wie folgt vor:

- ▶ Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:
  - Manual License Deployment: Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.
  - Automatic License Deployment (ALD): Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
  - Laden Sie drei Demo-Lizenzen herunter von <https://www.igel.com/download/>.

Wenn das Gerät eine Lizenz hat, fahren Sie mit [Update-Quelle konfigurieren](#) (see page 46) fort.


#### Update-Quelle konfigurieren

1. Gehen Sie im Setup unter **System > Update > Firmwareupdate** und konfigurieren Sie die Updatequelle für IGEL OS 11. Für mehr Information, siehe im Kapitel Firmware Update des IGEL OS Handbuchs.
2. Klicken Sie **Ok**.



Wenn die korrekte Update-Quelle konfiguriert ist, fahren Sie mit [Upgrade testen](#) (see page 47) fort.

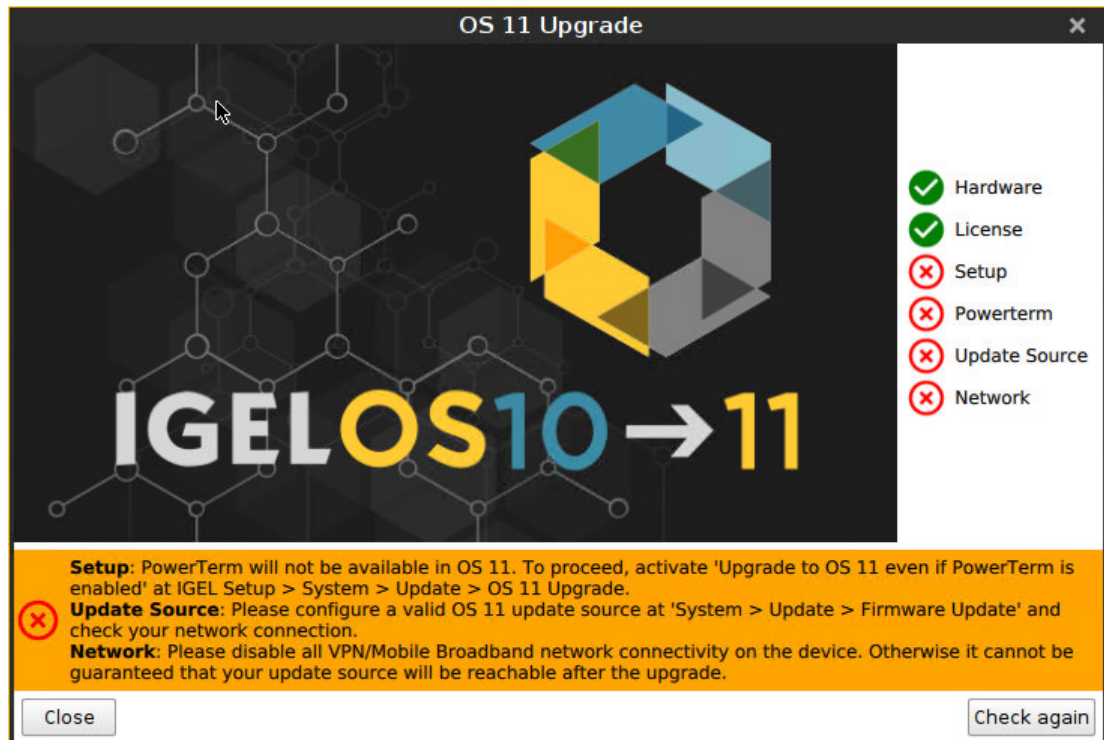
## Upgrade testen

1. Klicken Sie auf  und dann auf **Upgrade auf OS 11**. Das OS 11 Upgrade-Tool startet und zeigt an, ob alle Anforderungen erfüllt sind.

 Sie können das Starten der Startmethoden für das OS 11 Upgrade-Tool im Setup unter **Zubehör > OS11 Upgrade** ändern.

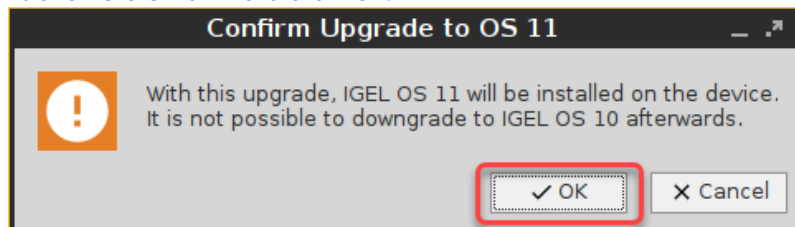


2. Überprüfen Sie die Ausgabe des OS 11 Upgrade-Tools und fahren Sie entsprechend fort:
  - Wenn jede Anforderung ein  Symbol hat, klicken Sie **OS Upgrade**, um den Upgrade-Vorgang zu starten.
  - Wenn eine oder mehrere Anforderungen ein  Symbol haben, überprüfen Sie die Meldungen und beheben Sie die Probleme. Klicken Sie anschließend auf **nochmal überprüfen**. Wenn alle Voraussetzungen erfüllt sind, ändert sich die Schaltfläche in **OS Upgrade**, und Sie können das Upgrade starten.

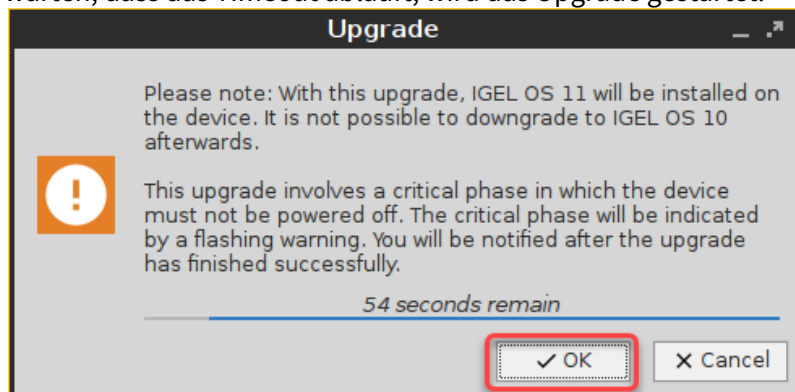


Wenn Sie das Upgrade starten, wird ein Warndialog angezeigt.

3. Klicken Sie **Ok** um fortzufahren.



Ein Warndialog mit einem Timeout wird angezeigt. Wenn Sie vor Ablauf des Timeouts auf **Abbrechen** klicken, wird das Upgrade abgebrochen. Wenn Sie auf **OK** klicken oder einfach darauf warten, dass das Timeout abläuft, wird das Upgrade gestartet.



Nachdem der Warndialog bestätigt oder der Timeout abgelaufen ist, startet das Gerät neu in eine spezielle IGEL OS 10 Umgebung, in der das System-Upgrade durchgeführt wird. Das



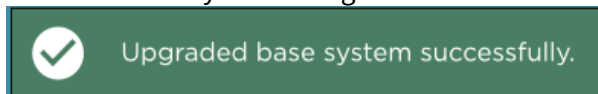
**Upgrade** Fenster zeigt den Fortschritt an.



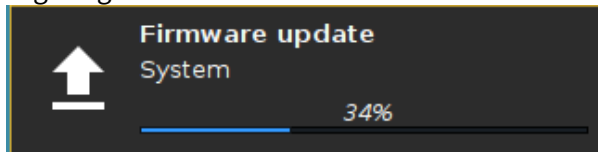
Während der kritischen Phase darf das Gerät nicht ausgeschaltet werden. In diesem Stadium des Fortschritts wird eine zusätzliche Warnung angezeigt.



Wenn das Basissystem erfolgreich aktualisiert wurde, wird eine Meldung angezeigt.



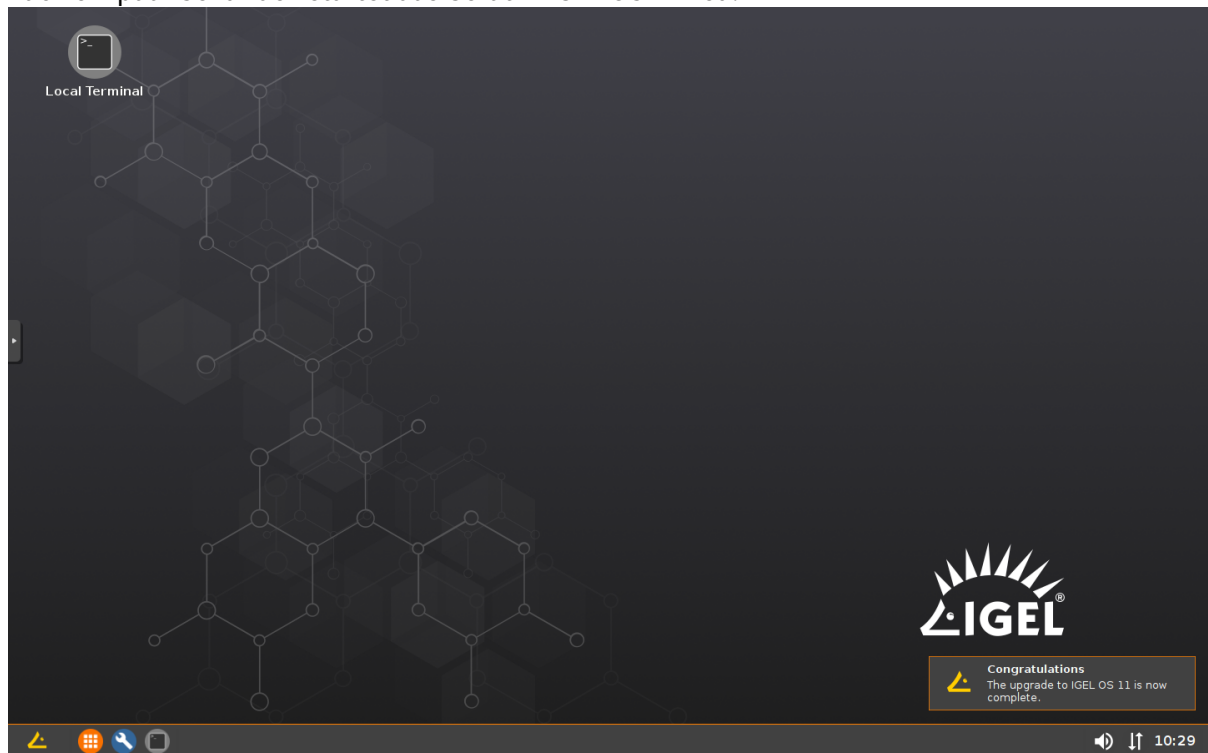
Die restlichen Komponenten der Firmware sind installiert, was durch Update-Meldungen angezeigt wird.



Wenn die Installation abgeschlossen ist, sieht das **Upgrade**-Fenster wie folgt aus:



Nach ein paar Sekunden startet das Gerät in IGEL OS 11 neu.



Wenn der Upgrade-Test erfolgreich war, können Sie das Massen-Upgrade aufsetzen. Fahren Sie mit [Anforderungen überprüfen](#) (see page 51) fort.

### Anforderungen überprüfen

Die folgenden Anforderungen müssen erfüllt sein:

- Das Upgrade wurde mit charakteristischen Geräten getestet.
- UMS 6.01.130 oder höher ist verfügbar.
- Die Firmware 10.05.800 (oder höher) ist der UMS bekannt. Zu diesem Zweck muss ein Gerät mit dieser Firmware-Version in der UMS registriert werden. Dies ist bereits der Fall, wenn Sie das Upgrade mit der gleichen UMS getestet haben, mit der Sie das Massensupgrade durchführen werden. Wenn nicht, müssen Sie jetzt ein Gerät mit der entsprechenden Firmware-Version registrieren.
- Alle Geräte sind mit einem normalen LAN verbunden (nicht mit OpenVPN, OpenConnect, Genucard oder mobilem Breitband).
- Alle Geräte befinden sich in einer sicheren Umgebung, in der der Aktualisierungsprozess nicht unterbrochen werden kann, z. B. durch Ausschalten der Geräte.

Wenn alle Anforderungen erfüllt sind, fahren Sie mit [Universal Firmware Updates erstellen](#) (see page 52) fort.

## Universal Firmware Updates erstellen

Detaillierte Informationen finden Sie im Kapitel Universal Firmware Update im UMS Handbuch.

**i** Wenn Sie die High-Availability-Erweiterung verwenden, beachten Sie, dass Universal Firmware Updates NICHT synchronisiert werden. Sie müssen Firmwareupdates entweder auf alle HA-Knoten herunterladen oder einen externen (FTP-) Server konfigurieren.

1. Erstellen Sie ein Universal Firmware Update für IGEL OS 10.05.800 (oder höher).
2. Nachdem Sie das Universal Firmware Update für IGEL OS 10.05.800 (oder höher) erstellt haben, erstellen Sie ein Universal Firmware Update für IGEL OS 11.

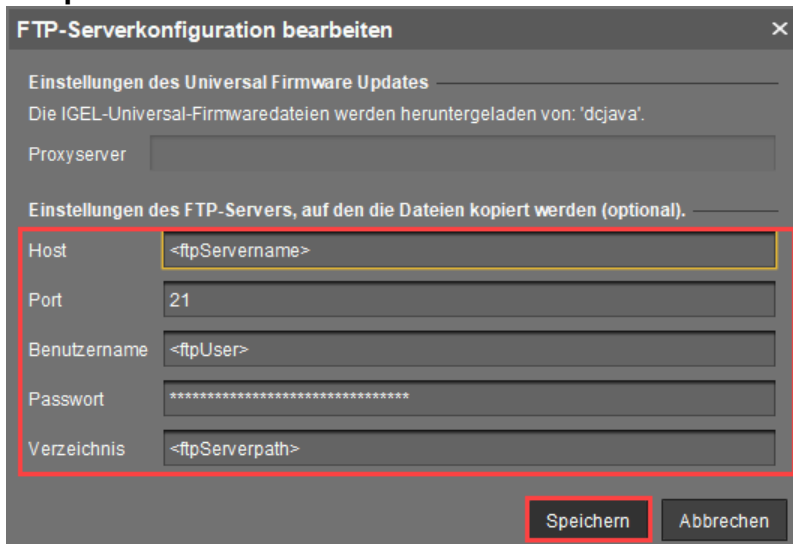
**!** Die Reihenfolge der Erstellung ist entscheidend, da die IGEL OS 11 Firmware eine höhere ID aufweisen muss, um vom Gerät ausgewählt werden zu können. Näheres hierzu siehe [Upgrade durchführen](#) (see page 64).

## Universal Firmware Update für ICG konfigurieren

Wenn Sie IGEL Cloud Gateway (ICG) verwenden, muss ein FTP-Server, der für alle Geräte zugänglich ist, als Updatequelle konfiguriert werden.

So konfigurieren Sie einen FTP-Server als Aktualisierungsquelle:

1. Gehen Sie in der UMS unter **UMS Administration > Universal Firmware Update** und klicken Sie auf **Editieren...**.
2. Geben Sie die für den Zugriff auf den FTP-Server erforderlichen Daten ein und klicken Sie auf **Speichern**.



**FTP-Serverkonfiguration bearbeiten**

Einstellungen des Universal Firmware Updates

Die IGEL-Universal-Firmwaredateien werden heruntergeladen von: 'dcjava'.

Proxyserver

Einstellungen des FTP-Servers, auf den die Dateien kopiert werden (optional).

Host: <ftpServername>

Port: 21

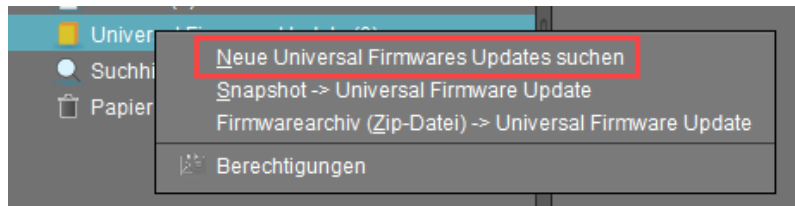
Benutzername: <ftpUser>

Passwort: \*\*\*\*\*

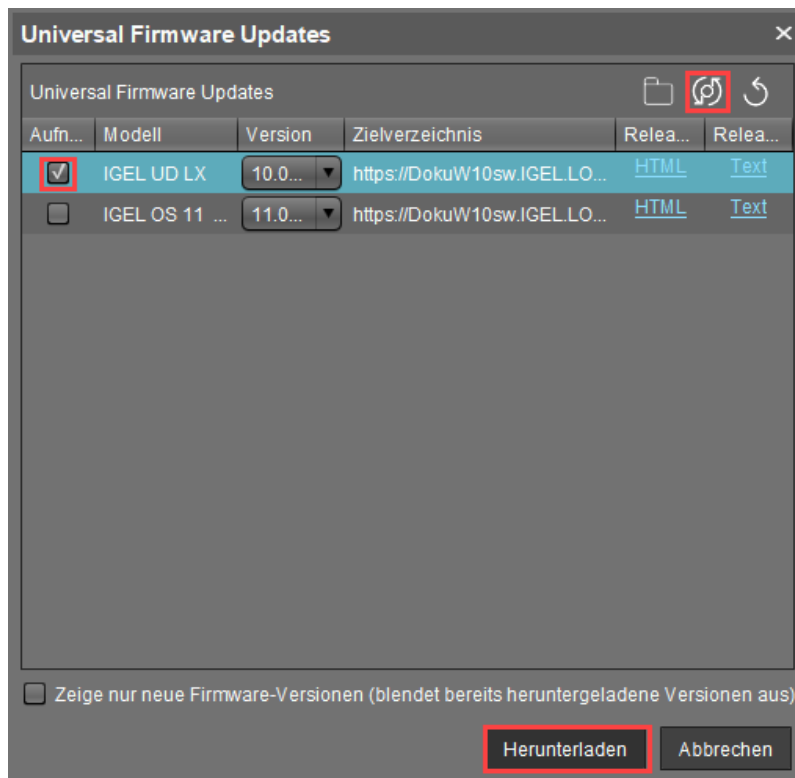
Verzeichnis: <ftpServerpath>

**Speichern**    Abbrechen

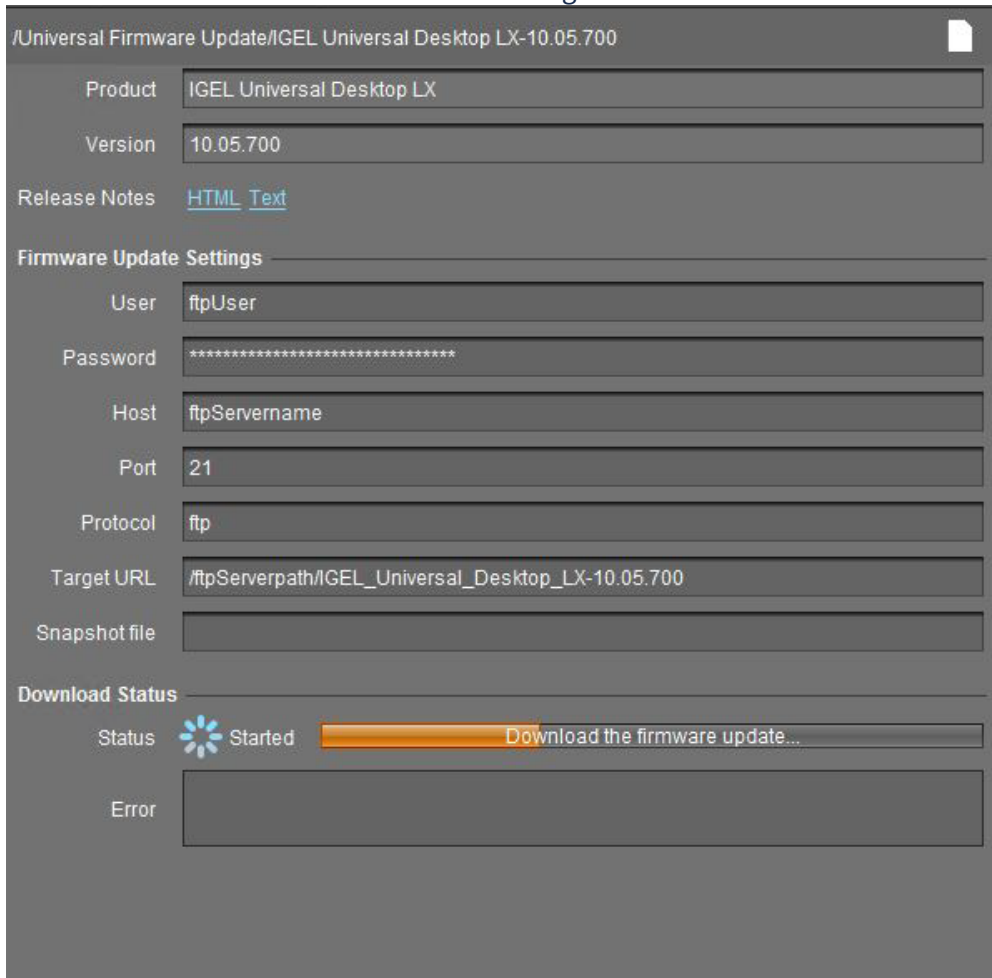
3. Gehen Sie unter **Server - [UMS Adresse] > Universal Firmware Update** und wählen Sie im Kontextmenü **Neue Universal Firmware Updates suchen**.




4. Wählen Sie den Eintrag für die 10.05.800 (oder höher) Firmware, klicken Sie  um den in Schritt 2 ausgewählten FTP-Server auszuwählen und klicken Sie **Herunterladen**.



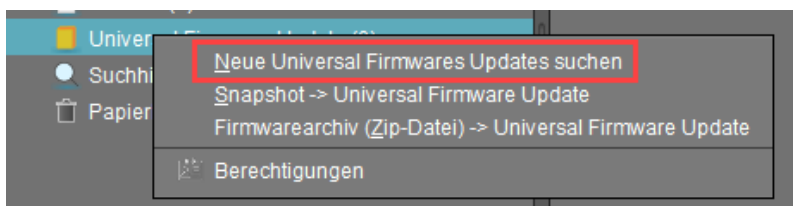
5. Die Firmware wird auf den FTP-Server übertragen.




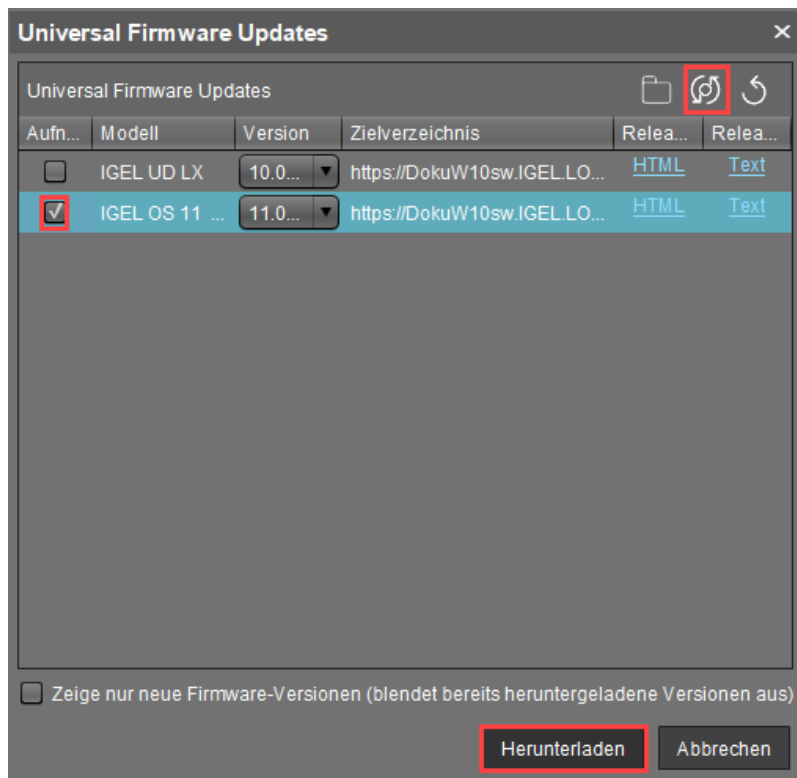
The screenshot shows the 'Universal Firmware Update' configuration window. The title bar reads '/Universal Firmware Update/IGEL Universal Desktop LX-10.05.700'. The configuration fields are as follows:

- Product: IGEL Universal Desktop LX
- Version: 10.05.700
- Release Notes: [HTML](#) [Text](#)
- Firmware Update Settings**
  - User: ftpUser
  - Password: [Redacted]
  - Host: ftpServername
  - Port: 21
  - Protocol: ftp
  - Target URL: /ftpServerpath/IGEL\_Universal\_Desktop\_LX-10.05.700
  - Snapshot file: [Empty]
- Download Status**
  - Status:  Started Download the firmware update...
  - Error: [Empty]

6. Gehen Sie unter **Server - [UMS Adresse] > Universal Firmware Update** und wählen Sie erneut im Kontextmenü **Neue Universal Firmwares Updates suchen**.



7. Wählen Sie den Eintrag für die IGEL OS 11 Firmware, klicken Sie  um den in Schritt 2 ausgewählten FTP-Server auszuwählen und klicken Sie **Herunterladen**.



8. Die Firmware wird auf den FTP-Server übertragen.

/Universal Firmware Update/IGEL OS 11-11.01.100

Product

Version

Release Notes [HTML](#) [Text](#)

**Firmware Update Settings**

User

Password

Host


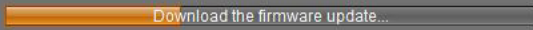
Port

Protocol

Target URL

Snapshot file

**Download Status**

Status  Started  Download the firmware update...

Error

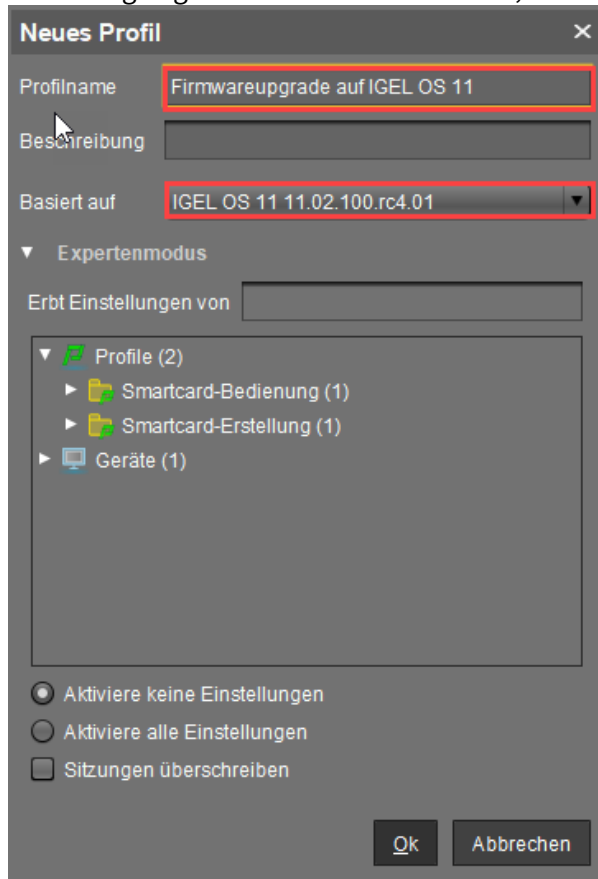
Die Geräte können die Firmware vom FTP-Server herunterladen.

Wenn das Universal Firmware Update bereit ist, fahren Sie mit [Profil erstellen](#) (see page 57) fort.

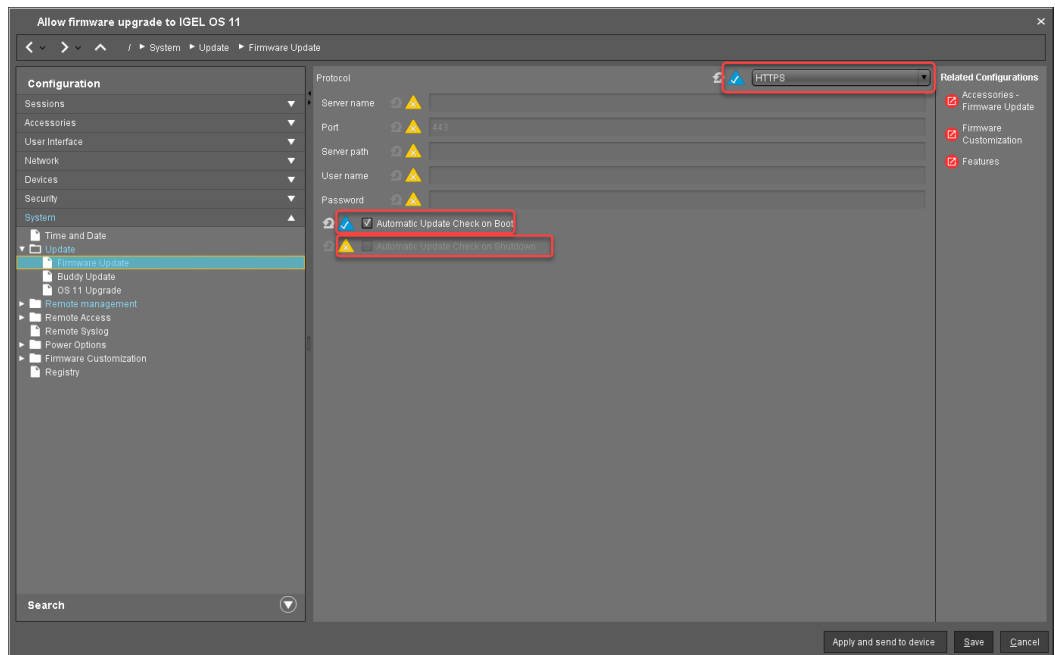


## Profil erstellen

1. Erstellen Sie ein Profil welches auf der IGEL OS 10 Firmware basiert (10.05.800 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Firmwareupgrade auf IGEL OS 11".

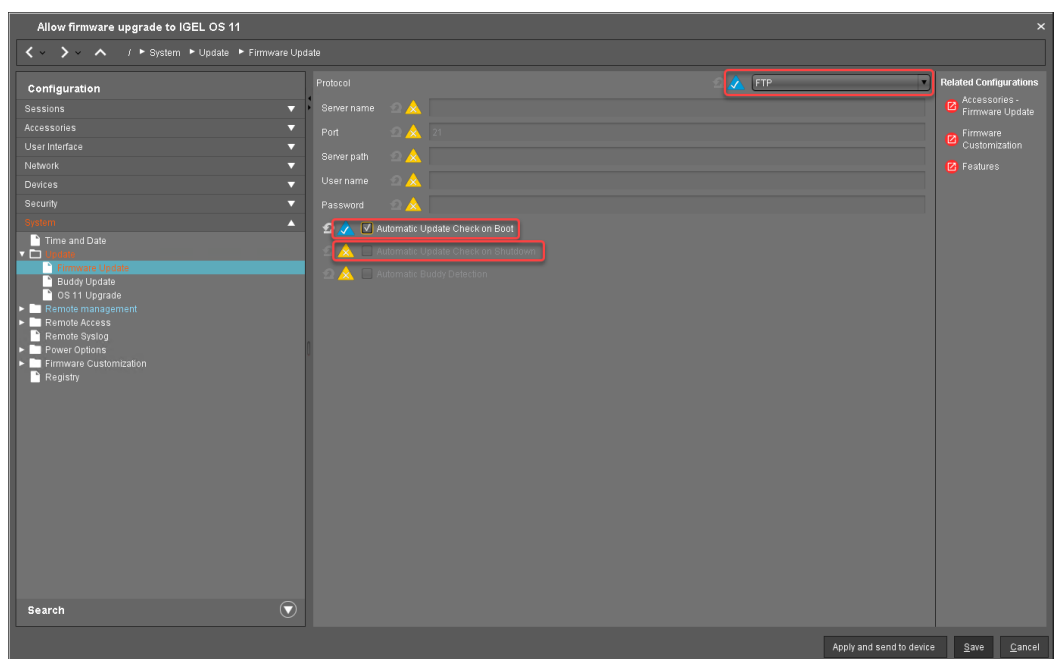


2. Gehen Sie im Konfigurationsdialog des Profils auf **System > Update > Firmwareupdate** und ändern Sie die Einstellungen entsprechend Ihrer Umgebung:
  - Wenn sich die UMS und die Geräte in ein und demselben Netzwerk befinden und kein IGEL Cloud Gateway (ICG) verwendet wird:
    - Wählen Sie "HTTPS" als **Protokoll**.
    - Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**.
    - Stellen Sie sicher, dass **Automatische Updatesuche beim Herunterfahren** deaktiviert ist. Andernfalls wird das Gerät heruntergefahren, wenn das Update abgeschlossen ist.

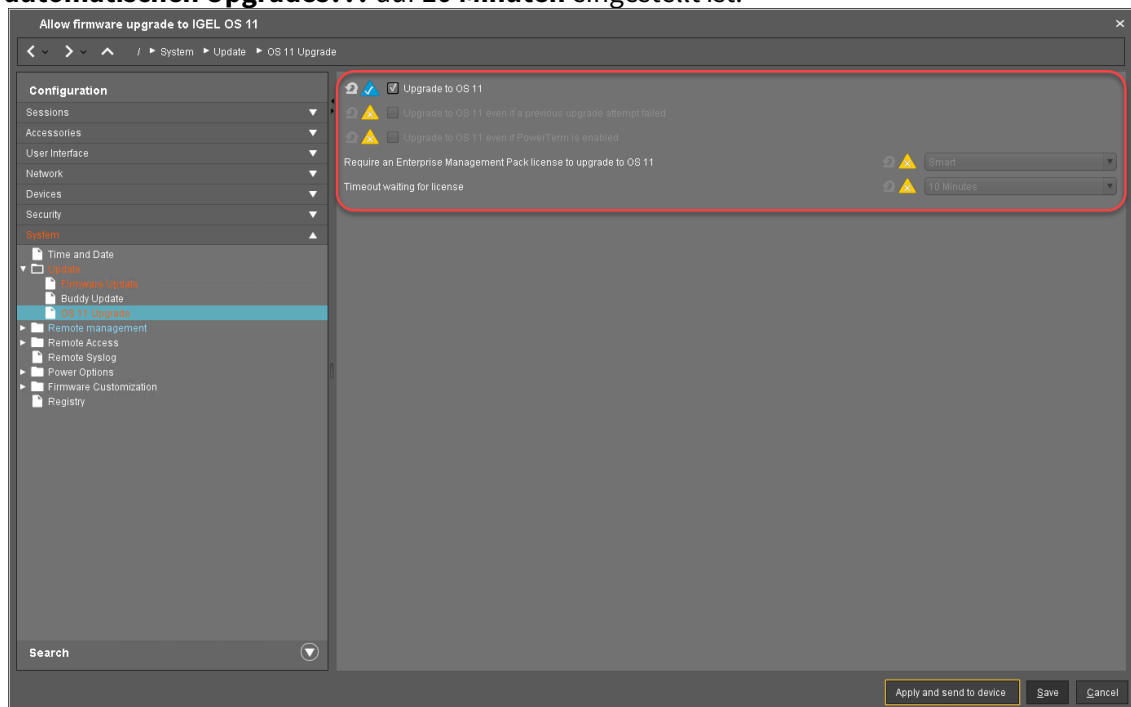


- Wenn IGEL Cloud Gateway (ICG) verwendet wird:

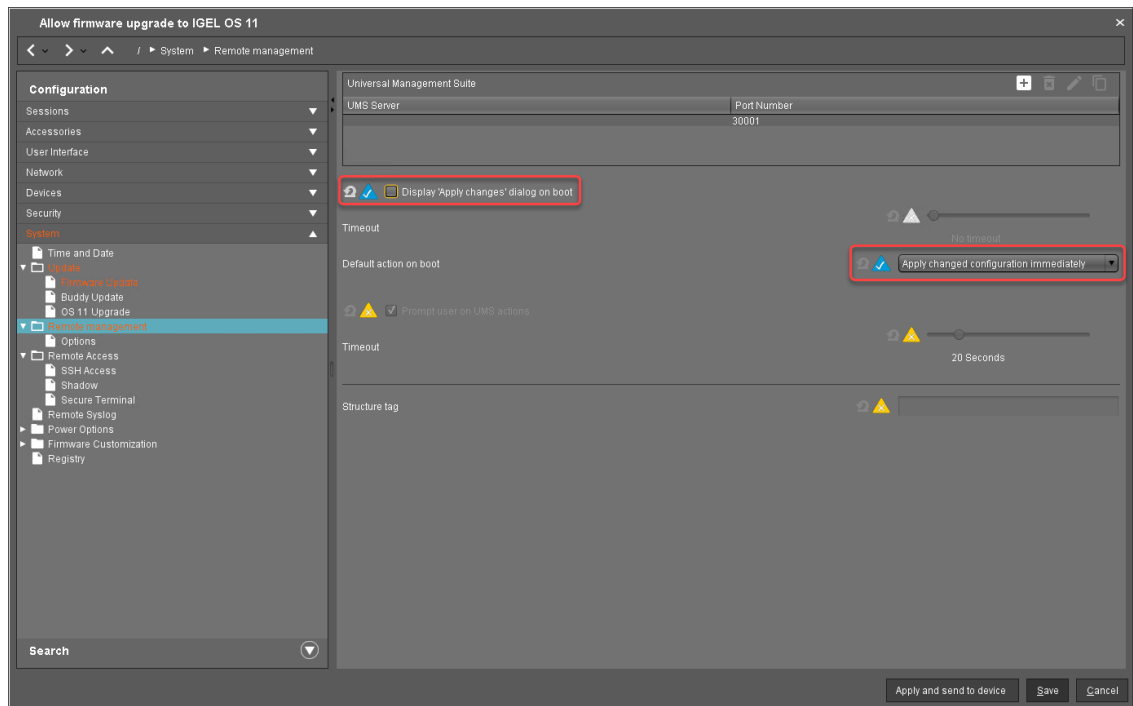
- Wählen Sie "FTP" als **Protokoll**.
- Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**.
- Stellen Sie sicher, dass **Automatische Updatesuche beim Herunterfahren** deaktiviert ist. Andernfalls wird das Gerät heruntergefahren, wenn das Update abgeschlossen ist.



3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test (Details zu den Einstellungen finden Sie unter [Setup anpassen](#) (see page 44)):
  - Aktivieren Sie **Upgrade auf OS 11**.
  - Stellen Sie **Upgrade auf OS 11, auch wenn PowerTerm aktiviert ist???** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Upgrade auf OS 11, auch wenn ein vorheriger Upgrade-Versuch fehlgeschlagen ist???** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Für das Upgrade auf OS 11 ist eine Enterprise Management Pack-Lizenz erforderlich???** nach Ihren Bedürfnissen ein.
  - Stellen Sie sicher, dass **Timeout beim Warten auf die OS 11-Lizenz zum Starten des automatischen Upgrades???** auf **10 Minuten** eingestellt ist.



4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:
  - deaktivieren Sie **Dialogfeld "Änderungen übernehmen" beim Booten anzeigen???**.
  - Setzen Sie **Standardaktion beim Booten???** auf **Geänderte Konfiguration sofort übernehmen???**.



5. Klicken Sie **Ok**.

Wenn das Profil erstellt ist, fahren Sie mit [Lizenzen bereitstellen](#) (see page 61) fort.

### Lizenzen bereitstellen

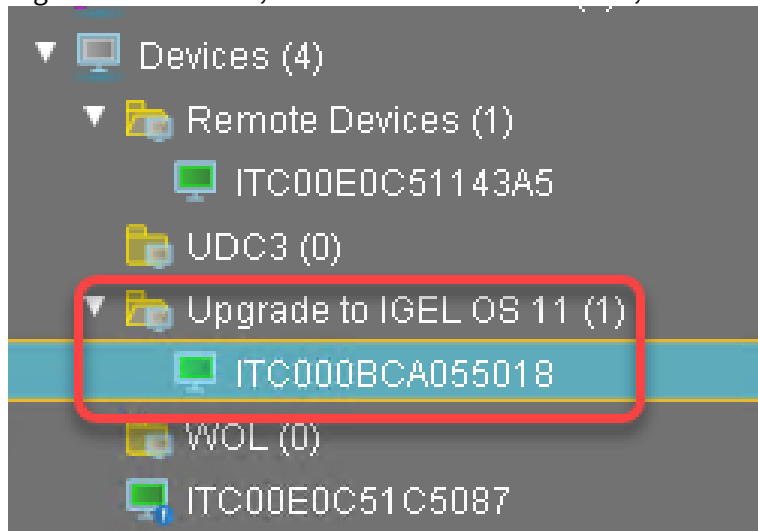
Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:

- **Automatic License Deployment (ALD):** Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
- **Manual License Deployment:** Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.

Wenn das Lizenz-Deployment aufgesetzt ist, fahren Sie mit [Alles zusammensetzen \(see page 62\)](#) fort.

## Alles zusammensetzen

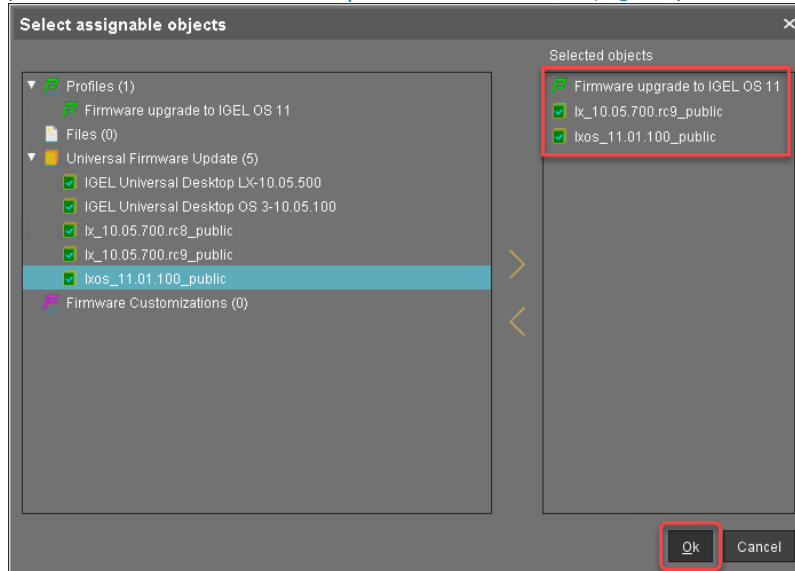
1. Legen Sie alle Geräte, die aktualisiert werden sollen, in ein Verzeichnis.



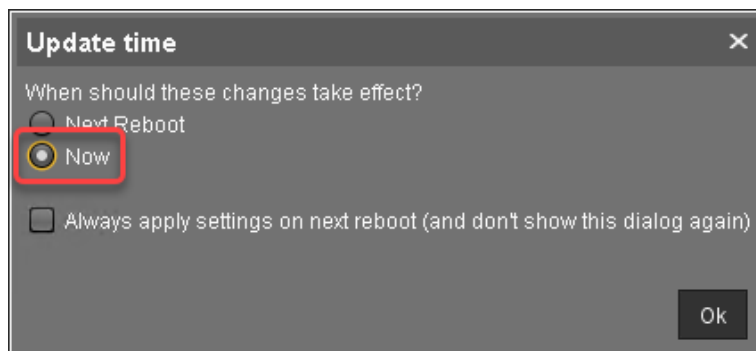
2. Wählen Sie das Verzeichnis und klicken Sie  im Bereich **Zugeordnete Objekte**.



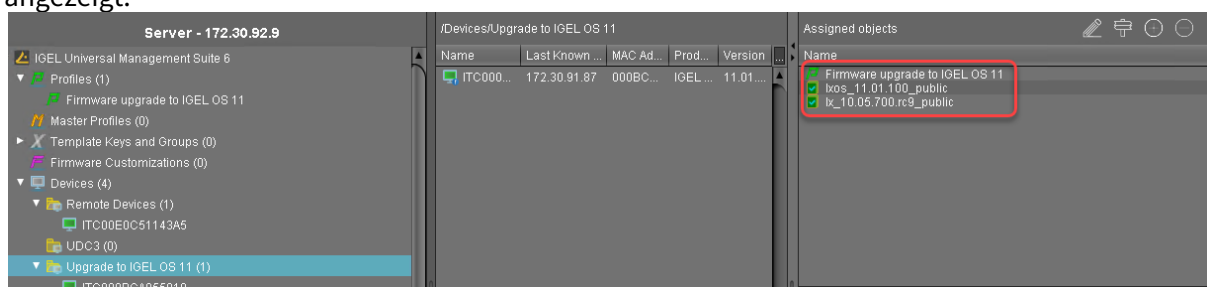
- Ordnen Sie das Profil (siehe [Profil erstellen](#) (see page 57)) und die beiden Universal Firmware Updates (siehe [Universal Firmware Updates erstellen](#) (see page 52)) dem Verzeichnis zu und klicken Sie **Ok**.



- Wählen Sie im Kontextmenü der Zuordnung **Jetzt???**.



Im Bereich **Zugeordnete Objekte**, werden das Profil und die Universal Firmware Updates angezeigt:




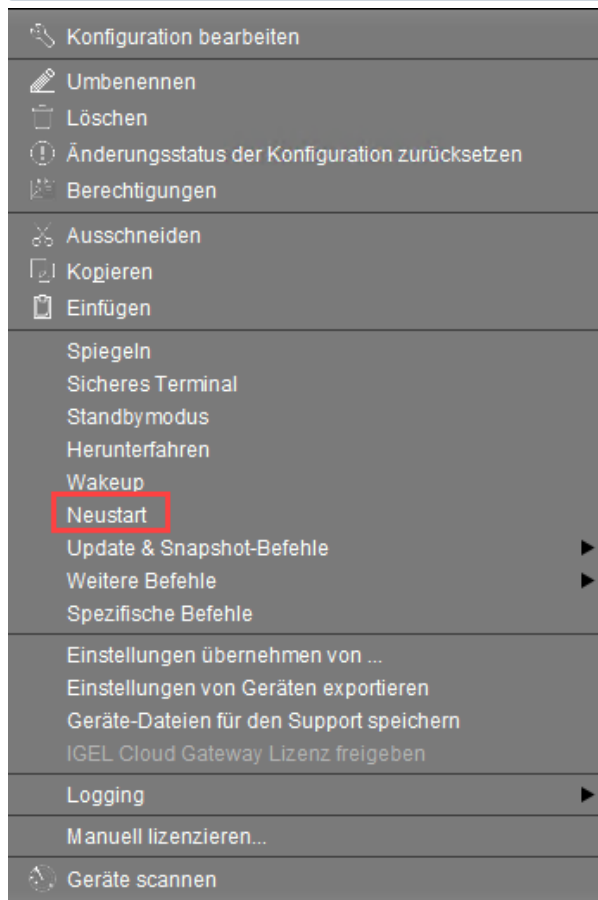
- Wenn Sie Automatic License Deployment (ALD) verwenden, ist es möglicherweise möglich, die Verteilung der Lizenzen auf das aktuelle Verzeichnis zu beschränken. Weitere Informationen finden Sie unter Verteilungsbedingungen konfigurieren, Abschnitt "Lizenzen auf Geräte in einem bestimmten Verzeichnis verteilen".

Wenn alles bereit ist, fahren Sie mit [Upgrade durchführen](#) (see page 64) fort.

## Upgrade durchführen

1. Wählen Sie in der UMS das Verzeichnis mit allen Geräten, die aktualisiert werden sollen, und starten Sie sie neu.

 Alternativ können Sie einen geplanten Auftrag für den Neustart oder das Aufwachen erstellen und ihn den Geräten oder dem Verzeichnis mit diesen Geräten zuweisen. Weitere Informationen finden Sie unter Aufgaben.



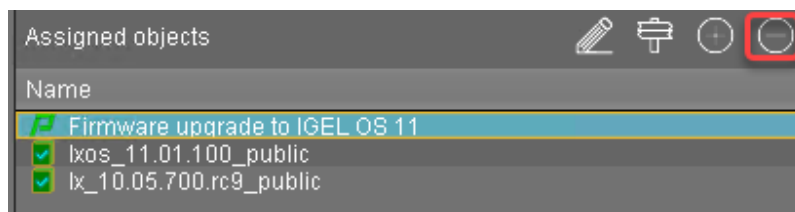
Beim Neustart oder Aufwachen aktualisieren die Geräte auf die passende IGEL OS 10 Firmware (10.05.800 oder höher). Mit dieser Version wird der Parameter **Upgrade auf OS 11** von den Geräten erkannt; außerdem fordern die Geräte IGEL OS 11-Lizenzen von der UMS an (Workspace Edition und bei Bedarf Enterprise Management Pack).

Wenn noch keine IGEL OS 11-Lizenzen auf den Geräten bereitgestellt wurden, sind die Lizenzen innerhalb weniger Minuten bereitgestellt. Das Upgrade wird gestartet, wenn die Lizenzen bereitgestellt werden. Die maximale Zeitspanne, in der das Gerät auf eine Lizenz wartet, wird durch den Parameter **Timeout beim Warten auf die OS 11-Lizenz zum Starten des automatischen Upgrades???** konfiguriert; Details finden Sie unter [Setup anpassen \(see page 44\)](#). Der Parameter **Automatische Updatesuche beim Booten** bewirkt, dass die Geräte wieder nach neuer Firmware suchen. Obwohl den Geräten zwei Universal Firmware Updates zugeordnet sind,



bietet die UMS die IGEL OS 11 Firmware an, da die ID der IGEL OS 11 Firmware höher ist als die ID der IGEL OS 10 Firmware.

2. Wenn alle Geräte erfolgreich aktualisiert wurden, entfernen Sie das Profil "Firmware-Upgrade auf IGEL OS 11" und die beiden Universal Firmware Updates aus dem Verzeichnis.



Das Upgrade ist vollständig.

## Zero-Touch-Bereitstellung mit Buddy Update

Diese Methode verwendet die Buddy-Update-Funktion von IGEL OS. Ein oder mehrere Geräte, die als Update-Buddy konfiguriert sind, greifen auf den Hauptserver zu und laden die Firmware herunter. Die anderen Geräte sind so konfiguriert, dass sie ihre Firmware von einem Update-Buddy herunterladen.

Lesen Sie alle folgenden Kapitel sorgfältig durch und folgen Sie den Anweisungen.

1. [Geräte, die auf Igel OS 11 aufgerüstet werden können \(see page 67\)](#)
2. [Wichtig! Berücksichtigen Sie dies vor dem Upgrade \(see page 83\)](#)
3. [Upgrade vorbereiten \(see page 85\)](#)
4. [Upgrade testen \(see page 90\)](#)
5. [Anforderungen überprüfen \(see page 94\)](#)
6. [Zwei Update Buddies konfigurieren \(see page 95\)](#)
7. [Profil erstellen \(see page 96\)](#)
8. [Lizenzen bereitstellen \(see page 98\)](#)
9. [Alles zusammensetzen \(see page 99\)](#)
10. [Upgrade durchführen \(see page 100\)](#)

Geräte, die auf IGEL OS 11 hochgerüstet werden können

✓ **Partnerlösungen für Peripheriegeräte**

Weitere unterstützte Hardware von IGEL Partnern, z.B. Headsets, finden Sie unter Partnerlösungen.

Grundvoraussetzungen

- CPU mit 64 Bit-Unterstützung
- CPU-Taktfrequenz:  $\geq 1$  GHz
- Arbeitsspeicher (RAM):  $\geq 2$  GB

- ⓘ Eine RAM-Größe von mehr als 2 GB wird empfohlen, wenn Sie das Folgende verwenden:
- Optimierungen für Unified Communications (verwendet eine clientseitige Media Engine)
  - Hochauflösende Grafikausgabe
  - Mehr als zwei Monitore

- ⓘ Bei Geräten mit 2 GB Arbeitsspeicher (RAM) und Shared Video Memory dürfen maximal 512 MB als Videospeicher verwendet werden.

- Speicher: Abhängig von der Release-Version von IGEL OS 11. Die Details sind unten aufgeführt:
  - Bis IGEL OS 11.03: Mindestens 2 GB;  $\geq 4$  GB empfohlen
  - Von IGEL OS 11.04 bis IGEL OS 11.07: Bei Verwendung des vollständigen Featuresets werden mindestens 2,4 GB an Speicherplatz benötigt. Eine Anleitung zur Reduktion des Featuresets finden Sie unter Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher.
  - Von IGEL OS 11.08 aufwärts: Bei Verwendung des vollständigen Featuresets werden mindestens 4 GB an Speicherplatz benötigt. Eine Anleitung zur Reduktion des Featuresets finden Sie unter Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher
- Kein VIA-Grafikadapter; diese werden von IGEL OS nicht mehr unterstützt.
- Legacy Bios und EFI/UEFI werden unterstützt.

Von OSC und UD Pocket mit IGEL OS 11 unterstützte Geräte

- ⚠ Die folgende Liste beinhaltet nur die Geräte, die **von IGEL getestet** werden (mit jeder Hauptversion von IGEL OS). Geräte, die nicht in dieser Liste enthalten sind, aber die Mindestanforderungen erfüllen, können ebenso als Kandidaten für eine Umstellung auf IGEL OS betrachtet werden. So ist von jedem x86-64-Gerät mit ausreichender Prozessorgeschwindigkeit und ausreichendem Arbeitsspeicher zu erwarten, dass es korrekt mit IGEL OS funktioniert. Im Rahmen einer IGEL OS Subscription oder aktiver Maintenance können Sie als Kunde davon ausgehen, dass Sie von IGEL die nötige Unterstützung erhalten. Dies gilt auch dann, wenn die entsprechenden Endgeräte nicht in der IGEL Knowledge Base oder anderswo aufgeführt sind (z. B. im IGEL Ready Showcase unter <https://www.igel.com/ready/showcase-categories/endpoints/>)."

Für Geräte, die hier oder im IGEL Ready-Showcase nicht aufgeführt sind, können Sie sich an den Hardwarehersteller wenden und ihn veranlassen, die Aufnahme dieser Geräte in das IGEL Ready-Programm zu beantragen.

Integrierte Treiber und unterstützte Peripheriegeräte werden in der [Datenbank für Drittanbieter-Hardware](#)<sup>19</sup> aufgelistet. Weitere Lösungen, die mit IGEL OS kompatibel sind, finden Sie unter Partnerlösungen.

**i** HP, Lenovo und LG Gerätemodelle sind ab Werk mit vorinstalliertem IGEL OS 11 erhältlich. Bitte wenden Sie sich an [IGEL Ready](#)<sup>20</sup>, um Informationen darüber zu erhalten, welche Gerätemodelle mit vorinstalliertem IGEL OS ausgeliefert werden.

**i** Für einige der hier aufgelisteten Geräte muss der Flash-Speicher auf  $\geq 2$  GB erweitert werden. Diese Geräte sind mit einem entsprechenden Hinweis versehen.

**i** Auf modernen Computern, wie z.B. auf Secured-Core-Rechnern (siehe <https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs>), kann es eine BIOS-Einstellung für Secure Boot geben, die die Verwendung des Microsoft Drittanbieterzertifikats für UEFI Secure Boot erlaubt. Die übliche Beschreibung einer solchen BIOS-Einstellung lautet "Allow Microsoft 3rd Party UEFI CA". Diese Einstellung muss aktiviert werden, da IGEL das Zertifikat eines Drittanbieters zur Unterstützung von UEFI Secure Boot verwendet. Wenn UEFI Secure Boot aktiviert ist, aber "Allow Microsoft 3rd Party UEFI CA" nicht aktiviert ist, können Sie IGEL OS Creator oder UD Pocket möglicherweise nicht starten. Wenn die Einstellung "Allow Microsoft 3rd Party UEFI CA" nach einer früheren Installation von IGEL OS deaktiviert wird, kann IGEL OS nicht gebootet werden. Informationen zur Aktivierung dieser Einstellung finden Sie unter Secured-Core PCs: Microsoft 3rd-Party UEFI Certificate for Secure Boot.

**i** Tasten mit [Fn] funktionieren möglicherweise auf einigen unterstützten und aufgelisteten Laptop-/Notebookmodellen nicht.

#### ADS-Tec

Name	Gerätekatgorie	Minimale Arbeitsspeicherröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
DVG-VMT9010	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9012	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

<sup>19</sup> <https://www.igel.de/linux-3rd-party-hardware-database/>

<sup>20</sup> <https://www.igel.com/technology-partners/>

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
DVG-VMT9015	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100
DVG-VMT9112	Industrial PC/ Terminal	4 GB 8 GB	64 GB eMMC	Intel Atom® x7-E3950	11.02.100

#### Advantech

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
POC-W213L	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100
POC-W243L* (see page 81)	Medical All in One	4 GB	32 GB	Intel Kaby Lake Core i5-7300U	11.01.110
POC-W243L* (see page 81)	Medical All in One	4 GB	128 GB	Intel Core i7-7300U	11.01.100

#### Advantech-DLoG

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
DLT-V6210	Industrie-PC/ Terminal	4 GB	32 GB	Intel Atom	11.01.100
DLT-V7210 K	Industrie-PC/ Terminal	4 GB	4 GB	Intel Atom E3845	11.01.100

#### Dell / Wyse

Name	Gerätekat egorie	Minimale Arbeitsspeich ergröße (RAM)	Festspeic her	Prozessor	Unterstützt ab IGEL OS Version	Hinweise
(AiO) 5040 / 5212	All in One	2 GB	2 GB	AMD G-T48E	11.01.100	
3040	Thin Client	2 GB	8 GB	Intel Atom x5-Z8350	11.01.100	
5020	Thin Client	2 GB	8 GB	AMD G- Series SoC	11.02.140	
5060	Thin Client	4 GB	8 GB	AMD GX-424CC	11.01.100	
5070	Thin Client	8 GB	32 GB	Intel Celeron J4105	11.01.100	
Latitude 5510	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-10210U	11.05.100	Wake-on-LAN- Funktionalität wird nicht unterstützt.
Optiplex 3000	Thin Client	4 GB	32 GB	Intel Celeron N5105	11.08.200	

#### Dynabook

Name	Gerätekat egorie	Minimale Arbeitsspeich ergröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Portegé X20W-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100
Portegé X30-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7300U	11.01.100
Tecra C50	Laptop/ Notebook	4 GB	500 GB	Intel i5-4210U	11.01.100
Tecra Z50-D	Laptop/ Notebook	8 GB	256 GB	Intel Core i5-7200U	11.01.100

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
SATELLITE R50	Laptop/ Notebook	4 GB	500 GB	Intel i3-6006U	11.01.100

## Elo

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
(AiO) i2 Touch (15 und 22 Zoll)	All in One	8 GB	128 GB	Intel Core i3-8100T	11.05.100

## Fujitsu

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Q957	Desktop-PC	8 GB	500 GB HDD	Intel Core i3-6100	11.02.100
FUTRO S740	Thin Client	4 GB	8 GB	Intel Celeron J4105	11.04.100

## HP

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version	WLAN-Chip	Hinweise
HP t420	Thin Client	2 GB	8 GB	AMD Embedded G-Series GX-209JA	11.02.100		

Name	Geräteka tegorie	Minimale Arbeitsspei chergröße (RAM)	Festspei cher	Prozessor	Unterstütz t ab IGEL OS Version	WLAN-Chip	Hinweise
HP t430	Thin Client	2 GB	16 GB	Intel®Celeron®N4020	11.01.110	Intel AC9260	
HP t530	Thin Client	4 GB	8 GB	AMD GX-215JJ Dual-Core	11.01.100		
HP t630	Thin Client	4 GB	8 GB	AMD GX-420GI	11.01.100		
HP t730	Thin Client	16 GB	8 GB	AMD RX-427BB APU	11.01.100		
HP t820	Thin Client	16 GB	16 GB	Intel Core i5-4570S	11.01.100		
HP t640	Thin Client	4 GB	16 GB	AMD Ryzen R1505G	11.04.100	Intel AC9260 Realtek RTL8852AE	
HP t540	Thin Client	16 GB	16 GB	AMD Ryzen Embedded R1305G	11.06.100	Intel AC926 0 Realtek RTL8852AE	
HP mt46	Mobile Thin Client	8 GB	32 GB	AMD Ryzen 3 PRO 4450U	11.07.100		Ohne Unterstützung für WWAN und Wake-on-LAN (beide Funktionen sind geplant)
HP Elite t655	Thin Client	4 GB / 8GB	32 GB	AMD Ryzen Embedded R2314	11.07.160	Realtek RTL8852BE	



Name	Geräteka- tegorie	Minimale Arbeitsspei- chergröße (RAM)	Festspei- cher	Prozessor	Unterstütz- t ab IGEL OS Version	WLAN-Chip	Hinweise
HP Elite mt645 G7	Mobile Thin Client	8 GB	256 GB	AMD Ryzen 3 5425U	11.08.230	Realtek RTL8852BE	Unterstützung für WWAN Intel XMM 7560 (ab 11.08.330)  Ohne Unterstützung für Wake-on- LAN (Funktion ist geplant)  Ohne Unterstützung für den integrierten Fingerabdrucks- ensor
				AMD Ryzen 5 5625U	11.08.330		
HP t740	Thin Client	8 GB	16 GB	AMD Ryzen Embedded V1756B	11.08.290	Realtek RTL8852AE	
HP Pro t550	Thin Client	4 GB	32 GB	Intel Celeron J6412	11.08.330	Realtek RTL8852CE (Unterstützt ab 11.09.150)	
HP Pro mt440 G3	Mobile Thin Client	8 GB	128 GB	Intel Celeron 7305	11.08.440	Realtek RTL8852BE	Unterstützung für WWAN Intel XMM 7560 (ab 11.09.260)
HP Elite t755	Thin Client	8 GB	128 GB	AMD Ryzen Embedded V2546	11.09.260	Realtek RTL8852CE	Dieses Modell unterstützt keine USB-C Docking- Stationen

#### HP Dockingstationen

Name	Unterstützt ab IGEL OS Version	Hinweise
HP USB-C Dockingstation G5	11.08.230	
HP USB-C G5 Essential Dock	11.08.290	Wird nicht von HP t640 unterstützt

## Intel

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
NUC 5i5MYHE	Desktop-PC	2 GB	32 GB	Intel i5-5300U	11.01.100
NUC 5i3RYH	Desktop-PC	2 GB	2 GB	Intel i3-5010U	11.01.100
NUC 7CJYH	Desktop-PC	2 GB	4 GB	Intel Celeron J4005	11.01.100

## Lenovo

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
ThinkCentre M625q	Desktop-PC	4 GB	32 GB	AMD E2-9000e	Intel AC9260	11.04.100	
		8 GB	128 GB	AMD A4-9120e	QCA6174 802.11ac	11.04.100	
ThinkCentre M75n	Desktop PC	8 GB	256 GB	AMD Ryzen 3 Pro 3300 U	Intel AC9260	11.05.100	
ThinkCentre M70q	Desktop PC	16 GB	256 GB	Intel i5-10500t	Comet Lake PCH CNVi WiFi, Intel	11.05.100	

Name	Gerätekatgorie	Minimale Arbeitsspeichgröße (RAM)	Festspeicher	Prozessor	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
ThinkCentre M70q Gen 3	Desktop PC	16 GB	256 GB	Intel Core i5-12500T	Intel AX201	11.08.240	
ThinkCentre M75q Gen 2	Desktop PC	4 GB	256 GB	AMD Ryzen 5 PRO 5650U	Intel AX200	11.08.240	
K14 AMD Gen 1	Laptop/ Notebook	8 GB	256 GB	AMD Ryzen 5 PRO 5650U	Mediatek MT7921	11.08.240	
ThinkPad L14 Gen 1	Laptop/ Notebook	64 GB	1 TB	AMD Ryzen 7 Pro 4750U	Wi-Fi 6 AX200, Intel	11.05.100	
14w	Laptop/ Notebook	4 GB	64 GB	AMD A6-9220C	QCA6174 802.11ac	11.05.100	
ThinkPad L14 AMD Gen 3	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 5 5625U	AMD RZ616 2X2AX (WiFi 6E)	11.08.230	Quectel EM05-G 4G CAT4 LTE-Unterstützung ab 11.08.360
ThinkCentre Neo50q Gen 4	Thin Client	8 GB	256 GB	Intel Core i3-1215U	Wi-Fi 6 RTL8852 BE	11.08.240	
		4 GB	256 GB	Intel Celeron 7305	Wi-Fi 6 AX201		

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeich er	Prozesso r	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinweise
K14 Intel Gen 1	Laptop/ Notebook	16 GB	256 GB	Intel Core i5-1135G7	Intel AX210 WiFi / BT combo	11.08.290	
ThinkPad L14 Intel Gen 3	Laptop/ Notebook	16 GB	512 GB	Intel Core i5-1235U	Intel Wi-Fi 6 AX201 2x2 AX vPro	11.08.330	Quectel EM05-G 4G CAT4 LTE-Unterstützung ab 11.08.360
ThinkEdge SE10	Thin Client	8 GB	1 TB	Intel Atom x6425RE	MediaTek MT7921LEN	11.08.360	
			256 GB	Intel Atom x6214RE	Intel AX210	11.08.360	
ThinkPad L14 AMD Gen 4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4
ThinkPad L15 AMD Gen4	Thin Client	8 GB	256 GB	AMD Ryzen 3 Pro 7330U	AMD RZ616 Realtek RTL8852CE	11.08.440	Quectel EM05-G 4G CAT4

Name	Gerätekatégorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeich er	Prozesso r	WLAN-Chip	Unterstützt ab IGEL OS Version	Hinw eise
ThinkPad L14 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L15 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX211	11.09.100	Quectel EM05-G 4G CAT4
ThinkPad L13 Intel Gen 4	Laptop/ Notebook	8 GB	256 GB	Intel Core i3-1315U	Intel AX201	11.09.210	Quectel EM05-G 4G CAT4 Kein integriertes LAN
ThinkPad L13 AMD Gen 4	Laptop/ Notebook	16 GB	256 GB	AMD Ryzen 3 PRO 7330U	AMD RZ616	11.09.210	Quectel EM05-G 4G CAT4 Kein integriertes LAN

#### Lenovo Dockingstationen

Name	Unterstützt ab IGEL OS Version
ThinkPad USB-C Hybrid Dock	11.07.100
IOBOX	11.07.100

Name	Unterstützt ab IGEL OS Version
Lenovo Universal USB-C Dock	11.08.440

## Lenovo USB-C-auf-Ethernet-Adapter

Name	Unterstützt ab IGEL OS Version	Unterstützt mit
USB-C-auf-Ethernet-Adapter	11.09.260	<ul style="list-style-type: none"> <li>• ThinkPad L13 Intel Gen4</li> <li>• ThinkPad L13 AMD Gen4</li> </ul>

## LG

Name	Gerätekatégorie	Minimale Arbeitsspeicherröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
24CK550* * (see page 82)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
24CK560* * (see page 82)	All in One	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
CK500	Thin Client	4 GB	32 GB	AMD G-Series GX-212JJ	11.01.100
38CK950	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
38CK900	All in One	8 GB	128 GB	AMD Ryzen 3	11.02.100
CL600N	Thin Client	4 GB	16 GB	Intel® Celeron J4105	11.03.100
CL600W	Thin Client	8 GB	128 GB	Intel® Celeron J4105	11.03.100
34CN650	All in One	4 GB	16 GB	Intel® Celeron J4105	11.05.100
24CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100
27CN650	All in One	8 GB	16 GB	Intel® Celeron J4105	11.05.100

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
CQ600	Thin Client	4 GB	16 GB	Intel Celeron N5105	11.08.330
24CQ650	All in One	4 GB	16 GB	Intel Celeron N5105	11.08.330
CQ601	Thin Client	4 GB	16 GB	Intel Pentium Silver N6005	11.08.360
24CR670	All in One	4 GB	16 GB	Intel Celeron N5105	11.09.110
34CR650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210
27CQ650	All in One	4GB	16 GB	Intel Celeron N5105	11.09.210

#### LG Dockingstationen

Name	Unterstützt ab IGEL OS Version
LG USB Multi Port Hub	11.09.100

#### OnLogic

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
CL210G-10	Industrie-PC/ Terminal	4 GB	32 GB	Intel Celeron N3350	11.04.100
KARBON 300	Desktop-PC	4 GB	32 GB	Intel Atom x5-E3930	11.04.100

#### Onyx Healthcare

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Venus 223	Medical All in One	4 GB	128 GB	Intel Quad-Core J1900	11.01.100

## Pepperl+Fuchs

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
BTC12N	Industrial Box Thin Client	4 GB	32 GB	Intel Apollo Lake N4200	11.09.100
BTC14N	Industrial Box Thin Client	4 GB	32 GB	AMD Ryzen Embedded V1202B	11.09.100

## Rein Medical

Name	Gerätekatgorie	Minimale Arbeitsspeicherg röße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
Silenio C122	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Silenio C124	All in One	8 GB	128 GB	Intel® Core™ i5 – 6th Generation	11.01.110
Clinio S 522TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100
Clinio S 524TCT	Medical All in One	8 GB	16 GB	Intel® Pentium® Silver J5005	11.04.100

## Secunet



Name	Gerätekatégorie	Minimale Arbeitsspeichergröße (RAM)	Festspeicher	Prozessor	Unterstützt ab IGEL OS Version
SINA Workstation S EliteDesk 800 G2	Workstation	16 GB	256 GB	Intel Core i7-6700	11.01.100

USB-Speichersticks, die als UD Pocket Hardware verwendet werden können

#### DIGITTRADE


Name	Speicherplatz	Unterstützt ab IGEL OS Version
Kobra Stick	≥ 4GB	11.05.133


#### Transcend

Name
<a href="#">Powered by IGEL UD Pocket (see page 67)</a>
<a href="#">Powered by IGEL UD Pocket 2 (see page 67)</a>

Offiziell unterstützte virtuelle Umgebungen

- Getestet mit Ubuntu (64-Bit) und Standardeinstellungen

 Beachten Sie, dass die Verwendung eines UD Pockets auf einer virtuellen Maschine von IGEL **nicht** unterstützt wird.

 Für einige Features sind mehr als 2 GB RAM erforderlich. Beispiel: Wenn Sie Umgebungen mit zwei Monitoren verwenden, muss eine virtuelle Maschine über mindestens 8 GB RAM verfügen.

Name	Arbeitsspeicher (RAM)	Festspeicher	Typ	Unterstützt ab IGEL OS Version
Oracle VM VirtualBox	≥ 2 GB	≥ 4 GB	Linux	11.04.100
VMware Workstation	≥ 2 GB	≥ 4 GB	Linux	11.04.100

\* Delock Adapter DP 1.2 zu DVI funktioniert nicht.


\*\* Wenn Sie an diesem Gerät einen zusätzlichen 4k-Bildschirm verwenden, ändern Sie bitte die BIOS-Einstellungen wie folgt:


1. Gehen Sie auf die Seite **Chipset**.
2. Setzen Sie **Integrated Graphics** auf "Force".
3. Setzen Sie **UMA Frame Buffer Size** auf "256M" oder höher.


Wenn Sie festgestellt haben, dass Ihre Geräte auf IGEL OS 11 hochgerüstet werden können, beachten Sie [Wichtig! Berücksichtigen Sie dies vor dem Upgrade](#) (see page 83).


### Wichtig! Vor dem Upgrade berücksichtigen


Um sicherzustellen, dass Ihr Upgrade erfolgreich sein kann, überprüfen Sie die folgenden Warnungen und Hinweise; ein Warnsymbol zeigt an, dass irreversible Schäden an Ihren Geräten auftreten können.


 **Vorhandene Partitionen:** Jede vorhandene Partition auf dem Ziellaufwerk Ihres Geräts wird gelöscht. Das Installationsprogramm partitioniert das Zielgerät neu. Die Gesamtgröße der neu erstellten Partitionen wird basierend auf dem verfügbaren Festplattenspeicher berechnet. Der minimale Festplattenverbrauch beträgt 2 GB, der maximale 16 GB.

 **Kein Downgrade**  
Nach der Migration auf IGEL OS 11 können Sie Ihr IGEL OS 10 System nicht mehr wiederherstellen. Der Gerätespeicher wird mit einem neuen Partitionierungsschema vollständig überschrieben.

 **Funktionen (z. B. Clients)**  
IGEL OS 11 verfügt nicht über den kompletten Funktionsumfang von IGEL OS 10. Stellen Sie sicher, dass die aktuelle Version von IGEL OS 11 Ihren Anforderungen entspricht. Einzelheiten finden Sie in den entsprechenden Release-Informationen.

 **Eigene Partitionen**  
Der Inhalt von benutzerdefinierten Partitionen wird durch das Upgrade gelöscht. Stellen Sie sicher, dass Sie den Inhalt sichern und nach Abschluss des Upgrades wiederherstellen. Neben der Dysfunktionalität nach dem Upgrade können Anwendungen und Kernaltreiber in einer benutzerdefinierten Partition das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Wir empfehlen, benutzerdefinierte Partitionen beim Upgrade zu deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

 **Eigene Befehle**  
Die Persistenz von benutzerdefinierten Befehlen kann nicht garantiert werden. Neben der Dysfunktionalität nach dem Upgrade können benutzerdefinierte Befehle das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Im Allgemeinen müssen benutzerdefinierte Befehle für IGEL OS 11 angepasst werden. Wir empfehlen, dass Sie benutzerdefinierte Befehle beim Aktualisieren deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

 **Stromversorgung**  
Achten Sie darauf, dass das Gerät nicht mit Batterie betrieben wird, d. h. dass es während des gesamten Upgrade-Prozesses an eine Stromversorgung angeschlossen wird.

 **Netzwerk**

Alle Geräte müssen an ein WLAN oder LAN angeschlossen sein. LAN ist die empfohlene Option. Das Gerät wird nicht aktualisiert, wenn es mit OpenVPN, OpenConnect, Genucard, NCP VPN oder mobilem Breitband verbunden ist.

Wenn Sie alles Relevante berücksichtigt haben, fahren Sie mit [Upgrade vorbereiten](#) (see page 85) fort.

## Upgrade vorbereiten

Dieser Abschnitt beschreibt die erforderlichen Vorbereitungen und Tests, bevor Produktivgeräte aktualisiert werden können. Die Prüfung sollte mit mindestens einem Gerät durchgeführt werden, das für Ihre Umgebung charakteristisch ist. Dieses Gerät sollte jede benutzerdefinierte Partition und jeden benutzerdefinierten Befehl enthalten, der möglicherweise in einem Ihrer Geräte vorhanden ist.

Um das Upgrade vorzubereiten, führen Sie die folgenden Schritte durch:

1. [UMS vorbereiten](#) (see page 86)
2. [Setup anpassen](#) (see page 87)
3. [Lizenz bereitstellen](#) (see page 88)
4. [Update-Quelle bereitstellen](#) (see page 89)

### UMS vorbereiten

Um Ihre Geräte auf IGEL OS 11 aufzurüsten, benötigen Sie die entsprechende Version der UMS. Außerdem müssen die Geräte bei der UMS registriert sein, um ihre Lizenzen zu erhalten.


1. Wenn Sie dies noch nicht getan haben, aktualisieren Sie Ihre UMS auf Version 6.01.130 oder höher. Anweisungen finden Sie unter UMS Installation aktualisieren.
2. Stellen Sie sicher, dass Ihre Geräte an der UMS registriert sind. Weitere Informationen finden Sie im Kapitel Geräte am UMS Server registrieren des UMS Handbuchs.

Wenn die UMS vorbereitet ist, fahren Sie mit [Setup anpassen \(see page 87\)](#) fort.

## Setup anpassen

Abhängig von den Funktionen, die jetzt verwendet werden oder in Zukunft verwendet werden, muss im Setup des Geräts ein bestimmter Parametersatz eingestellt werden.

1. Gehen Sie im Setup unter **System > Firmware Update > OS 11 Upgrade**.
2. Nehmen Sie die entsprechenden Einstellungen vor:
  - Aktivieren Sie **Upgrade auf OS 11**.

 Wenn das **Upgrade auf OS 11** aktiviert ist, sucht das Gerät nach einer Workspace Edition Lizenz und stoppt die Suche nach einer älteren UDC3- oder UD Pocket-Lizenz. Daher wird es in der UMS als nicht lizenziertes Gerät angezeigt, bis eine Workspace Edition Lizenz bereitgestellt wurde.

- Wenn Sie möchten, dass das Gerät das Upgrade sofort nach einem fehlgeschlagenen Versuch erneut durchführt, aktivieren Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist**. Das Gerät versucht das Upgrade 5 Mal erneut. Wenn der 5. Versuch fehlgeschlagen ist, wird eine Meldung im Fenster des Upgrade-Tools angezeigt.
  - Wenn Ihr Gerät über eine PowerTerm Lizenz verfügt und Sie auf IGEL OS 11 aktualisieren möchten, obwohl es PowerTerm nicht unterstützt, müssen Sie folgendes aktivieren **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist**.
  - Wählen Sie unter **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** die entsprechende Option:
    - Wenn Sie IGEL Cloud Gateway (ICG) oder Shared Workplace (SWP) oder eine benutzerdefinierte Partition verwenden und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn diese Funktionen weiterhin verwendet werden können, wählen Sie **Smart**. Wenn diese Option ausgewählt und eine dieser Funktionen aktiviert ist, wird das Upgrade nur durchgeführt, wenn das Gerät eine Lizenz von einem Enterprise Management Pack beziehen konnte.
    - Wenn Sie das Gerät zwingen möchten, eine Lizenz von einem Enterprise Management Pack abzurufen, und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn die Lizenz abgerufen werden kann, wählen Sie **Immer**.
    - Wenn Sie möchten, dass das Gerät auf IGEL OS 11 aktualisiert wird, ohne ein Enterprise Management Pack zu erhalten, ohne die möglicherweise aktivierten Funktionen zu berücksichtigen, wählen Sie **Niemals**.
  - Geben Sie unter **ZWartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** den Zeitraum an, in dem das Gerät in einem Massenbereitstellungsszenario auf eine Lizenz warten soll (siehe Zero-Touch-Bereitstellung mit Universal Firmware Update, Zero-Touch-Bereitstellung mit Buddy Update und [Massenbereitstellung über eine geplante Aufgabe \(see page 101\)](#)). Diese Einstellung verhindert, dass das Gerät das Upgrade zu einem ungünstigen Zeitpunkt startet, da die bereitgestellte Lizenz gerade installiert wird. Auf diese Weise verhindert die Einstellung ungewollte Unterbrechungen bei der Arbeit. Für ein Masseneinsatzszenario wird der Standardwert **10 Minuten** empfohlen.
3. Klicken Sie **Übernehmen**.

Wenn das Setup angepasst ist, fahren Sie mit [Lizenz bereitstellen \(see page 88\)](#) fort.

## Lizenz bereitstellen

Für ein Upgrade von IGEL OS 10 auf IGEL OS 11 benötigen Sie eine entsprechende Lizenz. Je nach Ihren Anforderungen werden eine oder mehrere dieser Lizenzen für jedes Gerät benötigt:

- Eine Workspace Edition-Lizenz für die Grundfunktionen. Weitere Informationen finden Sie unter Workspace Edition
- Wenn eines der folgenden Features verwendet wird, wird eine Enterprise Management Pack-Lizenz benötigt (siehe Enterprise Management Pack):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition, wenn IGEL OS 11.03.100 oder niedriger die Zielversion ist; mit IGEL OS 11.03.500 oder höher ist das Feature Custom Partition in der Workspace Edition enthalten.

Gehen Sie wie folgt vor:

- ▶ Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:
  - Manual License Deployment: Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.
  - Automatic License Deployment (ALD): Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
  - Laden Sie drei Demo-Lizenzen herunter von <https://www.igel.com/download/>.

Wenn das Gerät eine Lizenz hat, fahren Sie mit [Update-Quelle konfigurieren](#) (see page 89) fort.




#### Update-Quelle bereitstellen

1. Gehen Sie im Setup unter **System > Update > Firmwareupdate** und konfigurieren Sie die Updatequelle für IGEL OS 11. Für mehr Information, siehe im Kapitel Firmware Update des IGEL OS Handbuchs.
2. Klicken Sie **Ok**.



Wenn die korrekte Update-Quelle konfiguriert ist, fahren Sie mit [Upgrade testen \(see page 90\)](#) fort.

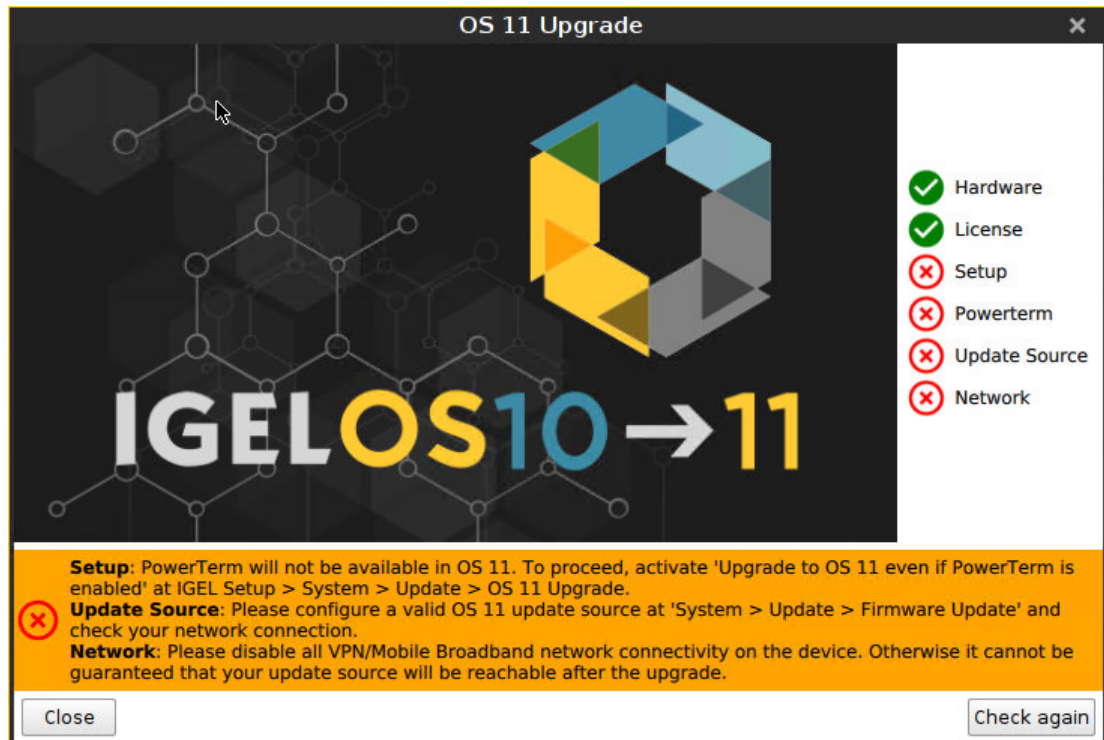
## Upgrade testen

1. Klicken Sie auf  und dann auf **Upgrade auf OS 11**. Das OS 11 Upgrade-Tool startet und zeigt an, ob alle Anforderungen erfüllt sind.

 Sie können das Starten der Startmethoden für das OS 11 Upgrade-Tool im Setup unter **Zubehör > OS11 Upgrade** ändern.

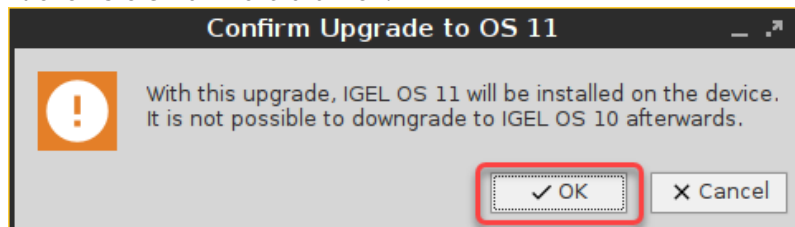


2. Überprüfen Sie die Ausgabe des OS 11 Upgrade-Tools und fahren Sie entsprechend fort:
  - Wenn jede Anforderung ein  Symbol hat, klicken Sie **OS Upgrade**, um den Upgrade-Vorgang zu starten.
  - Wenn eine oder mehrere Anforderungen ein  Symbol haben, überprüfen Sie die Meldungen und beheben Sie die Probleme. Klicken Sie anschließend auf **nochmal überprüfen**. Wenn alle Voraussetzungen erfüllt sind, ändert sich die Schaltfläche in **OS Upgrade**, und Sie können das Upgrade starten.

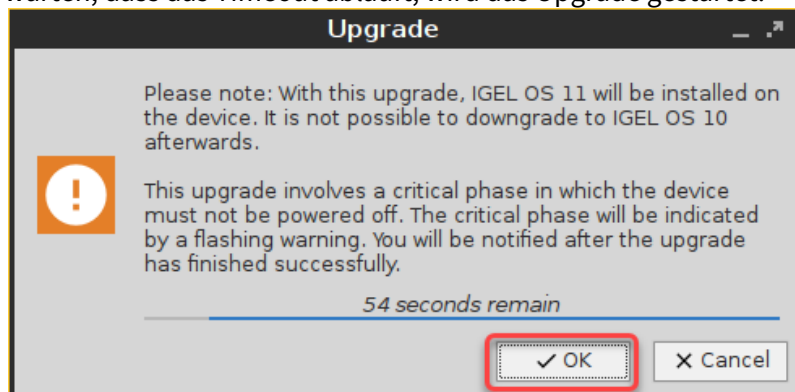


Wenn Sie das Upgrade starten, wird ein Warndialog angezeigt.

3. Klicken Sie **Ok** um fortzufahren.



Ein Warndialog mit einem Timeout wird angezeigt. Wenn Sie vor Ablauf des Timeouts auf **Abbrechen** klicken, wird das Upgrade abgebrochen. Wenn Sie auf **OK** klicken oder einfach darauf warten, dass das Timeout abläuft, wird das Upgrade gestartet.



Nachdem der Warndialog bestätigt oder der Timeout abgelaufen ist, startet das Gerät neu in eine spezielle IGEL OS 10 Umgebung, in der das System-Upgrade durchgeführt wird. Das

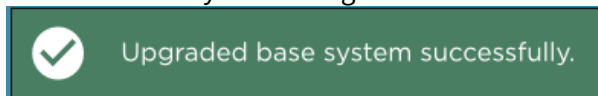
**Upgrade** Fenster zeigt den Fortschritt an.



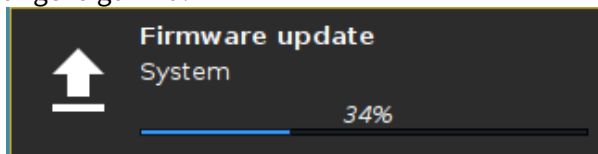
Während der kritischen Phase darf das Gerät nicht ausgeschaltet werden. In diesem Stadium des Fortschritts wird eine zusätzliche Warnung angezeigt.



Wenn das Basissystem erfolgreich aktualisiert wurde, wird eine Meldung angezeigt.



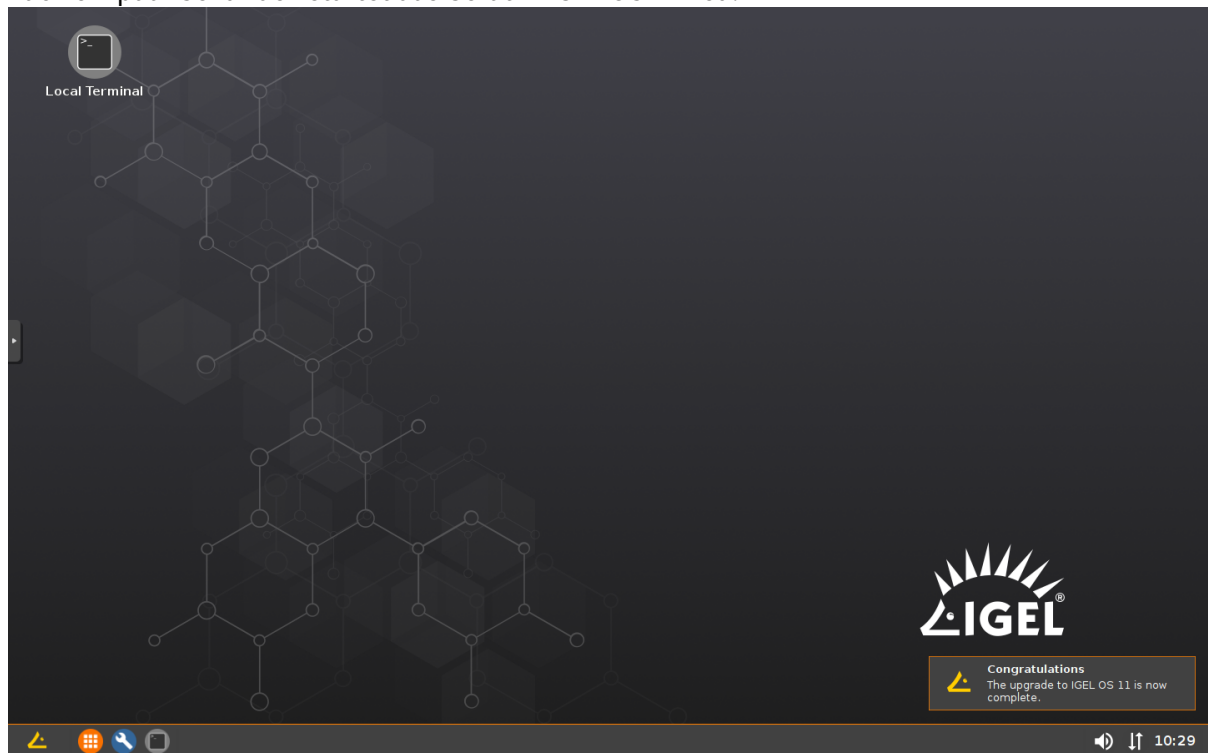
Die restlichen Komponenten der Firmware sind installiert, was durch Update-Meldungen angezeigt wird.



Wenn die Installation abgeschlossen ist, sieht das **Upgrade**-Fenster wie folgt aus:



Nach ein paar Sekunden startet das Gerät in IGEL OS 11 neu.



Wenn der Upgrade-Test erfolgreich war, können Sie das Massen-Upgrade aufsetzen. Fahren Sie mit [Anforderungen überprüfen](#) (see page 94) fort.

### Anforderungen überprüfen


Die folgenden Anforderungen müssen erfüllt sein:

- Das Upgrade wurde mit charakteristischen Geräten getestet.
- UMS 6.01.130 oder höher ist verfügbar.
- Die Firmware 10.05.800 (oder höher) ist der UMS bekannt. Zu diesem Zweck muss ein Gerät mit dieser Firmware-Version in der UMS registriert werden. Dies ist bereits der Fall, wenn Sie das Upgrade mit der gleichen UMS getestet haben, mit der Sie das Massensupgrade durchführen werden. Wenn nicht, müssen Sie jetzt ein Gerät mit der entsprechenden Firmware-Version registrieren.
- Alle Geräte sind mit einem normalen LAN verbunden (nicht mit OpenVPN, OpenConnect, Genucard oder mobilem Breitband).
- Alle Geräte befinden sich in einer sicheren Umgebung, in der der Aktualisierungsprozess nicht unterbrochen werden kann, z. B. durch Ausschalten der Geräte.

Wenn alle Anforderungen erfüllt sind, fahren Sie mit [Zwei Update Buddies konfigurieren](#) (see page 95) fort.

## Zwei Update Buddies konfigurieren

Informationen zum Einrichten von Buddy Updates finden Sie im How-To [Buddy Update einrichten](#) (see page 196).

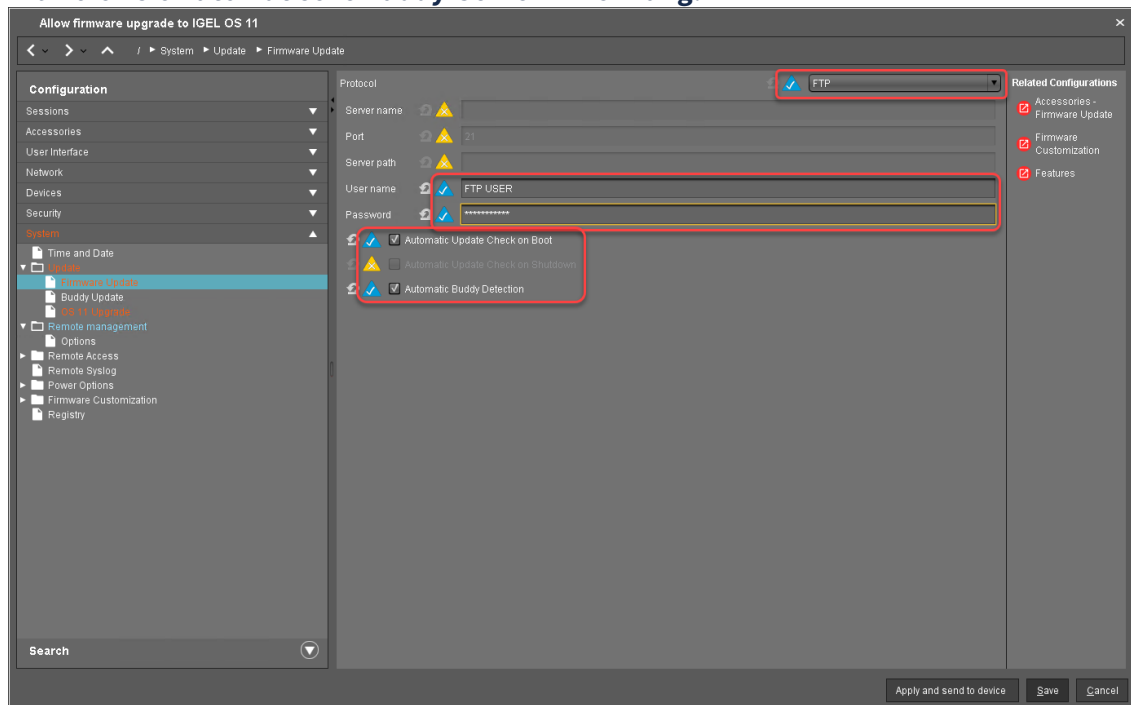
 Stellen Sie sicher, dass das Netzwerk nur die Update Buddies und die Geräte enthält, die aktualisiert werden sollen. Dadurch wird verhindert, dass andere Geräte versehentlich aktualisiert werden.

1. Aktualisieren Sie ein Gerät auf die passende IGEL OS 10 Firmware (10.05.800 oder höher) und konfigurieren Sie es als Update Buddy.
2. Aktualisieren Sie ein anderes Gerät auf IGEL OS 11 und konfigurieren Sie es als Update Buddy. Stellen Sie sicher, dass der IGEL OS 11 Update Buddy den gleichen **Benutzernamen** und das gleiche **Passwort** in **System > Update > Buddy Update** wie der IGEL OS 10 Update-Buddy hat.

Wenn die Update Buddies konfiguriert sind, fahren Sie mit [Profil erstellen](#) (see page 96) fort.

## Profil erstellen

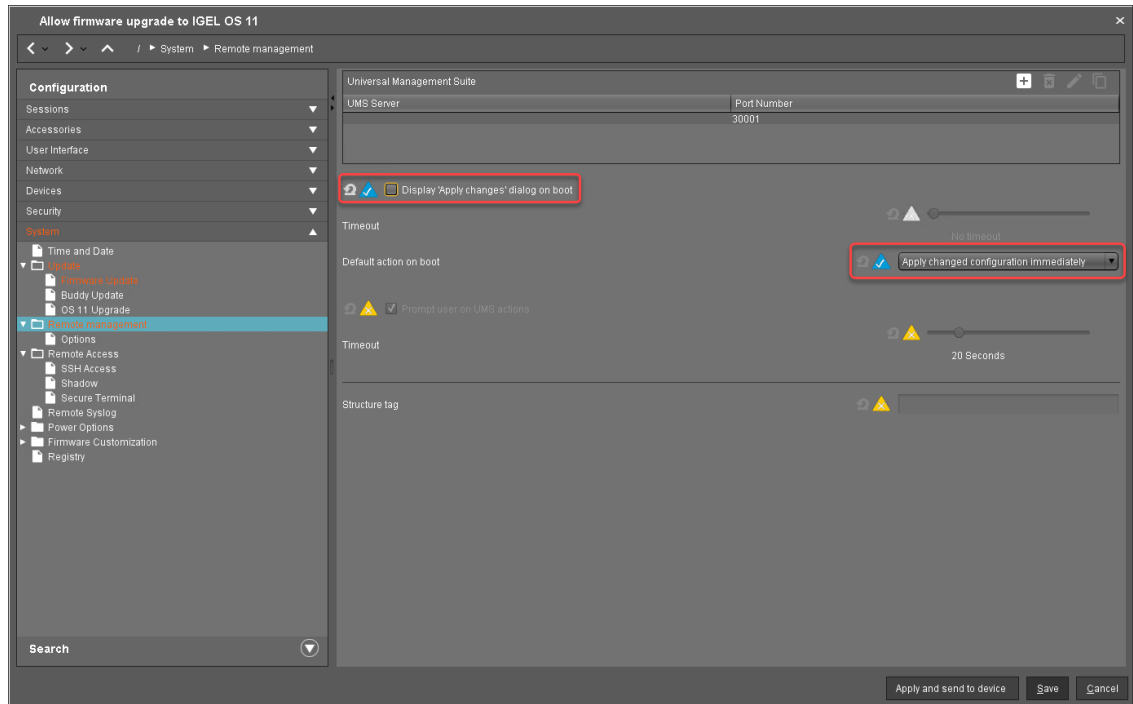
1. Erstellen Sie ein Profil, das auf der passenden IGEL OS 10 Version basiert (10.05.800 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Firmwareupgrade auf IGEL OS 11".
2. Gehen Sie im Konfigurationsdialog des Profils auf **System > Update > Firmware Update** und ändern Sie die Einstellungen wie folgt:
  - Wählen Sie "FTP" als **Protokoll**.
  - Geben Sie **Benutzername** und **Passwort** entsprechend dem Update Buddy Server ein.
  - Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**.
  - Stellen Sie sicher, dass **Automatische Updatesuche beim Herunterfahren** deaktiviert ist. Andernfalls wird das Gerät heruntergefahren, wenn das Upgrade auf OS 10.05.800 abgeschlossen ist.
  - Aktivieren Sie **Automatische Buddy-Server-Erkennung**.



3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test (Details zu den Einstellungen finden Sie unter [Setup anpassen](#) (see page 87)):
  - Aktivieren Sie **Upgrade auf OS 11**.
  - Stellen Sie **Upgrade auf OS 11, auch wenn PowerTerm aktiviert ist???** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Upgrade auf OS 11, auch wenn ein vorheriger Upgrade-Versuch fehlgeschlagen ist???** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Für das Upgrade auf OS 11 ist eine Enterprise Management Pack-Lizenz erforderlich???** nach Ihren Bedürfnissen ein.
  - Stellen Sie sicher, dass **Timeout beim Warten auf die OS 11-Lizenz zum Starten des automatischen Upgrades???** auf **10 Minuten** eingestellt ist.
4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:



- deaktivieren Sie **Dialogfeld "Änderungen übernehmen" beim Booten anzeigen???**.
- Setzen Sie **Standardaktion beim Booten???** auf **Geänderte Konfiguration sofort übernehmen???**.



5. Klicken Sie **Ok**.

### Lizenzen bereitstellen

Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:

- **Automatic License Deployment (ALD):** Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
- **Manual License Deployment:** Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.

Wenn das Lizenz-Deployment aufgesetzt ist, fahren Sie mit [Alles zusammensetzen \(see page 99\)](#) fort.

#### Alles zusammensetzen

1. Ordnen Sie das Profil allen Geräten zu, die aktualisiert werden sollen. Dies kann durch die Zuordnung des Profils zu dem Verzeichnis erfolgen, das diese Geräte enthält.


 Ordnen Sie das Profil nicht den Update Buddies zu.

2. Wählen Sie im Kontextmenü der Zuordnung **Jetzt**.
3. Für die automatische Lizenzbereitstellung kann eine Bedingung für das Verzeichnis festgelegt werden. Weitere Informationen finden Sie unter [Verteilungsbedingungen konfigurieren](#), Abschnitt "Lizenzen auf Geräte in einem bestimmten Verzeichnis verteilen".

Wenn alles bereit ist, fahren Sie mit [Upgrade durchführen](#) (see page 100) fort.

## Upgrade durchführen

1. Wählen Sie in der UMS alle Geräte aus, die aktualisiert werden sollen, und starten Sie sie neu.

 Alternativ können Sie einen geplanten Auftrag für den Neustart oder das Aufwachen erstellen und ihn den Geräten oder dem Verzeichnis mit diesen Geräten zuweisen. Weitere Informationen finden Sie unter [Aufgaben](#).

Beim Neustart oder Aufwachen wählen die Geräte den IGEL OS 10 Buddy. Sie ignorieren den IGEL OS 11 Buddy zum jetzigen Zeitpunkt, da ihnen diese Version noch nicht bekannt ist. Die Geräte werden auf die passende IGEL OS 10 Version (10.05.800 oder höher) aktualisiert. Mit dieser Version wird der Parameter **Upgrade auf OS 11** von den Geräten erkannt; außerdem fordern die Geräte IGEL OS 11-Lizenzen vom UMS (Workspace Edition und bei Bedarf Enterprise Management Pack) an.

Wenn noch keine IGEL OS 11-Lizenzen auf den Geräten bereitgestellt wurden, sind die Lizenzen innerhalb weniger Minuten bereitgestellt. Das Upgrade wird gestartet, wenn die Lizenzen bereitgestellt werden. Die maximale Zeitspanne, in der das Gerät auf eine Lizenz wartet, wird durch den Parameter **Timeout beim Warten auf die OS 11-Lizenz zum Starten des automatischen Upgrades** konfiguriert; Details finden Sie unter [Setup anpassen](#) (see page 87).

Die Parameter **Automatische Updatesuche beim Bootvorgang** und **Automatische Buddy-Server-Erkennung** veranlassen die Geräte, nach einer neuen Firmware zu suchen und auf die Antwort eines IGEL OS 11 Update Buddy zu warten. Wenn ein IGEL OS 11-Update-Buddy gefunden wird, starten die Geräte den Upgrade-Prozess.

2. Wenn alle Geräte erfolgreich aktualisiert wurden, entfernen Sie das Profil "Firmwareupgrade auf IGEL OS 11".

Das Upgrade ist vollendet.

## Massenbereitstellung über eine geplante Aufgabe

Dieses Szenario ist sinnvoll, wenn Sie bereits eine Arbeitsumgebung mit IGEL OS 10.05.800 (oder höher) haben und alle Geräte zu einem definierten Zeitpunkt auf IGEL OS 11 aktualisieren möchten.

Lesen Sie alle folgenden Kapitel sorgfältig durch und folgen Sie den Anweisungen.

1. [Anforderungen überprüfen](#) (see page 102)
2. [Profil erstellen](#) (see page 103)
3. [Lizenzen bereitstellen](#) (see page 107)
4. [Profil zuordnen](#) (see page 108)
5. [Geplante Aufgabe erstellen](#) (see page 110)

### Anforderungen überprüfen

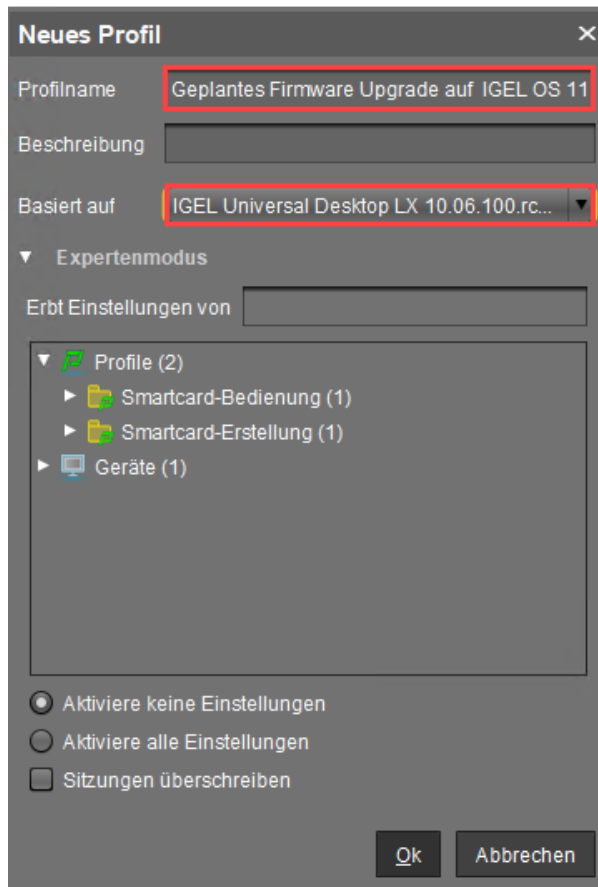
Die folgenden Anforderungen müssen erfüllt sein:

- Das Upgrade wurde mit charakteristischen Geräten getestet.
- UMS 6.01.130 oder höher ist verfügbar.
- Die Firmware 10.05.800 (oder höher) ist der UMS bekannt. Zu diesem Zweck muss ein Gerät mit dieser Firmware-Version in der UMS registriert werden. Dies ist bereits der Fall, wenn Sie das Upgrade mit der gleichen UMS getestet haben, mit der Sie das Massensupgrade durchführen werden. Wenn nicht, müssen Sie jetzt ein Gerät mit der entsprechenden Firmware-Version registrieren.
- Alle Geräte sind mit einem normalen LAN verbunden (nicht mit OpenVPN, OpenConnect, Genucard oder mobilem Breitband).
- Alle Geräte befinden sich in einer sicheren Umgebung, in der der Aktualisierungsprozess nicht unterbrochen werden kann, z. B. durch Ausschalten der Geräte.

Wenn alle Anforderungen erfüllt sind, fahren Sie mit [Profil erstellen \(see page 103\)](#) fort.

## Profil erstellen

1. Erstellen Sie ein Profil, das auf der passenden IGEL OS 10 Firmwareversion basiert (10.05.800 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Geplantes Firmware Upgrade auf IGEL OS 11".




2. Gehen Sie im Konfigurationsdialog des Profils unter **System > Update > Firmwareupdate** und ändern Sie die Einstellungen entsprechend Ihrer Umgebung:

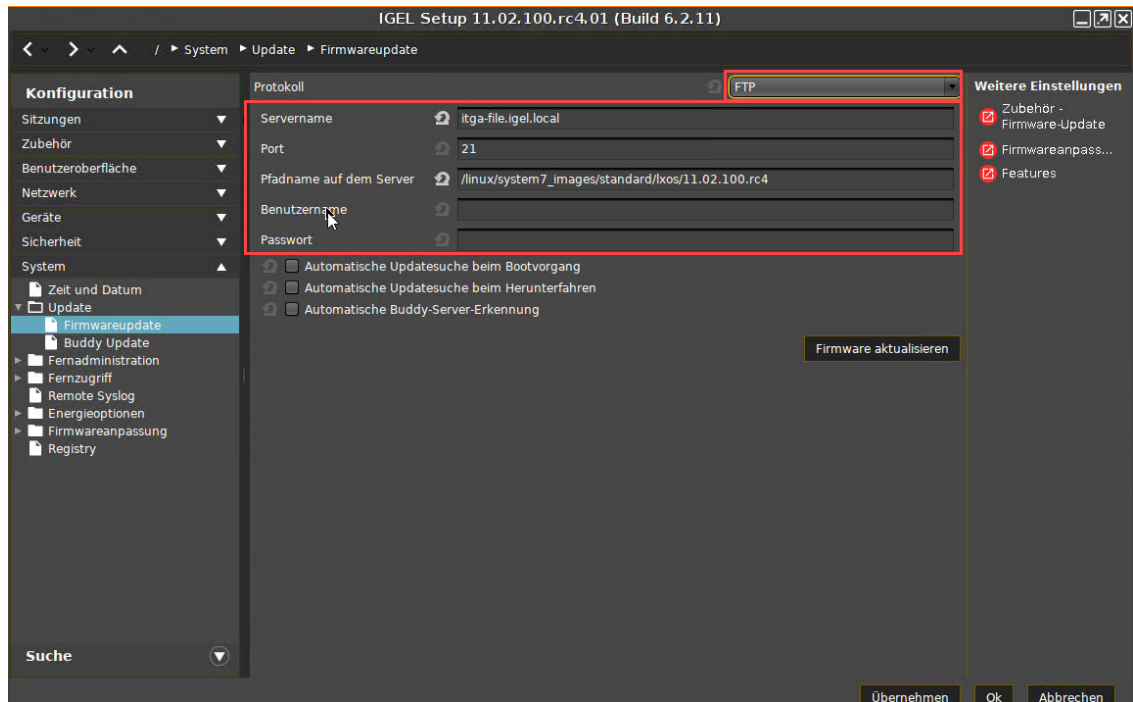
**i** Wenn Sie das [Universal Firmware Updates erstellen](#) (see page 52) für OS 11 benutzen, müssen Sie die in diesem Schritt beschriebenen Einstellungen nicht konfigurieren.

- Wählen Sie eine Aktualisierungsquelle für IGEL OS 11 aus, siehe Firmwareupdate-Einstellungen für IGEL OS.

**i** Wenn Sie **DATEI** als Protokoll (lokale Datei oder Netzlaufwerk) verwenden, zeigt das Gerät eine Fehlermeldung an und führt einen zusätzlichen Neustart durch. Abgesehen davon funktioniert das Upgrade normal.

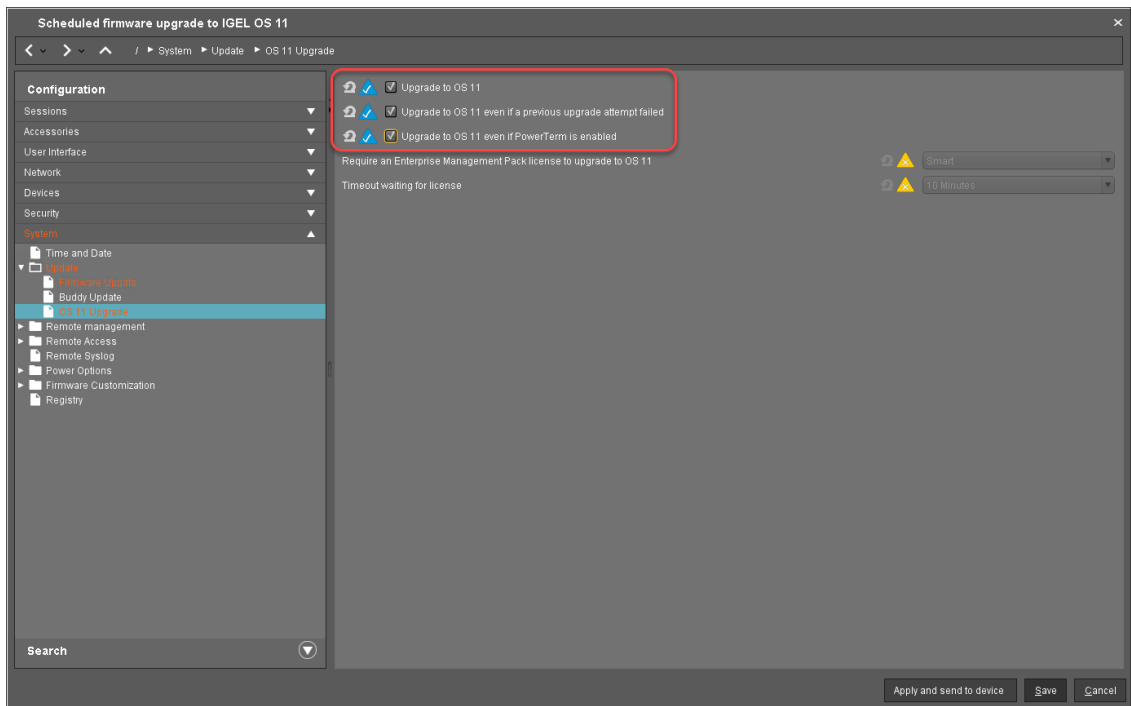
- Stellen Sie sicher, dass die **Automatische Updatesuche beim Bootvorgang** und die **Automatische Updatesuche beim Herunterfahren** deaktiviert sind.

 Im folgenden Screenshot wird FTP als Beispiel verwendet. Die anderen Protokolle können ebenfalls verwendet werden.

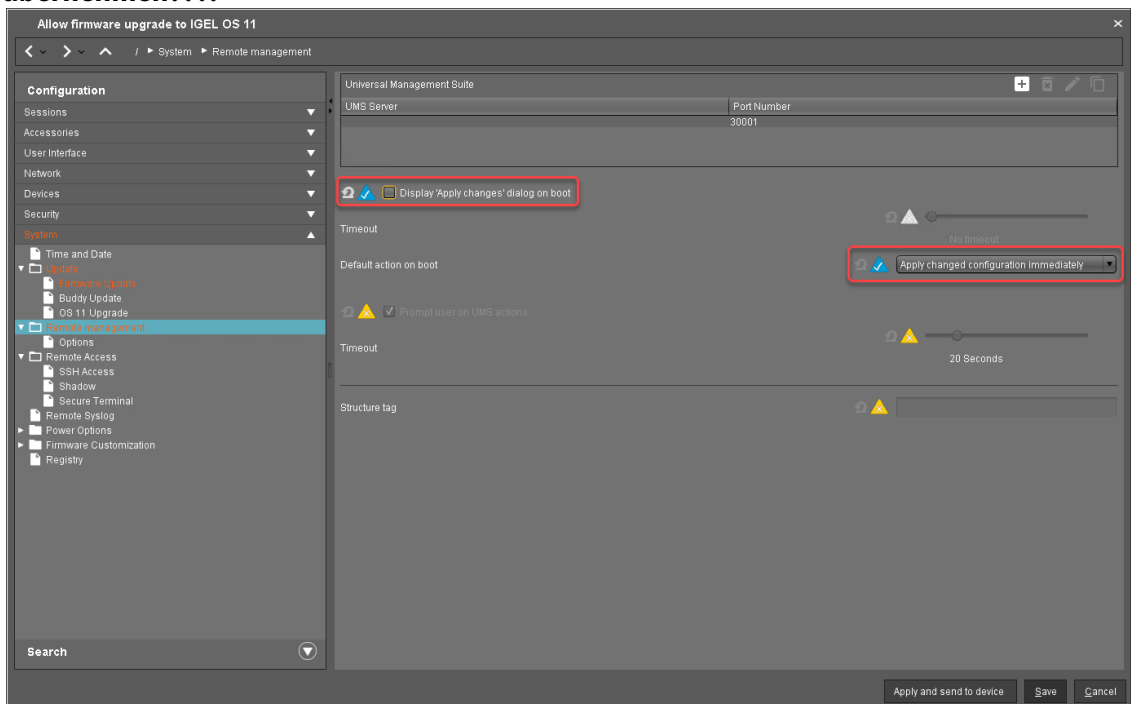


3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test:
  - Aktivieren Sie **Upgrade auf OS 11**.
  - Stellen Sie **Upgrade auf OS 11, auch wenn PowerTerm aktiviert ist???** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Upgrade auf OS 11, auch wenn ein vorheriger Upgrade-Versuch fehlgeschlagen ist???** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Für das Upgrade auf OS 11 ist eine Enterprise Management Pack-Lizenz erforderlich???** nach Ihren Bedürfnissen ein.
  - Stellen Sie sicher, dass **Timeout beim Warten auf die OS 11-Lizenz zum Starten des automatischen Upgrades???** auf **10 Minuten** eingestellt ist.





4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:
- deaktivieren Sie **Dialogfeld "Änderungen übernehmen" beim Booten anzeigen???**.
  - Setzen Sie **Standardaktion beim Booten???** auf **Geänderte Konfiguration sofort übernehmen???**.



5. Klicken Sie **Ok**.

Wenn das Profil erstellt ist, fahren Sie mit [Lizenzen bereitstellen](#) (see page 107) fort.

### Lizenzen bereitstellen

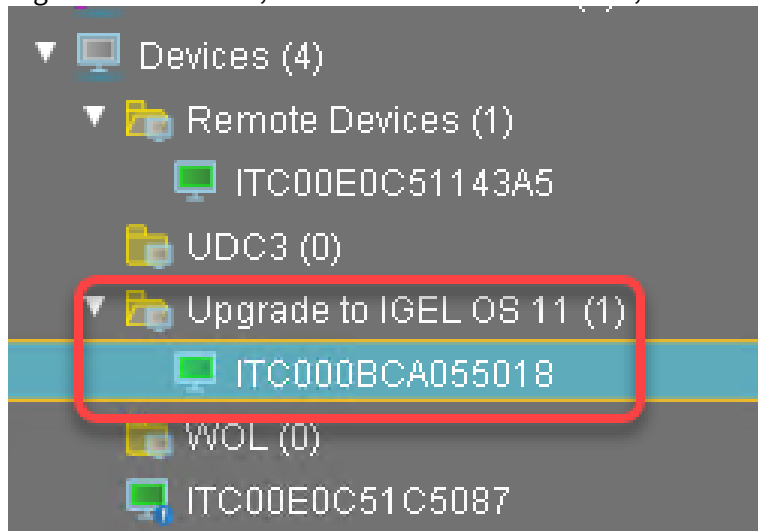
Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:

- **Automatic License Deployment (ALD):** Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
- **Manual License Deployment:** Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.

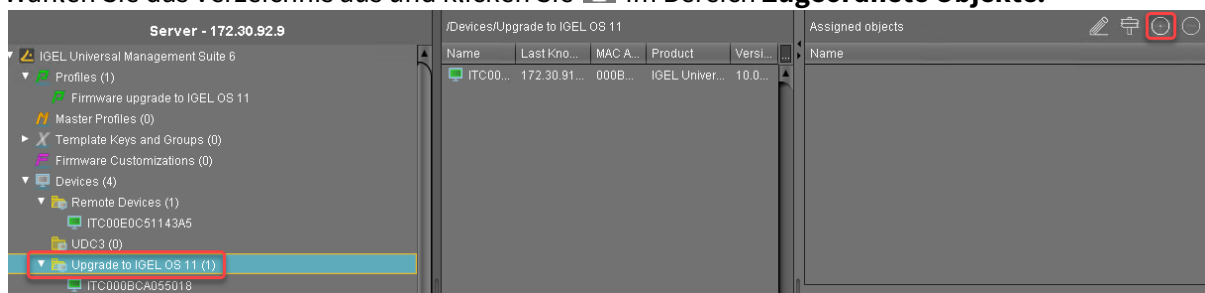
Wenn das Lizenz-Deployment aufgesetzt ist, fahren Sie mit [Profil zuordnen](#) (see page 108) fort.

## Profil zuordnen

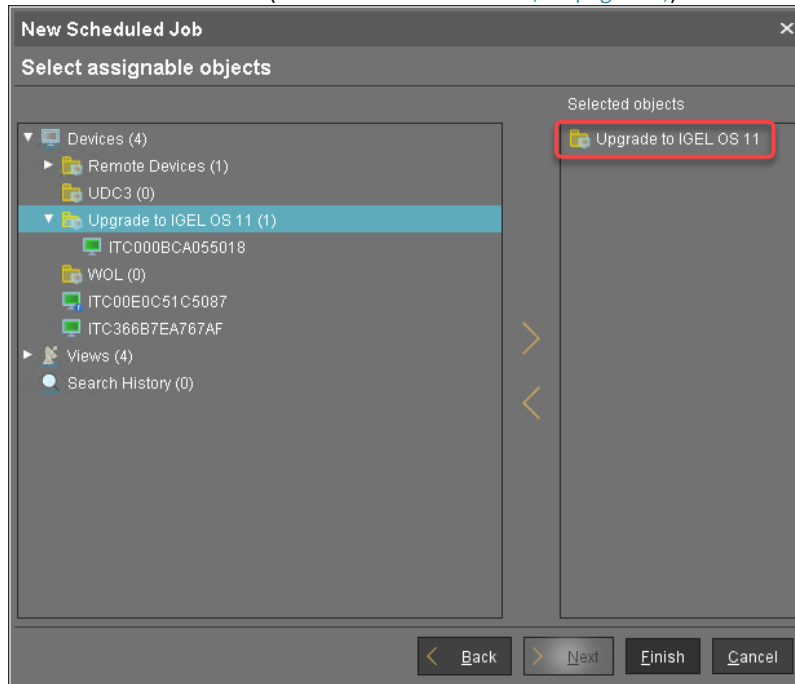
1. Legen Sie alle Geräte, die aktualisiert werden sollen, in ein Verzeichnis.



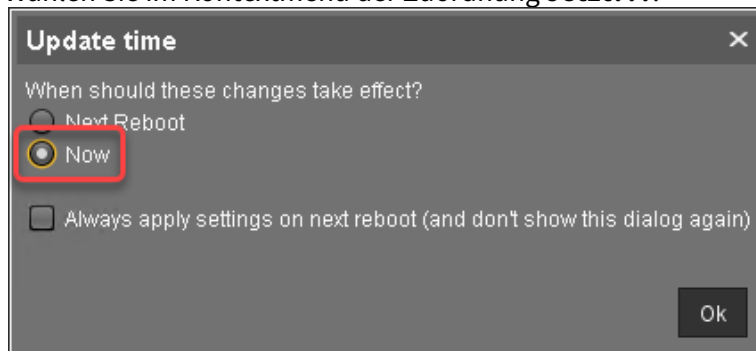
2. Wählen Sie das Verzeichnis aus und klicken Sie  im Bereich **Zugeordnete Objekte**.



3. Ordnen Sie das Profil (siehe [Profil erstellen](#) (see page 103)) dem Verzeichnis zu und klicken Sie **Ok**.



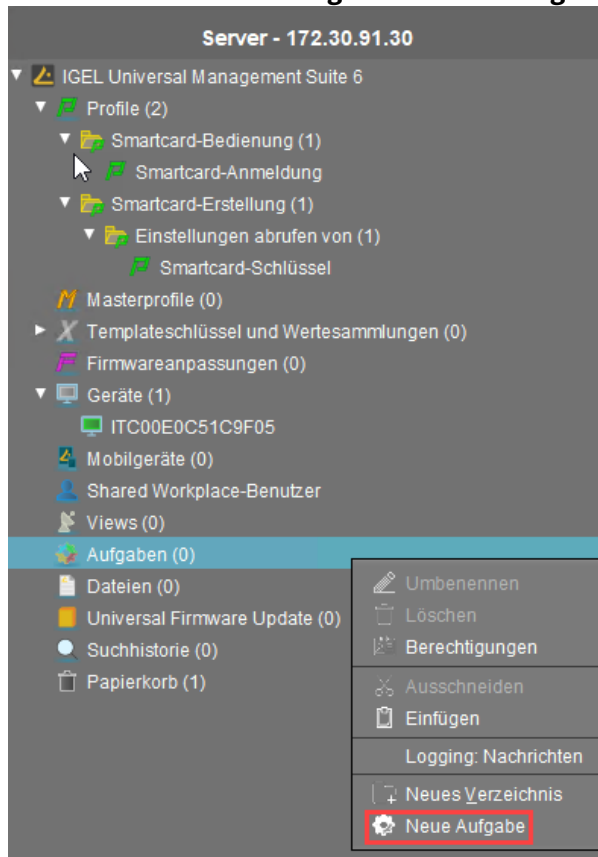
4. Wählen Sie im Kontextmenü der Zuordnung **Jetzt???**.



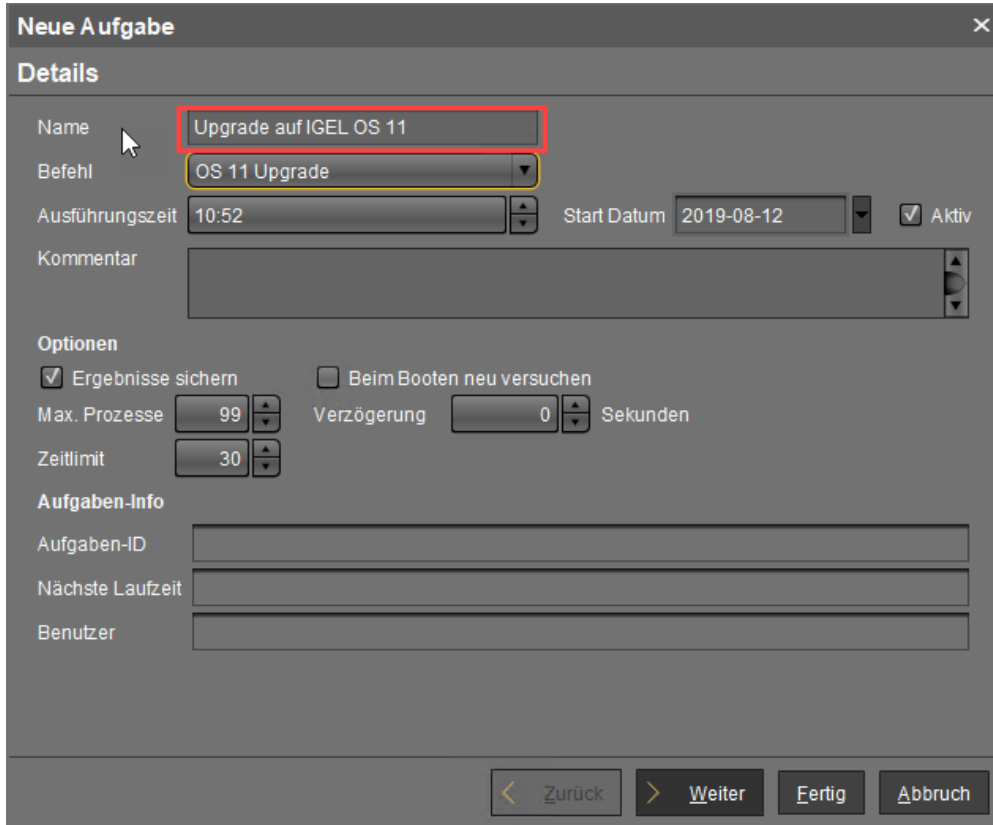
Wenn das Profil zugeordnet ist, fahren Sie mit [Geplante Aufgabe erstellen](#) (see page 110) fort.

Geplante Aufgabe erstellen

1. Wählen Sie in der UMS **Aufgaben > Neue Aufgabe**.



2. Geben Sie unter **Name** einen geeigneten Namen für die Aufgaben ein, z. B. "Upgrade auf IGEL OS 11".



**Neue Aufgabe** ✕

**Details**

Name

Befehl

Ausführungszeit  Start Datum   Aktiv

Kommentar

**Optionen**

Ergebnisse sichern  Beim Booten neu versuchen

Max. Prozesse  Verzögerung  Sekunden

Zeitlimit

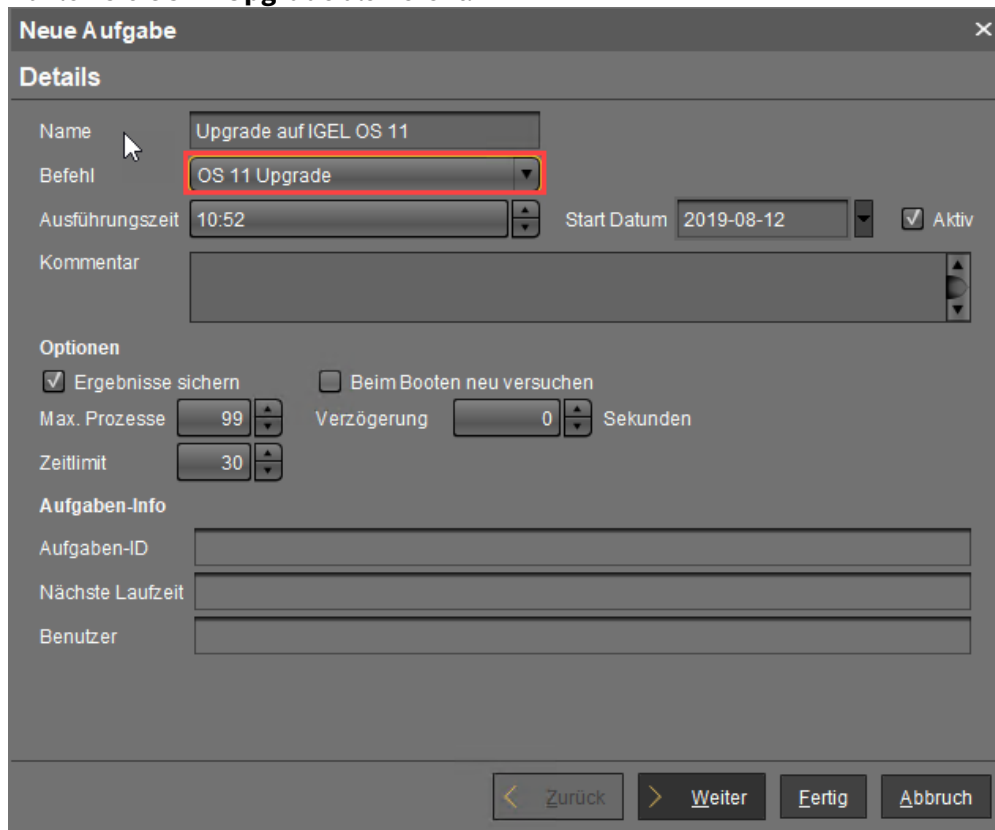
**Aufgaben-Info**

Aufgaben-ID

Nächste Laufzeit

Benutzer

3. Wählen Sie **OS 11 Upgrade** als **Befehl**.



**Neue Aufgabe** ×

**Details**

Name

Befehl

Ausführungszeit  Start Datum   Aktiv

Kommentar

**Optionen**

Ergebnisse sichern  Beim Booten neu versuchen

Max. Prozesse  Verzögerung  Sekunden

Zeitlimit

**Aufgaben-Info**

Aufgaben-ID

Nächste Laufzeit

Benutzer

4. Geben Sie unter **Ausführungszeit** und **Start Datum** die Uhrzeit ein, zu der das Upgrade ausgeführt werden soll und klicken Sie **Weiter**.



**Neue Aufgabe** ✕

**Details**

Name

Befehl

Ausführungszeit  Start Datum   Aktiv

Kommentar

**Optionen**

Ergebnisse sichern  Beim Booten neu versuchen

Max. Prozesse  Verzögerung  Sekunden

Zeitlimit

**Aufgaben-Info**

Aufgaben-ID

Nächste Laufzeit

Benutzer

5. Überprüfen Sie die Ausführungszeit und klicken Sie **Weiter**.

**Neue Aufgabe** ×

**Zeitplan**

Ausführungszeit  Start Datum

Ablaufdatum  Uhrzeit

**Aufgabe wiederholen**

Nie

Jeden  Tag  Stunde

Wochentage  Mo  Di  Mi  Do  Fr  Sa  So

Feiertage ausschließen  ...

Datum	Kommentar
-------	-----------

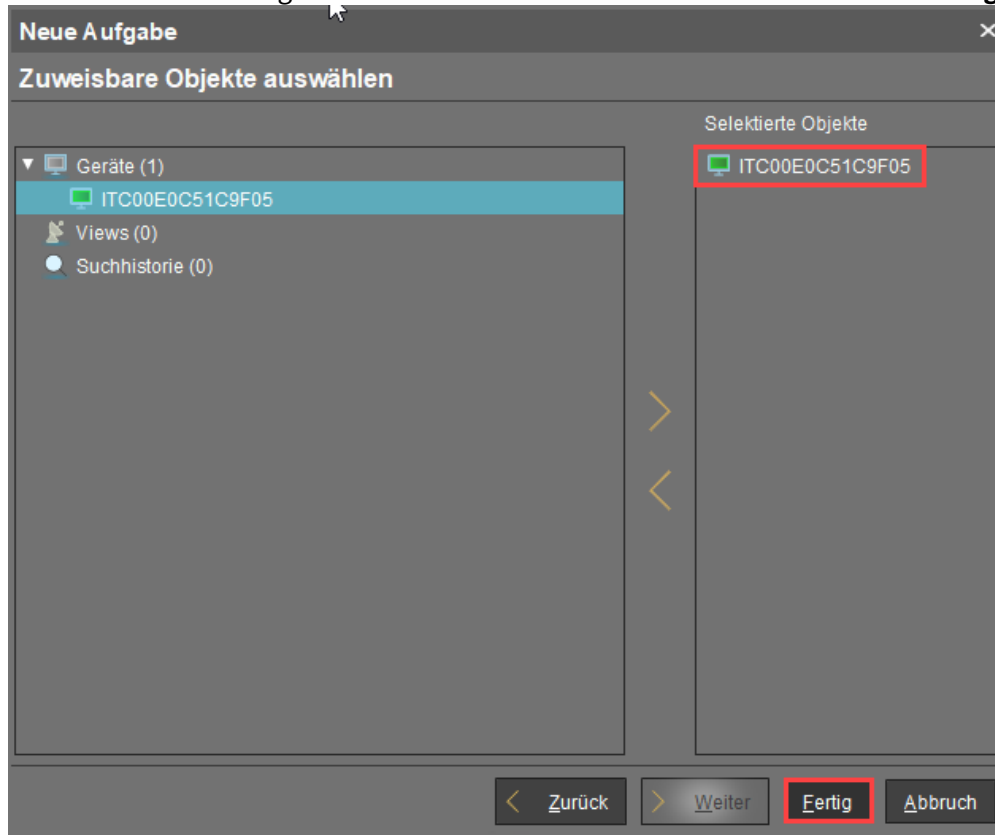
**Ausführung abbrechen**

Nie

Uhrzeit

Max. Dauer

6. Weisen Sie dem Auftrag das Verzeichnis mit den Geräten zu und klicken Sie **Fertig**.



Das Upgrade ist vollständig.

## Fehlerbehebung

In diesem Abschnitt werden mögliche Fehlerfälle und Lösungen beschrieben.

- [Brauchbares System wiederherstellen](#) (see page 117)
- [Fehlermeldung erhalten](#) (see page 118)
- [Neuen Upgrade Versuch starten](#) (see page 119)
- [Weiteren Upgrade Versuch nach 5 Wiederholungen starten](#) (see page 120)

## Brauchbares System wiederherstellen

Hier finden Sie typische Upgrade-Fehler und die entsprechenden Methoden, um ein brauchbares System wiederherzustellen.

Das Gerät wurde auf Igel OS 11 aktualisiert, bootet aber nicht mehr.

Um ein funktionierendes IGEL OS 11 System zu erhalten:

- ▶ Verwenden Sie den IGEL OS Creator, um das IGEL OS 11-System wiederherzustellen. Weitere Informationen finden Sie im IGEL OS Creator Handbuch.

10.05.700 Das Rettungssystem kann fehlende Partitionen nicht aktualisieren.

Wenn während des Upgrade-Vorgangs ein schwerer Fehler aufgetreten ist, bootet die Vorrichtung in ein minimal 10.05.700 oder 10.05.800 Rettungssystem. Wenn das Gerät unbeaufsichtigt ist, versucht es, die fehlenden Partitionen herunterzuladen und zu aktualisieren und startet bei einem Fehler neu.


Um ein komplettes 10.05.800 System wiederzuerlangen, haben Sie zwei Möglichkeiten:

- ▶ Starten Sie im Rettungssystem das Setup, gehen Sie zu **System > Update > Firmwareupdate** und stellen Sie eine gültige Updatequelle für IGEL OS 10.05.800 ein.

Oder:

- ▶ Konfigurieren Sie ein UMS-Profil, das eine gültige Aktualisierungsquelle für IGEL OS 10.05.800 enthält, unter **System > Update > Firmwareupdate** und weisen Sie es dem Gerät zu.

Fehlermeldung erhalten

- ▶ Öffnen Sie das OS 11 Upgrade Tool (Standardpfad: Klicken Sie  und dann auf **Upgrade auf OS 11**).

Das OS 11 Upgrade Tool zeigt eine Fehlermeldung. Der wichtigsten Nachricht ist ein **Wiederholungsversuch???** vorangestellt, siehe Beispiel unten:



- ▶ Weitere Informationen finden Sie im Hauptmigrationsprotokoll unter `/wfs/migration.log`.

**i** Sie können den Systemprotokoll-Viewer verwenden, um das Migrationsprotokoll zu überprüfen (Siehe Kapitel Systemprotokolle im IGEL OS Handbuch) oder speichern Sie die Protokolldateien, um sie an das IGEL Support Team zu senden (Finden Sie im Supportkapitel Gerätedateien für den Support speichern).

### Neuen Upgrade Versuch starten

Wenn Sie möchten, dass das Gerät mehrere Aktualisierungsversuche startet (und das Gerät nicht bereits dafür konfiguriert ist):

1. Gehen Sie im UMS Profil oder im Setup unter **System > Update > OS 11 Upgrade** und aktivieren Sie **Upgrade auf OS 11, auch wenn ein vorheriger Upgrade Versuch fehlgeschlagen ist???**.
2. Starten Sie das Gerät neu.

Weiteren Upgrade Versuch nach 5 Wiederholungen starten

Wenn **Upgrade auf OS 11 auch, wenn ein vorheriger Upgrade Versuch fehlgeschlagen ist???** und das Upgrade jedes Mal fehlgeschlagen ist, stoppt das System den Versuch nach 5 Versuchen.

Um den Wiederholungszähler zurückzusetzen:

1. Gehen Sie im Setup oder im UMS-Profil unter **System > Update > OS 11 Upgrade** und deaktivieren Sie das **Upgrade auf OS 11, auch wenn ein vorheriger Upgrade Versuch fehlgeschlagen ist???**.
2. Wenn die Einstellung für die Geräte wirksam ist, gehen Sie erneut unter **System > Update > OS 11 Upgrade** und aktivieren Sie **Upgrade auf OS 11 ist auch dann möglich, wenn ein vorheriger Upgrade Versuch fehlgeschlagen ist???**.

Der Wiederholungszähler wird zurückgesetzt, und die Geräte werden versuchen, bei Bedarf 5 weitere Male ein Upgrade durchzuführen.



## IGEL Geräte von IGEL OS 10 nach IGEL OS 11 upgraden

Dieses Dokument beschreibt, wie Sie eine beliebige Anzahl von IGEL Geräten (UD) von IGEL OS 10 auf IGEL OS 11 aktualisieren können.

Für das Upgrade auf IGEL OS 11 ist IGEL OS 10.05.700 oder höher erforderlich. Wenn Sie eine ältere Version von IGEL OS 10 haben, müssen Sie zuerst auf Version 10.05.700 oder eine höhere Version aktualisieren.

Die folgenden Methoden der massenhaften Bereitstellung werden hier beschrieben:

- [Zero-Touch-Bereitstellung mit Universal Firmware Update \(see page 122\)](#): Massenumgrade von jeder Version von IGEL OS 10 auf IGEL OS 11 in einem Schritt mit Universal Firmware Update. Diese Methode kann sofort oder als geplanter Auftrag (Aufwachen oder Neustart) gestartet werden.
- [Zero-Touch-Bereitstellung mit Buddy Update \(see page 154\)](#): Massenumgrade von jeder Version von IGEL OS 10 auf IGEL OS 11 in einem Schritt mit zwei Geräten als Update-Buddies. Diese Methode kann sofort oder als geplanter Auftrag (Aufwachen oder Neustart) gestartet werden.
- [Massenbereitstellung über einen geplante Aufgabe \(see page 175\)](#): Aktualisieren Sie Geräte, auf denen bereits IGEL OS 10.05.700 (oder höher) läuft, mit einem bestimmten geplanten Auftrag.

## Zero-Touch-Bereitstellung mit Universal Firmware Update

Diese Methode ist der bequemste Weg, um von IGEL OS 10 auf IGEL OS 11 zu aktualisieren. Das Verfahren verwendet die Funktion Universal Firmware Update der UMS (Universal Management Suite) und ein Profil.

Lesen Sie die folgenden Kapitel sorgfältig durch und folgen Sie den Anweisungen.

1. [IGEL Geräte, die auf IGEL OS 11 hochgerüstet werden können \(see page 123\)](#)
2. [Wichtig! Vor dem Upgrade berücksichtigen \(see page 126\)](#)
3. [Upgrade vorbereiten \(see page 128\)](#)
4. [Upgrade testen \(see page 133\)](#)
5. [Anforderungen überprüfen \(see page 137\)](#)
6. [Universal Firmware Updates erstellen \(see page 138\)](#)
7. [Profil erstellen \(see page 143\)](#)
8. [Lizenzen bereitstellen \(see page 148\)](#)
9. [Alles zusammensetzen \(see page 173\)](#)
10. [Upgrade durchführen \(see page 174\)](#)

IGEL Geräte, die auf IGEL OS 11 hochgerüstet werden können

Grundvoraussetzungen für IGEL OS 11

- CPU mit 64 Bit-Unterstützung
- CPU-Taktfrequenz:  $\geq 1$  GHz
- Arbeitsspeicher (RAM):  $\geq 2$  GB

- i** Eine RAM-Größe von mehr als 2 GB wird empfohlen, wenn Sie das Folgende verwenden:
- Optimierungen für Unified Communications (verwendet eine clientseitige Media Engine)
  - Hochauflösende Grafikausgabe  
Details zu den unterstützten grafikbezogenen Merkmalen von IGEL Geräten finden Sie unter Grafik auf IGEL Geräten oder, für ältere Geräte, Grafik auf Legacy IGEL Geräten.
  - Mehr als zwei Monitore

- Festspeicher: mindestens 2 GB;  $\geq 4$  GB empfohlen

- i** **Speicheranforderungen für IGEL OS 11.04 oder höher**
- IGEL OS 11.04.100 oder höher erfordert mindestens 2,4 GB Speicherplatz, wenn der volle Funktionsumfang genutzt wird. Daher muss der Funktionsumfang entsprechend angepasst werden; weitere Informationen finden Sie unter Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher.

IGEL Geräte, die von IGEL OS 11 unterstützt werden

IGEL UD (Universal Desktop)

Produktlinie	Gerätetyp	Hardware-ID	64-Bit	Arbeitsspeicher (RAM)	Festspeicher	HW-Videobeschleunigung
UD2**** (see page 124)	D220	40	Ja	2 GB	4 GB	Ja
UD2* (see page 124)	M250C	50	Ja	2 GB	4 GB	Ja
UD2	M250C	51 / 52**** (see page 124)	Ja	2 oder 4 GB	8 GB	Ja
UD3* (see page 124)	M340C	50	Ja	2 GB	4 GB	Ja

Produktlinie	Gerätetyp	Hardware-ID	64-Bit	Arbeitsspeicher (RAM)	Festspeicher	HW-Videobeschleunigung
UD3* (see page 124)	M340C	51	Ja	2 GB	4 GB	Ja
UD3	M350C	60	Ja	4 GB	8 GB	Ja
UD5* (see page 124)	H830C	50	Ja	2 GB	4 GB	Ja
UD6* (see page 124)	H830C	51	Ja	2 GB	4 GB	Ja
UD7	H850C	10	Ja	4 GB	4 GB	Ja
UD7** (see page 124)	H850C	11	Ja	4 GB	4 GB	Ja
UD7	H860C	20	Ja	8 GB	8 GB	Ja
UD9* (see page 124)	TC215B	40 / 41 (Touch)	Ja	2 GB	4 GB	Ja

\* IGEL UD3-LX 50 und UD5-LX 50 werden offiziell bis zu IGEL OS 11.05 unterstützt, inkl. Private Builds.  
 IGEL UD9-LX 40 / 41 (Touch) Geräte werden offiziell bis zu IGEL OS 11.07.910 unterstützt.  
 IGEL UD2-LX 50-Geräte werden bis zu IGEL OS 11.09.160 unterstützt.  
 IGEL UD3-LX 51-Geräte werden bis zu IGEL OS 11.09.160 unterstützt.  
 IGEL UD6-LX 51-Geräte werden bis zu IGEL OS 11.09.160 unterstützt.

\*\* Ab Dezember 2019 ist der IGEL UD7, Modell H850C, mit dem AMD Secure Processor ausgerüstet; weitere Informationen siehe UD7 Model H850C.

\*\*\* IGEL UD2-LX 52 wird mit IGEL OS 11.06.140 und höher unterstützt.

UD2-LX 40 (Modell D220) wird bis IGEL OS 11.08.200 unterstützt. Einen Überblick über die Daten von end-of-sales (EOS) und end-of-maintenance (EOM) finden Sie unter [IGEL OS 11 or Higher \(see page 123\)](#).

## IGEL Zero

### Hinweis zu IZ-Geräten

Bei den unten aufgezählten IZ-Geräten ist ein Upgrade auf IGEL OS 11 möglich. Bitte kontaktieren Sie Ihren IGEL Vertriebsrepräsentanten, damit Sie ein Upgrade Ihrer IZ-Geräte vornehmen können. Siehe auch <https://www.igel.com/os11migration/>.

Produktlinie	Gerätetyp	Hardware-ID	64-Bit	Arbeitsspeicher (RAM)	Festspeicher	UEFI-Secure-Boot	HW-Videobeschleunigung
IZ2	D220	40	Ja	2 GB	4 GB	Ja	Ja
IZ3	M340C	50	Ja	2 GB	4 GB	Ja	Ja
IZ3	M340C	51	Ja	2 GB	4 GB	Ja	Ja

Wenn Sie festgestellt haben, dass Ihre Geräte auf IGEL OS 11 hochgerüstet werden können, beachten Sie [Wichtig! Vor dem Upgrade berücksichtigen](#) (see page 126).

Wichtig! Vor dem Upgrade berücksichtigen

Um sicherzustellen, dass Ihr Upgrade erfolgreich sein kann, überprüfen Sie die folgenden Warnungen und Hinweise; ein Warnsymbol zeigt an, dass irreversible Schäden an Ihren Geräten auftreten können.

#### **Kein Downgrade**

Nach der Migration auf IGEL OS 11 können Sie Ihr IGEL OS 10-System nicht mehr wiederherstellen. Der Gerätespeicher wird mit einem neuen Partitionierungsschema vollständig überschrieben.

#### **Funktionen (z. B. Clients)**

IGEL OS 11 verfügt nicht über den kompletten Funktionsumfang von IGEL OS 10. Stellen Sie sicher, dass die aktuelle Version von IGEL OS 11 Ihren Anforderungen entspricht. Einzelheiten finden Sie in den entsprechenden Release-Informationen.

#### **Eigene Partitionen**

Der Inhalt von benutzerdefinierten Partitionen wird durch das Upgrade gelöscht. Stellen Sie sicher, dass Sie den Inhalt sichern und nach Abschluss des Upgrades wiederherstellen. Neben der Dysfunktionalität nach dem Upgrade können Anwendungen und Kerneltreiber in einer benutzerdefinierten Partition das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Wir empfehlen, benutzerdefinierte Partitionen beim Upgrade zu deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

#### **Eigene Befehle**

Die Persistenz von benutzerdefinierten Befehlen kann nicht garantiert werden. Neben der Dysfunktionalität nach dem Upgrade können benutzerdefinierte Befehle das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Im Allgemeinen müssen benutzerdefinierte Befehle für IGEL OS 11 angepasst werden. Wir empfehlen, dass Sie benutzerdefinierte Befehle beim Aktualisieren deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

#### **Netzwerk**

Alle Geräte müssen an ein WLAN oder LAN angeschlossen sein. LAN ist die empfohlene Option. Das Gerät wird nicht aktualisiert, wenn es mit OpenVPN, OpenConnect, Genucard, NCP VPN oder mobilem Breitband verbunden ist.

#### **Hardwareunterstützung**

Stellen Sie sicher, dass Ihre Geräte IGEL OS 11 unterstützen; siehe IGEL Geräte, die von IGEL OS 11 unterstützt werden. Dieses Dokument beschreibt die Aktualisierungsmethoden für IGEL UD und IGEL IZ Geräte. Die Aktualisierungsmethoden für IGEL UDC3 und UD Pocket sind unter UDC3-Geräte von IGEL OS 10 auf IGEL OS 11 upgraden beschrieben.

**i Lizenz**

- Für jedes Gerät muss eine gültige Lizenz einer IGEL Workspace Edition (WE) verfügbar sein. Allgemeine Informationen finden Sie unter IGEL Softwarelizenzen - Übersicht. Informationen zur Bereitstellung von Lizenzen finden Sie unter Automatic License Deployment (ALD) einrichten oder Manuelle Lizenz-Bereitstellung für IGEL OS.
- IZ Geräte dürfen nicht auf IGEL OS 11 aktualisiert werden. Wenden Sie sich an Ihren IGEL Vertriebsmitarbeiter, um eine UD Upgrade Lizenz zu erhalten, die es Ihnen ermöglicht, Ihre IZ Geräte zu aktualisieren.

**i UMS Version**

Für das Upgrade von IGEL OS 10 auf IGEL OS 11 ist die UMS Version 6.01.130 oder höher erforderlich.

Wenn Sie alles Relevante berücksichtigt haben, fahren Sie fort mit [Upgrade vorbereiten](#) (see page 128).

### Upgrade vorbereiten

Dieser Abschnitt beschreibt die erforderlichen Vorbereitungen und Tests, bevor Produktivgeräte aktualisiert werden können. Die Prüfung sollte mit mindestens einem Gerät durchgeführt werden, das für Ihre Umgebung charakteristisch ist. Dieses Gerät sollte jede benutzerdefinierte Partition und jeden benutzerdefinierten Befehl enthalten, der möglicherweise in einem Ihrer Geräte vorhanden ist.

Zunächst sollten Sie gründlich prüfen, ob IGEL OS 11 über alle Funktionen verfügt, die für Ihre Zwecke erforderlich sind.

- ▶ Fahren Sie mit [UMS vorbereiten \(see page 129\)](#) fort.



### UMS vorbereiten

Um Ihre Geräte auf IGEL OS 11 aufzurüsten, benötigen Sie die entsprechende Version der UMS. Außerdem müssen die Geräte bei der UMS registriert sein, um ihre Lizenzen zu erhalten.

1. Wenn Sie dies noch nicht getan haben, aktualisieren Sie Ihre UMS auf Version 6.01.130 oder höher. Anweisungen finden Sie unter UMS Installation aktualisieren.
2. Stellen Sie sicher, dass Ihre Geräte an der UMS registriert sind. Weitere Informationen finden Sie im Kapitel Geräte am UMS Server registrieren des UMS Handbuchs.

Wenn die UMS vorbereitet ist, fahren Sie mit [Setup anpassen \(see page 130\)](#) fort.

## Setup anpassen

Abhängig von den Funktionen, die jetzt oder in Zukunft verwendet werden, muss im Setup des Geräts ein bestimmter Parametersatz eingestellt werden.

1. Gehen Sie im Setup unter **System > Update > OS 11 Upgrade**.
2. Nehmen Sie die entsprechenden Einstellungen vor:
  - Aktivieren Sie **Upgrade auf OS 11**.
  - Wenn Sie möchten, dass das Gerät das Upgrade sofort nach einem fehlgeschlagenen Versuch erneut durchführt, aktivieren Sie die Option **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist**. Das Gerät versucht das Upgrade 5 mal erneut. Wenn der 5. Versuch fehlgeschlagen ist, wird eine Meldung im Fenster des Upgrade-Tools angezeigt.
  - Wenn Ihr Gerät über eine PowerTerm-Lizenz verfügt und Sie auf IGEL OS 11 aktualisieren möchten, obwohl es PowerTerm nicht unterstützt, müssen Sie folgendes aktivieren **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist**.
  - Wählen Sie unter **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** die entsprechende Option:
    - Wenn Sie IGEL Cloud Gateway (ICG) oder Shared Workplace (SWP) oder eine benutzerdefinierte Partition verwenden und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn diese Funktionen weiterhin verwendet werden können, wählen Sie **Smart**. Wenn diese Option ausgewählt und eine dieser Funktionen aktiviert ist, wird das Upgrade nur durchgeführt, wenn das Gerät eine Lizenz von einem Enterprise Management Pack beziehen konnte.
    - Wenn Sie das Gerät zwingen möchten, eine Lizenz von einem Enterprise Management Pack abzurufen, und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn die Lizenz abgerufen werden kann, wählen Sie **Immer**.
    - Wenn Sie möchten, dass das Gerät auf IGEL OS 11 aktualisiert wird, ohne ein Enterprise Management Pack zu erhalten, ohne die möglicherweise aktivierten Funktionen zu berücksichtigen, wählen Sie **Niemals**.
  - Geben Sie unter **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** den Zeitraum an, in dem das Gerät in einem Massenbereitstellungsszenario auf eine Lizenz warten soll (siehe [Zero-Touch-Bereitstellung mit Universal Firmware Update \(see page 122\)](#), [Zero-Touch-Bereitstellung mit Buddy Update \(see page 154\)](#) und [Massenbereitstellung über einen geplante Aufgabe \(see page 175\)](#)). Diese Einstellung verhindert, dass das Gerät das Upgrade zu einem ungünstigen Zeitpunkt startet, da die bereitgestellte Lizenz gerade installiert wird. Auf diese Weise verhindert die Einstellung ungewollte Unterbrechungen bei der Arbeit. Für ein Masseneinsatzszenario wird der Standardwert **10 Minuten** empfohlen.
3. Klicken Sie **Übernehmen**.
4. Fahren Sie mit [Lizenz bereitstellen \(see page 131\)](#) fort.

## Lizenz bereitstellen

Für ein Upgrade von IGEL OS 10 auf IGEL OS 11 benötigen Sie eine entsprechende Lizenz. Je nach Ihren Anforderungen werden eine oder mehrere dieser Lizenzen für jedes Gerät benötigt:

- Eine Workspace Edition-Lizenz für die Grundfunktionen. Weitere Informationen finden Sie unter Workspace Edition.
- Wenn eines der folgenden Features verwendet wird, wird eine Enterprise Management Pack-Lizenz benötigt (siehe Enterprise Management Pack):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - wenn die Zielversion IGEL OS 11.03.100 oder niedriger ist; mit IGEL OS 11.03.500 oder höher ist das Feature Custom Partition in der Workspace Edition enthalten.

Gehen Sie wie folgt vor:

- ▶ Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:
  - Manual License Deployment: Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.
  - Automatic License Deployment (ALD): Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
  - Laden Sie drei Demo-Lizenzen herunter von <https://www.igel.com/download/>.

Wenn das Gerät eine Lizenz hat, fahren sie mit [Update Source konfigurieren](#) (see page 132) fort.


#### Update Source konfigurieren

1. Gehen Sie im Setup unter **System > Update > Firmware Update** und konfigurieren Sie die Update Source für IGEL OS 11. Für mehr Information, siehe im Kapitel Firmware Update des IGEL OS Handbuchs.
2. Klicken Sie **Ok**.



Wenn die korrekte Updatequelle konfiguriert ist, fahren Sie mit [Upgrade testen \(see page 133\)](#) fort.

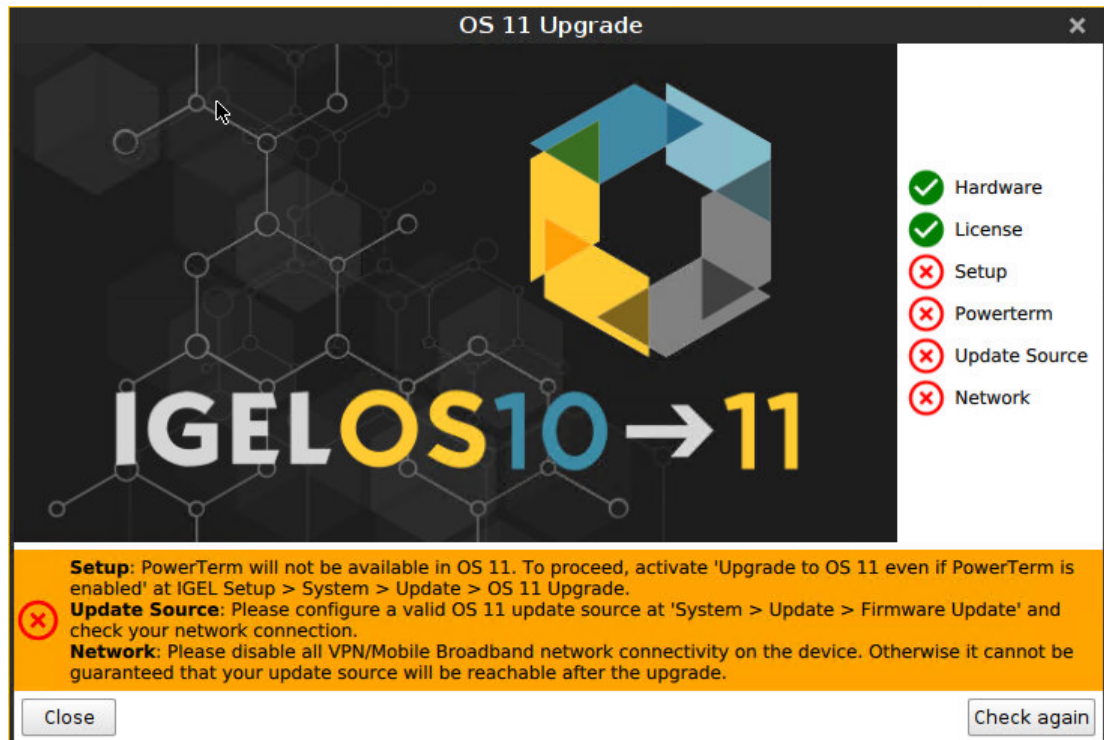
## Upgrade testen

1. Klicken Sie auf  und dann auf **Upgrade auf OS 11**. Das OS 11 Upgrade-Tool startet und zeigt an, ob alle Anforderungen erfüllt sind.

 Sie können das Starten der Startmethoden für das OS 11 Upgrade-Tool im Setup unter **Zubehör > OS11 Upgrade** ändern.

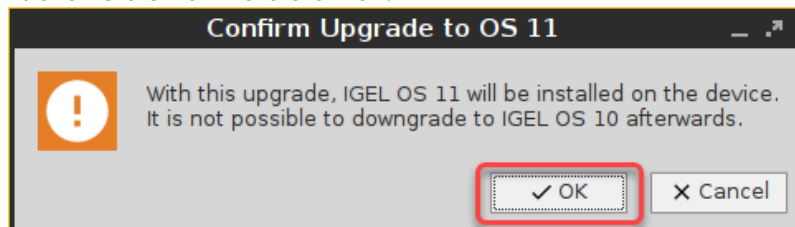


2. Überprüfen Sie die Ausgabe des OS 11 Upgrade-Tools und fahren Sie entsprechend fort:
  - Wenn jede Anforderung ein  Symbol hat, klicken Sie **OS Upgrade**, um den Upgrade-Vorgang zu starten.
  - Wenn eine oder mehrere Anforderungen ein  Symbol haben, überprüfen Sie die Meldungen und beheben Sie die Probleme. Klicken Sie anschließend auf **nochmal überprüfen**. Wenn alle Voraussetzungen erfüllt sind, ändert sich die Schaltfläche in **OS Upgrade**, und Sie können das Upgrade starten.

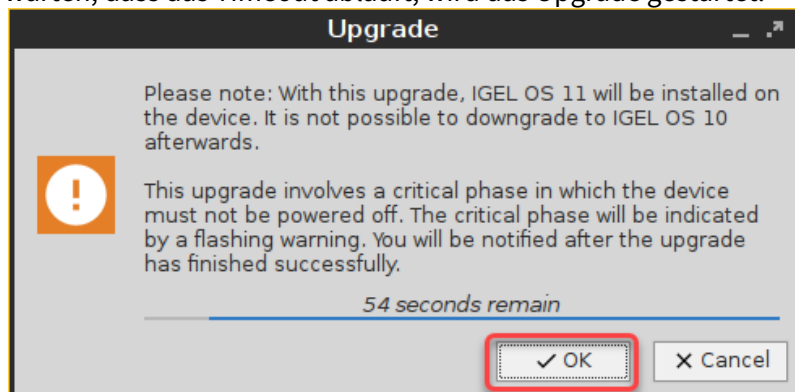


Wenn Sie das Upgrade starten, wird ein Warndialog angezeigt.

3. Klicken Sie **Ok** um fortzufahren.



Ein Warndialog mit einem Timeout wird angezeigt. Wenn Sie vor Ablauf des Timeouts auf **Abbrechen** klicken, wird das Upgrade abgebrochen. Wenn Sie auf **OK** klicken oder einfach darauf warten, dass das Timeout abläuft, wird das Upgrade gestartet.



Nachdem der Warndialog bestätigt oder der Timeout abgelaufen ist, startet das Gerät neu in eine spezielle IGEL OS 10 Umgebung, in der das System-Upgrade durchgeführt wird. Das

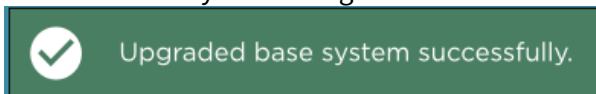
**Upgrade** Fenster zeigt den Fortschritt an.



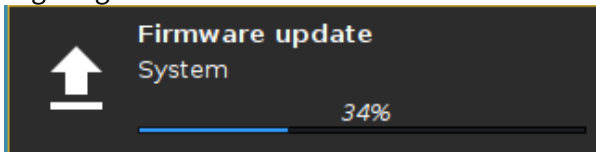
Während der kritischen Phase darf das Gerät nicht ausgeschaltet werden. In diesem Stadium des Fortschritts wird eine zusätzliche Warnung angezeigt.



Wenn das Basissystem erfolgreich aktualisiert wurde, wird eine Meldung angezeigt.



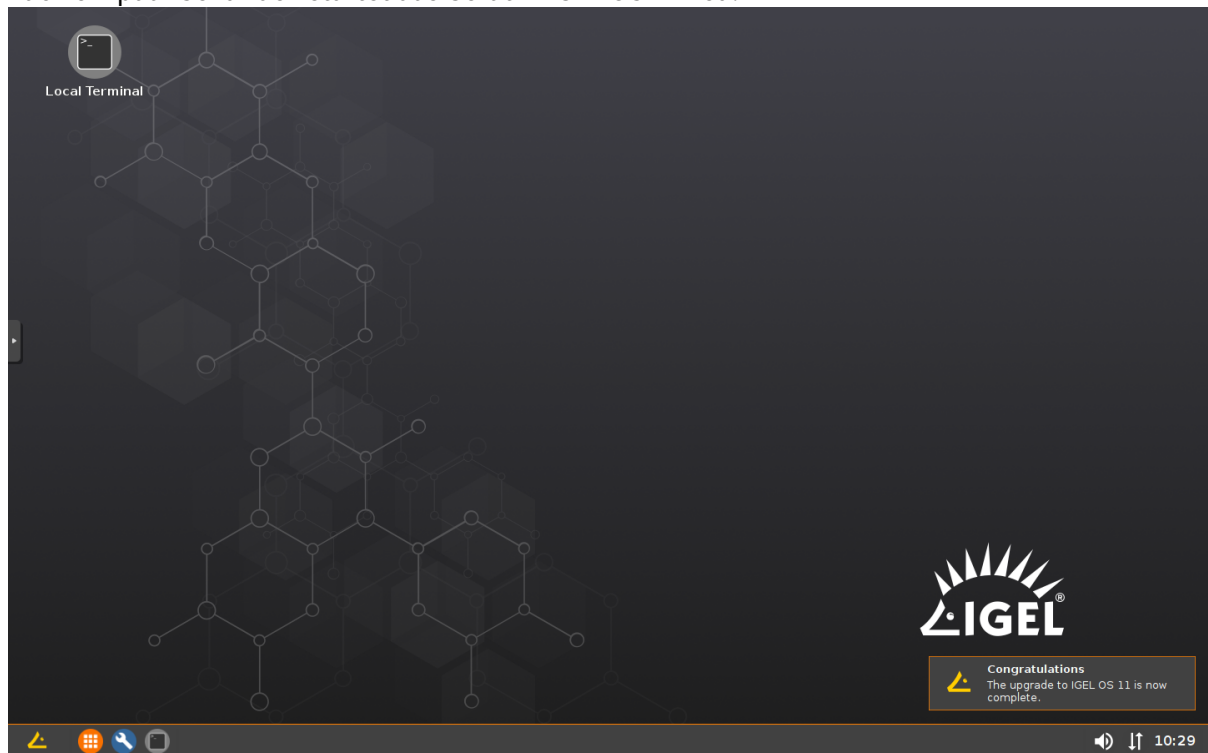
Die restlichen Komponenten der Firmware sind installiert, was durch Update-Meldungen angezeigt wird.



Wenn die Installation abgeschlossen ist, sieht das **Upgrade**-Fenster wie folgt aus:



Nach ein paar Sekunden startet das Gerät in IGEL OS 11 neu.



Wenn alle Testgeräte erfolgreich getestet wurden, fahren Sie mit [Anforderungen überprüfen](#) (see page 137) fort.



### Anforderungen überprüfen

Die folgenden Anforderungen müssen erfüllt sein:

- Das Upgrade wurde mit charakteristischen Geräten getestet.
- UMS 6.01.130 oder höher ist verfügbar.
- Die passende IGEL OS 10 Firmwareversion (10.05.700 oder höher) ist der UMS bekannt. Zu diesem Zweck muss ein Gerät mit dieser Firmwareversion in der UMS registriert werden. Dies ist bereits der Fall, wenn Sie das Upgrade mit der gleichen UMS getestet haben, mit der Sie das Massensupgrade durchführen werden. Wenn nicht, müssen Sie jetzt ein Gerät mit der passenden Firmwareversion registrieren.
- Alle Geräte sind mit einem normalen LAN verbunden (nicht mit OpenVPN, OpenConnect, Genucard oder mobilem Breitband).
- Alle Geräte befinden sich in einer sicheren Umgebung, in der der Aktualisierungsprozess nicht unterbrochen werden kann, z. B. durch Ausschalten der Geräte.

Wenn alle Anforderungen erfüllt sind, fahren Sie mit [Universal Firmware Updates erstellen](#) (see page 138) fort.

## Universal Firmware Updates erstellen

Detaillierte Informationen finden Sie im Kapitel Universal Firmware Update im UMS Handbuch.

**i** Wenn Sie die High-Availability-Erweiterung verwenden, beachten Sie, dass Universal Firmware Updates NICHT synchronisiert werden. Sie müssen Firmwareupdates entweder auf alle HA-Knoten herunterladen oder einen externen (FTP-) Server konfigurieren.

1. Erstellen Sie ein Universal Firmware Update für die passende IGEL OS 10 Firmwareversion (10.05.700 oder höher).
2. Nachdem Sie das Universal Firmware Update für IGEL OS 10 erstellt haben, erstellen Sie ein Universal Firmware Update für IGEL OS 11.

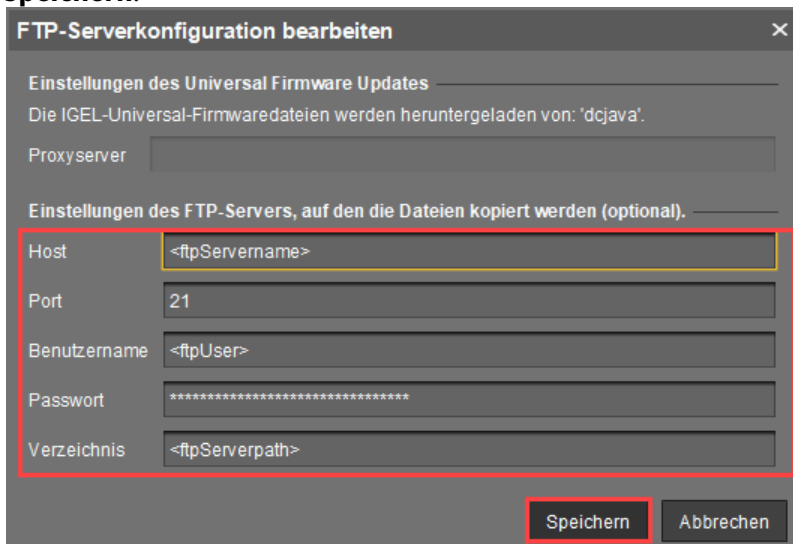
**!** Die Reihenfolge der Erstellung ist entscheidend, da die IGEL OS 11 Firmware eine höhere ID aufweisen muss, um vom Gerät ausgewählt werden zu können. Näheres hierzu siehe [Upgrade durchführen](#) (see page 152).

## Universal Firmware Update für ICG konfigurieren

Wenn Sie IGEL Cloud Gateway (ICG) verwenden, muss ein FTP-Server, der für alle Geräte zugänglich ist, als Updatequelle konfiguriert werden.

So konfigurieren Sie einen FTP-Server als Updatequelle:

1. Gehen Sie in der UMS unter **UMS Administration > Universal Firmware Update** und klicken Sie **Editieren...**.
2. Geben Sie die für den Zugriff auf den FTP-Server erforderlichen Daten ein und klicken Sie auf **Speichern**.



**FTP-Serverkonfiguration bearbeiten**

Einstellungen des Universal Firmware Updates

Die IGEL-Universal-Firmwaredateien werden heruntergeladen von: 'dcjava'.

Proxyserver

Einstellungen des FTP-Servers, auf den die Dateien kopiert werden (optional).

Host: <ftpServername>

Port: 21

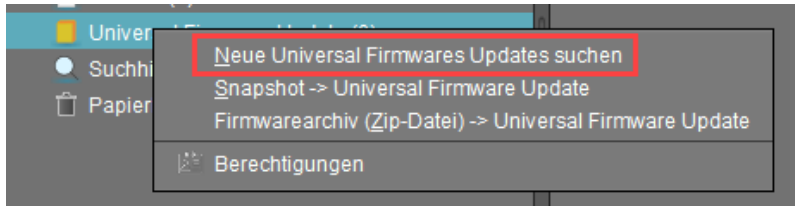
Benutzername: <ftpUser>


Passwort: \*\*\*\*\*

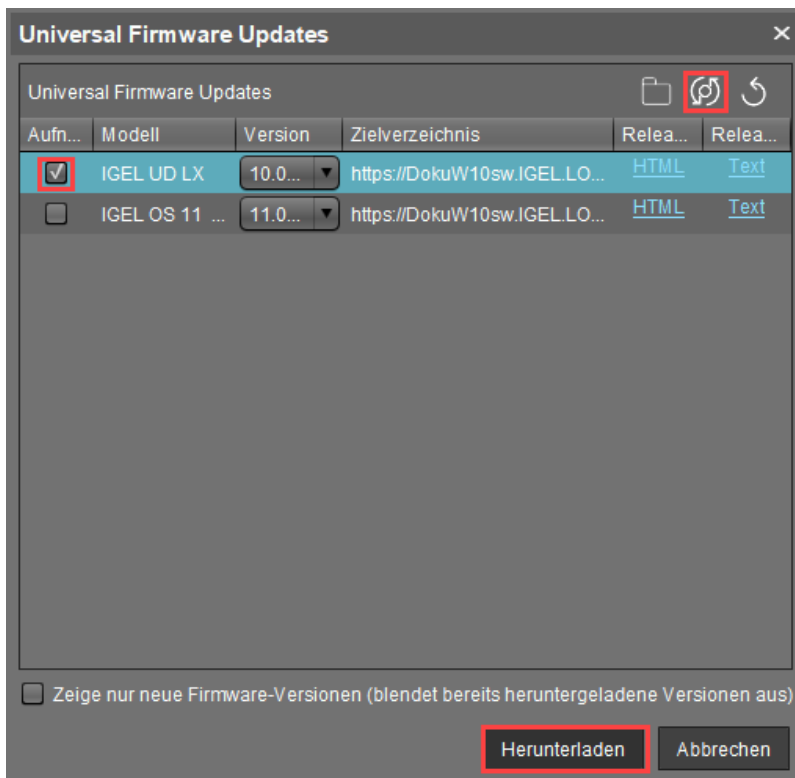
Verzeichnis: <ftpServerpath>

**Speichern** **Abbrechen**

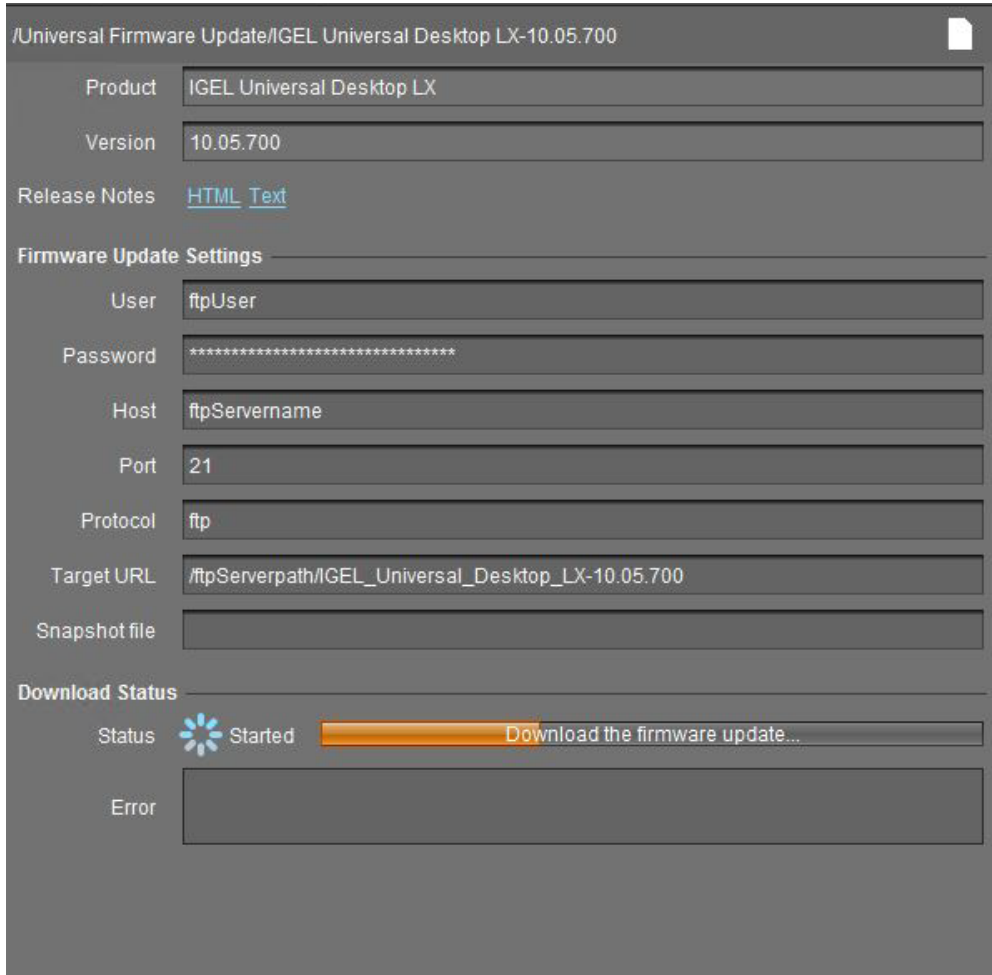
3. Gehen Sie unter **Server - [UMS Adresse] > Universal Firmware Update** und wählen Sie im Kontextmenü **Neue Universal Firmware Updates suchen**.



4. Wählen Sie den Eintrag für die passende IGEL OS 10 Firmware, klicken Sie  um den in Schritt 2 ausgewählten FTP-Server auszuwählen und klicken Sie **Herunterladen**.



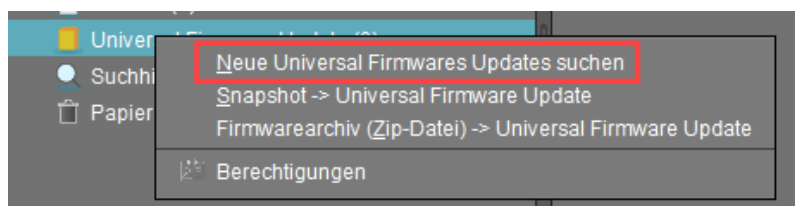
5. Die Firmware wird auf den FTP-Server übertragen.




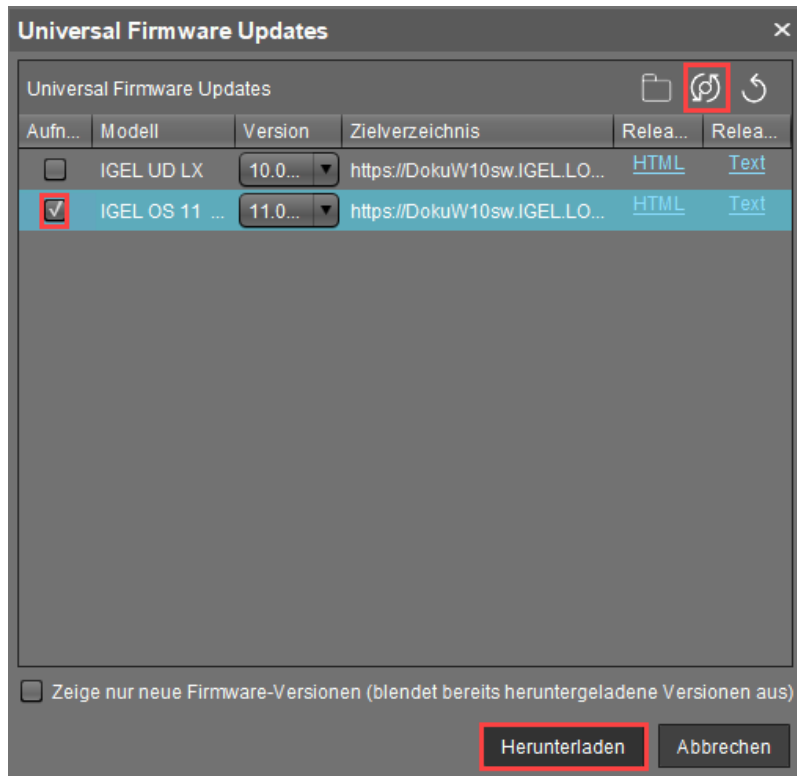
The screenshot shows the 'Universal Firmware Update' configuration window for 'IGEL Universal Desktop LX-10.05.700'. The fields are as follows:

- Product: IGEL Universal Desktop LX
- Version: 10.05.700
- Release Notes: [HTML](#) [Text](#)
- Firmware Update Settings**
  - User: ftpUser
  - Password: [Redacted]
  - Host: ftpServername
  - Port: 21
  - Protocol: ftp
  - Target URL: /ftpServerpath/IGEL\_Universal\_Desktop\_LX-10.05.700
  - Snapshot file: [Empty]
- Download Status**
  - Status: Started (with a progress bar at approximately 50% completion and the text 'Download the firmware update...')
  - Error: [Empty]

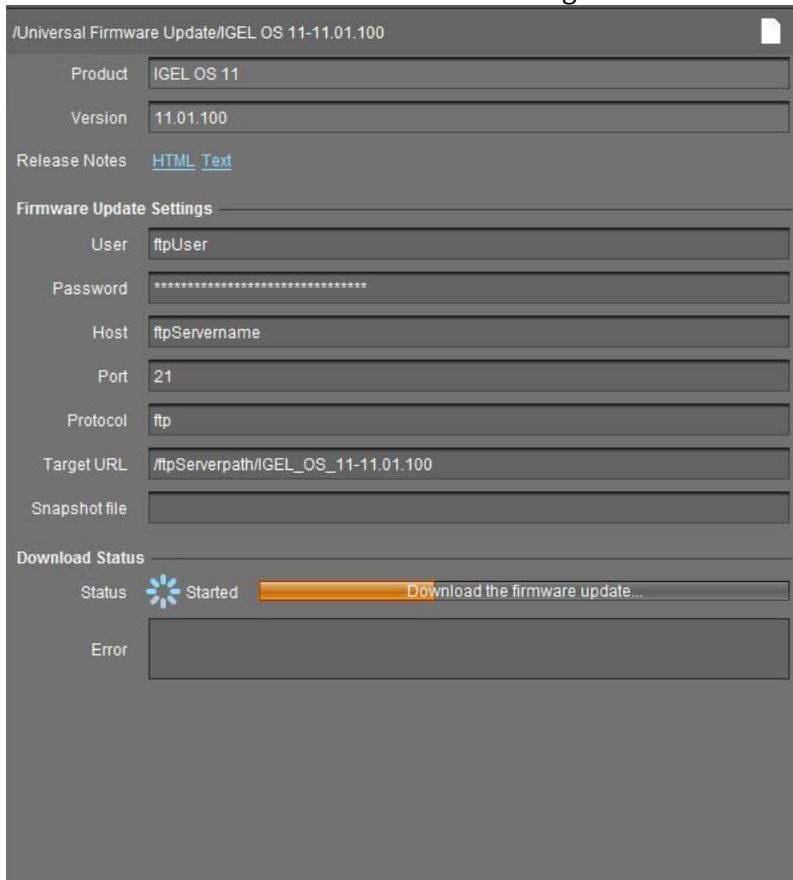
6. Gehen Sie unter **Server - [UMS Adresse] > Universal Firmware Update** und wählen Sie erneut im Kontextmenü **Neue Universal Firmware Updates suchen**.



7. Wählen Sie den Eintrag für die IGEL OS 11 Firmware, klicken Sie  um den in Schritt 2 ausgewählten FTP-Server auszuwählen und klicken Sie **Herunterladen**.



## 8. Die Firmware wird auf den FTP-Server übertragen.



./Universal Firmware Update/IGEL OS 11-11.01.100

Product

Version

Release Notes [HTML](#) [Text](#)

**Firmware Update Settings**

User

Password

Host


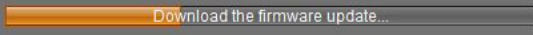
Port

Protocol

Target URL

Snapshot file

**Download Status**

Status  Started  Download the firmware update...

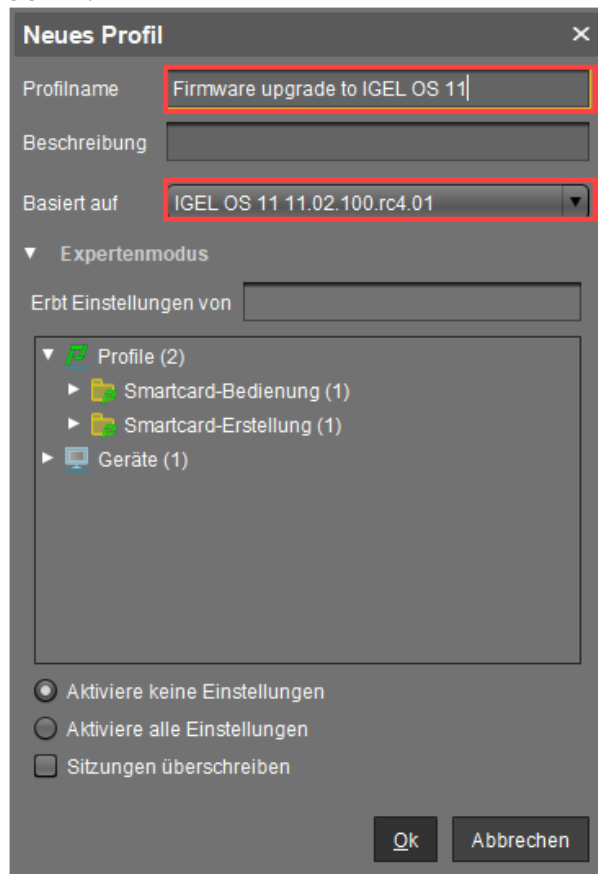
Error

Die Geräte können die Firmware vom FTP-Server herunterladen.

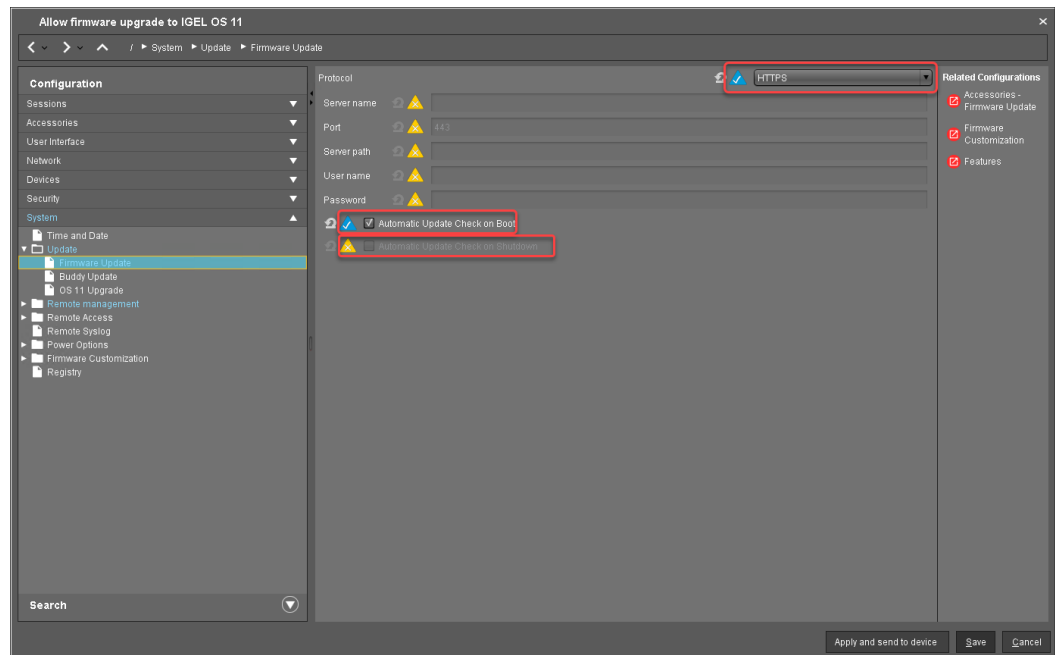
Wenn das Universal Firmware Update bereit ist, fahren Sie mit [Profil erstellen](#) (see page 143) fort.

## Profil erstellen

1. Erstellen Sie ein Profil welches auf der passenden IGEL OS 10 Firmwareversion basiert (10.05.700 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Firmware-Upgrade auf IGEL OS 11".

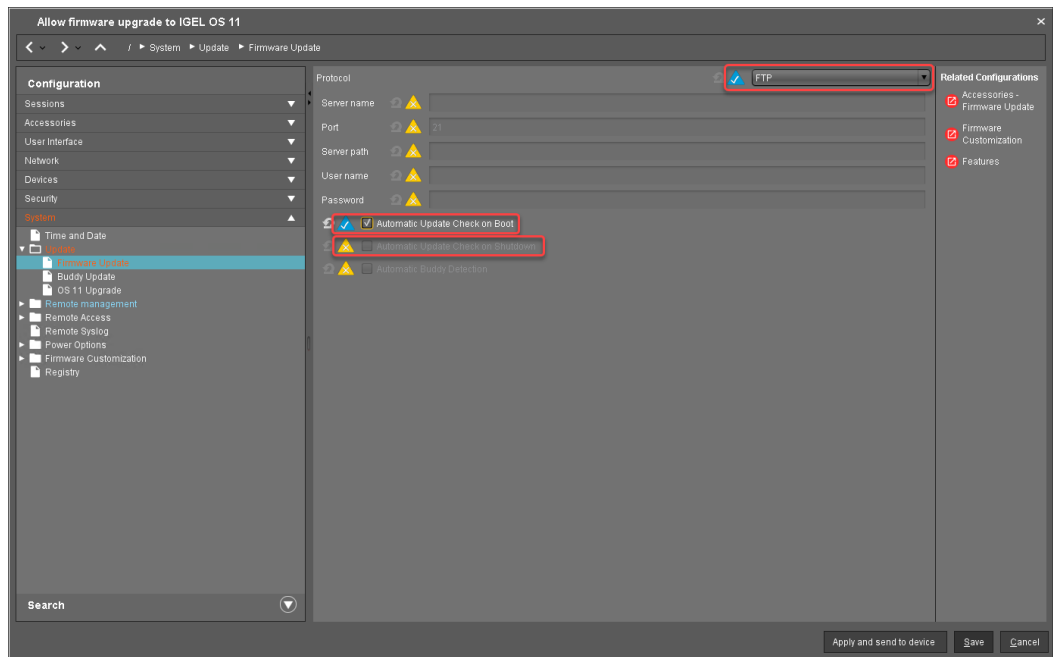


2. Gehen Sie im Konfigurationsdialog des Profils auf **System > Update > Firmware Update** und ändern Sie die Einstellungen entsprechend Ihrer Umgebung:
  - Wenn sich die UMS und die Geräte in ein und demselben Netzwerk befinden und kein IGEL Cloud Gateway (ICG) verwendet wird:
    - Wählen Sie "HTTPS" als **Protokoll**.
    - Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**.
    - Stellen Sie sicher, dass **Automatische Updatesuche beim Herunterfahren** deaktiviert ist. Andernfalls wird das Gerät heruntergefahren, wenn das Update abgeschlossen ist.

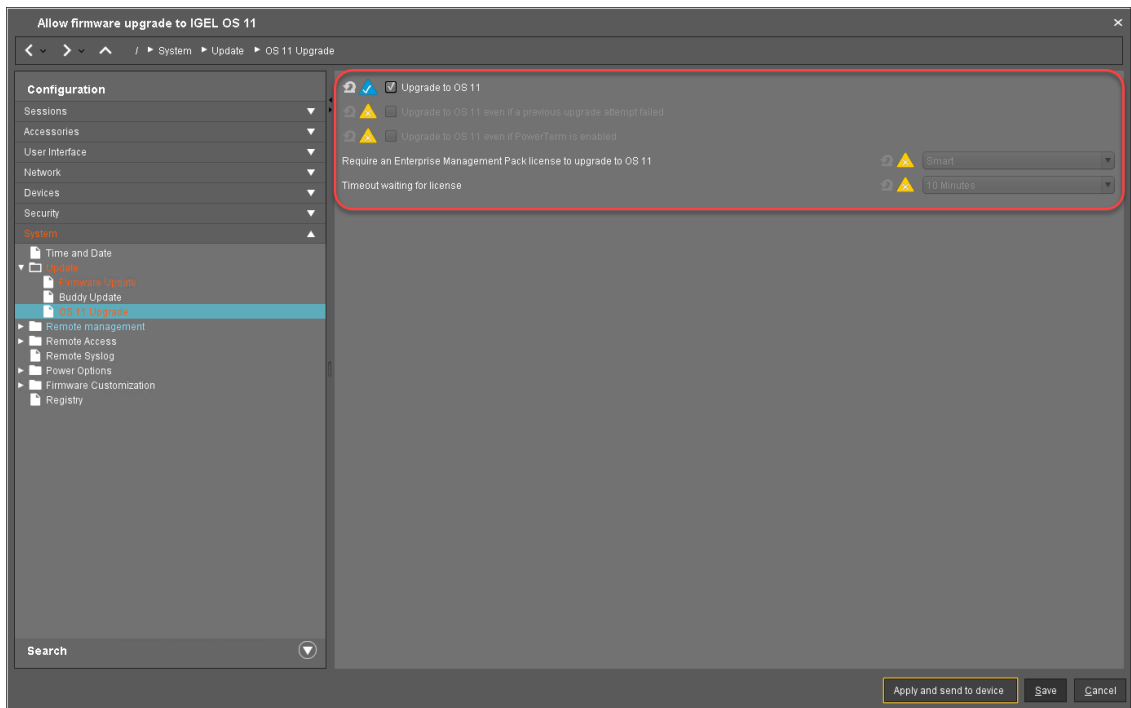


- Wenn IGEL Cloud Gateway (ICG) verwendet wird:
  - Wählen Sie "FTP" als **Protokoll**.
  - Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**.
  - Stellen Sie sicher, dass **Automatische Updatesuche beim Herunterfahren** deaktiviert ist. Andernfalls wird das Gerät heruntergefahren, wenn das Upgrade auf OS 10.05.700 abgeschlossen ist.

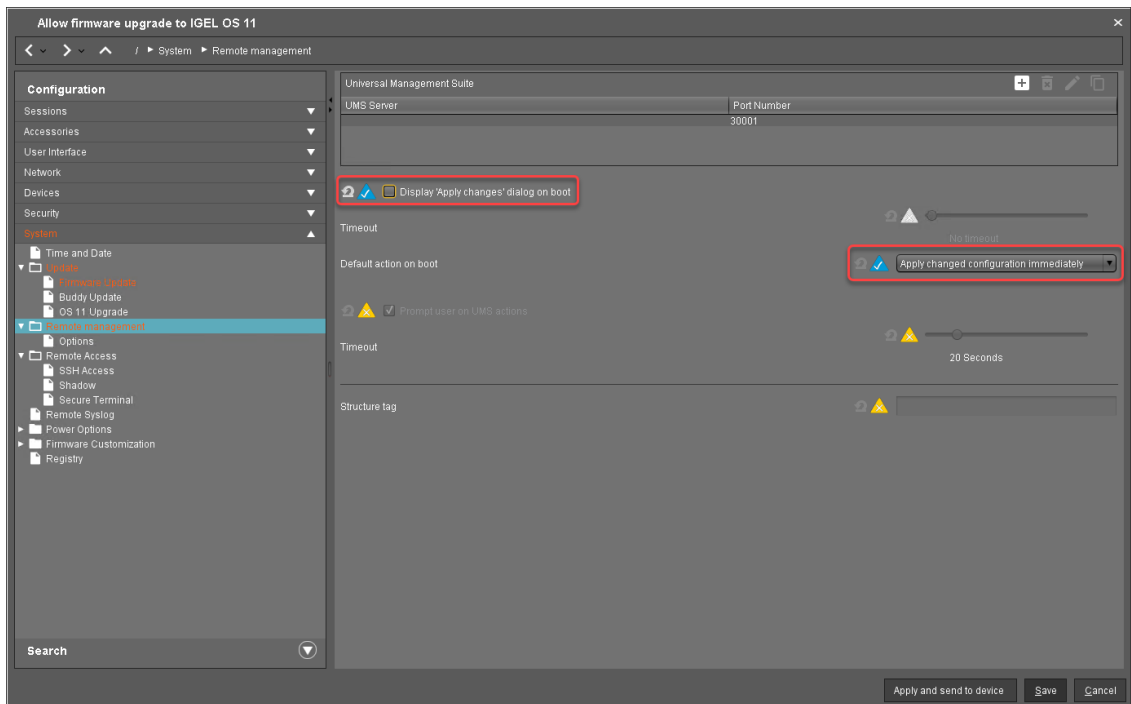




3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test:
  - Aktivieren Sie **Upgrade auf OS 11**.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** nach Ihren Bedürfnissen ein.
  - Stellen Sie sicher, dass **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** auf **10 Minuten** eingestellt ist.



4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:
- Deaktivieren Sie **'Einstellungen anwenden'-Dialog während des Bootvorgangs anzeigen**.
  - Setzen Sie **Standardaktion während des Bootvorgangs** auf **Geänderte Einstellungen sofort anwenden**.



5. Klicken Sie **Ok**.

Wenn das Profil erstellt ist, fahren Sie mit [Lizenzen bereitstellen](#) (see page 148) fort.

### Lizenzen bereitstellen

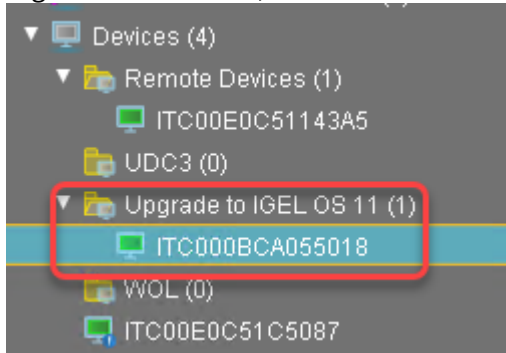
Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:


- **Automatic License Deployment (ALD):** Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
- **Manual License Deployment:** Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.

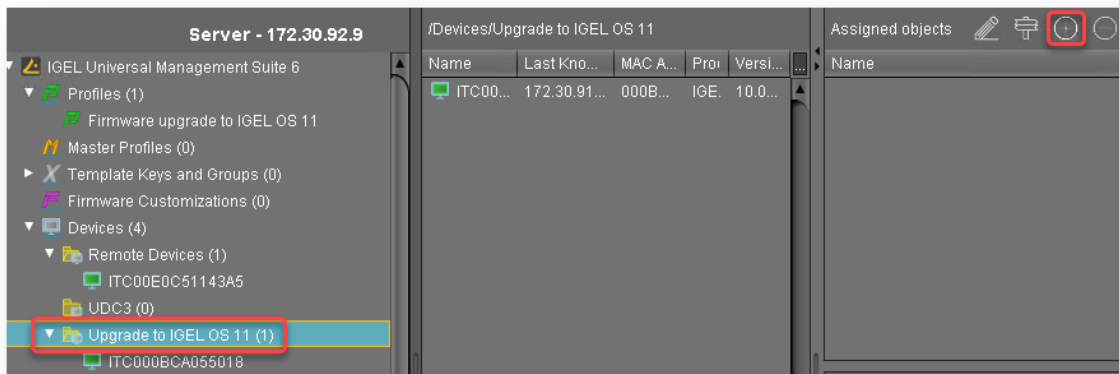
Wenn die Bereitstellung der Lizenzen aufgesetzt ist, fahren Sie fort mit [Alles zusammensetzen](#) (see page 149).

## Alles zusammensetzen

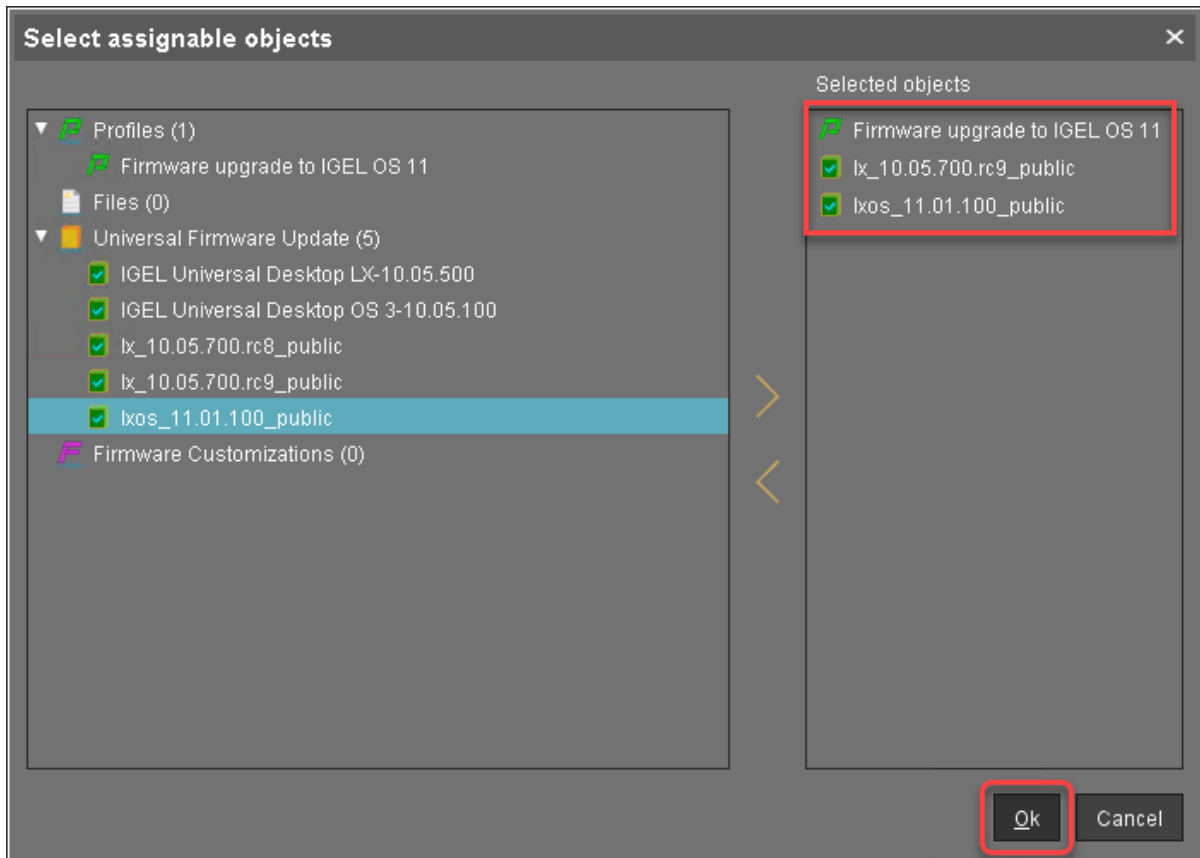
1. Legen Sie alle Geräte, die aktualisiert werden sollen, in ein Verzeichnis.



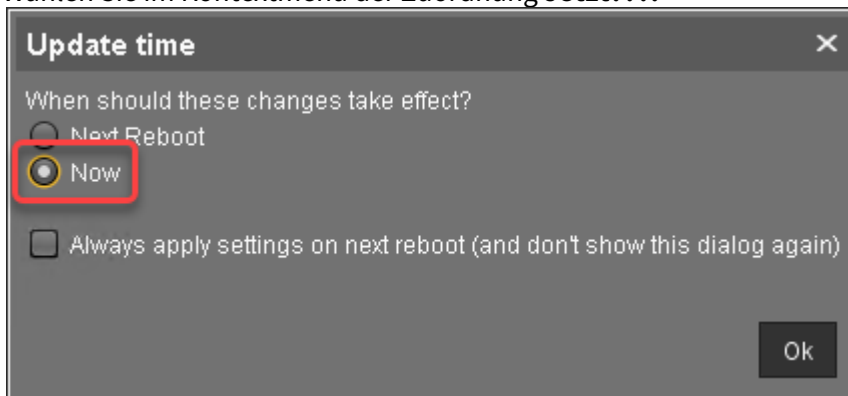
2. Wählen Sie das Verzeichnis und klicken Sie  im Bereich **Zugeordnete Objekte**.



3. Ordnen Sie das Profil (siehe [Profil erstellen \(see page 143\)](#)) und die beiden Universal Firmware Updates (siehe [Universal Firmware Updates erstellen \(see page 138\)](#)) dem Verzeichnis zu und klicken Sie **Ok**.

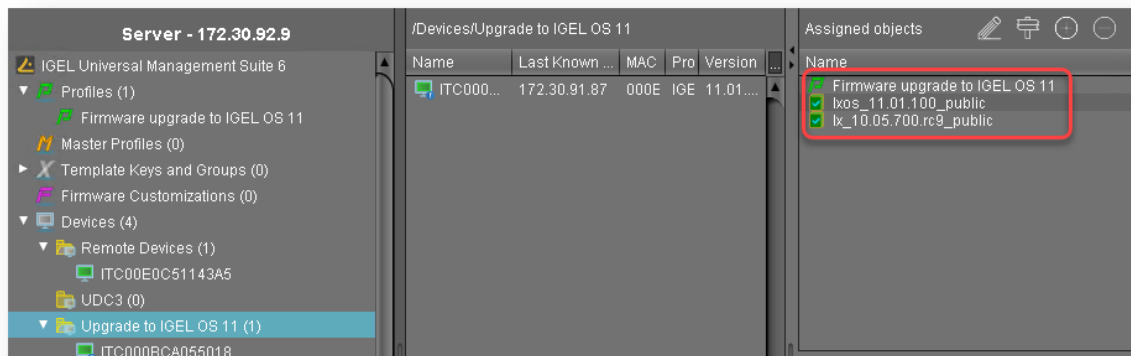


4. Wählen Sie im Kontextmenü der Zuordnung **Jetzt???**.



Im Bereich **Zugeordnete Objekte**, werden das Profil und die Universal Firmware Updates

angezeigt:




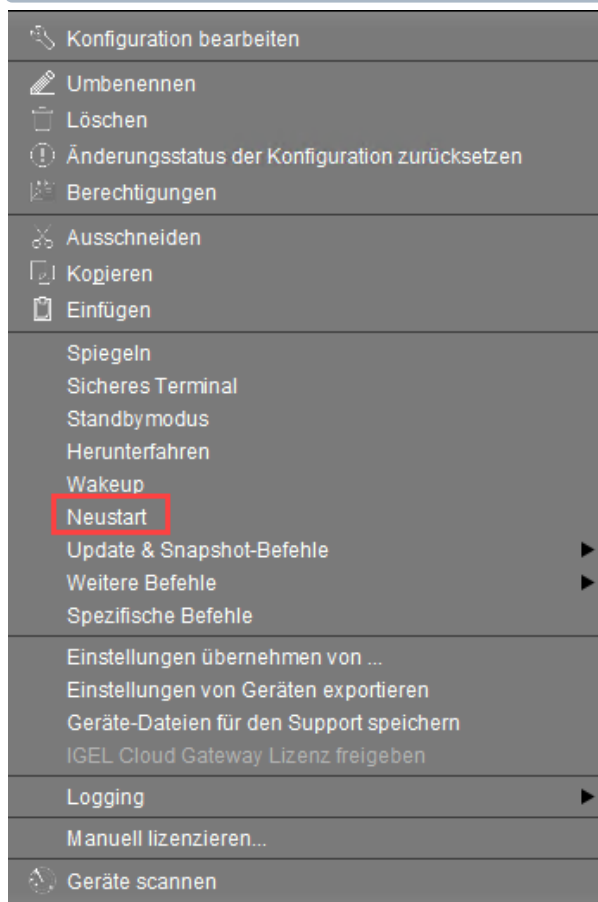
5. Wenn Sie Automatic License Deployment (ALD) verwenden, ist es möglicherweise möglich, die Verteilung der Lizenzen auf das aktuelle Verzeichnis zu beschränken. Weitere Informationen finden Sie unter Verteilungsbedingungen konfigurieren, Abschnitt "Lizenzen auf Geräte in einem bestimmten Verzeichnis verteilen".

Wenn alles bereit ist, fahren Sie mit [Upgrade durchführen](#) (see page 152) fort.

## Upgrade durchführen

1. Wählen Sie in der UMS das Verzeichnis mit allen Geräten, die aktualisiert werden sollen, und starten Sie sie neu.

 Alternativ können Sie einen geplanten Auftrag für den Neustart oder das Aufwachen erstellen und ihn den Geräten oder dem Verzeichnis mit diesen Geräten zuweisen. Weitere Informationen finden Sie unter Aufgaben.



Beim Neustart oder Aufwachen aktualisieren die Geräte auf die passende IGEL OS 10 Firmwareversion (10.05.700 oder höher). Mit dieser Version wird der Parameter **Upgrade auf OS 11** von den Geräten erkannt; außerdem fordern die Geräte IGEL OS 11-Lizenzen von der UMS an (Workspace Edition und bei Bedarf Enterprise Management Pack).

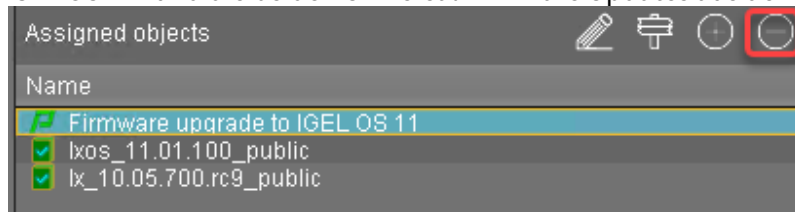
Wenn noch keine IGEL OS 11-Lizenzen auf den Geräten bereitgestellt wurden, sind die Lizenzen innerhalb weniger Minuten bereitgestellt. Das Upgrade wird gestartet, wenn die Lizenzen bereitgestellt werden. Die maximale Zeitspanne, in der das Gerät auf eine Lizenz wartet, wird durch den Parameter **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** konfiguriert; Details finden Sie unter [Setup anpassen \(see page 130\)](#).

Der Parameter **Automatische Updatesuche beim Booten** bewirkt, dass die Geräte wieder nach neuer Firmware suchen. Obwohl den Geräten zwei Universal Firmware Updates zugeordnet sind,



bietet die UMS die IGEL OS 11 Firmware an, da die ID der IGEL OS 11 Firmware höher ist als die ID der IGEL OS 10 Firmware.

2. Wenn alle Geräte erfolgreich aktualisiert wurden, entfernen Sie das Profil "Firmware-Upgrade auf IGEL OS 11" und die beiden Universal Firmware Updates aus dem Verzeichnis.



Das Upgrade ist vollendet.

## Zero-Touch-Bereitstellung mit Buddy Update

Diese Methode verwendet die Buddy-Update-Funktion von IGEL OS. Ein oder mehrere Geräte, die als Update-Buddy konfiguriert sind, greifen auf den Hauptserver zu und laden die Firmware herunter. Die anderen Geräte sind so konfiguriert, dass sie ihre Firmware von einem Update-Buddy herunterladen.

Lesen Sie dir folgenden Kapitel sorgfältig durch und folgen Sie den Anweisungen.

1. [IGEL Geräte, die auf IGEL OS 11 hochgerüstet werden können \(see page 155\)](#)
2. [Wichtig! Vor dem Upgrade berücksichtigen \(see page 126\)](#)
3. [Upgrade vorbereiten \(see page 128\)](#)
4. [Upgrade testen \(see page 133\)](#)
5. **Checking the Requirements**
6. [Zwei Update Buddies konfigurieren \(see page 169\)](#)
7. [Profil erstellen \(see page 170\)](#)
8. [Lizenzen bereitstellen \(see page 172\)](#)
9. [Alles zusammensetzen \(see page 173\)](#)
10. [Upgrade durchführen \(see page 174\)](#)

IGEL Geräte, die auf IGEL OS 11 hochgerüstet werden können

Grundvoraussetzungen für IGEL OS 11

- CPU mit 64 Bit-Unterstützung
- CPU-Taktfrequenz:  $\geq 1$  GHz
- Arbeitsspeicher (RAM):  $\geq 2$  GB

- i** Eine RAM-Größe von mehr als 2 GB wird empfohlen, wenn Sie das Folgende verwenden:
- Optimierungen für Unified Communications (verwendet eine clientseitige Media Engine)
  - Hochauflösende Grafikausgabe  
Details zu den unterstützten grafikbezogenen Merkmalen von IGEL Geräten finden Sie unter Grafik auf IGEL Geräten oder, für ältere Geräte, Grafik auf Legacy IGEL Geräten.
  - Mehr als zwei Monitore

- Festspeicher: mindestens 2 GB;  $\geq 4$  GB empfohlen

- i** **Speicheranforderungen für IGEL OS 11.04 oder höher**
- IGEL OS 11.04.100 oder höher erfordert mindestens 2,4 GB Speicherplatz, wenn der volle Funktionsumfang genutzt wird. Daher muss der Funktionsumfang entsprechend angepasst werden; weitere Informationen finden Sie unter Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher.

IGEL Geräte, die von IGEL OS 11 unterstützt werden

IGEL UD (Universal Desktop)

Produktlinie	Gerätetyp	Hardware-ID	64-Bit	Arbeitsspeicher (RAM)	Festspeicher	HW-Videobeschleunigung
UD2**** (see page 156)	D220	40	Ja	2 GB	4 GB	Ja
UD2* (see page 156)	M250C	50	Ja	2 GB	4 GB	Ja
UD2	M250C	51 / 52**** (see page 156)	Ja	2 oder 4 GB	8 GB	Ja
UD3* (see page 156)	M340C	50	Ja	2 GB	4 GB	Ja

Produktlinie	Gerätetyp	Hardware-ID	64-Bit	Arbeitsspeicher (RAM)	Festspeicher	HW-Videobeschleunigung
UD3* (see page 156)	M340C	51	Ja	2 GB	4 GB	Ja
UD3	M350C	60	Ja	4 GB	8 GB	Ja
UD5* (see page 156)	H830C	50	Ja	2 GB	4 GB	Ja
UD6* (see page 156)	H830C	51	Ja	2 GB	4 GB	Ja
UD7	H850C	10	Ja	4 GB	4 GB	Ja
UD7** (see page 156)	H850C	11	Ja	4 GB	4 GB	Ja
UD7	H860C	20	Ja	8 GB	8 GB	Ja
UD9* (see page 156)	TC215B	40 / 41 (Touch)	Ja	2 GB	4 GB	Ja

\* IGEL UD3-LX 50 und UD5-LX 50 werden offiziell bis zu IGEL OS 11.05 unterstützt, inkl. Private Builds.  
 IGEL UD9-LX 40 / 41 (Touch) Geräte werden offiziell bis zu IGEL OS 11.07.910 unterstützt.  
 IGEL UD2-LX 50-Geräte werden bis zu IGEL OS 11.09.160 unterstützt.  
 IGEL UD3-LX 51-Geräte werden bis zu IGEL OS 11.09.160 unterstützt.  
 IGEL UD6-LX 51-Geräte werden bis zu IGEL OS 11.09.160 unterstützt.

\*\* Ab Dezember 2019 ist der IGEL UD7, Modell H850C, mit dem AMD Secure Processor ausgerüstet; weitere Informationen siehe UD7 Model H850C.

\*\*\* IGEL UD2-LX 52 wird mit IGEL OS 11.06.140 und höher unterstützt.

UD2-LX 40 (Modell D220) wird bis IGEL OS 11.08.200 unterstützt. Einen Überblick über die Daten von end-of-sales (EOS) und end-of-maintenance (EOM) finden Sie unter [IGEL OS 11 or Higher \(see page 155\)](#).

## IGEL Zero

### Hinweis zu IZ-Geräten

Bei den unten aufgezählten IZ-Geräten ist ein Upgrade auf IGEL OS 11 möglich. Bitte kontaktieren Sie Ihren IGEL Vertriebsrepräsentanten, damit Sie ein Upgrade Ihrer IZ-Geräte vornehmen können. Siehe auch <https://www.igel.com/os11migration/>.

Produktlinie	Gerätetyp	Hardware-ID	64-Bit	Arbeitsspeicher (RAM)	Festspeicher	UEFI-Secure-Boot	HW-Videobeschleunigung
IZ2	D220	40	Ja	2 GB	4 GB	Ja	Ja
IZ3	M340C	50	Ja	2 GB	4 GB	Ja	Ja
IZ3	M340C	51	Ja	2 GB	4 GB	Ja	Ja

Wenn Sie festgestellt haben, dass Ihre Geräte auf IGEL OS 11 hochgerüstet werden können, beachten Sie **Wichtig! Vor dem Upgrade berücksichtigen** (see page 158).

Wichtig! Vor dem Upgrade berücksichtigen

Um sicherzustellen, dass Ihr Upgrade erfolgreich sein kann, überprüfen Sie die folgenden Warnungen und Hinweise; ein Warnsymbol zeigt an, dass irreversible Schäden an Ihren Geräten auftreten können.

#### **Kein Downgrade**

Nach der Migration auf IGEL OS 11 können Sie Ihr IGEL OS 10-System nicht mehr wiederherstellen. Der Gerätespeicher wird mit einem neuen Partitionierungsschema vollständig überschrieben.

#### **Funktionen (z. B. Clients)**

IGEL OS 11 verfügt nicht über den kompletten Funktionsumfang von IGEL OS 10. Stellen Sie sicher, dass die aktuelle Version von IGEL OS 11 Ihren Anforderungen entspricht. Einzelheiten finden Sie in den entsprechenden Release-Informationen.

#### **Eigene Partitionen**

Der Inhalt von benutzerdefinierten Partitionen wird durch das Upgrade gelöscht. Stellen Sie sicher, dass Sie den Inhalt sichern und nach Abschluss des Upgrades wiederherstellen. Neben der Dysfunktionalität nach dem Upgrade können Anwendungen und Kerneltreiber in einer benutzerdefinierten Partition das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Wir empfehlen, benutzerdefinierte Partitionen beim Upgrade zu deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

#### **Eigene Befehle**

Die Persistenz von benutzerdefinierten Befehlen kann nicht garantiert werden. Neben der Dysfunktionalität nach dem Upgrade können benutzerdefinierte Befehle das Upgrade beschädigen. Stellen Sie daher sicher, dass Sie das Upgrade zunächst auf einem charakteristischen Gerät testen. Im Allgemeinen müssen benutzerdefinierte Befehle für IGEL OS 11 angepasst werden. Wir empfehlen, dass Sie benutzerdefinierte Befehle beim Aktualisieren deaktivieren; Sie können sie aktivieren, sobald das Upgrade erfolgreich abgeschlossen wurde.

#### **Netzwerk**

Alle Geräte müssen an ein WLAN oder LAN angeschlossen sein. LAN ist die empfohlene Option. Das Gerät wird nicht aktualisiert, wenn es mit OpenVPN, OpenConnect, Genucard, NCP VPN oder mobilem Breitband verbunden ist.

#### **Hardwareunterstützung**

Stellen Sie sicher, dass Ihre Geräte IGEL OS 11 unterstützen; siehe IGEL Geräte, die von IGEL OS 11 unterstützt werden. Dieses Dokument beschreibt die Aktualisierungsmethoden für IGEL UD und IGEL IZ Geräte. Die Aktualisierungsmethoden für IGEL UDC3 und UD Pocket sind unter UDC3-Geräte von IGEL OS 10 auf IGEL OS 11 upgraden beschrieben.

**i Lizenz**

- Für jedes Gerät muss eine gültige Lizenz einer IGEL Workspace Edition (WE) verfügbar sein. Allgemeine Informationen finden Sie unter IGEL Softwarelizenzen - Übersicht. Informationen zur Bereitstellung von Lizenzen finden Sie unter Automatic License Deployment (ALD) einrichten oder Manuelle Lizenz-Bereitstellung für IGEL OS.
- IZ Geräte dürfen nicht auf IGEL OS 11 aktualisiert werden. Wenden Sie sich an Ihren IGEL Vertriebsmitarbeiter, um eine UD Upgrade Lizenz zu erhalten, die es Ihnen ermöglicht, Ihre IZ Geräte zu aktualisieren.

**i UMS Version**

Für das Upgrade von IGEL OS 10 auf IGEL OS 11 ist die UMS Version 6.01.130 oder höher erforderlich.

Wenn Sie alles Relevante berücksichtigt haben, fahren Sie mit [Upgrade vorbereiten](#) (see page 160) fort.

## Upgrade vorbereiten

Dieser Abschnitt beschreibt die erforderlichen Vorbereitungen und Tests, bevor Produktivgeräte aktualisiert werden können. Die Prüfung sollte mit mindestens einem Gerät durchgeführt werden, das für Ihre Umgebung charakteristisch ist. Dieses Gerät sollte jede benutzerdefinierte Partition und jeden benutzerdefinierten Befehl enthalten, der möglicherweise in einem Ihrer Geräte vorhanden ist.

Um das Upgrade vorzubereiten, führen Sie die folgenden Schritte durch:

1. [UMS vorbereiten](#) (see page 161)
2. [Setup anpassen](#) (see page 162)
3. [Lizenz bereitstellen](#) (see page 163)
4. [Update-Quelle konfigurieren](#) (see page 164)



### UMS vorbereiten

Um Ihre Geräte auf IGEL OS 11 aufzurüsten, benötigen Sie die entsprechende Version der UMS. Außerdem müssen die Geräte bei der UMS registriert sein, um ihre Lizenzen zu erhalten.

1. Wenn Sie dies noch nicht getan haben, aktualisieren Sie Ihre UMS auf Version 6.01.130 oder höher. Anweisungen finden Sie unter UMS Installation aktualisieren.
2. Stellen Sie sicher, dass Ihre Geräte an der UMS registriert sind. Weitere Informationen finden Sie im Kapitel Geräte am UMS Server registrieren des UMS Handbuchs.

Wenn die UMS vorbereitet ist, fahren Sie mit [Setup anpassen \(see page 162\)](#) fort.

## Setup anpassen

Abhängig von den Funktionen, die jetzt oder in Zukunft verwendet werden, muss im Setup des Geräts ein bestimmter Parametersatz eingestellt werden.

1. Gehen Sie im Setup unter **System > Update > OS 11 Upgrade**.
2. Nehmen Sie die entsprechenden Einstellungen vor:
  - Aktivieren Sie **Upgrade auf OS 11**.
  - Wenn Sie möchten, dass das Gerät das Upgrade sofort nach einem fehlgeschlagenen Versuch erneut durchführt, aktivieren Sie die Option **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist**. Das Gerät versucht das Upgrade 5 mal erneut. Wenn der 5. Versuch fehlgeschlagen ist, wird eine Meldung im Fenster des Upgrade-Tools angezeigt.
  - Wenn Ihr Gerät über eine PowerTerm-Lizenz verfügt und Sie auf IGEL OS 11 aktualisieren möchten, obwohl es PowerTerm nicht unterstützt, müssen Sie folgendes aktivieren **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist**.
  - Wählen Sie unter **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** die entsprechende Option:
    - Wenn Sie IGEL Cloud Gateway (ICG) oder Shared Workplace (SWP) oder eine benutzerdefinierte Partition verwenden und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn diese Funktionen weiterhin verwendet werden können, wählen Sie **Smart**. Wenn diese Option ausgewählt und eine dieser Funktionen aktiviert ist, wird das Upgrade nur durchgeführt, wenn das Gerät eine Lizenz von einem Enterprise Management Pack beziehen konnte.
    - Wenn Sie das Gerät zwingen möchten, eine Lizenz von einem Enterprise Management Pack abzurufen, und sicherstellen möchten, dass das Upgrade nur durchgeführt wird, wenn die Lizenz abgerufen werden kann, wählen Sie **Immer**.
    - Wenn Sie möchten, dass das Gerät auf IGEL OS 11 aktualisiert wird, ohne ein Enterprise Management Pack zu erhalten, ohne die möglicherweise aktivierten Funktionen zu berücksichtigen, wählen Sie **Niemals**.
  - Geben Sie unter **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** den Zeitraum an, in dem das Gerät in einem Massenbereitstellungsszenario auf eine Lizenz warten soll (siehe [Zero-Touch-Bereitstellung mit Universal Firmware Update \(see page 122\)](#), [Zero-Touch-Bereitstellung mit Buddy Update \(see page 154\)](#) und [Massenbereitstellung über einen geplante Aufgabe \(see page 175\)](#)). Diese Einstellung verhindert, dass das Gerät das Upgrade zu einem ungünstigen Zeitpunkt startet, da die bereitgestellte Lizenz gerade installiert wird. Auf diese Weise verhindert die Einstellung ungewollte Unterbrechungen bei der Arbeit. Für ein Masseneinsatzszenario wird der Standardwert **10 Minuten** empfohlen.
3. Klicken Sie **Übernehmen**.

Wenn das Setup angepasst ist, fahren Sie mit [Lizenz bereitstellen \(see page 163\)](#) fort.

## Lizenz bereitstellen

Für ein Upgrade von IGEL OS 10 auf IGEL OS 11 benötigen Sie eine entsprechende Lizenz. Je nach Ihren Anforderungen werden eine oder mehrere dieser Lizenzen für jedes Gerät benötigt:

- Eine Workspace Edition-Lizenz für die Grundfunktionen. Weitere Informationen finden Sie unter Workspace Edition.
- Wenn eines der folgenden Features verwendet wird, wird eine Enterprise Management Pack-Lizenz benötigt (siehe Enterprise Management Pack):
  - IGEL Cloud Gateway (ICG)
  - Shared Workplace (SWP)
  - Custom Partition - wenn die Zielversion IGEL OS 11.03.100 oder niedriger ist; mit IGEL OS 11.03.500 oder höher ist das Feature Custom Partition in der Workspace Edition enthalten.

Gehen Sie wie folgt vor:

- ▶ Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:
  - Manual License Deployment: Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.
  - Automatic License Deployment (ALD): Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
  - Laden Sie drei Demo-Lizenzen herunter von <https://www.igel.com/download/>.

Wenn das Gerät eine Lizenz hat, fahren Sie mit [Update-Quelle konfigurieren](#) (see page 164) fort.


#### Update-Quelle konfigurieren

1. Gehen Sie im Setup unter **System > Update > Firmware Update** und konfigurieren Sie die Update Source für IGEL OS 11. Für mehr Information, siehe im Kapitel Firmware Update des IGEL OS Handbuchs.
2. Klicken Sie **Ok**.



Wenn die korrekte Update-Quelle konfiguriert ist, fahren Sie mit [Upgrade testen](#) (see page 165) fort.

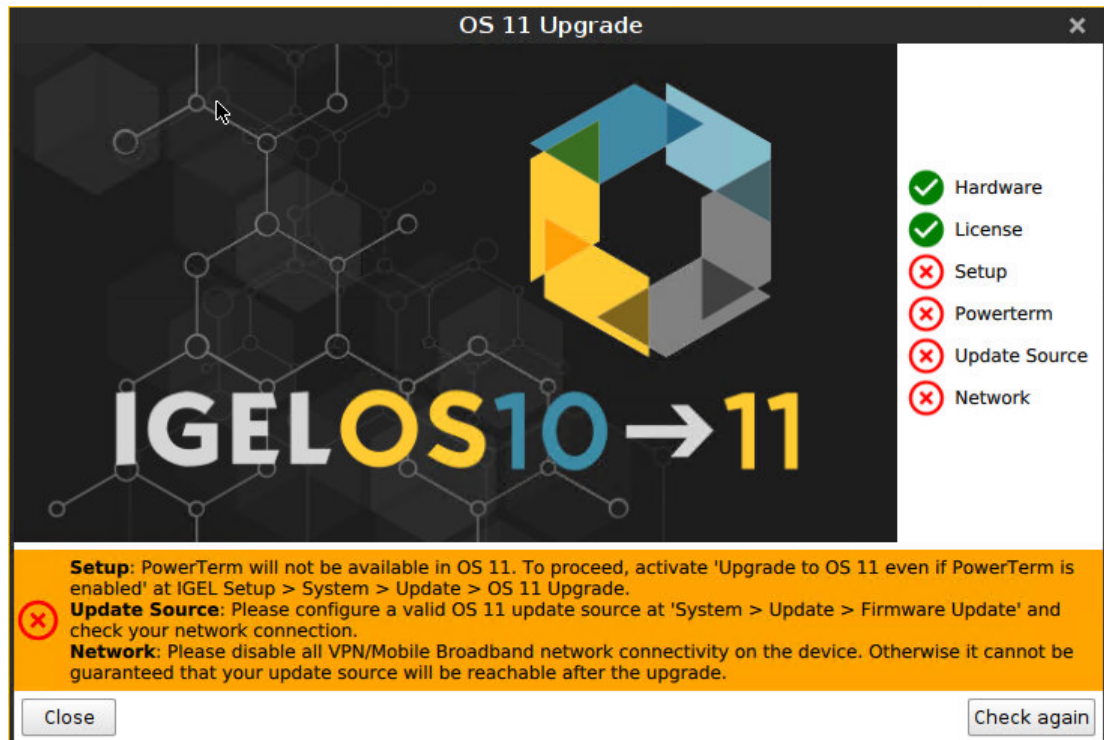
## Upgrade testen

1. Klicken Sie auf  und dann auf **Upgrade auf OS 11**. Das OS 11 Upgrade-Tool startet und zeigt an, ob alle Anforderungen erfüllt sind.

 Sie können das Starten der Startmethoden für das OS 11 Upgrade-Tool im Setup unter **Zubehör > OS11 Upgrade** ändern.

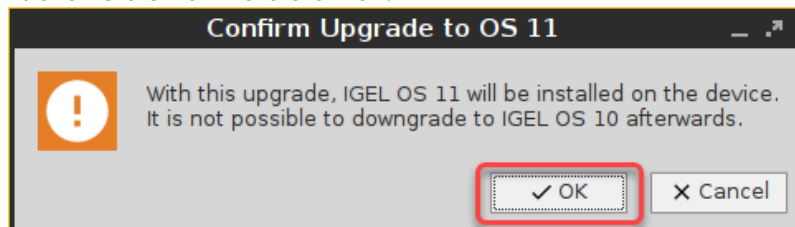


2. Überprüfen Sie die Ausgabe des OS 11 Upgrade-Tools und fahren Sie entsprechend fort:
  - Wenn jede Anforderung ein  Symbol hat, klicken Sie **OS Upgrade**, um den Upgrade-Vorgang zu starten.
  - Wenn eine oder mehrere Anforderungen ein  Symbol haben, überprüfen Sie die Meldungen und beheben Sie die Probleme. Klicken Sie anschließend auf **nochmal überprüfen**. Wenn alle Voraussetzungen erfüllt sind, ändert sich die Schaltfläche in **OS Upgrade**, und Sie können das Upgrade starten.

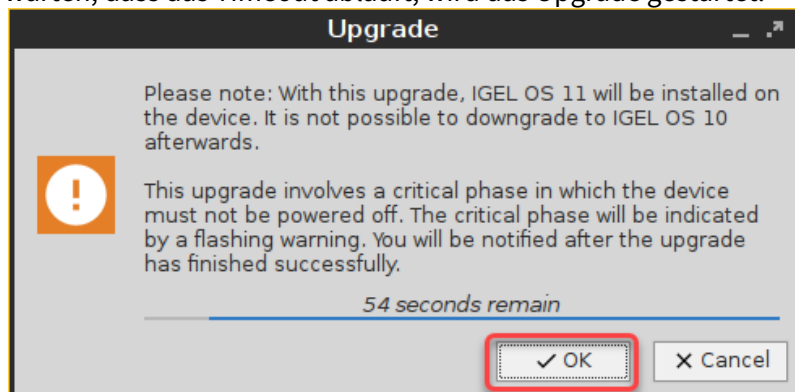


Wenn Sie das Upgrade starten, wird ein Warndialog angezeigt.

3. Klicken Sie **Ok** um fortzufahren.



Ein Warndialog mit einem Timeout wird angezeigt. Wenn Sie vor Ablauf des Timeouts auf **Abbrechen** klicken, wird das Upgrade abgebrochen. Wenn Sie auf **OK** klicken oder einfach darauf warten, dass das Timeout abläuft, wird das Upgrade gestartet.



Nachdem der Warndialog bestätigt oder der Timeout abgelaufen ist, startet das Gerät neu in eine spezielle IGEL OS 10 Umgebung, in der das System-Upgrade durchgeführt wird. Das

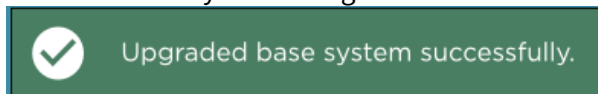
**Upgrade** Fenster zeigt den Fortschritt an.



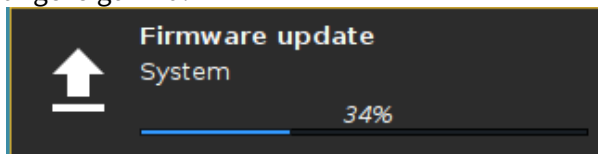
Während der kritischen Phase darf das Gerät nicht ausgeschaltet werden. In diesem Stadium des Fortschritts wird eine zusätzliche Warnung angezeigt.



Wenn das Basissystem erfolgreich aktualisiert wurde, wird eine Meldung angezeigt.



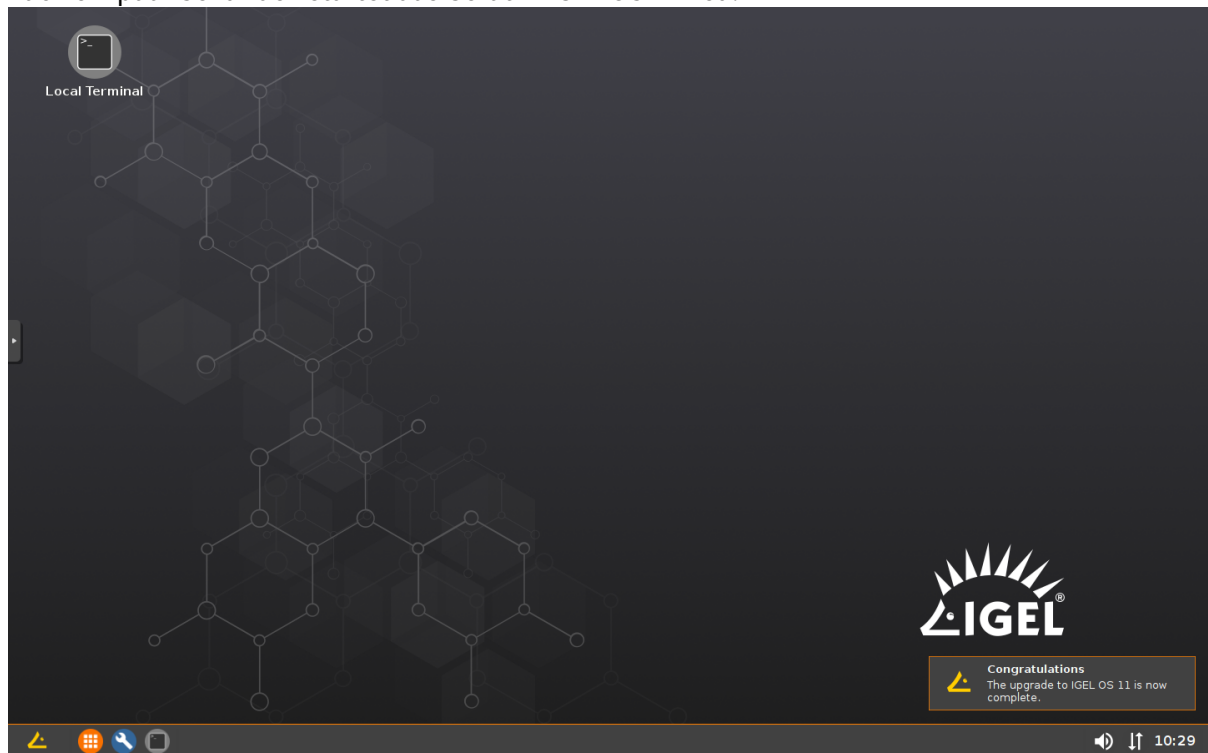
Die restlichen Komponenten der Firmware sind installiert, was durch Update-Meldungen angezeigt wird.



Wenn die Installation abgeschlossen ist, sieht das **Upgrade**-Fenster wie folgt aus:



Nach ein paar Sekunden startet das Gerät in IGEL OS 11 neu.




Wenn der Upgrade-Test erfolgreich war, können Sie das Massen-Upgrade aufsetzen. Fahren Sie mit Checking the Requirements fort.



## Zwei Update Buddies konfigurieren

Informationen zum Einrichten von Buddy Updates finden Sie im How-To [Buddy Update einrichten](#) (see page 196).

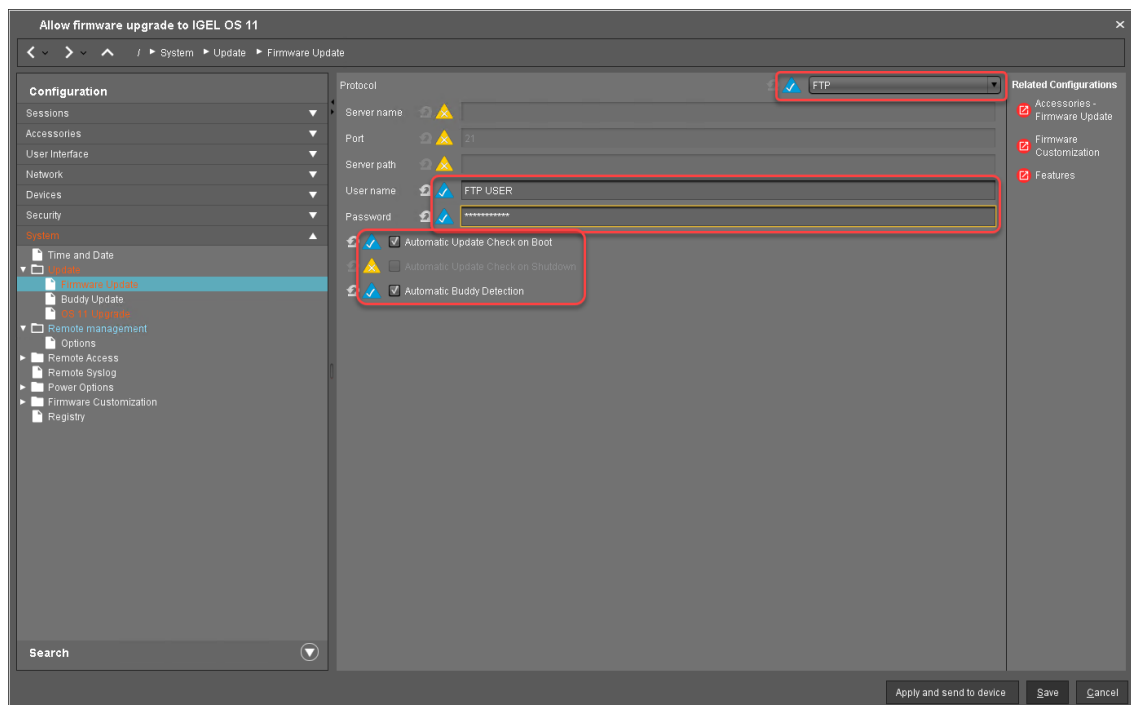
 Stellen Sie sicher, dass das Netzwerk nur die Update Buddies und die Geräte enthält, die aktualisiert werden sollen. Dadurch wird verhindert, dass andere Geräte versehentlich aktualisiert werden.

1. Aktualisieren Sie ein Gerät auf die passende IGEL OS 10 Firmware (10.05.700 oder höher) und konfigurieren Sie es als Update Buddy.
2. Aktualisieren Sie ein anderes Gerät auf IGEL OS 11 und konfigurieren Sie es als Update Buddy. Stellen Sie sicher, dass der IGEL OS 11 Update Buddy den gleichen **Benutzernamen** und das gleiche **Passwort** in **System > Update > Buddy Update** wie der IGEL OS 10 Update-Buddy hat.

Wenn die Update Buddies konfiguriert sind, fahren Sie mit [Profil erstellen](#) (see page 170) fort.

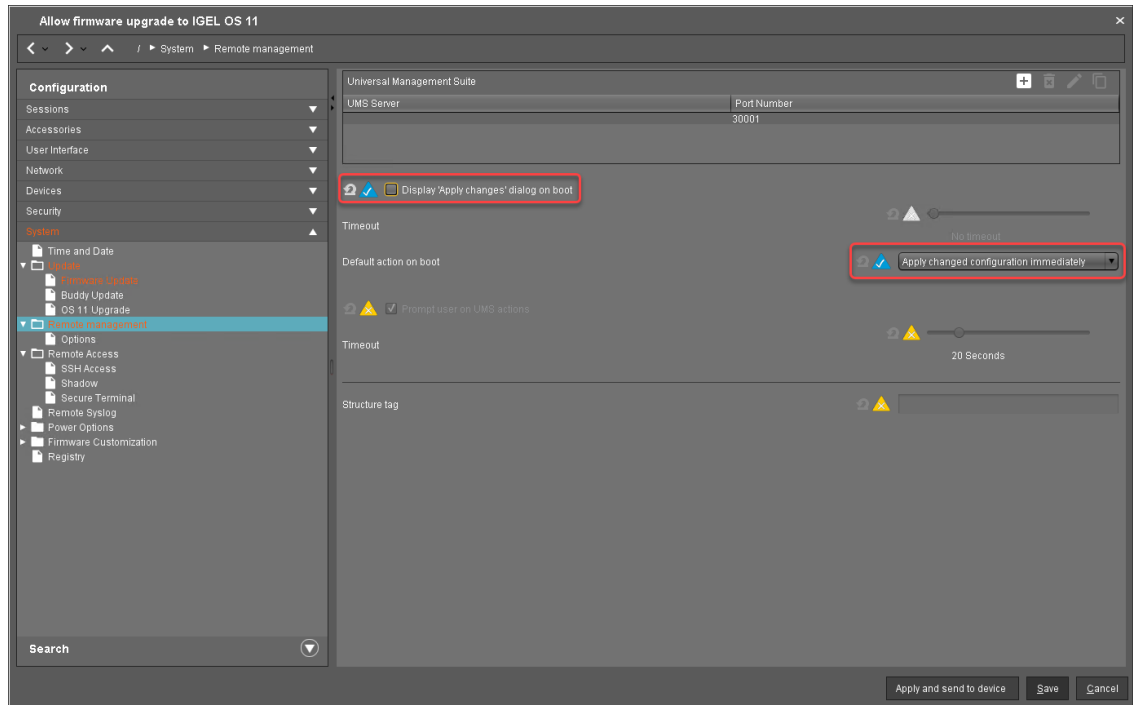
## Profil erstellen

1. Erstellen Sie ein Profil, das auf der passenden IGEL OS Firmware basiert (10.05.700 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Firmwareupgrade auf IGEL OS 11".
2. Gehen Sie im Konfigurationsdialog des Profils auf **System > Update > Firmware Update** und ändern Sie die Einstellungen wie folgt:
  - Wählen Sie "FTP" als **Protokoll**.
  - Geben Sie **Benutzername** und **Passwort** entsprechend dem Update Buddy Server ein.
  - Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**.
  - Stellen Sie sicher, dass **Automatische Updatesuche beim Herunterfahren** deaktiviert ist. Andernfalls wird das Gerät heruntergefahren, wenn das Update abgeschlossen ist.
  - Aktivieren Sie **Automatische Buddy-Server-Erkennung**.



3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test:
  - Aktivieren Sie **Upgrade to OS 11**.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** nach Ihren Bedürfnissen ein.
  - Stellen Sie sicher, dass **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades auf 10 Minuten** eingestellt ist.
4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:
  - Deaktivieren Sie **'Einstellungen anwenden'-Dialog während des Bootvorgangs anzeigen**.

- Setzen Sie **Standardaktion während des Bootvorgangs** auf **Geänderte Einstellungen sofort anwenden**.



5. Klicken Sie **Ok**.

Wenn das Profil erstellt ist, fahren Sie mit [Lizenzen bereitstellen](#) (see page 172) fort.

### Lizenzen bereitstellen


Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:

- **Automatic License Deployment (ALD):** Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
- **Manual License Deployment:** Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.

Wenn das Lizenz-Deployment aufgesetzt ist, fahren Sie mit [Alles zusammensetzen \(see page 173\)](#) fort.

#### Alles zusammensetzen

1. Ordnen Sie das Profil allen Geräten zu, die aktualisiert werden sollen. Dies kann durch die Zuordnung des Profils zu dem Verzeichnis erfolgen, das diese Geräte enthält.


 Ordnen Sie das Profil nicht den Update Buddies zu.

2. Wählen Sie im Kontextmenü der Zuordnung **Sofort**.
3. Für die automatische Lizenzbereitstellung kann eine Bedingung für das Verzeichnis festgelegt werden. Weitere Informationen finden Sie unter [Verteilungsbedingungen konfigurieren](#), Abschnitt "Lizenzen auf Geräte in einem bestimmten Verzeichnis verteilen".

Wenn alles bereit ist, fahren Sie mit [Upgrade durchführen](#) (see page 174) fort.

## Upgrade durchführen

1. Wählen Sie in der UMS alle Geräte aus, die aktualisiert werden sollen, und starten Sie sie neu.

 Alternativ können Sie einen geplanten Auftrag für den Neustart oder das Aufwachen erstellen und ihn den Geräten oder dem Verzeichnis mit diesen Geräten zuweisen. Weitere Informationen finden Sie unter [Aufgaben](#).

Beim Neustart oder Aufwachen wählen die Geräte den IGEL OS 10 Buddy. Sie ignorieren den IGEL OS 11-Buddy zum jetzigen Zeitpunkt, da ihnen diese Version noch nicht bekannt ist. Die Geräte werden auf die passende Version von IGEL OS 10 (10.05.700 oder höher) aktualisiert. Mit dieser Version wird der Parameter Upgrade auf OS 11 von den Geräten erkannt; außerdem fordern die Geräte IGEL OS 11-Lizenzen vom UMS (Workspace Edition und bei Bedarf Enterprise Management Pack) an.

Wenn noch keine IGEL OS 11-Lizenzen auf den Geräten bereitgestellt wurden, sind die Lizenzen innerhalb weniger Minuten bereitgestellt. Das Upgrade wird gestartet, wenn die Lizenzen bereitgestellt sind. Die maximale Zeitspanne, in der das Gerät auf eine Lizenz wartet, wird durch den Parameter **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades** konfiguriert; Details finden Sie unter [Setup einstellen](#).

Die Parameter **Automatische Updatesuche beim Bootvorgang** und **Automatische Buddy-Server-Erkennung** veranlassen die Geräte, nach einer neuen Firmware zu suchen und auf die Antwort eines IGEL OS 11 Update Buddy zu warten. Wenn ein IGEL OS 11-Update-Buddy gefunden wird, starten die Geräte den Upgrade-Prozess.

2. Wenn alle Geräte erfolgreich aktualisiert wurden, entfernen Sie das Profil "Firmwareupgrade auf IGEL OS 11".

Das Upgrade ist vollendet.

## Massenbereitstellung über einen geplante Aufgabe

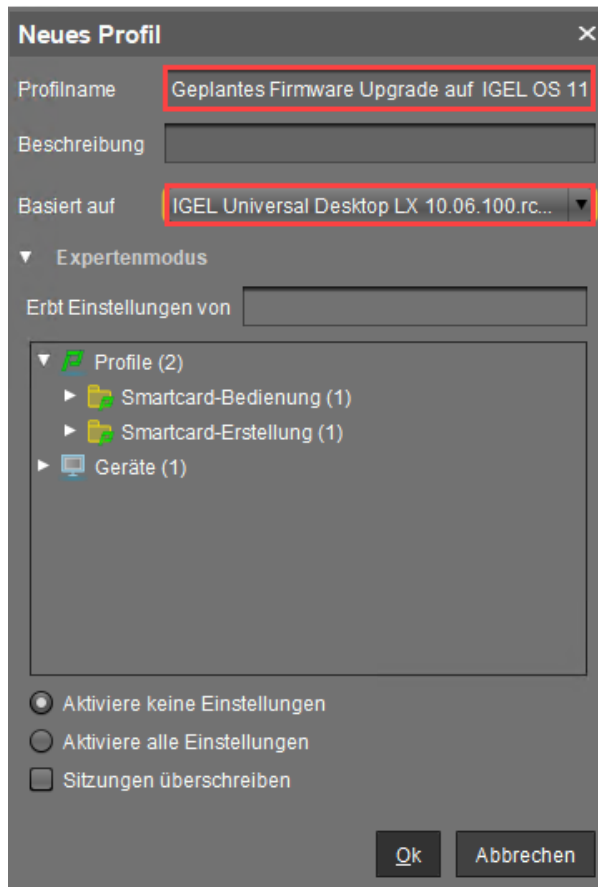
Dieses Szenario ist sinnvoll, wenn Sie bereits eine Arbeitsumgebung mit IGEL OS 10.05.700 (oder höher) haben und alle Geräte zu einem definierten Zeitpunkt auf IGEL OS 11 aktualisieren möchten.

Lesen Sie alle folgenden Kapitel sorgfältig durch und folgen Sie den Anweisungen.

1. [Anforderungen überprüfen](#) (see page 176)
2. [Profil erstellen](#) (see page 180)
3. [Lizenzen bereitstellen](#) (see page 184)
4. [Profil zuordnen](#) (see page 185)
5. [Geplante Aufgabe erstellen](#) (see page 187)

## Anforderungen überprüfen

1. Erstellen Sie ein Profil, das auf der passenden IGEL OS 10 Firmwareversion basiert (OS 10.05.700 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Geplantes Firmware Upgrade auf IGEL OS 11".



2. Gehen Sie im Konfigurationsdialog des Profils unter **System > Update > Firmwareupdate** und ändern Sie die Einstellungen entsprechend Ihrer Umgebung:


**i** Wenn Sie das [Universal Firmware Update](#) (see page 138) für OS 11 benutzen, müssen Sie die in diesem Schritt beschriebenen Einstellungen nicht konfigurieren.

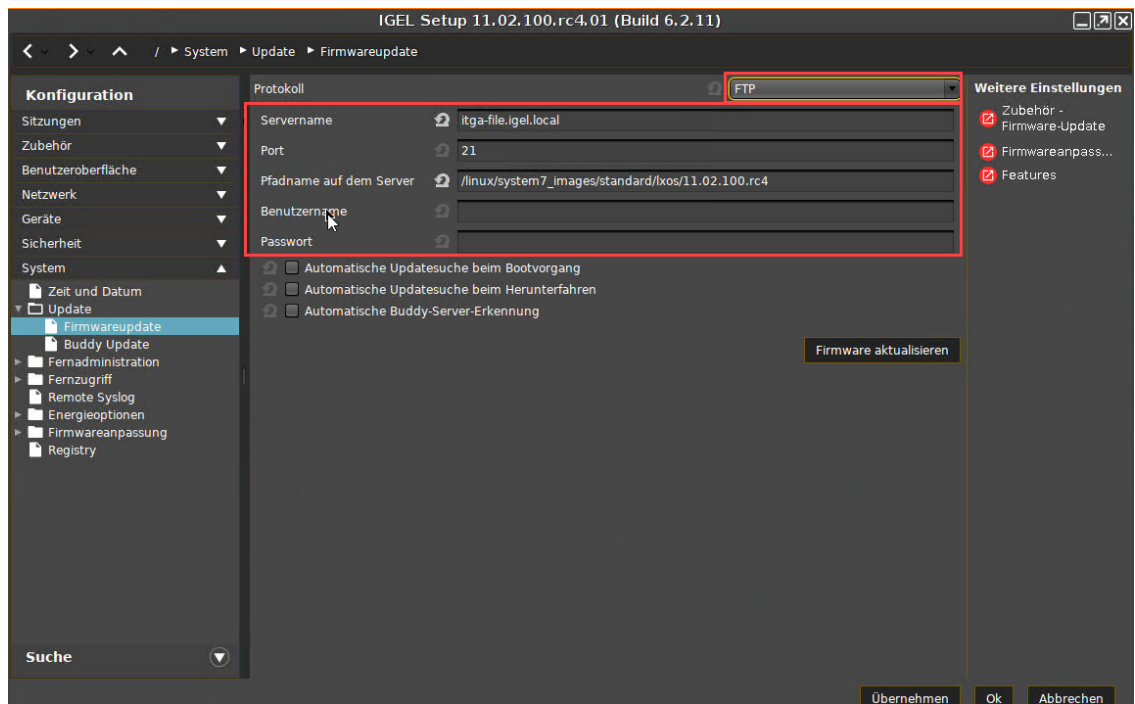
- Wählen Sie eine Updatequelle für IGEL OS 11 aus, siehe Firmware Update.

**i** Wenn Sie **DATEI** als Protokoll (lokale Datei oder Netzlaufwerk) verwenden, zeigt das Gerät eine Fehlermeldung an und führt einen zusätzlichen Neustart durch. Abgesehen davon funktioniert das Upgrade normal.

- Stellen Sie sicher, dass die **Automatische Updatesuche beim Bootvorgang** und die **Automatische Updatesuche beim Herunterfahren** deaktiviert sind.

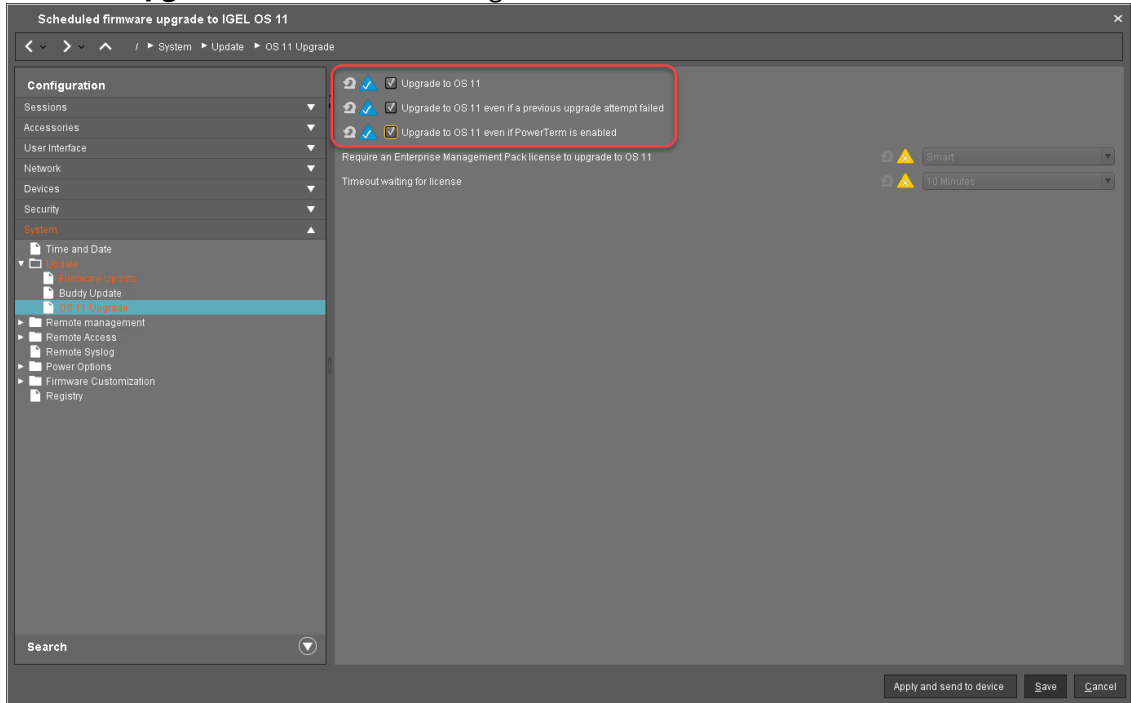


 Im folgenden Screenshot wird FTP als Beispiel verwendet. Die anderen Protokolle können ebenfalls verwendet werden.

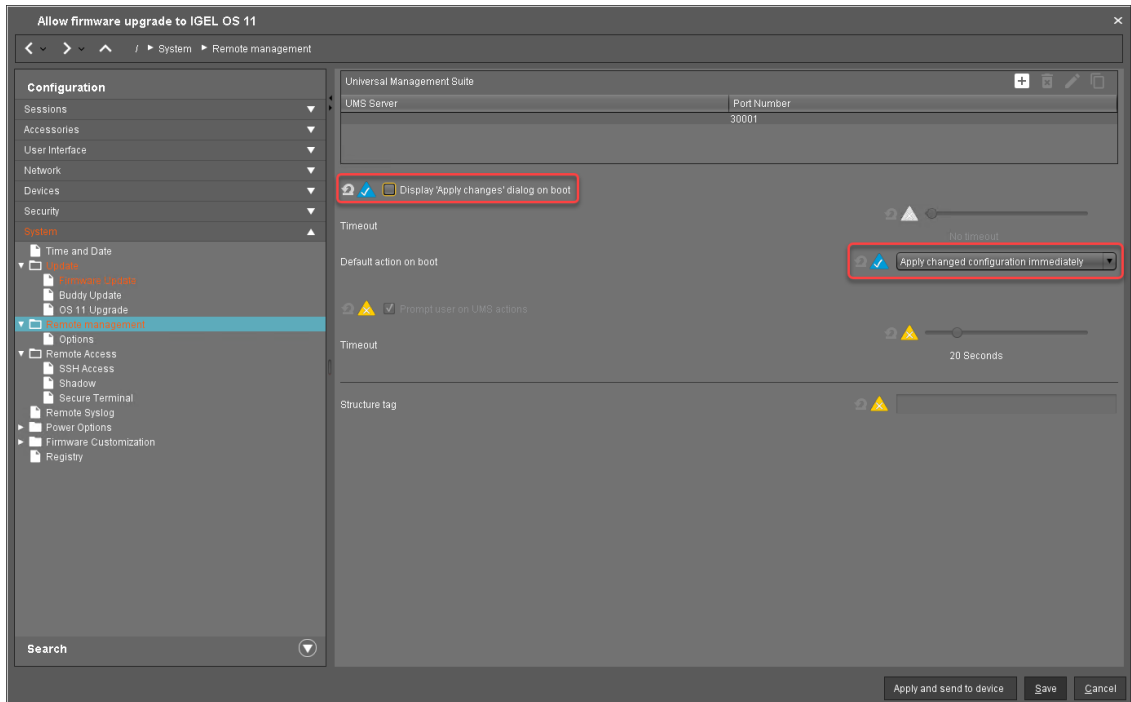


3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test (Details zu den Einstellungen finden Sie unter Setup einstellen):
  - Aktivieren Sie **Upgrade to OS 11**.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** nach Ihren Bedürfnissen ein.

- Stellen Sie sicher, dass **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades auf 10 Minuten** eingestellt ist.



4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:
  - deaktivieren Sie 'Einstellungen anwenden'-Dialog während des Bootvorgangs anzeigen.
  - Setzen Sie **Standardaktion während des Bootvorgangs auf Geänderte Einstellungen sofort anwenden.**



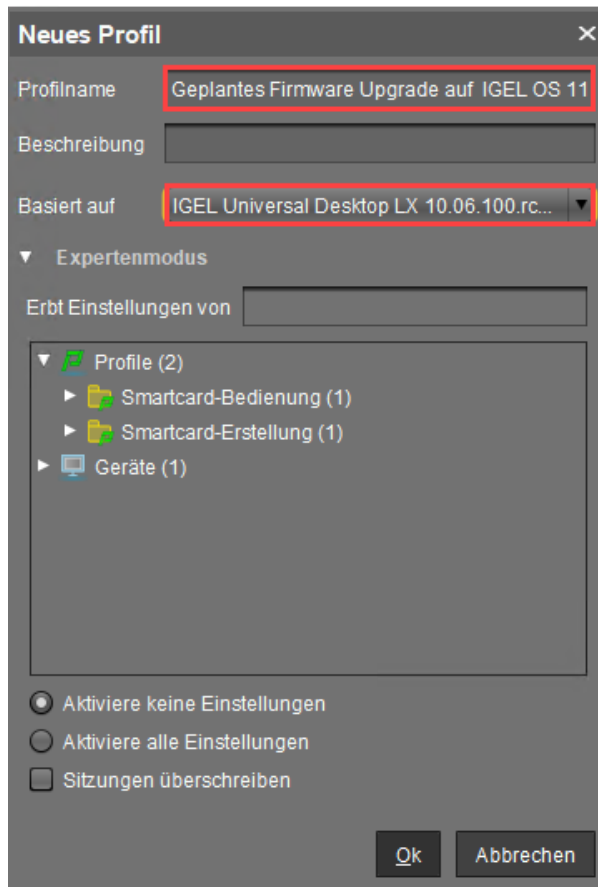
5. Klicken Sie **Ok**.

Wenn das Profil erstellt ist, fahren Sie mit [Lizenzen bereitstellen](#) (see page 184) fort.

Wenn alle Anforderungen erfüllt sind, fahren Sie mit [Profil erstellen](#) (see page 180) fort.

## Profil erstellen

1. Erstellen Sie ein Profil, das auf der passenden IGEL OS 10 Firmwareversion basiert (OS 10.05.700 oder höher). Suchen Sie einen geeigneten Namen für das Profil, z. B. "Geplantes Firmware Upgrade auf IGEL OS 11".




2. Gehen Sie im Konfigurationsdialog des Profils unter **System > Update > Firmwareupdate** und ändern Sie die Einstellungen entsprechend Ihrer Umgebung:

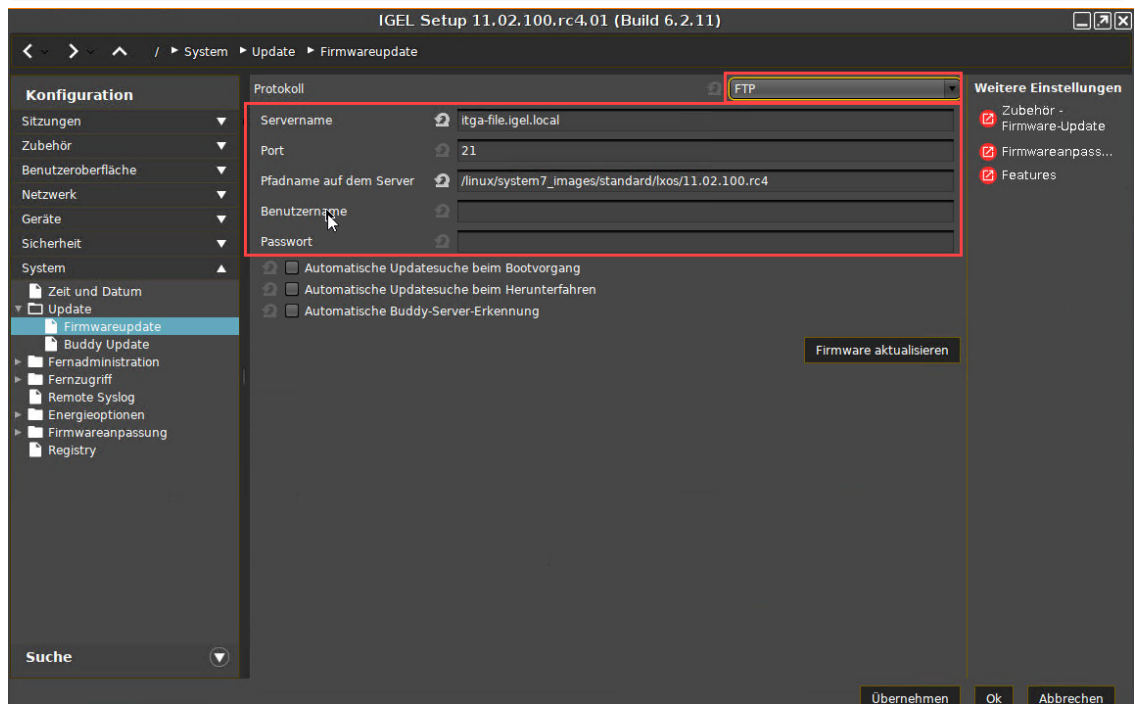
**i** Wenn Sie das [Universal Firmware Update](#) (see page 138) für OS 11 benutzen, müssen Sie die in diesem Schritt beschriebenen Einstellungen nicht konfigurieren.

- Wählen Sie eine Updatequelle für IGEL OS 11 aus, siehe Firmware Update.

**i** Wenn Sie **DATEI** als Protokoll (lokale Datei oder Netzlaufwerk) verwenden, zeigt das Gerät eine Fehlermeldung an und führt einen zusätzlichen Neustart durch. Abgesehen davon funktioniert das Upgrade normal.

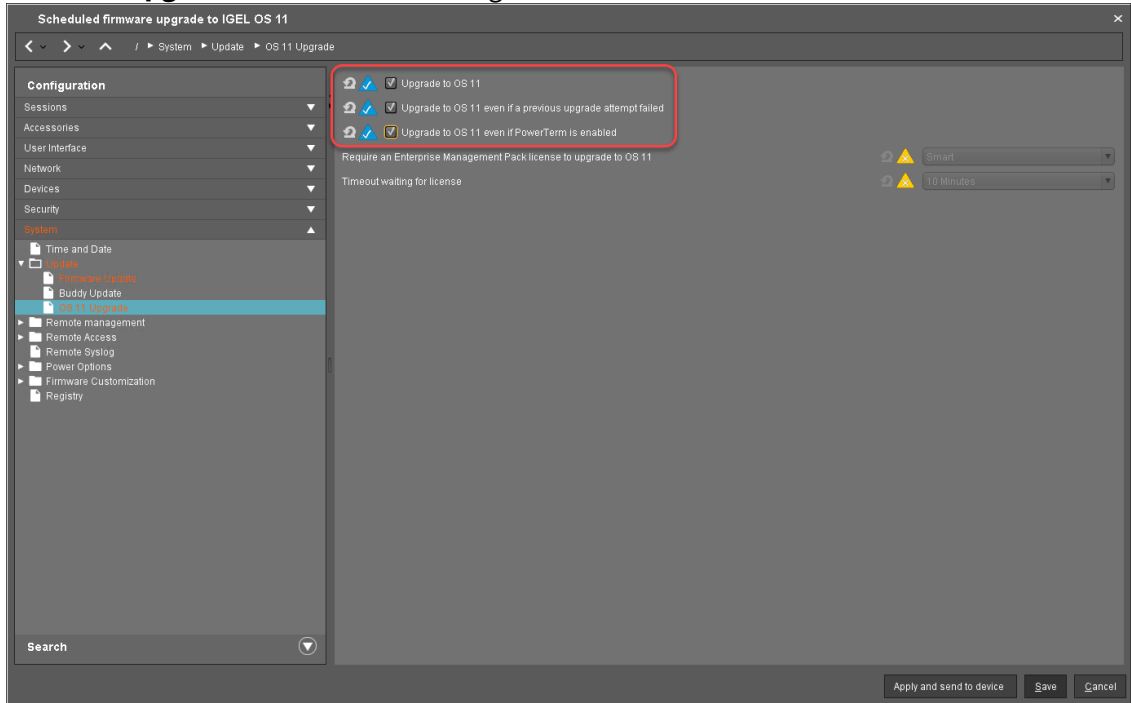
- Stellen Sie sicher, dass die **Automatische Updatesuche beim Bootvorgang** und die **Automatische Updatesuche beim Herunterfahren** deaktiviert sind.

 Im folgenden Screenshot wird FTP als Beispiel verwendet. Die anderen Protokolle können ebenfalls verwendet werden.

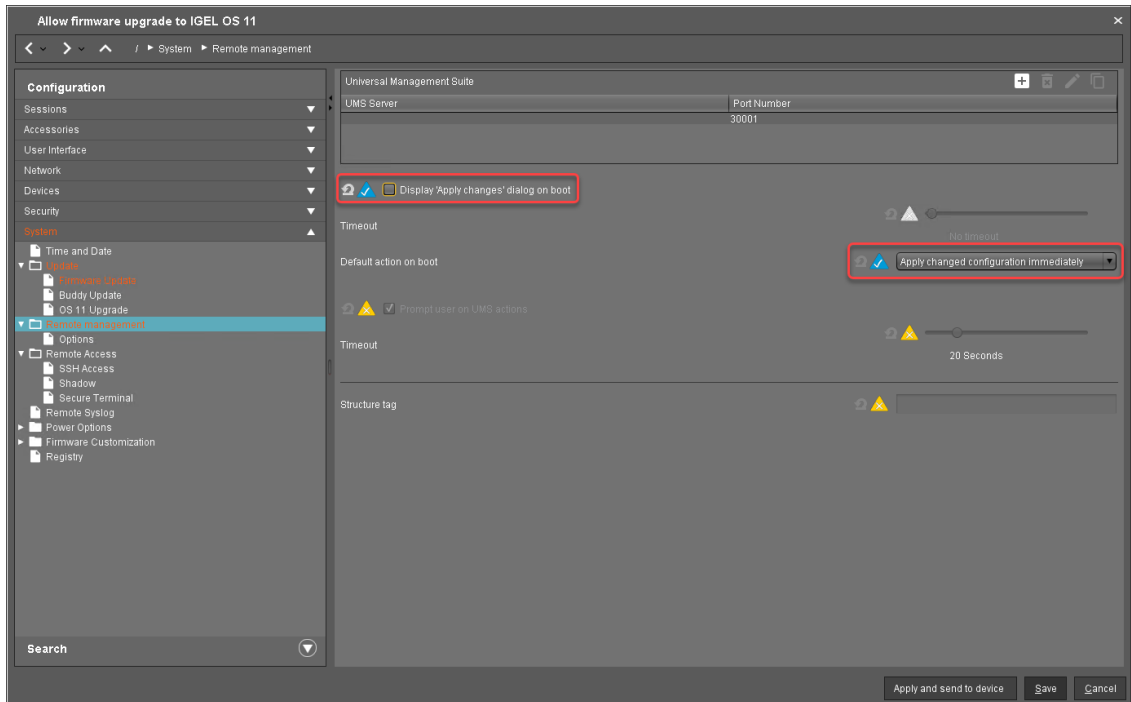


3. Gehen Sie unter **System > Update > OS 11 Upgrade** und ändern Sie die folgenden Einstellungen entsprechend Ihrem erfolgreichen Upgrade-Test (Details zu den Einstellungen finden Sie unter Setup einstellen):
  - Aktivieren Sie **Upgrade to OS 11**.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn PowerTerm aktiviert ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist** nach Ihren Bedürfnissen ein.
  - Stellen Sie **Enterprise Management Pack-Lizenz erforderlich, um Upgrade auf OS 11 durchzuführen** nach Ihren Bedürfnissen ein.

- Stellen Sie sicher, dass **Wartezeit für das Beziehen der OS 11 Lizenz zum automatischen Start des Upgrades auf 10 Minuten** eingestellt ist.



4. Gehen Sie unter **System > Remote Management** und ändern Sie die Einstellung wie folgt:
  - deaktivieren Sie 'Einstellungen anwenden'-Dialog während des Bootvorgangs anzeigen.
  - Setzen Sie **Standardaktion während des Bootvorgangs auf Geänderte Einstellungen sofort anwenden.**



5. Klicken Sie **Ok**.

Wenn das Profil erstellt ist, fahren Sie mit [Lizenzen bereitstellen](#) (see page 184) fort.

### Lizenzen bereitstellen

Stellen Sie die Lizenzen für IGEL OS 11 nach der Methode bereit, die Ihren Anforderungen entspricht:

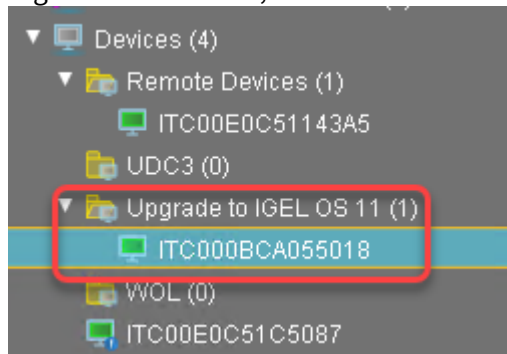
- **Automatic License Deployment (ALD):** Lizenzen werden automatisch erstellt und auf jedem Gerät bereitgestellt, das eine Lizenz benötigt. Anweisungen finden Sie unter Automatic License Deployment (ALD) einrichten.
- **Manual License Deployment:** Lizenzen werden manuell erstellt und bereitgestellt. Anweisungen finden Sie unter Manuelle Lizenz-Bereitstellung für IGEL OS.

Wenn das Lizenz-Deployment aufgesetzt ist, fahren Sie mit [Profil zuordnen](#) (see page 185) fort.



## Profil zuordnen

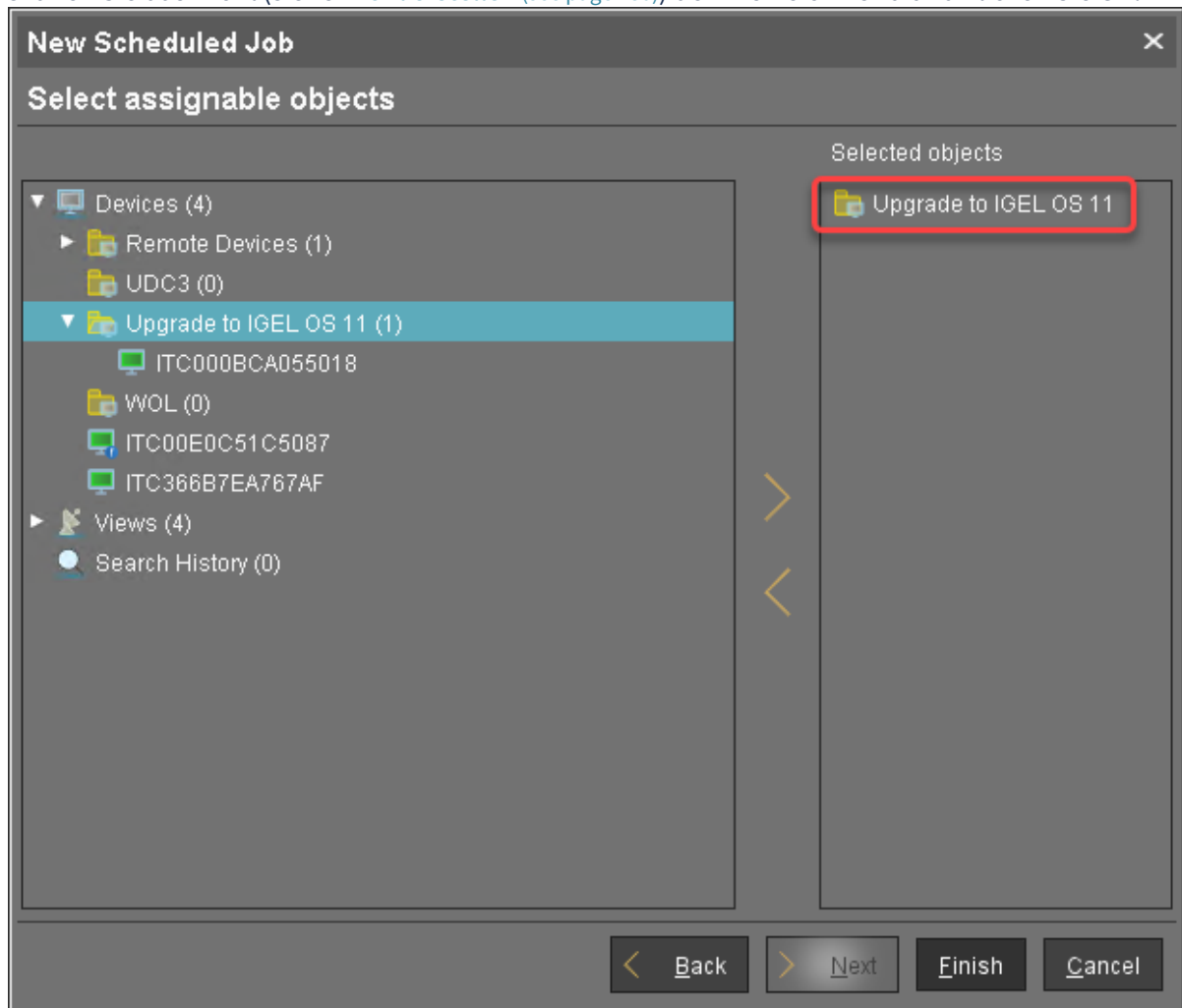
1. Legen Sie alle Geräte, die aktualisiert werden sollen, in ein Verzeichnis.



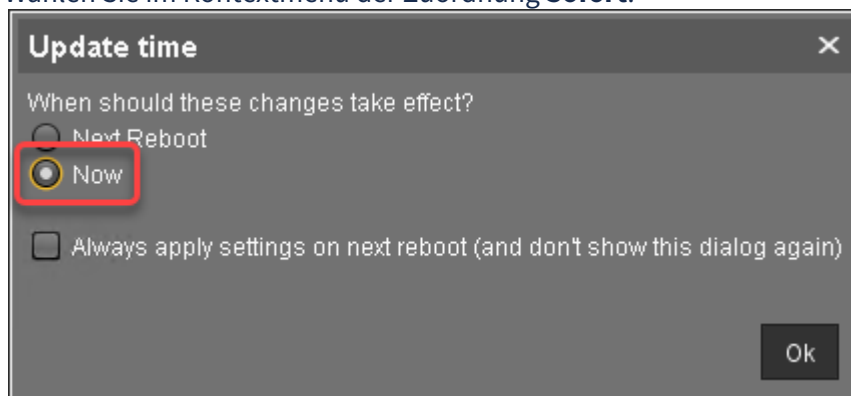
2. Wählen Sie das Verzeichnis aus und klicken Sie  im Bereich **Zugeordnete Objekte**.



3. Ordnen Sie das Profil (siehe [Profil erstellen](#) (see page 180)) dem Verzeichnis zu und klicken Sie **Ok**.



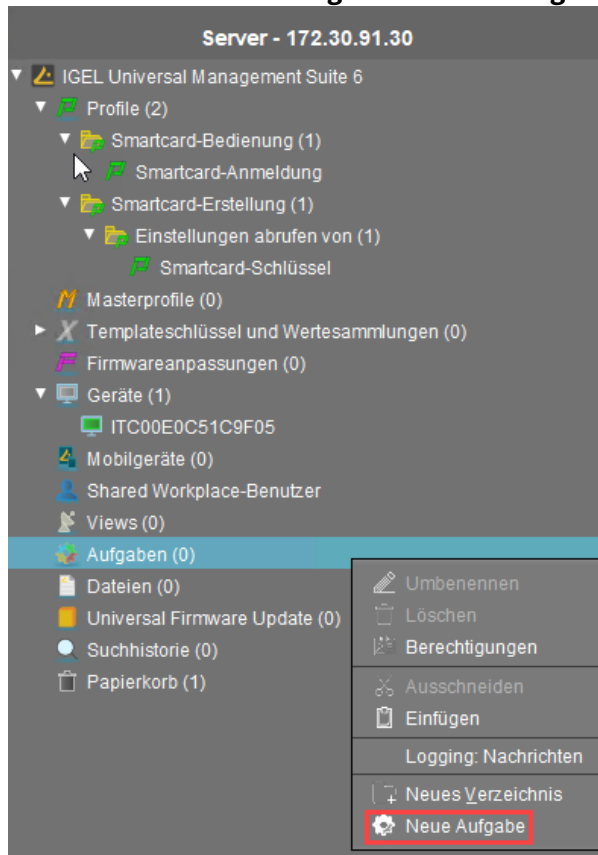
4. Wählen Sie im Kontextmenü der Zuordnung **Sofort**.



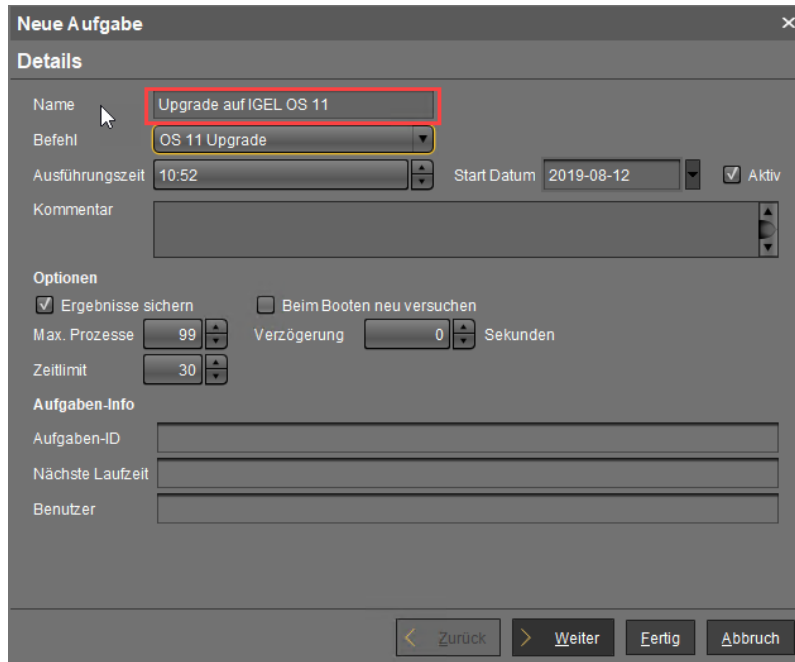
Wenn das Profil zugeordnet ist, fahren Sie mit [Geplante Aufgabe erstellen](#) (see page 187) fort.

Geplante Aufgabe erstellen

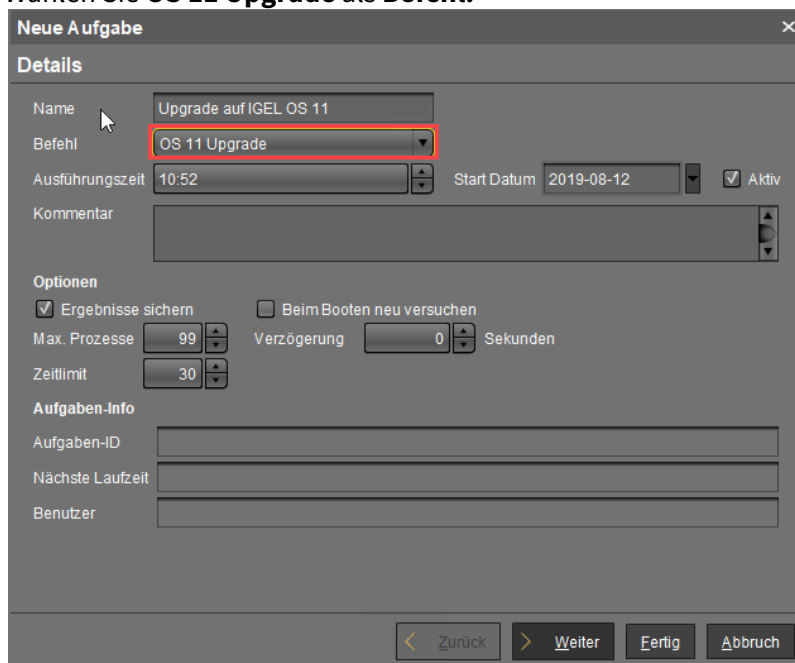
1. Wählen Sie in der UMS **Aufgaben > Neue Aufgabe**.



2. Geben Sie unter **Name** einen geeigneten Namen für die Aufgabe ein, z. B. "Upgrade auf IGEL OS 11".



3. Wählen Sie **OS 11 Upgrade** als **Befehl**.



4. Geben Sie unter **Ausführungszeit** und **Start Datum** die Uhrzeit ein, zu der das Upgrade ausgeführt werden soll, und klicken Sie **Weiter**.

**Neue Aufgabe**

**Details**

Name: Upgrade auf IGEL OS 11

Befehl: OS 11 Upgrade

Ausführungszeit: 10:52 Start Datum: 2019-08-12  Aktiv

Kommentar:

**Optionen**

Ergebnisse sichern  Beim Booten neu versuchen

Max. Prozesse: 99 Verzögerung: 0 Sekunden

Zeitlimit: 30

**Aufgaben-Info**

Aufgaben-ID:

Nächste Laufzeit:

Benutzer:

5. Überprüfen Sie die Ausführungszeit und klicken Sie **Weiter**.

**Neue Aufgabe**

**Zeitplan**

Ausführungszeit: 10:52 Start Datum: 2019-08-12

Ablaufdatum:  Uhrzeit: 10:52

**Aufgabe wiederholen**

Nie

Jeden:  Tag  Stunde

Wochentage:  Mo  Di  Mi  Do  Fr  Sa  So

Feiertage ausschließen:

Datum	Kommentar
-------	-----------

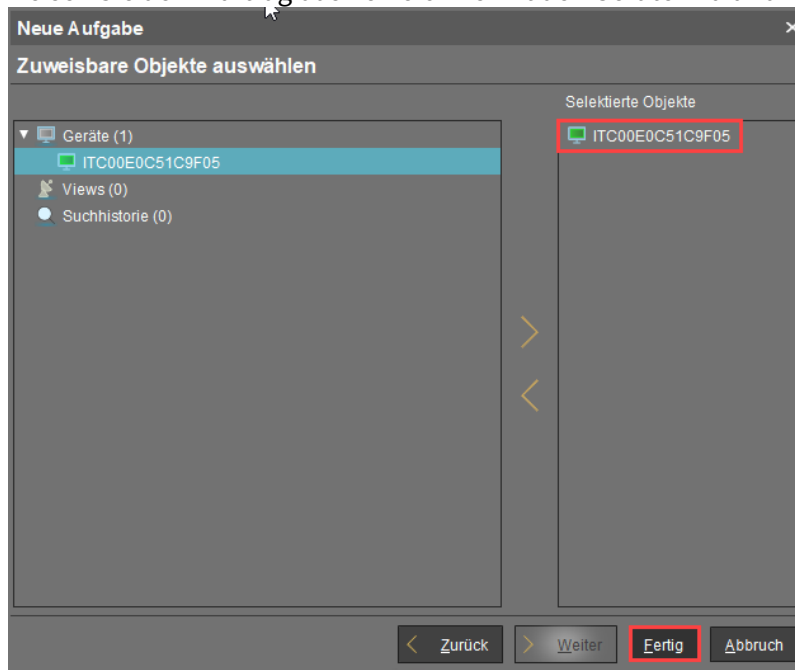
**Ausführung abbrechen**

Nie

Uhrzeit:

Max. Dauer:

6. Weisen Sie dem Auftrag das Verzeichnis mit den Geräten zu und klicken Sie **Fertig**.



## Fehlerbehebung

In diesem Abschnitt werden mögliche Fehlerfälle und Lösungen beschrieben.

- [Funktionsfähiges System wiederherstellen](#) (see page 192)
- [Fehlermeldungen erhalten](#) (see page 193)
- [Neuen Upgradeversuch starten](#) (see page 194)
- [Weiteren Upgradeversuch nach 5 Wiederholungen starten](#) (see page 195)

## Funktionsfähiges System wiederherstellen

Hier finden Sie typische Upgrade-Fehler und die entsprechenden Methoden, um ein funktionsfähiges System wiederherzustellen.

Das Gerät wurde auf Igel OS 11 aktualisiert, bootet aber nicht mehr.

Um ein funktionierendes IGEL OS 11 System zu erhalten:

- ▶ Verwenden Sie den IGEL OS Creator, um das IGEL OS 11-System wiederherzustellen. Weitere Informationen finden Sie im IGEL OS Creator Handbuch.

Das IGEL OS 10 Rettungssystem kann fehlende Partitionen nicht aktualisieren.

Wenn während des Upgrade-Vorgangs ein schwerer Fehler aufgetreten ist, bootet das Gerät in Version 10.05.700 (oder höher) als "Rettungssystem". Wenn das Gerät unbeaufsichtigt ist, versucht es, die fehlenden Partitionen herunterzuladen und zu aktualisieren und startet bei einem Fehler neu.

Um ein komplettes IGEL OS 10 System wiederzuerlangen, haben Sie zwei Möglichkeiten:


- ▶ Starten Sie im Rettungssystem das Setup, gehen Sie zu **System > Update > Firmwareupdate** und stellen Sie eine gültige Updatequelle für die passende IGEL OS 10 Firmwareversion ein (10.05.700 oder höher).

Oder:

- ▶ Konfigurieren Sie ein UMS-Profil, das eine gültige Updatequelle für die passende IGEL OS 10 Firmwareversion ein (10.05.700 oder höher) enthält, unter **System > Update > Firmwareupdate** und weisen Sie es dem Gerät zu.




Fehlermeldungen erhalten

- ▶ Öffnen Sie das OS 11 Upgrade-Tool (Standardpfad: Klicken Sie  und dann auf **Upgrade to OS 11**).

Das OS 11 Upgrade-Tool zeigt eine Fehlermeldung. Der wichtigsten Nachricht ist ein **Retries** vorangestellt, siehe Beispiel unten:



- ▶ Weitere Informationen finden Sie im Hauptmigrationsprotokoll unter `/wfs/migration.log`.

 Sie können den Systemprotokoll-Viewer verwenden, um das Migrationsprotokoll zu überprüfen (Siehe Kapitel Systemprotokolle im IGEL OS Handbuch) oder speichern Sie die Protokolldateien, um sie an das IGEL Support Team zu senden (Finden Sie im Supportkapitel Gerätedateien für den Support speichern).

### Neuen Upgradeversuch starten

Wenn Sie möchten, dass das Gerät mehrere Aktualisierungsversuche startet (und das Gerät nicht bereits dafür konfiguriert ist):

1. Gehen Sie im UMS Profil oder im Setup unter **System > Update > OS 11 Upgrade** und aktivieren Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist.**
2. Starten Sie das Gerät neu.

Weiteren Upgradeversuch nach 5 Wiederholungen starten

Wenn **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist** und das Upgrade jedes Mal fehlgeschlagen ist, stoppt das System den Versuch nach 5 Versuchen.

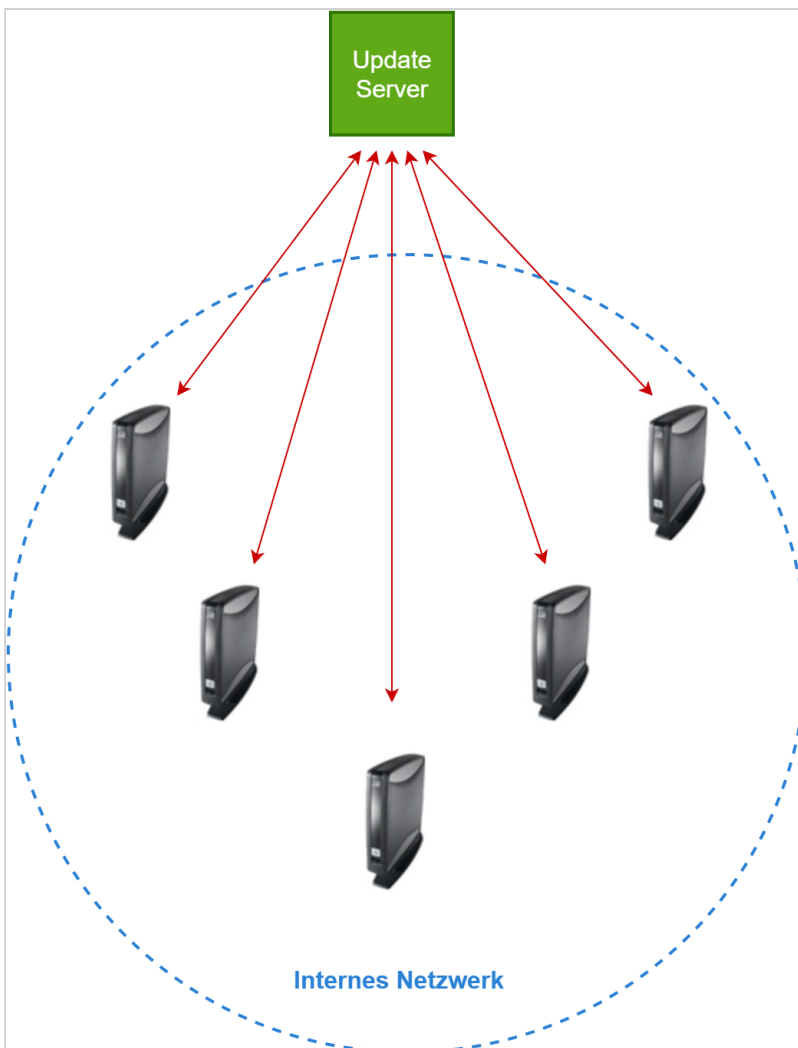
Um den Wiederholungszähler zurückzusetzen:

1. Gehen Sie im Setup oder im UMS-Profil unter **System > Update > OS 11 Upgrade** und deaktivieren Sie das **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist**.
2. Wenn die Einstellung für die Geräte wirksam ist, gehen Sie erneut unter **System > Update > OS 11 Upgrade** und aktivieren Sie **Upgrade auf OS 11 durchführen, auch wenn ein vorausgegangener Versuch fehlgeschlagen ist**.

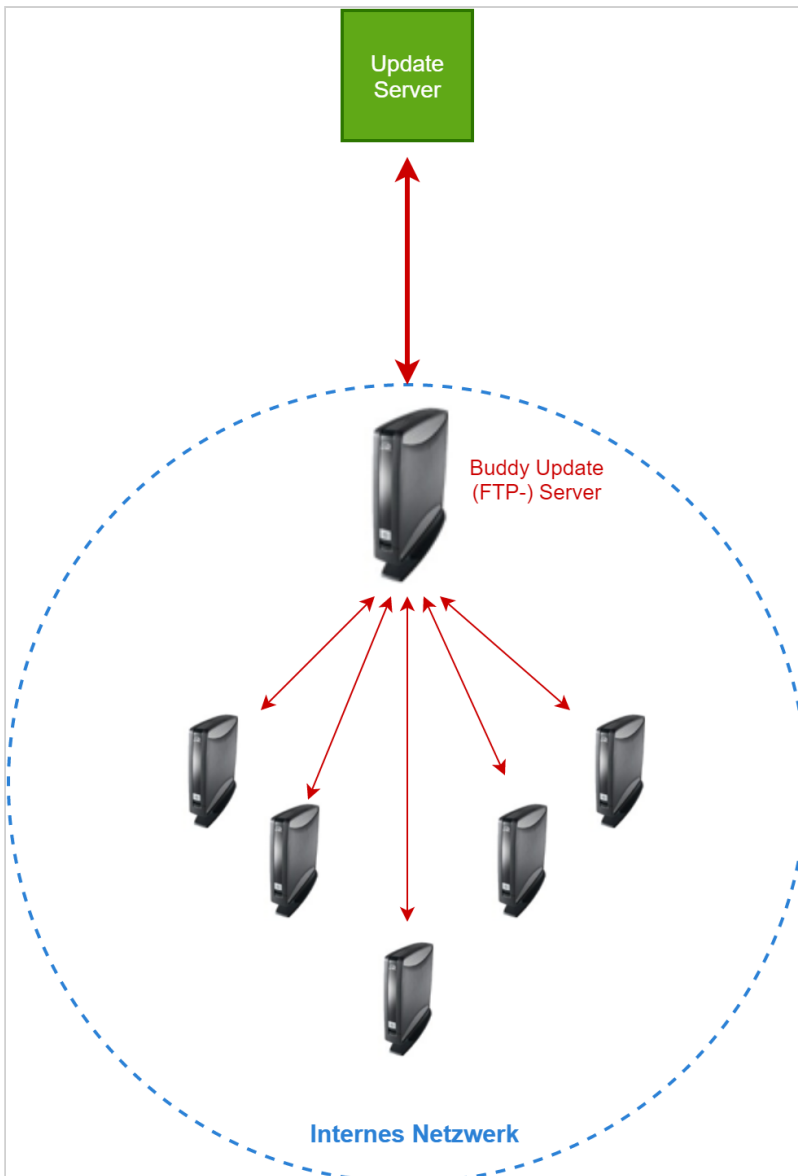
Der Wiederholungszähler wird zurückgesetzt, und die Geräte werden versuchen, bei Bedarf 5 weitere Male ein Upgrade durchzuführen.

## Buddy Update einrichten

Eine bestimmte Anzahl von mit IGEL OS betriebenen Geräten in Ihrem Unternehmen muss regelmäßig aktualisiert werden. Wenn jedes Gerät einzeln, vielleicht sogar über eine große geografische Entfernung, auf den Haupt-Update-Server zugreift, kann das Update sehr lange dauern und die gesamte Verbindung überlasten.



Richten Sie eines Ihrer Geräte als so genannten Buddy Update-Server ein. In Zukunft wird nur noch dieser Client auf den Hauptserver zugreifen, um die Updates herunterzuladen. Alle anderen Clients greifen von innerhalb des Netzwerks auf den lokalen Buddy Update-Server zu und belasten das äußere Netzwerk nicht mehr.



Als Buddy Update-Server wird ausschließlich ein FTP-Server verwendet.

Für Konfigurationsdetails siehe:

- [Buddy Update-Server konfigurieren](#) (see page 199)
- [Buddy Update-Client konfigurieren](#) (see page 201)

## TechChannel



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=IVUIFtOT5uE>


## Buddy Update-Server konfigurieren

### **Kein Downgrade von IGEL OS 11.03**

Ein Downgrade von IGEL OS 11.03 oder höher zu einer Version vor IGEL OS 11.03 ist nicht möglich, außer zu IGEL OS 11.02.200. Dies liegt daran, dass ab IGEL OS 11.03 die Systempartitionen signiert sind, um ihre Integrität zu garantieren; es ist nicht möglich, von einem System mit signierten Partitionen auf ein System mit unsignierten Partitionen zu wechseln. IGEL OS 11.02.200 ist eine spezielle Variante von IGEL OS 11.02, die über signierte Systempartitionen verfügt. IGEL OS 11.02.200 ist nur über das IGEL Support Team erhältlich.

## Grundkonfiguration

1. Gehen Sie im Setup zu **System > Update > Buddy Update**.
2. Aktivieren Sie die Einstellung **Updateserver aktivieren**.
3. Geben Sie bei **Benutzername** und **Passwort** die Anmeldedaten ein.
4. Legen Sie einen Wert für **Max. gleichzeitige Anmeldungen** fest.
5. Klicken Sie **Übernehmen**, um die Änderungen zu übernehmen.
6. Führen Sie ein vollständiges Firmware-Update auf dem Server durch.
7. Starten Sie den Server neu.

 Wenn ein Buddy Update-Server eine Firmwareaktualisierung erhalten hat, muss er neu gestartet werden, bevor er die neue Firmware an andere Geräte verteilen kann.

## Konfiguration für verschiedene Firmwareversionen

Dieses Feature ist für die folgenden Versionen von IGEL OS verfügbar:

- IGEL OS 10: 10.06.100 oder höher
- IGEL OS 11: 11.02.100 oder höher

Wenn Sie eine Umgebung haben, in der es erforderlich ist, dass zwei oder mehr Firmwareversionen gleichzeitig laufen, können Sie die Buddy Update-Methode verwenden, um jeden Buddy Update-Client mit der richtigen Firmwareversion zu versorgen. Ein typischer Anwendungsfall wären zwei Gruppen von Mitarbeitern, von denen die eine eine ältere Version des Browsers oder eine ältere Version des Citrix Receivers benötigt, während die andere Gruppe die neueste Version von IGEL OS erhalten soll. Hierzu werden Server und Clients in Gruppen aufgeteilt. Jeder Gruppe wird eine bestimmte Firmwareversion zugewiesen, indem zuerst diese Version auf den Update-Servern der Gruppe installiert wird. So können Sie beispielsweise IGEL OS 10.07.100 der Gruppe 1 und IGEL OS 10.08.100 der Gruppe 2 zuweisen.

In der nachfolgenden Beschreibung wird aus Gründen der Einfachheit das lokale Setup verwendet; in einer produktiven Umgebung jedoch wird empfohlen, Profile zu verwenden. Weitergehende Informationen siehe Profile.

So weisen Sie einen Server einer Gruppe zu:

1. Konfigurieren Sie den Server wie oben beschrieben ([Grundkonfiguration \(see page 199\)](#)); verwenden Sie dabei die Firmware, die dieser Gruppe zugewiesen ist.
2. Gehen Sie im Setup auf **Registry > update > ftp > buddy\_group\_id**.

3. Setzen Sie im Feld **Buddy Group ID** die richtige Gruppen-ID.
4. Klicken Sie **Ok**.
5. Starten Sie das Gerät neu. Das Gerät stellt die Firmwareaktualisierung für die ihm zugewiesene Gruppe bereit.


Zur Konfiguration des Clients siehe [Buddy Update-Client konfigurieren \(see page 201\)](#), "Konfiguration für verschiedene Firmwareversionen".



## Buddy Update-Client konfigurieren

### Grundkonfiguration

1. Gehen Sie im Setup zu **System > Update > Firmwareupdate**.
2. Legen Sie folgende Einstellungen fest:  
**Servername:** IP-Adresse des Buddy Update-Servers.  
**Port:** 21 (Standardport von FTP)  
**Pfadname auf dem Server:** (Feld leer lassen)  
**Benutzername:** Benutzername des Buddy Update-Servers.  
**Passwort:** Passwort des Buddy Update-Servers.

 Stellen Sie sicher, dass alle Server im Netzwerk die gleichen Zugangsdaten verwenden. Aus Sicherheitsgründen müssen Sie die Zugangsdaten eingeben. Dies ist auch dann erforderlich, wenn Sie keinen bestimmten Server angegeben haben.

3. Aktivieren Sie **Automatische Updatesuche beim Bootvorgang**, wenn Sie wollen, dass der Client beim Bootvorgang automatisch prüft, ob neue Updates auf dem Server verfügbar sind.
4. Aktivieren Sie **Automatische Buddy-Server-Erkennung**, wenn Sie wollen, dass der Client selbständig nach einem Buddy Update-Server sucht.  
Diese Einstellung ist nützlich, wenn Sie mehr als einen Buddy Update-Server betreiben und keinen bestimmten festlegen möchten.  
Wenn Sie keinen bestimmten Server festlegen möchten, dann lassen Sie die Felder **Servername** und **Port** sowie **Pfadname auf dem Server** leer. Falls Sie dennoch einen Servernamen festlegen, wird das System diesen als Fallback-Wert verwenden. Somit können Sie sicher sein, dass das System auf jeden Fall diesen einen Server findet, falls es keine anderen findet.

### Konfiguration für verschiedene Firmwareversionen

Dieses Feature ist für die folgenden Versionen von IGEL verfügbar:

- IGEL OS 10: 10.06.100 oder höher
- IGEL OS 11: 11.02.100 or höher

Das Feature ist beschrieben unter [Buddy Update-Server konfigurieren \(see page 199\)](#), "Konfiguration für verschiedene Firmwareversionen".

In der nachfolgenden Beschreibung wird aus Gründen der Einfachheit das lokale Setup verwendet; in einer produktiven Umgebung jedoch wird empfohlen, Profile zu verwenden. Weitergehende Informationen siehe Profile.

So weisen Sie einen Client einer Gruppe zu:

1. Gehen Sie im Setup zu **Registry > update > ftp > buddy\_group\_id**.
2. Geben Sie im Feld **Buddy-Gruppen-ID** die ID der Gruppe ein, welcher die gewünschte Firmware zugewiesen ist.
3. Klicken Sie **Ok**.
4. Starten Sie das Gerät neu.  
Das Gerät verwendet die Firmwareaktualisierung für die Gruppe, der das Gerät zugewiesen ist.

## Serverlast ausbalancieren

Dieses Feature ist für die folgenden Versionen von IGEL verfügbar:

- IGEL OS 10: 10.06.100 oder höher
- IGEL OS 11: 11.02.100 oder höher

Es ist möglich, die Last zwischen verschiedenen Buddy Update-Servern auszubalancieren. Wenn **System > Update > Firmwareupdate > Automatische Buddy-Server-Erkennung** aktiviert ist, senden die Clients einen Broadcast in ihrem Netzwerk, um herauszufinden, welche Buddy-Server verfügbar sind. Jeder Server, der innerhalb eines festgelegten Timeouts antwortet, wird einer Liste hinzugefügt, deren Maximallänge festgelegt werden kann. Wenn die Liste vollständig ist, entweder weil ihre Maximallänge erreicht ist oder weil der Timeout abgelaufen ist, wählt der Client einen zufälligen Server aus der Liste aus. Auf diese Weise wird die Last der Buddy-Server gleichmäßig verteilt.

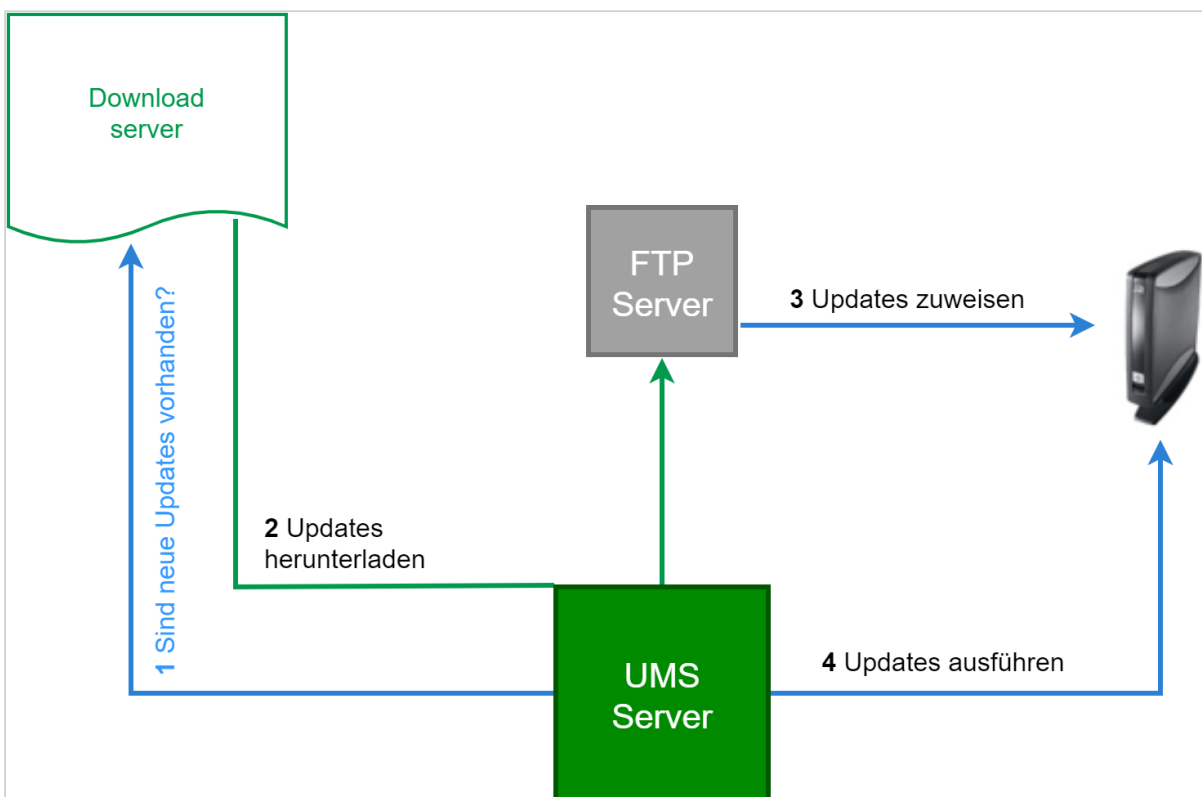
So konfigurieren Sie einen Client für das Ausbalancieren der Serverlast:

1. Gehen Sie im Setup auf **Registry > update > ftp > buddy\_server\_candidates**.
2. Geben Sie im Feld **Buddy Update Server Candidates** die maximale Anzahl von Servern ein, die der Client auflisten soll. Wenn die Anzahl 1 ist, wird der Server ausgewählt, der als erster antwortet.
3. Klicken Sie **Ok**.
4. Starten Sie das Gerät neu.

## Firmwareupdate

Hier zeigen wir Ihnen den idealen Weg, wie Sie ein Firmwareupdate von unserem [Downloadserver](#)<sup>21</sup> herunterladen und an verschiedene Thin Clients in Ihrem Unternehmen verteilen können:

1. Gehen Sie auf unseren [Downloadserver](#)<sup>22</sup> und prüfen Sie, ob ein Update verfügbar ist, das Ihren Anforderungen entspricht.
2. Laden Sie die relevante Updatedateien herunter.
3. Installieren Sie für die Dateien ein Update-Verzeichnis im UMS Server oder in Ihrem FTP-Server.
4. Ordnen Sie dieses Updateverzeichnis Ihrem Gerät zu.
5. Starten Sie den Updateprozess manuell oder über einen [Aktualisierungsprozess](#) (see page 206).



- [Updates herunterladen und auf einem FTP Server speichern](#) (see page 204)
- [Aktualisierungsprozess ausführen](#) (see page 206)

<sup>21</sup> <https://www.igel.com/software-downloads/>

<sup>22</sup> <https://www.igel.com/software-downloads/>

## Updates herunterladen und auf einem FTP Server speichern

Sie können Ihre Update-Datei entweder direkt auf dem UMS-Server oder auf Ihren firmeneigenen FTP-Server speichern. Wenn Sie viele Geräte aktualisieren müssen, sollten Sie mit dem FTP-Server arbeiten, da dies die Verteilung von großen Datenmengen im lokalen Netzwerk erleichtert.

### **Kein Downgrade von IGEL OS 11.03**

Ein Downgrade von IGEL OS 11.03 oder höher zu einer Version vor IGEL OS 11.03 ist nicht möglich, außer zu IGEL OS 11.02.200. Dies liegt daran, dass ab IGEL OS 11.03 die Systempartitionen signiert sind, um ihre Integrität zu garantieren; es ist nicht möglich, von einem System mit signierten Partitionen auf ein System mit unsignierten Partitionen zu wechseln. IGEL OS 11.02.200 ist eine spezielle Variante von IGEL OS 11.02, die über signierte Systempartitionen verfügt. IGEL OS 11.02.200 ist nur über das IGEL Support Team erhältlich.

### **Wichtiger Hinweis zum Downgrade von IGEL OS 11.06 oder höher**

- Wenn Sie Ihr IGEL OS 11.06-Gerät verschlüsselt haben, führt ein Downgrade auf IGEL OS 11.05 oder niedriger aufgrund unterschiedlicher Partitionsschemata zu einem Datenverlust auf den folgenden Partitionen:
  - Browsing-Verlauf der Browser Firefox und Chromium
  - Custom Partitions
- Die Geräteeinstellungen und die UMS-Verbindung bleiben erhalten.
- Das Passwort für die Geräteverschlüsselung muss vom Benutzer eingegeben werden.

## Vorbereitung

1. Klicken Sie auf Ihrer UMS Console in der UMS Administration auf **Universal Firmware Update**.
2. Klicken Sie **Editieren...**
3. Geben Sie unter **Host** Ihren FTP-Server ein, um die Update-Datei in diesem Speicherort zu sichern.
4. Fügen Sie weiter Details, wie Speicherpfad und Zugriffsdaten für den Server hinzu.
5. Sichern Sie Ihre Einstellung und klicken Sie **Serververbindung testen**.

## Update herunterladen


1. Rechtsklicken Sie auf **Universal Firmware Update**.
2. Wählen Sie im Kontextmenü **Auf neue Firmware Updates überprüfen**
3. Wählen Sie eine **Version** in der Auswahlliste.
4. Klicken Sie **Information**, um die Versionshinweise der einzelnen Updates anzuzeigen.
5. Aktivieren Sie das Auswahlkästchen **Hinzufügen**, um ein bestimmtes Update herunterzuladen.
6. Klicken Sie **Download**, um den Prozess zu starten.  
Das Update wird zum Strukturbaum hinzugefügt und der aktuelle Prozessstatus wird angezeigt. Die entpackten Firmware-Dateien befinden sich schließlich im Zielverzeichnis auf dem FTP-Server.

## Updates den Geräten zuweisen

Fügen Sie das heruntergeladene Update per Drag & Drop Ihrem Geräteverzeichnis hinzu. Wenn Sie nun auf das Verzeichnis klicken, sehen Sie das Firmware-Update im rechten Fenster unter **Zugeordnete Objekte**. Die Geräte wissen nun, wo sie im Falle eines Aktualisierungsbefehls das Firmware-Update finden.

## Aktualisierungsprozess ausführen

1. Erstellen Sie eine oder mehrere neue **View** um zu unterscheiden, welche Geräte das neue Upgrade bekommen.
2. Erstellen Sie einen neuen **Aufgabe** und geben Sie ihr einen Namen, z. B. "Firmware Update".
3. Klicken Sie **Weiter**.
4. Geben Sie im Dialog **Zeitplan** an, wann die Aktualisierung durchgeführt werden soll.

 Die Option **Aufgabe wiederholen** sollte nicht für die Befehle **Update**, **Update on boot** oder **Update on shutdown** aktiviert sein.

5. Fügen Sie im Dialog **Zuweisbare Objekte auswählen** eine oder mehrere **Views** hinzu.
6. Speichern Sie den Job.

Der Updateprozess wird gemäß dem im Auftrag angegebenen Zeitplan durchgeführt.

### **Update kann nach Timeout abgebrochen werden**

Ein laufendes Update kann vom Benutzer abgebrochen werden, wenn der Status "network online" nicht innerhalb von 10 Sekunden nach Beginn des Firmware-Updates erreicht werden konnte. Wenn der Benutzer das Update abgebrochen hat, wird die normale Desktop-Umgebung gestartet, genau wie vor dem Update. Dies gilt für die folgenden Fälle:

- Normales Firmware-Update, z.B. von IGEL OS 10.03.500 to IGEL OS 11.04
- Ein Feature wurde aktiviert, z.B. VPN OpenConnect.
- Eine Custom Partition wurde aktiviert oder geändert.

## IGEL OS mit einem USB-Gerät aktualisieren


Sie können ein USB-Speichergerät zum lokalen Aktualisieren von IGEL OS verwenden. Dieses Verfahren ist besonders geeignet, wenn nur ein Gerät oder nur wenige Geräte aktualisiert werden sollen und es sich nicht lohnt, einen FTP- oder HTTP-Server für das Update zu installieren.

Um die Firmware des Geräts ohne Zugriff auf das lokale Setup zu aktualisieren, lesen Sie bitte [Firmware über die Linux-Konsole aktualisieren](#) (see page 209).

---

Gehen Sie wie folgt vor, um IGEL OS über ein USB-Speichergerät zu aktualisieren:

1. Laden Sie die Update-Datei (.zip) für Ihr Gerät vom [IGEL Download Server](#)<sup>23</sup> herunter.
2. Entpacken Sie die Update-Dateien und speichern Sie diese auf einem USB-Speichergerät.

 Die offiziell unterstützten Dateisysteme finden Sie unter Hotplug-Speichergerät.

3. Öffnen Sie das IGEL Setup auf dem Gerät und wählen Sie die Option **Geräte > Speichergeräte > Hotplug-Speichergeräte**.
4. Setzen Sie **Laufwerkszuordnung** auf **Statisch**.
5. Aktivieren Sie **Eigener Laufwerksbuchstabe für Speicherlaufwerke**.
6. Setzen Sie **Zahl der Laufwerke** auf mindestens 1.
7. Klicken Sie **Übernehmen**, so dass die Änderungen für das Gerät wirksam sind.

 Weitere Informationen finden Sie im Kapitel Hotplug-Speichergerät.

8. Verbinden Sie das USB-Speichergerät mit dem Gerät und warten Sie, bis das USB-Speichergerät erkannt wurde.
9. Wählen Sie **System > Update > Firmwareupdate**.
10. Setzen Sie **Protokoll** auf **DATEI**.

11. Starten Sie die Dateiauswahl (**Pfadname auf dem Server**), navigieren Sie zu `/userhome/  
media/Label des USB-Speichergeräts/lxos.inf` und klicken Sie **Öffnen**.

 Verwenden Sie KEINE Leerzeichen im Namen des USB-Geräts.

---

<sup>23</sup> <https://www.igel.com/software-downloads/workspace-edition/>

12. Klicken Sie auf **Firmware aktualisieren** und bestätigen Sie die Warnmeldung.  
Das Gerät wird beim Aktualisieren der Firmware neu gestartet. Entfernen Sie das USB-Gerät erst, wenn das Update abgeschlossen ist.

 Achten Sie darauf, dass Sie nicht vom USB-Speichergerät starten. Möglicherweise müssen Sie die Startreihenfolge im BIOS/UEFI ändern.



## Firmware über die Linux-Konsole aktualisieren

Das Firmware-Update des Geräts kann auch direkt auf der Linux-Konsole selbst ohne IGEL-Setup durchgeführt werden:

1. Starten Sie das Gerät neu.
2. Drücken Sie die [ESC]-Taste während des Neustarts um in das Boot-Menü zu gelangen.
3. Wählen Sie **Komplexer Boot** des Boot-Menüs.
4. Bei Aufforderung, wechseln Sie die Konsole indem Sie [CTRL-ALT-F11] oder [CTRL-ALT-F12] drücken.
5. Drücken Sie die [RETURN]-Taste um sich anzumelden.  
Sie müssen gegebenenfalls Ihr Passwort eingeben

Führen Sie die Aktualisierung durch: Die genaue Vorgehensweise hängt von dem zu verwendenden Protokoll ab, d. h. FILE, HTTP oder FTP; siehe die folgenden Anweisungen. Mit dem Befehl `get` können Sie überprüfen, ob die korrekten Parameterwerte übergeben wurden. z. B. `get update.protocol`

### HTTP

1. Richten Sie bei Bedarf eine statische IP-Adresse ein (DHCP ist standardmäßig aktiv)  
`setparam network.interfaces.ethernet.device0.usedhcp false`  
`setparam network.interfaces.ethernet.device0.manual true`  
`setparam network.interfaces.ethernet.device0.ipaddr`  
`setparam network.interfaces.ethernet.device0.netmask`
2. Den Update Servers konfigurieren  
`setparam update.protocol http`  
`setparam update.http.server`  
`setparam update.http.port`

 Der Standard UMS-Port ist 9080

```
setparam update.http.path
setparam update.http.user
setcryptparam update.http.crypt_password
```

3. Starten Sie den Aktualisierungsvorgang im Verzeichnis `/` mit dem Befehl `update`

## FTP


1. Richten Sie bei Bedarf eine statische IP-Adresse ein (DHCP ist standardmäßig aktiv)  
`setparam network.interfaces.ethernet.device0.usedhcp false`  
`setparam network.interfaces.ethernet.device0.manual true`  
`setparam network.interfaces.ethernet.device0.ipaddr`  
`setparam network.interfaces.ethernet.device0.netmask`
2. Update Servers konfigurieren  
`setparam update.protocol ftp`  
`setparam update.ftp.server`  
`setparam update.ftp.port`

 Der Standard Port ist 21

```
setparam update.ftp.path
setparam update.ftp.user
setcryptparam update.ftp.crypt_password
```

3. Starten Sie den Aktualisierungsvorgang im Verzeichnis / mit dem Befehl `update`


## FILE

 Voraussetzung: Die nicht komprimierten Aktualisierungsdateien befinden sich im Stammverzeichnis eines FAT32-formatierten USB-Speichergeräts.


1. Konfigurieren Sie mindestens ein Hotplug USB-Gerät:  
`setparam devices.hotplug.usb-storage.numdevices 1`
2. Übernehmen Sie Ihre Änderungen:  
`kill_postsetupd`
3. Verbinden Sie das USB-Speichergerät mit dem Gerät.
4. Warten Sie, bis das USB-Speichergerät automatisch eingelegt wird.
5. Bestimmen Sie den Befestigungspunkt:  
`ls /media/`
6. Konfigurieren Sie die Aktualisierungs-Parameter:  
`setparam update.protocol file`  
`setparam update.file.path /media/<name of USB storage device>`

7. Starten Sie den Aktualisierungsvorgang im Verzeichnis `/` mit dem Befehl `update`


## Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Error: "legacy ICG Root (CA) certificate" When Updating to Igel OS 11.04 on Devices Connected via ICG

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Device Does Not Connect to ICG after Update to IGEL OS 11.04 or Higher

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Automatic Update Service


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## BIOS Tools


- [BIOS Tools for Selected HP Devices \(see page 217\)](#)
- [BIOS Update for Devices Supported by LVFS \(see page 218\)](#)



## BIOS Tools for Selected HP Devices

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## BIOS Update for Devices Supported by LVFS

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Citrix

- [Performanz \(see page 220\)](#)
- [Maus \(see page 225\)](#)
- [Citrix Native USB Redirection konfigurieren \(see page 232\)](#)
- [Citrix Fabulatech Scanner Redirection in IGEL OS \(see page 234\)](#)
- [USB-Speichergerät in Citrix Sitzungen bereitstellen \(see page 236\)](#)
- [Symbolleiste im Appliance-Modus automatisch ausblenden \(see page 238\)](#)
- [Eine nahtlos, transparente Benutzeroberfläche mit dem Appliance-Modus erstellen \(see page 239\)](#)
- [Verbindung zu Citrix-Farm herstellen \(see page 240\)](#)
- [Ein Self-Service-Setup mit Hilfe von Schnelleinstellungen erstellen \(see page 247\)](#)
- [Anmeldung fehlgeschlagen aufgrund des abgelaufenen AD-Passworts \(see page 249\)](#)
- [Automatisches Anmelden für Citrix Virtual Desktops konfigurieren \(see page 251\)](#)
- [Citrix-Abmeldung per Hotkey erzwingen \(see page 256\)](#)
- [Warnmeldung: \[Citrix Store\] kann sich nicht mit dem Citrix-Server verbinden \(see page 257\)](#)
- [Citrix-Sitzungen mit hardwarebeschleunigtem H.264 Deep Compression Codec einrichten \(see page 259\)](#)
- [Using Font Smoothing \(ClearType\) in Citrix Sessions](#)
- [Hochsicherer XenServer hat Probleme mit dem LD\\_BIND\\_NOW Workaround \(see page 260\)](#)
- [Fehlerbehebung für Citrix Receiver X-Fehler \(see page 261\)](#)
- [Problem mit Citrix HTML5 Receiver \(see page 262\)](#)
- [Tastaturbelegung für Macbook innerhalb der Citrix Sitzung \(see page 263\)](#)
- [Citrix Feature Matrix \(see page 264\)](#)
- [Lync / Skype for Business mit Citrix HDX RealTime Optimization Pack verwenden \(see page 265\)](#)
- [Citrix Advanced Endpoint Analysis \(EPA\) Client on IGEL OS \(see page 266\)](#)
- [Citrix Netscaler Gateway Client \(NSGClient\) for Netscaler VPN Connections \(see page 267\)](#)
- [Unexpected Keyboard Layout in a Citrix Session \(see page 268\)](#)

## Performanz

- [Schlechte Performanz: Schwarze Blöcke und Streifen in Citrix Sitzungen \(see page 221\)](#)
- [Schlechte Leistung mit Citrix XenDesktop 7.6 Deep Compression \(see page 222\)](#)
- [Citrix: Graue Blöcke in Excel 2013 \(see page 223\)](#)
- [Das Scannen von Barcodes ist über Citrix langsam \(see page 224\)](#)

## Schlechte Performanz: Schwarze Blöcke und Streifen in Citrix Sitzungen

### Symptom

In der Citrix Sitzung sind manchmal schwarze Blöcke, Rahmen oder Streifen zu beobachten.

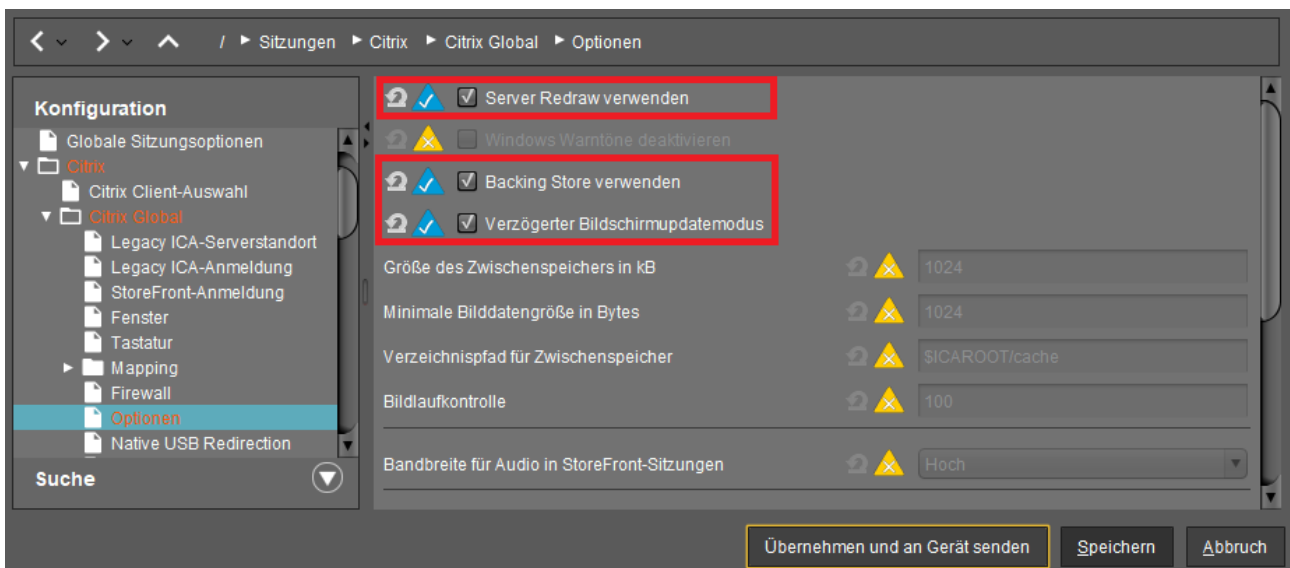
### Problem

Schlechte Performanz ist häufig mit der verzögerten oder langsamen Aktualisierung der Bildschirm Inhalte verbunden.

### Lösung

► In IGEL Setup oder im Konfigurationsdialog in der UMS aktivieren Sie alle oder einen der folgenden Parameter unter **Sitzungen > Citrix > Citrix Global > Optionen**:

- **Server Redraw verwenden**
- **Backing Store verwenden**
- **Verzögerter Bildschirmupdatemodus**



Siehe auch Optionen im Handbuchkapitel für Citrix.

 Wenn dies nicht funktioniert, sehen Sie auch [Schwarze Box neben dem Mauszeiger](#) (see page 231).

## Schlechte Leistung mit Citrix XenDesktop 7.6 Deep Compression

### Symptom

Bei der Verwendung von XenDesktop 7.6 auf Windows Server 2008R2 mit Citrix Receiver 13.0.4, 13.1.4 oder 13.2.1 mit H.264 Deep Compression Codec wird die Windows-Verzögerung verschoben und die Leistung ist im Allgemeinen schlecht.

### Problem

Server und/oder Client haben nicht genügend Rechenleistung für den H.264 Deep Compression Codec.

### Lösung

Aktivieren Sie den Legacy-Grafikmodus auf dem XenDesktop 7.6-Server über eine Richtlinie.

## Citrix: Graue Blöcke in Excel 2013

### Symptom

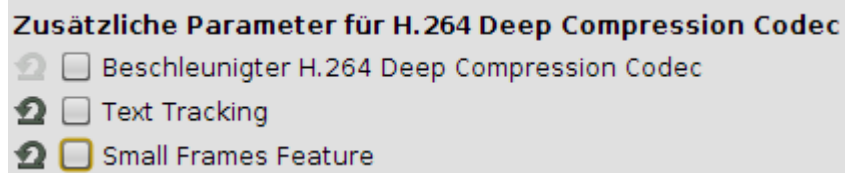
Bei der Verwendung von Microsoft Excel 2013 auf XenDesktop 7.6 mit Citrix Receiver 13.1.3, 13.1.4 oder 13.2 erscheinen graue Blöcke, insbesondere wenn Sie mehrere Zellen markieren.

### Problem

Codec-Parameter sind für diesen Anwendungsfall möglicherweise nicht optimal.

### Lösung

1. Gehen Sie im IGEL Setup unter **Sitzungen > Citrix > Citrix Global > Codec**.
2. Deaktivieren Sie **Text Tracking**.
3. Deaktivieren Sie **Small Frames Feature**.



## Das Scannen von Barcodes ist über Citrix langsam

### Lösung beruht auf Erfahrungen im Feld

Dieser Artikel stellt eine Lösung bereit, die nicht durch die IGEL Forschungs- und Entwicklungsabteilung geprüft wurde. Daher kann IGEL keinen offiziellen Support leisten. Soweit durchführbar, testen Sie die Lösung, bevor Sie diese in einer Produktivumgebung zum Einsatz bringen.

### Problem

Das Scannen von Strichcodes ist über Citrix langsam.

### Umgebung

- Firmware Version: Jede
- UMS Version: Jede

### Beschreibung

Der USB-fähige Barcodescanner ist über Citrix sehr langsam.

### Lösung

Um den Barcodescanner korrekt zu lesen, möchten Sie, dass es sich um eine HID handelt, so dass er als HID durchläuft, anstatt die Native USB-Umleitung zu verwenden. Eine schnelle Möglichkeit, dies zu ermitteln, besteht darin, ein Terminal in IGEL OS zu öffnen und einfach etwas zu scannen. Wenn es Daten im Terminal füllt, dann ist es als HID konfiguriert. Lesen Sie auch die Konfigurationsanleitung für den jeweiligen Scanner, den Sie verwenden. Die Konfigurationsanleitung ist einfach ein Bündel von Barcodes, die das Gerät scannen kann. Sobald ein Code gescannt wurde, piept das Gerät zweimal und das ändert die Konfiguration auf dem Scanner. Auf einigen Geräten gibt es eine Einstellung für Alternate OS Linux/MACOS. In der Standardeinstellung des Scanners ist dies in der Regel nicht aktiviert. Nachdem die Einstellung vorgenommen wurde, wurde alles sehr schnell gescannt und in der gleichen Geschwindigkeit in Citrix angezeigt.



## Maus

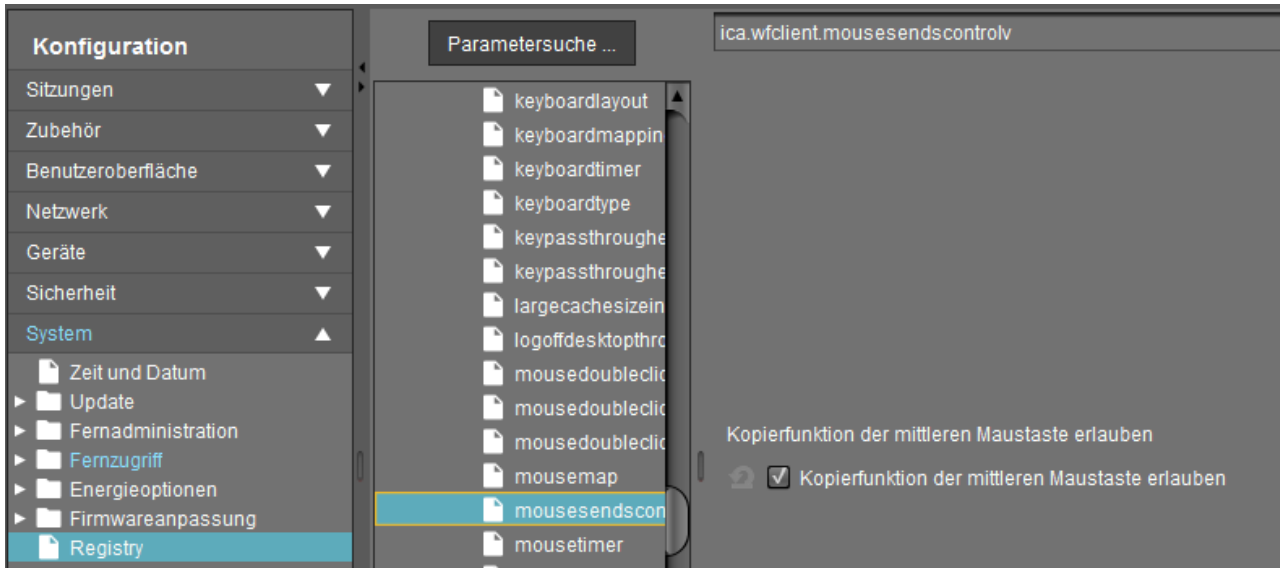
- [Mittlere Maustastenfunktion für Citrix Sitzung und lokalen Firefox Browser ändern \(see page 226\)](#)
- [Verwendung einer SpaceMouse in einer Citrix Sitzung \(see page 227\)](#)
- [SpaceMouse USB Reset Problem lösen \(see page 229\)](#)
- [Kabellose Maus-Tastatur-Set Logitech k520 friert in Citrix Sitzung ein \(see page 230\)](#)
- [Schwarze Box neben dem Mauszeiger \(see page 231\)](#)

## Mittlere Maustastenfunktion für Citrix Sitzung und lokalen Firefox Browser ändern

Die mittlere Maustaste kann nicht für ein reibungsloses Scrollen in Anwendungen wie Excel oder Internet Explorer innerhalb einer Citrix-Sitzung oder mit dem lokalen Firefox Browser verwendet werden.

Die Standardfunktion der mittleren Maustaste ist kopieren und einfügen.

- ▶ Öffnen Sie die IGEL Registry im lokalen Setup.



- ▶ Für Citrix Sitzungen:
  - **System > Registry > ica.wfclient.mousesendscontrolv**
- ▶ Für lokalen Firefox Browser:
  - **System > Registry > browserglobal.app.middlemouse\_contentloadurl**
  - **System > Registry > browserglobal.app.middlemouse\_paste**

Mehr Information über die Firefox Parameter finden sie unter:


<http://kb.mozillazine.org/Middlemouse.contentLoadURL>


<http://kb.mozillazine.org/Middlemouse.paste>

Die Änderungen werden nach dem Neustart des Thin Clients wirksam.

## Verwendung einer SpaceMouse in einer Citrix Sitzung

Dieser Artikel beschreibt, wie Sie eine 3Dconnexion SpaceMouse in einer Citrix Sitzung verwenden.

 Verwenden Sie eine SpaceMouse ausschließlich als eine zusätzliche, d.h. zweite, Maus.

 Ab **Version 10.06.100** und **11.02.100** stört die SpaceMouse den lokalen Mauszeiger nicht mehr, da ein Registry Key standardmäßig aktiviert ist.

Dieser Registry Key ignoriert die SpaceMouse für die IGEL grafische Benutzeroberfläche:

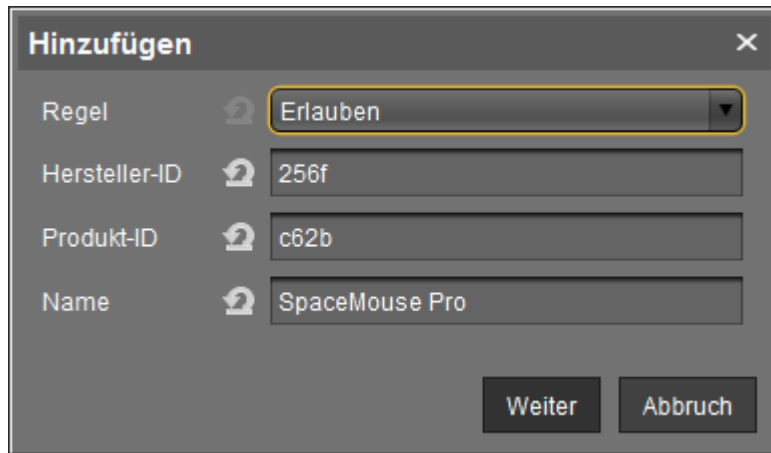
IGEL Setup	System > Registry
Parameter	Deactivates 3Dconnexion/Logitech SpaceMouse products as a standard mouse
Registry Key	userinterface.mouse.spacemouse.x11_ignore
Wert	aktiviert/deaktiviert
Info	"aktiviert" bedeutet, dass die SpaceMouse an die Sitzung weitergeleitet und von der lokalen GUI ignoriert wird. "deaktiviert" bedeutet, dass die SpaceMouse auch für die lokale GUI verwendet wird.

So konfigurieren Sie die SpaceMouse für Citrix Sitzungen:


1. Gehen Sie im Setup zu **Sitzungen > Citrix > Citrix Global > Native USB Redirection**.
2. Aktivieren Sie das Kontrollkästchen **Native USB Redirection**.
3. Setzen Sie die **Vorgaberegeln** auf **Verbieten**.
4. Fügen Sie eine Geräteausnahmeregel wie im folgenden Screenshot mit der Hersteller- und Produkt-ID Ihrer spezifischen SpaceMouse hinzu:


**SpaceMouse-Produkte, die enthalten sind (Hersteller-ID, Produkt-ID, Hersteller, Produkt)**


- 0x046D; 0xC603; Logitech, Inc.; 3Dconnexion Spacemouse Plus XT
- 0x046D; 0xC605; Logitech, Inc.; 3Dconnexion CADman
- 0x046D; 0xC606; Logitech, Inc.; 3Dconnexion Spacemouse Classic
- 0x046D; 0xC621; Logitech, Inc.; 3Dconnexion Spaceball 5000
- 0x046D; 0xC623; Logitech, Inc.; 3Dconnexion Space Traveller 3D Mouse
- 0x046D; 0xC625; Logitech, Inc.; 3Dconnexion Space Pilot 3D Mouse
- 0x046D; 0xC626; Logitech, Inc.; 3Dconnexion Space Navigator 3D Mouse
- 0x046D; 0xC627; Logitech, Inc.; 3Dconnexion Space Explorer 3D Mouse
- 0x046D; 0xC628; Logitech, Inc.; 3Dconnexion Space Navigator for Notebooks
- 0x046D; 0xC629; Logitech, Inc.; 3Dconnexion SpacePilot Pro 3D Mouse
- 0x046D; 0xC62B; Logitech, Inc.; 3Dconnexion Space Mouse Pro
- 0x256F; \*; 3Dconnexion; SpaceMouse




**Hinzufügen** [X]

Regel  Erlauben

Hersteller-ID  256f

Produkt-ID  c62b

Name  SpaceMouse Pro

[Weiter] [Abbruch]

5. Speichern Sie die Einstellungen.

Jetzt ist die SpaceMouse betriebsbereit.

-  Um zu erreichen, dass sich die Maus in CAD-Programmen wie gewohnt verhält, ändern Sie die Konfiguration wie folgt:
1. Gehen Sie zu **IGEL Setup > System > Registry > ica.wfclient.mousesendscontrolv.**
  2. Setzen Sie den Parameter auf **deaktivieren**.

-  Wenn die SpaceMouse nach der vorherigen Citrix Sitzung nicht ordnungsgemäß funktioniert, muss zusätzlich der USB Reset konfiguriert werden. Folgen Sie die Anleitungen unter [Solve 3Dconnexion SpaceMouse USB Reset Problem](#) (see page 229).

## SpaceMouse USB Reset Problem lösen

### Umgebung

Gültig für IGEL Hardware H850C, H830C und M340C

### Problem

Nach einer vorherigen Citrix Sitzung funktioniert die SpaceMouse nicht mehr richtig (z. B. findet nach Beendigung der Citrix Sitzung kein Reset der SpaceMouse statt; infolgedessen bleibt das Display der SpaceMouse immer leuchtend).

### Lösung

Verwenden Sie einen Power-Cycle-Befehl, um alle USB-Geräte automatisch aus- und wieder einzuschalten:

1. Gehen Sie im IGEL Setup unter **System > Firmwareanpassung > Eigene Befehle > Nach Sitzungsende**.
2. Unter **Sitzungstyp** wählen Sie **Citrix**.
3. Geben Sie unter **Kommando nach Sitzungsende** den folgenden Befehl ein: `/etc/igel/usb-power-reset/igel-usb-power-ctl -p cycle`

 Für diese Aktion benötigen Sie keine Root-Rechte.

Nun sollte das Display der SpaceMouse nach Beendigung der Citrix Sitzung für etwa 1 Sekunde dunkel und dann wieder hell werden, was das Ergebnis des konfigurierten USB-Stromkreises ist.

Sehen Sie auch [Verwendung einer SpaceMouse in einer Citrix Sitzung](#) (see page 227).

## Kabellose Maus-Tastatur-Set Logitech k520 friert in Citrix Sitzung ein

### Lösung beruht auf Erfahrungen im Feld

Dieser Artikel stellt eine Lösung bereit, die nicht durch die IGEL Forschungs- und Entwicklungsabteilung geprüft wurde. Daher kann IGEL keinen offiziellen Support leisten. Soweit durchführbar, testen Sie die Lösung, bevor Sie diese in einer Produktivumgebung zum Einsatz bringen.

### Problem

Kabellose Maus-Tastatur Set Logitech k520 friert in Citrix-Sitzung ein.

### Umgebung

- IGEL OS 11
- UMS 6.01 und höher

### Beschreibung

Wenn das Infrarotsignal der kabellosen Maus-Tastatur gestört ist, friert sie ein.

### Lösung

Dieses spezielle Gerät verwendet einen Infrarot-Dongle. BT-Geräte sollten als Workaround gut funktionieren und wir empfehlen, diese zu verwenden. Citrix rät davon ab, die IR-Dongles zu verwenden.

## Schwarze Box neben dem Mauszeiger

### Beschreibung

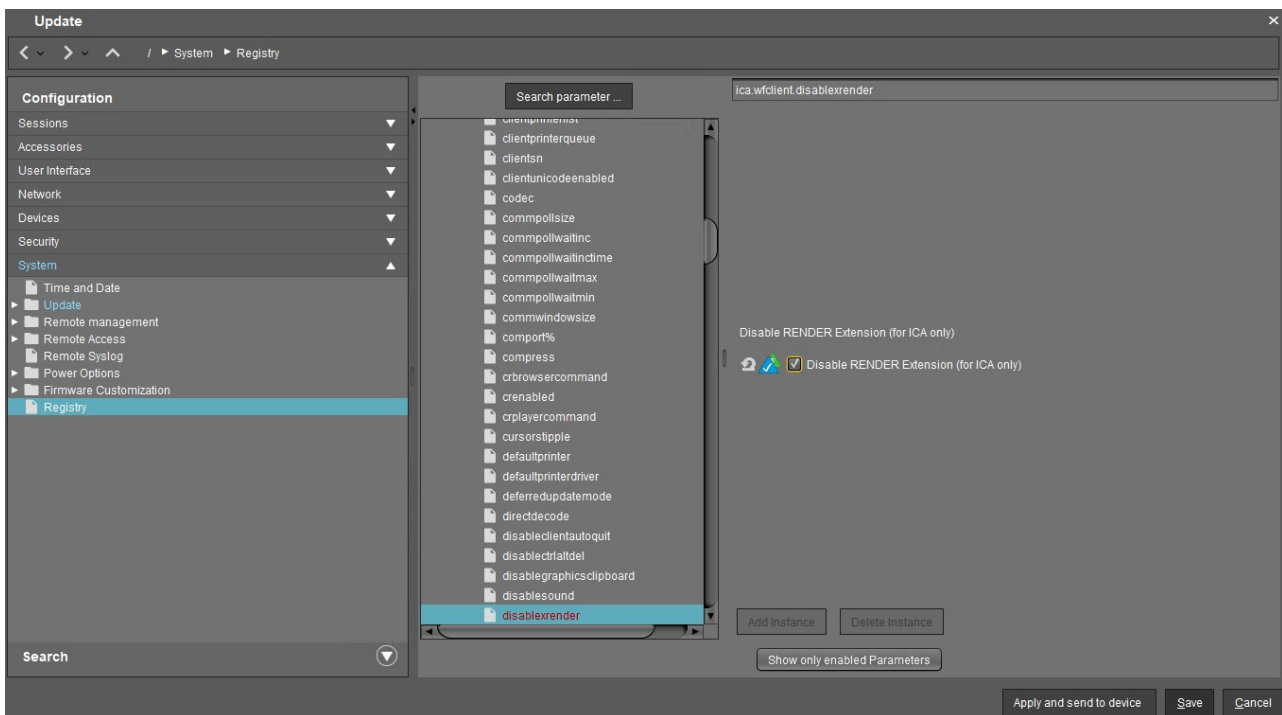
Bei bestimmten Programmen (Adobe Reader, Visual Studio, ...) wird in XenDesktop VMs immer ein schwarzer Kasten neben dem Mauszeiger angezeigt.

### Problem

Das geschieht nur, wenn eine Verbindung zu einem IGEL Gerät hergestellt wird und verschwindet, sobald ein Windows-Gerät angeschlossen wird. Die Box ist nur direkt auf dem Client sichtbar (nicht über VNC). Das Problem tritt sowohl auf dem UD7 als auch auf Intel NUCs auf.

### Lösung

► Deaktivieren Sie im IGEL Setup unter **System > Registry > ica.wfclient.disablexrender** den Parameter **Disable RENDER Extension (only for ICA)**:



Sehen Sie auch bei Citrix: <https://support.citrix.com/article/CTX212013>

## Citrix Native USB Redirection konfigurieren

Die native USB-Umleitung leitet die gängigsten USB-Geräte an die Citrix-Sitzung weiter. Um diese Funktion nutzen zu können, müssen Sie mindestens **XenDesktop 7.6** installiert haben. Darüber hinaus müssen die Richtlinien für die USB-Umleitung definiert werden. Weitere Informationen finden Sie auf den folgenden Seiten.

- [Citrix Generic USB Redirection Configuration Guide](#)<sup>24</sup>
- [Generic USB redirection and client drive considerations](#)<sup>25</sup>

Die folgenden USB-Gerätetypen werden standardmäßig **nicht** für die Verwendung in einer **Citrix Virtual App** und **Desktop**-Sitzung unterstützt:

- Bluetooth-Dongles
- Integrated NICs
- USB hubs

Die folgenden Gerätetypen werden direkt in einer **Citrix Virtual App** und **Desktop**-Sitzung unterstützt und verwenden daher keine USB-Unterstützung:

- Tastaturen
- Mäuse
- Smartcards
- Headsets
- Webcams

Zusätzlich zu den Serverrichtlinien muss die USB-Umleitung auch am Client aktiviert werden:

1. Gehen Sie im Setup auf **Sitzungen > Citrix > Citrix Global > Native USB Redirection**.
2. Aktivieren Sie **Native USB Redirection**.
3. Stellen Sie die **Vorgaberegeln** auf **Verbieten** oder **Erlauben**:
  - **Erlauben**: Alle Geräte, die standardmäßig zugelassen sind, werden umgeleitet.
  - **Verbieten**: Es wird kein Gerät umgeleitet.



### Tipp

Um Ihr Endgerät zu sichern, wird allgemein empfohlen, die **Vorgaberegeln** auf **Verbieten** zu setzen und die **Erlauben**-Regeln nur für die erforderlichen USB-Geräte und USB-Geräteklassen zu konfigurieren.

4. Um die USB-Umleitung anzupassen, können Sie Klassen oder Gerätereignisse erstellen, um z. B. Bloomberg-Tastaturen oder eine 3D Spacemouse umzuleiten.



### Informationen zu USB-Geräten erhalten

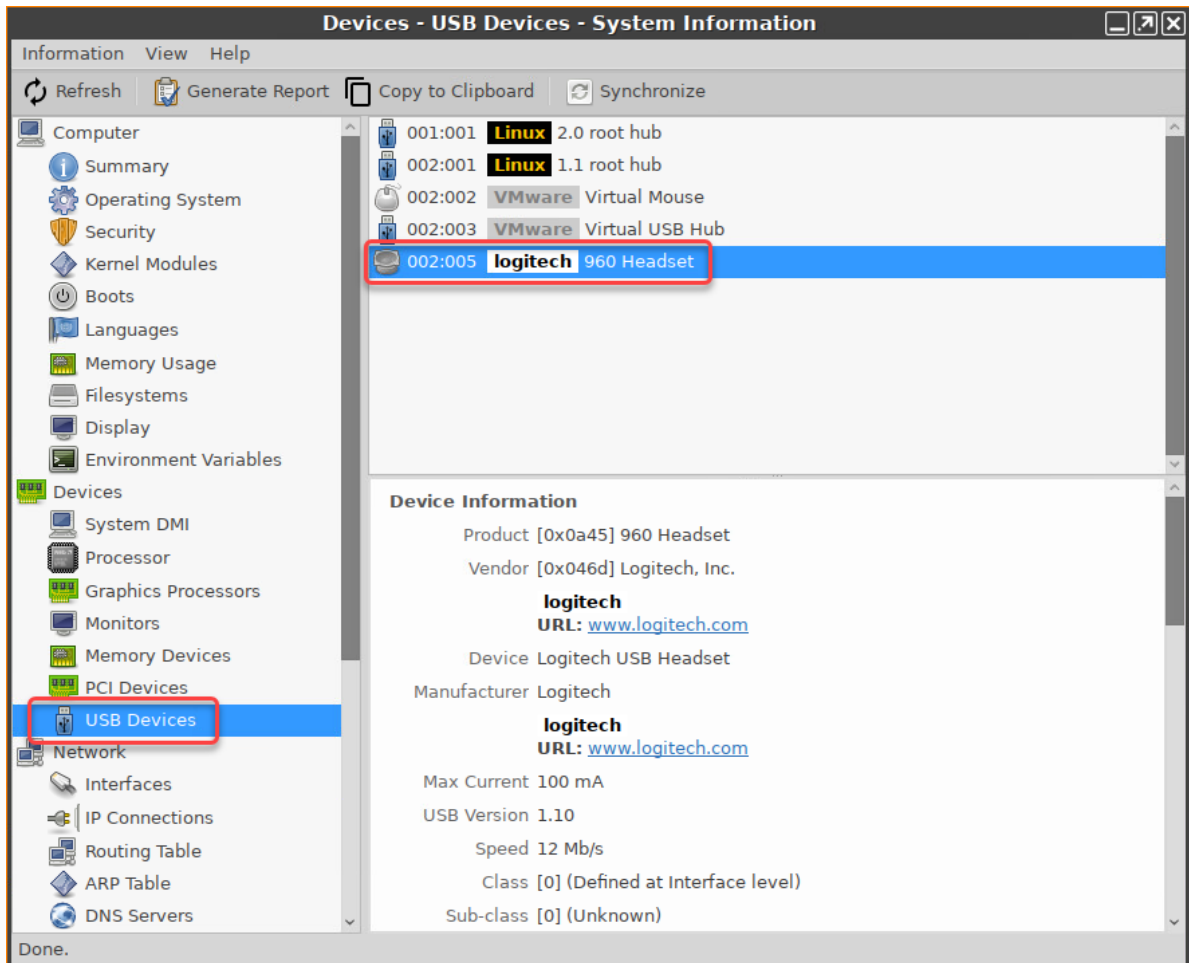
Um die **Klassen-ID**, die **Unterklassen-ID**, die **Hersteller-ID** und die **Produkt-ID** des angeschlossenen USB-Geräts herauszufinden, können Sie die Funktion **Systeminformationen** verwenden. Weitere Informationen finden Sie unter Using "System Information" Function.

Beispiel für die Systeminformationen:

<sup>24</sup> <https://support.citrix.com/article/CTX137939>

<sup>25</sup> <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/general-content-redirection/usb.html>





Alternativ können Sie auch den Befehl `lsusb` (oder `lsusb | grep -i [Suchbegriff]`) im Terminal verwenden.

Beispiel für `lsusb` :

```

Lokales Terminal
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 005: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#

```

- i** Verwenden Sie für eine Ausnahmeregel für Geräte die [SpaceMouse](#) (see page 227)-Anleitung. Weitere Informationen zu den USB-Umleitungsregeln finden Sie unter Native USB Redirection für Citrix Sitzungen in IGEL OS und in der Dokumentation der jeweiligen Citrix Workspace app.

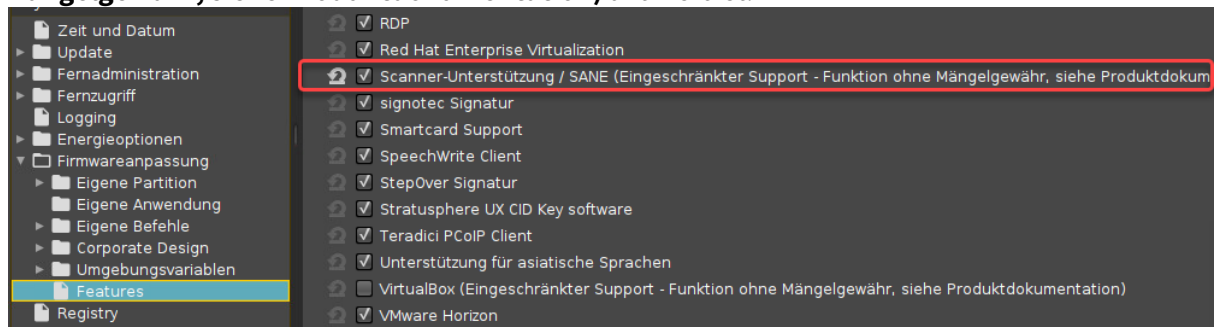
## Citrix Fabulatech Scanner Redirection in IGEL OS

Der folgende Artikel beschreibt, wie Sie die Fabulatech Scanner Redirection für Citrix Sitzungen aktivieren können.

**⚠** Beachten Sie, dass Fabulatech Scanner for Remote Desktop auch auf dem Backend-Server installiert werden muss. Weitere Informationen und eine kostenlose Testversion finden Sie unter <https://www.scanner-for-remote-desktop.com/>.

### Fabulatech Scanner Redirection für Citrix aktivieren

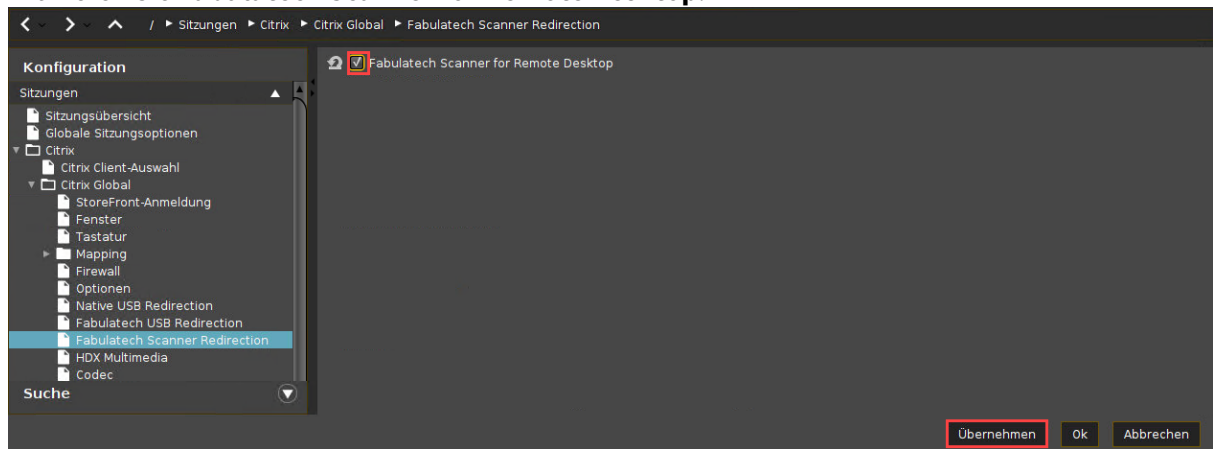
1. Gehen Sie im IGEL Setup auf **System > Firmwareanpassung > Features** und stellen Sie sicher, dass **Scanner-Unterstützung / SANE (Eingeschränkter Support - Funktion ohne Mängelgewähr, siehe Produktdokumentation)** aktiviert ist.



- Wenn die Option bereits aktiviert ist, fahren Sie mit Schritt 2 fort.
- Wenn die Option noch nicht aktiviert war, muss die Softwarekomponente erst heruntergeladen werden. Stellen Sie hierzu sicher, dass die Quelle der aktuellen Firmware korrekt gesetzt ist:
  - Wenn Sie Universal Firmware Update nutzen, stellen Sie sicher, dass das Gerät der aktuellen Firmware zugewiesen ist. Die Einzelheiten finden Sie unter Universal Firmware Update und Updates zuweisen.
  - Wenn Sie Universal Firmware Update nicht nutzen, stellen Sie sicher, dass **System > Update > Firmwareupdate** auf die Quelle der aktuellen Firmware gesetzt ist. Die Einzelheiten finden Sie unter Firmwareupdate-Einstellungen für IGEL OS.
- Nachdem Sie **OK** geklickt haben, um Ihre Änderungen zu speichern, müssen Sie das System neu starten.

2. Gehen Sie im IGEL Setup zu **Sitzungen > Citrix > Citrix Global > Fabulatech Scanner Redirection**.

### 3. Aktivieren Sie **Fabulatech Scanner for Remote Desktop**.



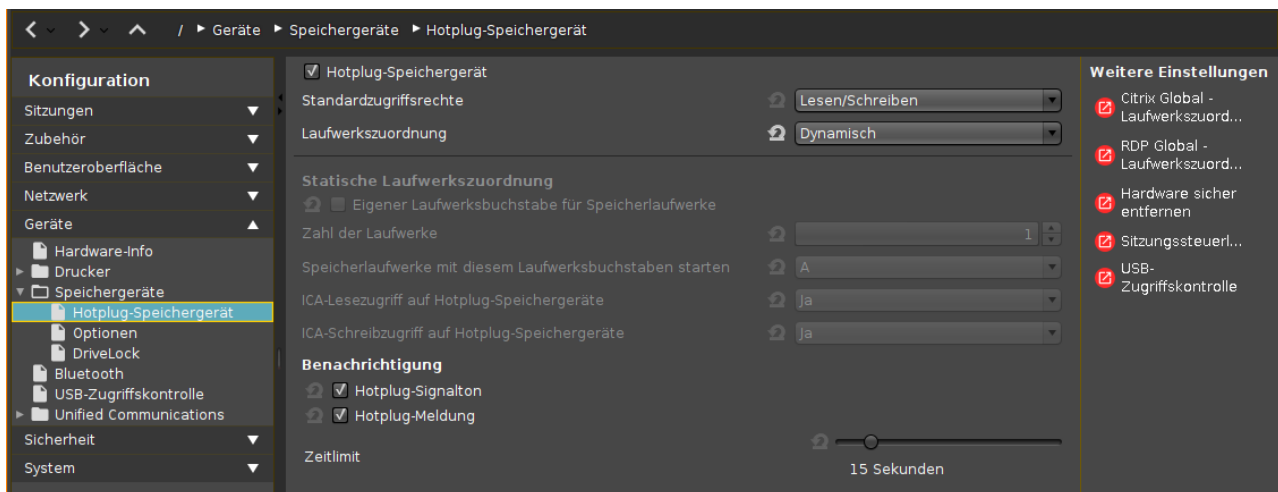
### 4. Klicken Sie **Übernehmen** oder **Ok**, um die Einstellungen zu übernehmen.

## USB-Speichergerät in Citrix Sitzungen bereitstellen

In diesem How-To erfahren Sie, wie Sie an das IGEL OS Gerät angeschlossene USB-Speichergeräte in Citrix Sitzungen bereitstellen.

**i** Die Bereitstellung von USB-Speichergeräten ist für Geräte der Klasse "USB-Massenspeicher" möglich. Der Zugriff auf den Speicher von Smartphones oder Digitalkameras erfolgt normalerweise über das MTP-Protokoll. Das MTP-Protokoll wird ab IGEL OS 10.04.100 unterstützt, siehe [Mobilgeräte-Zugriff verwenden](#) (see page 773).

### Grundkonfiguration



In IGEL Setup oder einem UMS Profil müssen Sie folgende Parameter konfigurieren:

- ▶ Aktivieren Sie **Geräte > Speichergeräte > Hotplug-Speichergerät > Laufwerkszuordnung > Dynamisch**.

Durch diese Einstellung werden neue Speichergeräte, die an dem Endgerät angeschlossen wurden, automatisch erkannt. Das Endgerät gibt einen Beep-Ton aus und zeigt einen Hinweis an, während das neue Gerät eingebunden wird. Das Speichergerät steht jetzt automatisch in Citrix/ICA-Sitzungen zur Verfügung.

**!** Um die Datenintegrität nicht zu gefährden, müssen eingebundene Geräte sicher entfernt werden. Dies kann über die **Laufwerksverwaltung**, das **Disk Removal Tool** oder ein Systray-Symbol erfolgen.

### Zusätzlich zu prüfende Parameter

▶ Die folgenden Parameter sind standardmäßig eingestellt, so dass die Speicherzuordnung funktioniert, aber vielleicht haben Sie diese aus irgendeinem Grund geändert und müssen sie anpassen, um die Speicherzuordnung zu ermöglichen:

**Sitzungen > Citrix > Citrix Global > Mapping > Laufwerkszuordnung > Laufwerkszuordnung** (Häkchen setzen)

**Sitzungen > Citrix > Citrix Global > Native USB Redirection > Native USB Redirection** (Häkchen entfernen)

**Sitzungen > Citrix > Citrix Global > Fabulatech USB Redirection > Fabulatech USB Redirection** (Häkchen entfernen)

**Geräte > USB-Zugriffskontrolle > Aktivieren** (Häkchen entfernen)

**Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > USB Redirection > Native USB Redirection** (auf **Globale Einstellung** setzen)

**Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > Mapping > Laufwerkszuordnung aktivieren** (auf **Globale Einstellung** setzen)

## Laufwerksbuchstaben innerhalb der Sitzung zuweisen (optional)

► Wenn Sie nicht nur das Laufwerk in der Sitzung wie z.B. "A auf IGEL-123456789" sehen möchten, sondern das Laufwerk innerhalb der Sitzung mit einem echten Laufwerksbuchstaben ansprechen möchten, können Sie einen dieser Befehle ausführen:

```
subst T: \\tsclient\t
```

oder

```
net use T: \\tsclient\t
```

In diesem Beispiel ist "T auf IGEL-123456789" dem Laufwerksbuchstaben T: in der Sitzung zugewiesen. Sie können das zugeordnete Laufwerk auch einem anderen Laufwerksbuchstaben zuweisen, der im Namen verwendet wird.

## Konfiguration auf der Serverseite

Auf der Serverseite, z.B. bei Windows Server 2008R2, hat ein Benutzer in der Gruppe "Benutzer" mit Zugriff auf den Terminalserver den Mapping-Standard. Dies gilt für einen neu installierten Server. Aber das Mapping kann durch eine Änderung der Richtlinien verhindert werden:

**i Umleitung des Laufwerks nicht zulassen** gibt an, ob die Zuordnung von Geräte-Laufwerken in einer Remote Desktop Services-Sitzung verhindert werden soll (Laufwerksumleitung). Standardmäßig ordnet ein RD-Sitzungshost-Server Gerät-Laufwerke automatisch nach der Verbindung zu. Zugeordnete Laufwerke erscheinen im Sitzungsordnerbaum des Windows Explorers oder Computers im Format [Laufwerksbuchstabe] auf [Computername]. Mit dieser Einstellung können Sie dieses Verhalten außer Kraft setzen." Quelle: <https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx>

## Symbolleiste im Appliance-Modus automatisch ausblenden

### Voraussetzung

IGEL Linux v5.x oder neuer

### Problem

Im Appliance-Modus wird die Symbolleiste oben auf dem Bildschirm dauerhaft angezeigt.

Sie möchten die Symbolleiste so konfigurieren, dass sie sich automatisch ausblendet, wenn sie den Fokus des Mauszeigers verliert.

### Lösung

1. In IGEL Setup gehen Sie auf **System > Registry > `userinterface.igel_toolbar.show_always_in_appliance_mode`**.
2. Deaktivieren Sie **Symbolleiste immer im Appliance-Modus anzeigen**.
3. Klicken Sie **Ok**, um die Änderungen zu speichern.

 Damit die Änderungen wirksam werden, müssen Sie die aktiven Appliance-Modus-Sitzungen neu starten.

## Eine nahtlos, transparente Benutzeroberfläche mit dem Appliance-Modus erstellen

Mit dem Appliance-Modus können Sie das Gerät auf eine bestimmte Sitzung eingrenzen. Im Appliance-Modus, verschwindet das Gerät selbst im Hintergrund und die Sitzung wird dem Nutzer auf die einfachste Weise präsentiert. Der Nutzer muss sich daher nicht mit einem Linux Desktop, mehreren Anmeldeverfahren, dem Umschalten zwischen Windows und der Gerätekonfiguration befassen.

Verwenden Sie den Appliance-Modus, um den Zugriff nur auf eine bestimmte Sitzung zu ermöglichen. Beim Start des Gerätes wird der Nutzer direkt auf den Anmeldebildschirm des virtuellen Desktops geleitet.

Der Appliance-Modus kann bei folgenden Sitzungstypen eingestellt werden:

- VMware Horizon
- Citrix Self-Service (nur für veröffentlichte Desktops, nicht für veröffentlichte Sitzungen)
- RHEV/Spice
- Imprivata
- RDP MultiPoint Server
- XDMCP für dieses Display

So konfigurieren Sie eine Sitzung, die im Appliance-Modus ausgeführt wird:

1. Öffnen sie das Setup und gehen Sie zu **Sitzungen > Appliance-Modus**
2. Wählen Sie den Sitzungstyp der gewünschten Sitzung über das Dropdown-Menü **Appliance-Modus** aus.
3. Konfigurieren Sie die Appliance-Modus-Sitzung entsprechend.

Weitere Informationen finden Sie im Handbuchkapitel Appliance-Modus.

## Verbindung zu Citrix-Farm herstellen

Durch die Verbindung zu einer Citrix-Farm, werden Ihre Daten und Anwendungen zentral auf einer Citrix-Farm gespeichert. Anwendungen müssen den Benutzern sofort und überall auf jedem Gerät zur Verfügung gestellt werden.

Es gibt mehrere Möglichkeiten, sich mit einer Citrix-Farm zu verbinden und Sitzungen zu starten. Im Folgenden beschreiben wir drei Best Practice-Varianten:

- [Citrix StoreFront \(see page 241\)](#): Integriert veröffentlichte Anwendungen in die IGEL GUI.
- [Citrix Self-Service \(see page 242\)](#): Die Benutzer werden zu einer Weboberfläche geleitet, wo sie vordefinierte veröffentlichte Anwendungen finden und weitere veröffentlichte Anwendungen hinzufügen können.
- [Appliance Mode \(see page 246\)](#): Zeigt nur die Weboberfläche der Farm an und blendet die IGEL GUI vollständig aus.



## Citrix StoreFront

### Voraussetzungen:

- Trust root certificate in directory /wfs/ca-certs (siehe [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen](#) (see page 523))

So stellen Sie eine Verbindung über Citrix StoreFront her:

1. Klicken Sie im Konfigurationsbaum des IGEL-Setups auf **Sitzungen**.
2. Navigieren Sie zu **Citrix > Citrix StoreFront > Server**.
3. Klicken Sie unter **Serverstandort** auf **Hinzufügen +**.  
Die Maske **Hinzufügen** wird geöffnet.
4. Geben Sie die **Adresse der Webseite des Citrix-Stores** und den **Namen des Stores** an.
5. Klicken Sie **Weiter**.
6. Klicken Sie **Citrix StoreFront > Desktopintegration**.
7. Geben Sie "Citrix Storefront" unter **Anmeldesitzungsname** ein.
8. Wählen Sie **Desktop** unter **Startmöglichkeiten der Sitzung**.
9. Klicken Sie **Speichern**, um die Änderungen zu speichern.  
Das Setup wird geschlossen.
10. Doppelklicken Sie auf das Citrix-Symbol auf dem Desktop.  
Das Anmeldefenster wird geöffnet.
11. Geben Sie im Anmeldefenster die Zugangsdaten eines Benutzers ein.  
Die veröffentlichten Anwendungen der Citrix-Farm erscheinen auf dem Desktop.
12. Doppelklicken Sie auf ein Anwendungssymbol auf dem Desktop, um das Programm zu starten.

## Citrix Self-Service

### Voraussetzungen

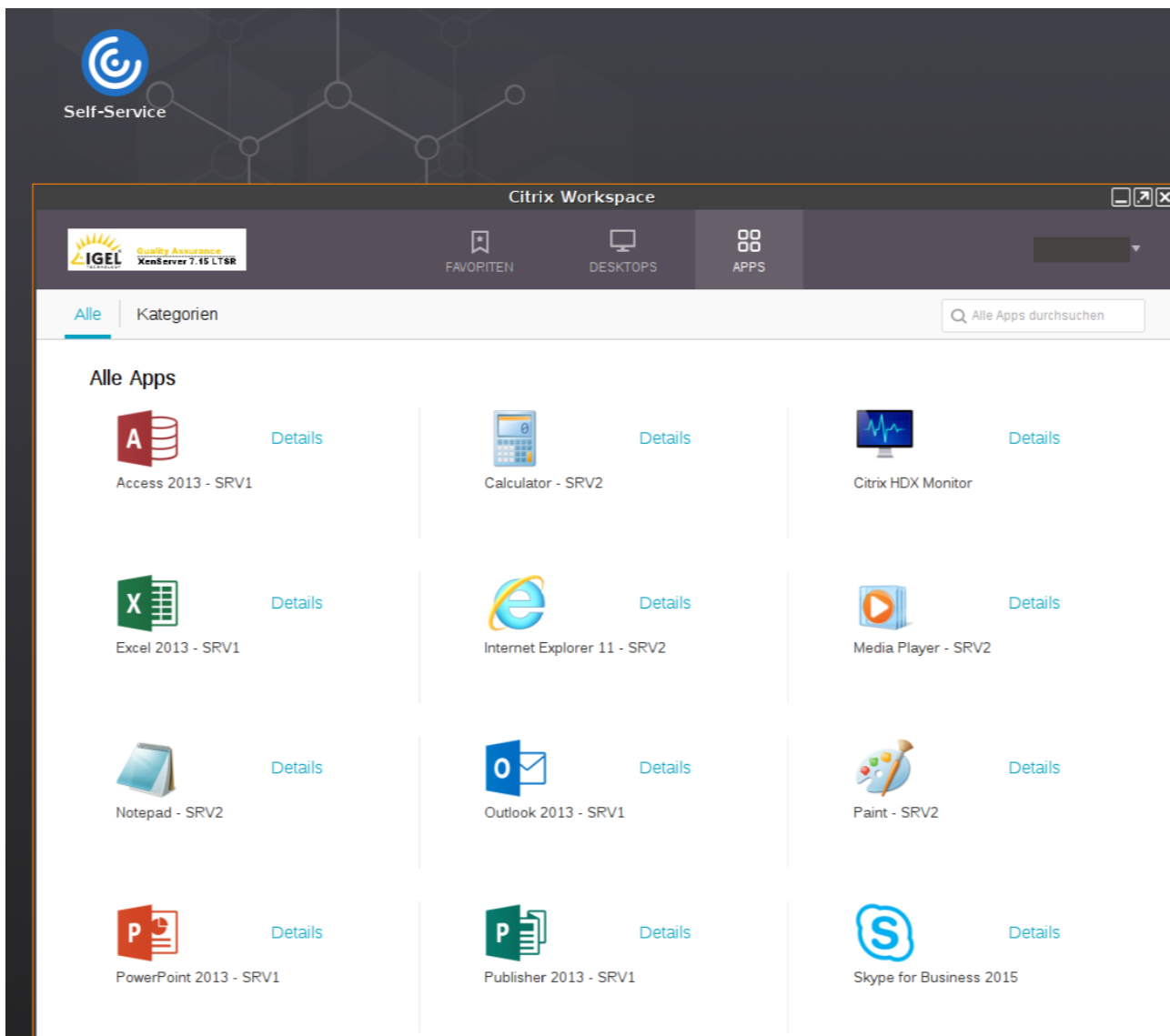
- Trust root certificate in directory /wfs/ca-certs (see Vertrauenswürdige Stammzertifikate einspielen)

So stellen Sie eine Verbindung via StoreFront her:

1. Gehen Sie in IGEL Setup zu **Sitzungen > Citrix > Citrix Self-Service > Server**.
2. Klicken Sie im Bereich **Server: Storefront** das +-Icon.  
Der Dialog **Hinzufügen** öffnet sich.
3. Geben Sie **Server**, **Pfad zum Store** sowie **Name des Stores** ein.
4. Bestätigen Sie mit **Weiter**.
5. Gehen Sie zu **Citrix Self-Service > Desktopintegration**.
6. Geben Sie bei **Self-Service Sitzung** "Citrix Self-Service" ein.
7. Aktivieren Sie bei **Startmöglichkeiten der Sitzung** die Option **Desktop**.
8. Klicken Sie **Ok**, um die Änderungen zu speichern.  
Das Setup wird beendet.
9. Doppelklicken Sie auf das Citrix-Startsymbol auf dem Desktop.  
Das Anmeldefenster öffnet sich.
10. Geben Sie im Anmeldefenster die Anmeldedaten eines Benutzers ein.  
Die in der Citrix Farm veröffentlichten Anwendungen erscheinen in der Benutzeroberfläche von Citrix Self-Service.
11. Doppelklicken Sie ein Anwendungssymbol, um eine zu starten.

## Citrix Self-Service verwenden

1. Starten Sie **Citrix Self-Service**, z. B. über ein Desktopsymbol.
2. Melden Sie sich am Server an.
3. Fügen Sie der Liste veröffentlichte Anwendungen hinzu (+-Button links).
4. Klicken Sie auf eine veröffentlichte Anwendung, um sie zu starten.
5. Verwenden Sie die Suchzeile, um nach einer veröffentlichten Applikation zu suchen.
6. Verwenden Sie das Benutzermenü, um Einstellungen zu ändern.



- [Vollbildmodus einrichten](#) (see page 245)

### Vollbildmodus einrichten

Verwenden Sie den folgenden Parameter in einem [Custom Command script](#), um für Citrix Self-Service den Vollbildmodus zu aktivieren:

▶ `$ICADIR/storebrowse -c FullscreenMode=[0/1/2]`

Ihnen stehen folgende Optionen zur Verfügung:

- `0` = Das Fenster wird nicht im Vollbildmodus angezeigt.
- `1` = Das Fenster wird im Vollbildmodus angezeigt.
- `2` = Das Fenster wird maximiert und ohne Dekoration angezeigt. Die Taskbar der Desktopumgebung wird nicht verdeckt.

## Appliance Mode

### Über Selfservice GUI zu Citrix verbinden

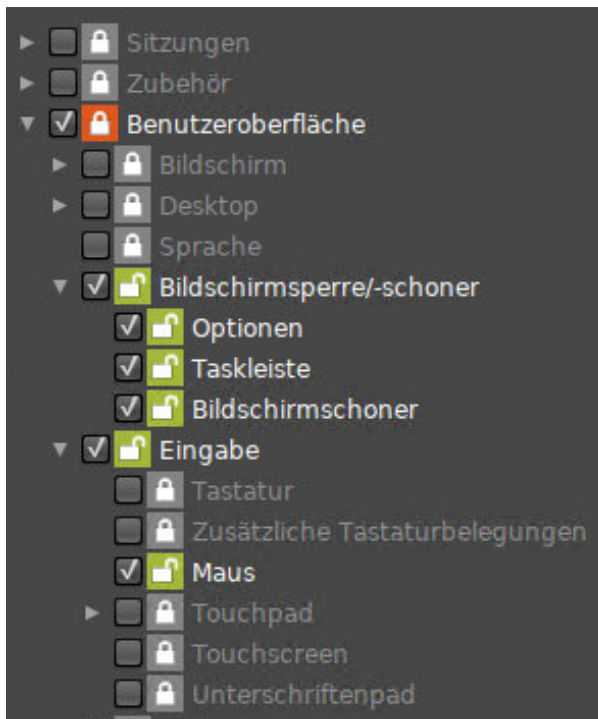
1. Klicken Sie **Sitzungen > Appliance Modus**.
2. **Wählen Sie Citrix Self-Service** unter **Appliance mode**.
3. Geben Sie die **URL** des Deliver-Servers ein.
4. Klicken Sie **OK**, um die Änderungen zu speichern und um das Setup zu schließen.
5. Befolgen Sie die Anweisungen auf dem Bildschirm.

## Ein Self-Service-Setup mit Hilfe von Schnelleinstellungen erstellen

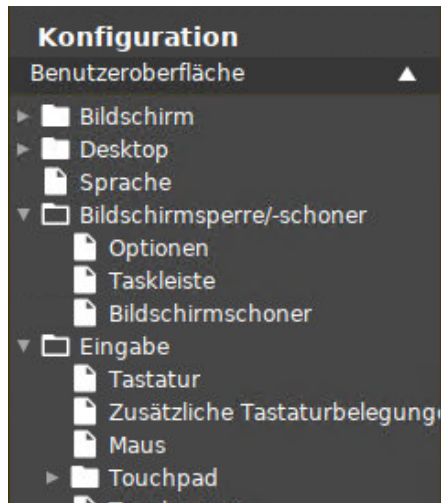
Normalerweise, sollte der Nutzer keinen vollen Zugriff auf das Setup des Geräts haben. Es kann sich jedoch als sinnvoll erweisen, dass Nutzer bestimmte Einstellungen schnell selbst vornehmen können, ohne ein Passwort zu benötigen. Typische Beispiele sind Einstellungen der Tastatur, der Maus oder des Bildschirms. Dies kann über die Quicksetup erfolgen.

So können Sie die Setup-Seiten für eine schnelle Einrichtung einstellen:

1. Öffnen sie Setup und gehen Sie zu **Zubehör > Quicksetup > Seitenberechtigung Setup-Benutzer**
2. Wählen Sie die Setup-Seiten aus, auf die der Nutzer Zugriff haben soll, z. B.: **Benutzeroberfläche > Eingabe > Maus**, oder **Bildschirm Sperre/-schoner**.



3. Klicken Sie **Übernehmen** oder **OK**. Wenn der Nutzer **Quicksetup** startet, werden die zuvor ausgewählten Optionen angezeigt.



Quicksetup legt Berechtigungen für Setup-Bildschirme fest. Wenn Sie Berechtigungen für einzelne Parameter festlegen möchten, können Sie UMS-Profile verwenden.


Weitere Informationen finden sie unter Profile.



## Anmeldung fehlgeschlagen aufgrund des abgelaufenen AD-Passworts

### Problem

Wenn Sie versuchen, sich bei einer nativen **Citrix StoreFront**-Sitzung anzumelden, erhalten Sie die Fehlermeldung "Anmeldung fehlgeschlagen!", da Ihr Active Directory-Passwort abgelaufen ist. Sie können Ihr Passwort nicht ändern, da das lokale Login keine Option dafür bietet.

 Bevor Sie diesen Anweisungen folgen, überprüfen Sie, ob die Ports offen sind, vielleicht können Sie das Problem dadurch beheben:


- Anmeldung auf dem Client -> Port: 88
- Passwort ändern -> Port: 464

Hier finden Sie eine Übersicht über die Ports des Domain Controllers: [Required Ports to Communicate with Domain Controller](#)<sup>26</sup>

### Lösung

Aktivieren Sie die **Active Directory/Kerberos** Authentifizierung für die **StoreFront** Sitzung. Beim nächsten Versuch, sich im IGEL OS anzumelden, werden Sie aufgefordert, Ihr Passwort zu ändern.

### Ändern eines abgelaufenen Active Directory Passworts

 Bei der Verwendung von Sitzungen mit Passthrough-Authentifizierung ist es wichtig, dass Sie den Bildschirm Ihres Geräts sperren, wenn es unbeaufsichtigt bleibt.

### Active Directory/Kerberos-Authentifizierung für StoreFront-Sitzungen aktivieren

1. Gehen Sie im IGEL Setup unter **Security > Anmeldung > Active Directory/Kerberos**.
2. Aktivieren Sie **Anmeldung an Active-Directory-Domäne**.
3. Gehen Sie unter **Sicherheit > Active Directory/Kerberos**.
4. Setzen Sie ein Häkchen bei **Aktivieren**.
5. Geben Sie die **Standarddomäne (vollständiger Domänenname)** ein.
6. Gehen Sie unter **Sitzungen > Citrix > Citrix StoreFront > Anmeldung**.
7. Aktivieren Sie **Passthrough-Authentifizierung verwenden**.
8. Klicken Sie **Übernehmen** oder **Ok**.

<sup>26</sup> <https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS>

**i** Bitte beachten Sie, dass das Gerät nun lokal und nicht mehr in der Sitzung gesperrt sein muss, um zu verhindern, dass eine andere Person über den Passthrough ohne Angabe des Passworts in die Sitzung gelangt.

## Bildschirmsperre aktivieren

1. Gehen Sie im IGEL Setup unter **Benutzeroberfläche > Bildschirmsperre/-schoner**.
2. Aktivieren Sie **Hotkey**.
3. Wählen Sie unter **Steuertasten** **Win**.
4. Geben Sie unter **Hotkey** "L" ein.
5. Gehen Sie auf **Benutzeroberfläche > Bildschirmsperre/-schoner > Optionen**.
6. Aktivieren Sie **Benutzerpasswort**.

Der Hotkey "Win + L" sperrt nun das IGEL-Gerät anstelle des Sitzungsdesktops.

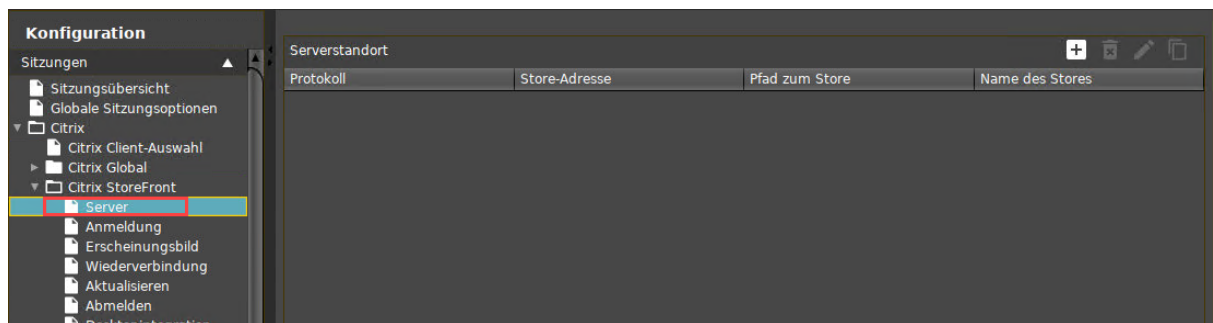
Zur Aktivierung der IGEL-Geräte muss das AD-Passwort eingegeben werden.

## Automatisches Anmelden für Citrix Virtual Desktops konfigurieren

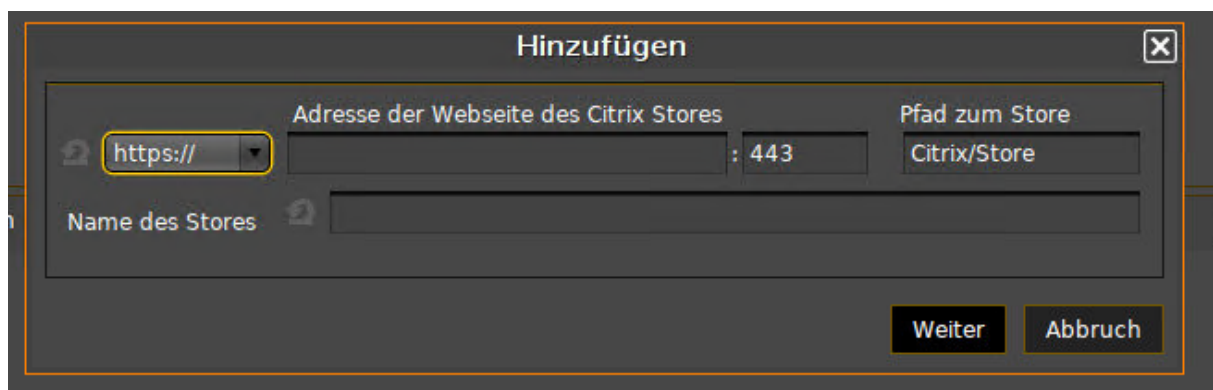
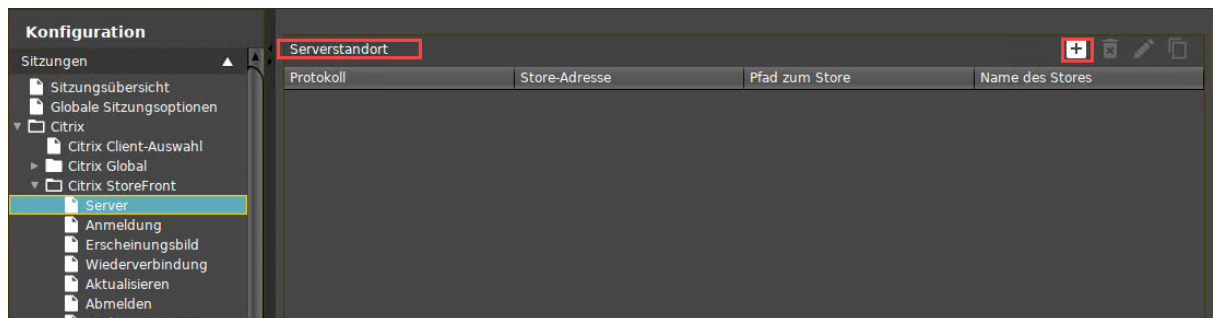
In diesem How-To erfahren Sie, wie Sie automatisches Anmelden für Citrix Virtual Desktops konfigurieren.

### Schritte

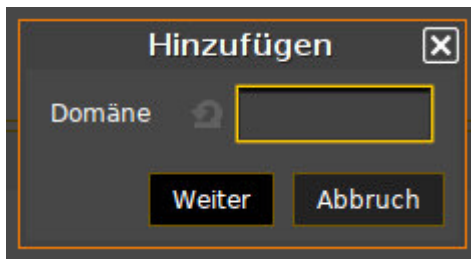
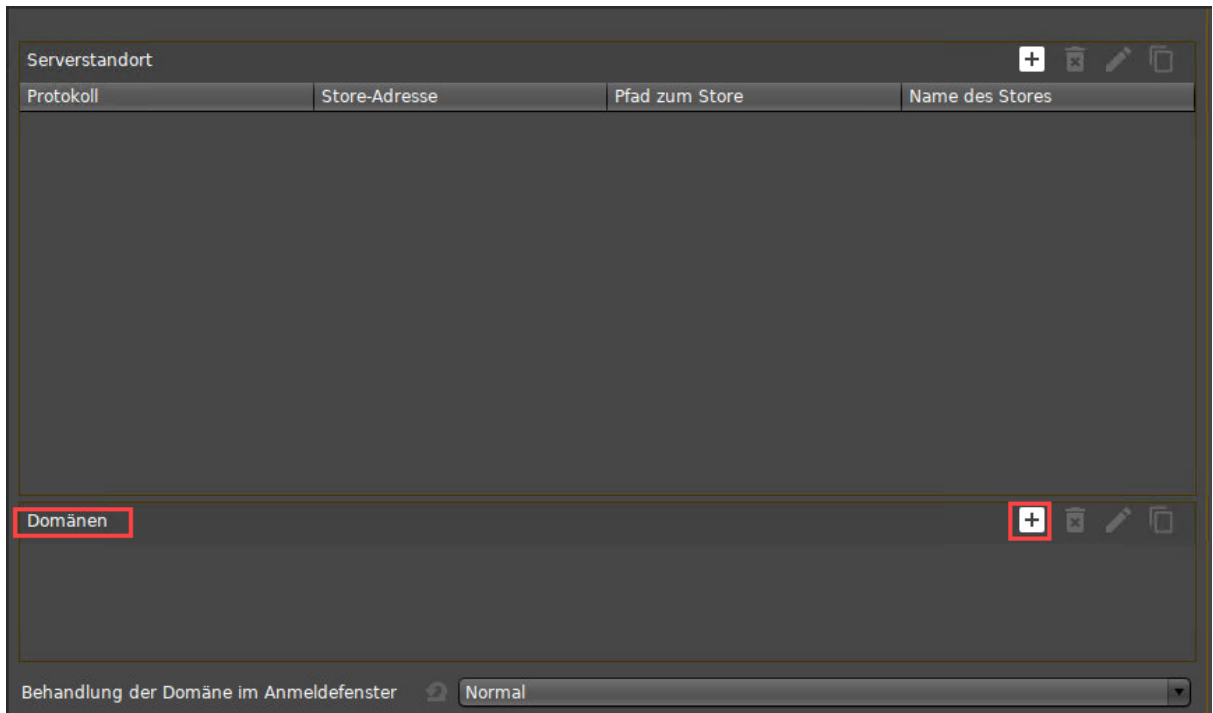
1. Gehen Sie in IGEL Setup zu **Sitzungen > Citrix > Citrix StoreFront > Server**.



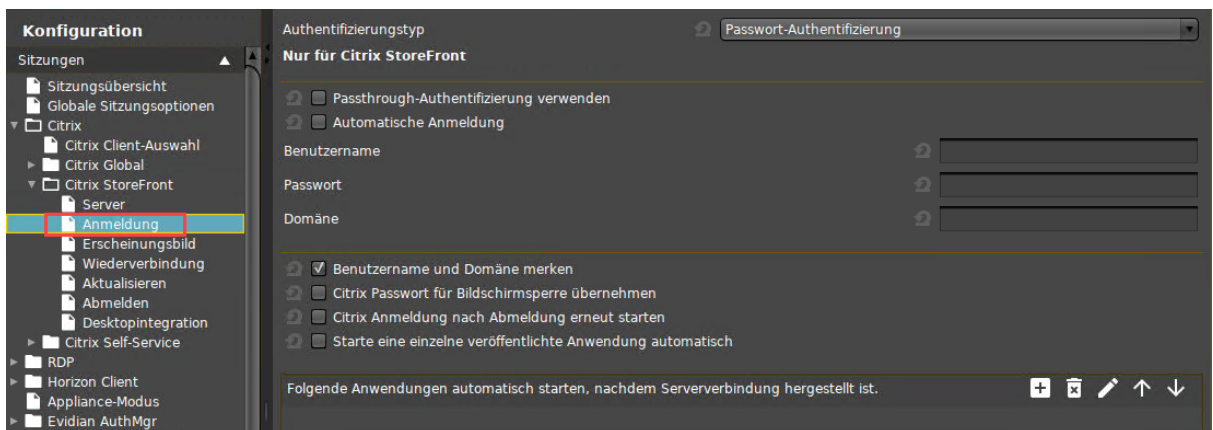
2. Fügen Sie im Bereich **Serverstandort** eine Konfiguration hinzu.



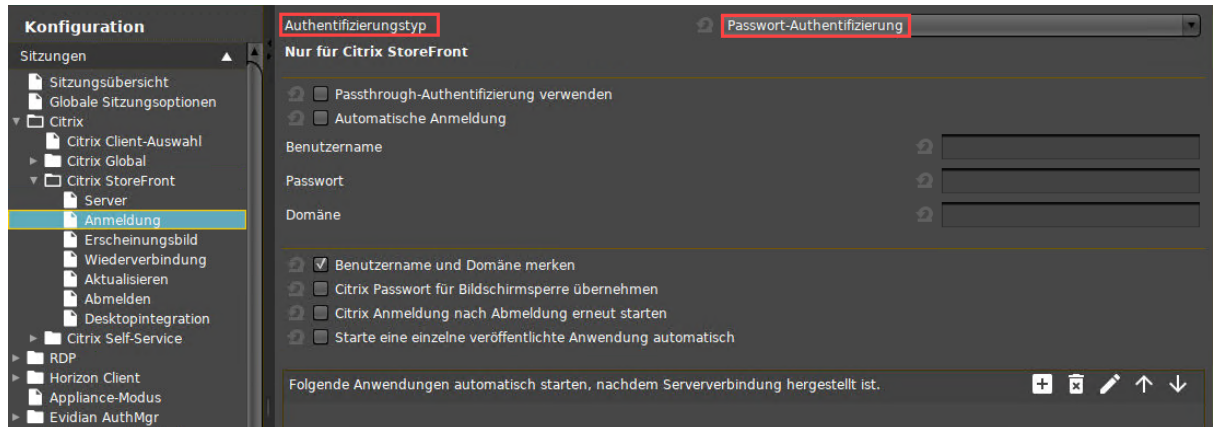
3. Fügen Sie im Bereich **Domänen** Ihre Active Directory-Domäne hinzu. Achten Sie darauf, den Fully Qualified Domain Name (FQDN) einzugeben.



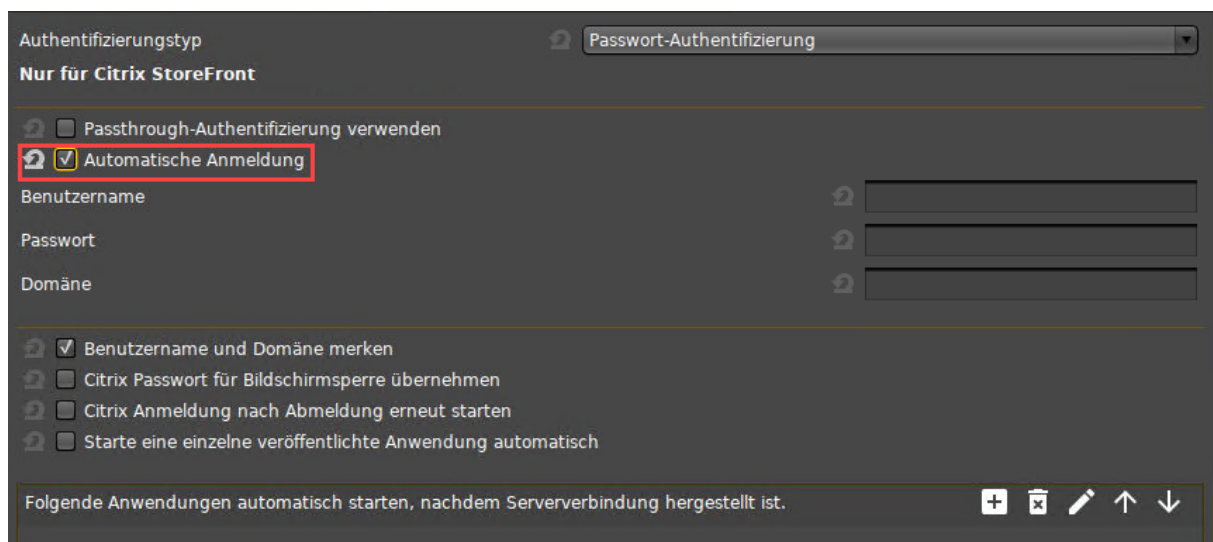
4. Gehen Sie zu **Sitzungen > Citrix > Citrix StoreFront > Anmeldung**.



5. Setzen Sie die Einstellung **Authentifizierungstyp** auf **Passwort-Authentifizierung**.



6. Aktivieren Sie **Automatische Anmeldung**.



7. Geben Sie bei **Benutzername** den Active Directory-Benutzernamen ein.

Authentifizierungstyp Passwort-Authentifizierung

**Nur für Citrix StoreFront**

Passthrough-Authentifizierung verwenden

Automatische Anmeldung

Benutzername

Passwort

Domäne

Benutzername und Domäne merken

Citrix Passwort für Bildschirmsperre übernehmen

Citrix Anmeldung nach Abmeldung erneut starten

Starte eine einzelne veröffentlichte Anwendung automatisch

Folgende Anwendungen automatisch starten, nachdem Serververbindung hergestellt ist. + - ✎ ↑ ↓

8. Geben Sie das **Passwort** des Active Directory-Benutzers ein.

Authentifizierungstyp Passwort-Authentifizierung

**Nur für Citrix StoreFront**

Passthrough-Authentifizierung verwenden

Automatische Anmeldung

Benutzername

Passwort

Domäne

Benutzername und Domäne merken

Citrix Passwort für Bildschirmsperre übernehmen

Citrix Anmeldung nach Abmeldung erneut starten

Starte eine einzelne veröffentlichte Anwendung automatisch

Folgende Anwendungen automatisch starten, nachdem Serververbindung hergestellt ist. + - ✎ ↑ ↓

9. Geben Sie für **Domain** den Fully Qualified Domain Name (FQDN) Ihrer Active Directory-Domäne ein. Dies ist der gleiche Wert wie in Schritt 3.

Authentifizierungstyp ↻ Passwort-Authentifizierung

**Nur für Citrix StoreFront**

↻  Passthrough-Authentifizierung verwenden  
↻  Automatische Anmeldung

Benutzername ↻

Passwort ↻


**Domäne** ↻

↻  Benutzername und Domäne merken  
↻  Citrix Passwort für Bildschirmsperre übernehmen  
↻  Citrix Anmeldung nach Abmeldung erneut starten  
↻  Starte eine einzelne veröffentlichte Anwendung automatisch

Folgende Anwendungen automatisch starten, nachdem Serververbindung hergestellt ist. + ✕ ✎ ↑ ↓

## Citrix-Abmeldung per Hotkey erzwingen

Die Anleitung finden Sie unter [Citrix: Freeze at Logout](#) (see page 256).

 Diese Seite wird demnächst gelöscht. Zukünftig verwenden Sie bitte den obigen Link.



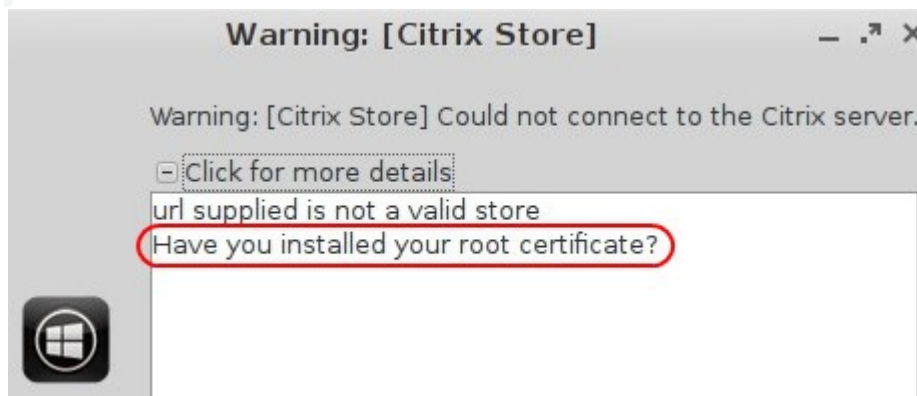
## Warnmeldung: [Citrix Store] kann sich nicht mit dem Citrix-Server verbinden

### Voraussetzung

- Sie benutzen Citrix Receiver 13.0.x oder neuer.
- Sie haben einen Citrix StoreFront-Sitzungstyp konfiguriert.

### Symptom

- Beim Verbindungsaufbau erscheint eine Warnmeldung:  
Warning: [Citrix Store] Could not connect to the Citrix server.



oder



## Problem

Citrix Receiver 13.0.x oder neuer unter Linux unterstützt nur Verbindungen über HTTPS, und Sie müssen sicherstellen, dass das Gerät über ein gültiges Root-Zertifikat der Zertifizierungsstelle (CA) verfügt. Wenn das Root-Zertifikat fehlt, schlägt die Verbindung fehl.

## Lösung

Installieren Sie ein entsprechendes Root-Zertifikat auf dem Gerät, um HTTPS-Verbindungen mit Ihrem Citrix-Server zu ermöglichen.

Informationen zur Verteilung des Zertifikats finden Sie unter [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen](#) (see page 523).

## Citrix-Sitzungen mit hardwarebeschleunigtem H.264 Deep Compression Codec einrichten

In diesem Dokument erfahren Sie, wie Sie den H.264 Deep Compression Codec aktivieren.

### Voraussetzungen

- Gültige Lizenz für IGEL Multimedia Codec Pack
- IGEL UD Gerät mit Hardware-Videobeschleunigung, siehe das FAQ [Hardware-Videobeschleunigung auf IGEL OS](#) (see page 853)
- Server für Citrix Virtual Apps and Desktops mit aktiviertem H.264-Anzeigemodus  
Wie Sie herausfinden, welcher Anzeigemodus aktiv ist, erfahren Sie hier: <https://support.citrix.com/article/CTX200370>

### Codec aktivieren

1. Gehen Sie in IGEL Setup zu **System > Firmwareanpassungen > Features**.
2. Aktivieren Sie **Hardware-Videobeschleunigung**.
3. Gehen Sie zu **Sitzungen > Citrix > Citrix Client-Auswahl**.
4. Wählen Sie **Citrix Client Version**.
5. Gehen Sie zu **Sitzungen > Citrix > Citrix Global > Codec**.
6. Setzen Sie **Graphical codec** auf **H.264 Deep Compression Codec**.
7. Aktivieren Sie **Beschleunigter H.264 Deep Compression Codec**.

- i** Known Issues bei VIA-basierten IGEL-Geräten der Geräteklassen UD3-LX 40/41/42 sowie UD10-LX:
- Hardwarebeschleunigtes HDX funktioniert nur, wenn 256 MB Grafikspeicher oder mehr verfügbar ist. Der Grafikspeicher muss im BIOS eingestellt werden. Der Standardwert ist 128 MB.
  - Seamless-Window-Mode wird nicht unterstützt.
  - Desktop-Sitzungen, die über mehr als zwei Monitor gehen, werden nicht unterstützt.
  - Desktop-Sitzungen auf rotierten Bildschirmen können flackern (dies ist abhängig von der Bildschirmauflösung).

- i** Wenn Sie den **Citrix Receiver 13.5** oder älteren in Kombination mit einem **Citrix Server 7.15** verwenden, wird die option **Build to Lossless** unter **Visual Quality** unter Linux nicht funktionieren. Für IGEL Linux Version 10.05.100 kann die Option **Build to Lossless** der **Visual Quality** Policy funktionieren wenn Sie einen **Citrix Receiver 13.6** oder jünger verwenden und Sie die **Use Video Codec** Policy auf **For actively changing regions** setzen.


## Hochsicherer XenServer hat Probleme mit dem LD\_BIND\_NOW Workaround

### Problem

Sie möchten mehrere Desktopsitzungen mit RTME und H.264-Beschleunigung starten, aber es funktioniert nicht.

### Lösung

1. Gehen Sie im **IGEL Setup** unter **System > Registry > ica > workaround-dual-rtme**. (Parametersuche: **ica.workaround-dual-rtme**)
2. Aktivieren Sie **Activate workaround for dual RTME sessions and H264 acceleration**.
3. Klicken Sie **Übernehmen** oder **Ok**, um die Änderungen zu speichern.

 Dieser Registry Key sollte nicht verwendet werden, wenn "Enable Secure ICA" für die jeweilige Bereitstellungsgruppe aktiv ist. Sie müssen sich entscheiden, ob Sie den Workaround verwenden oder die Sicherheit reduzieren wollen.

## Fehlerbehebung für Citrix Receiver X-Fehler

### Problem

Beim Start von Citrix XenApp erhalten Sie die folgenden Citrix Receiver-Fehler auf Ihren Linux-Geräten:

```
The X Request 55.0 caused error: "9: BadDrawable (invalid Pixmap or Window parameter)"
```

```
The X Request 60.0 caused error: "13: BadGC (invalid GC parameter)".
```

### Voraussetzung

- Citrix XenApp 7.15
- Citrix Receiver z. B. 13.2, 13.3, 13.7, 13.8

### Lösung

Zwei Parameter müssen im IGEL Setup aktiviert werden:

1. Gehen Sie unter **System > Registry > ica > forceignoreerrors**.
2. Aktivieren Sie **X Fehlermeldungsdialoge unterdrücken**.
3. Gehen Sie unter **System > Registry > ica > wfclient > ignoreerrors**.
4. Aktivieren Sie **IgnoreXErrors** und geben Sie die Parameter ein: **55.0/9, 60.0/13**

Siehe auch den entsprechenden Eintrag im [Citrix-Forum](https://discussions.citrix.com/topic/393872-possible-workaround-citrix-receiver-x-error-on-linux-thin-clients/)<sup>27</sup>.

---

<sup>27</sup> <https://discussions.citrix.com/topic/393872-possible-workaround-citrix-receiver-x-error-on-linux-thin-clients/>

## Problem mit Citrix HTML5 Receiver

### Betroffene Versionen

- IGEL OS 10.05.100 oder höher
- IGEL OS 11.01.100 oder höher

### Problem

Durch den Wegfall der Plugin-Technologie in Firefox 60+ wird die unter Linux installierte Workspace-App nicht mehr automatisch erkannt.


### Lösung

1. Wenn Ihr Gerät IGEL OS 10.05 hat, aktualisieren Sie es auf IGEL OS 10.06; wenn anwendbar, können Sie es auf IGEL 11.02 aktualisieren.  
Wenn Ihr Gerät IGEL OS 11.01 hat, aktualisieren Sie es auf IGEL OS 11.02.  
IGEL OS 10.06 und IGEL OS 11.02 wurden für einen Workaround angepasst, der serverseitige Modifikationen erfordert.
2. Ändern Sie die serverseitigen Einstellungen entsprechend der Anleitung unter <https://support.citrix.com/article/CTX237727>.


## Tastaturbelegung für Macbook innerhalb der Citrix Sitzung

Damit die Macbook-Tastaturbelegung innerhalb von Citrix Sitzungen korrekt funktioniert, gehen Sie wie folgt vor:

1. Unter **Sitzungen > Citrix > Citrix Global > Tastatur > Datei für Tastaturbelegung** wählen Sie "Linux".
2. Unter **Benutzeroberfläche > Eingabe > Tastatur > Tastaturtyp** wählen Sie "Macbook".  
Alle anderen Einstellungen für Tastaturbelegung können Sie unverändert lassen, d. h. wie standardmäßig eingestellt.

 Um Sonderzeichen wie € und # einzugeben, verwenden Sie die rechte Alt-/Option-Taste, nicht die linke Taste.

## Citrix Feature Matrix

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.



## Lync / Skype for Business mit Citrix HDX RealTime Optimization Pack verwenden

### Thema

Sie möchten Microsoft Lync oder Skype for Business über eine Citrix Sitzung mit IGEL OS-Geräten verwenden.

### Lösung

IGEL OS wird mit vorinstallierter Citrix HDX RealTime Media Engine (RTME) ausgeliefert: Setup > **Sitzungen** > **Citrix** > **Citrix Global** > **Unified Communications** > **Skype for Business**. Siehe auch HDX Multimedia-Einstellungen für eine IGEL OS Citrix Sitzung.

- IGEL OS 11.04.100 oder höher beinhaltet RTME 2.9 (standardmäßig aktiviert).
- IGEL OS 11.02.100 oder höher beinhaltet RTME 2.8 (standardmäßig aktiviert).
- IGEL OS 11.01.100 beinhaltet RTME 2.7 (standardmäßig deaktiviert).
  
- IGEL OS 10.06.100 beinhaltet RTME 2.8 (standardmäßig deaktiviert).
- IGEL OS 10.05.500 beinhaltet RTME 2.6 (standardmäßig deaktiviert).
- IGEL OS 10.05.100 beinhaltet RTME 2.6 (standardmäßig deaktiviert).

Weitere Informationen finden Sie unter [Citrix HDX RealTime Optimization Pack](#).<sup>28</sup>

---

<sup>28</sup> <https://docs.citrix.com/de-de/hdx-optimization/>

## Citrix Advanced Endpoint Analysis (EPA) Client on IGEL OS

**i** Dieser Artikel ist gültig für IGEL OS 11.08.290 oder höher.


Mit Version 11.08.290 wurde der Citrix Advanced Endpoint Analysis (EPA) Client in IGEL OS integriert. Clientseitig ist keine Konfiguration notwendig. Wenn die Netscaler-URL auf dem Browser des Geräts (Chromium oder Firefox) geöffnet wird, werden die in Netscaler konfigurierten NSEPA-Prüfungen automatisch durchgeführt.

Da dynamische Aktualisierungen in IGEL OS wegen des Read-Only-Systems nicht möglich sind, müssen Sie die automatische Aktualisierung in Netscaler abschalten:


- ▶ Setzen Sie in Netscaler die Option **Linux EPA Plugin Upgrade** auf **Never**.

The screenshot shows the configuration page for a VPN Virtual Server in Netscaler. The page is titled "VPN Virtual Server" and has a "Basic Settings" section. The "Linux EPA Plugin Upgrade" dropdown menu is highlighted with a red box and set to "Never". Other settings include "Windows EPA Plugin Upgrade" and "Web EPA Plugin Upgrade". The "Advanced Settings" section on the right includes "Content Switching Policies", "SSL Profile", "SSL Policies", "Intranet IP Addresses", "Intranet Applications", and "EULA".

## Citrix Netscaler Gateway Client (NSGClient) for Netscaler VPN Connections

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Unexpected Keyboard Layout in a Citrix Session

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## RDP

- [USB-Speichergeräte in RDP-Sitzungen bereitstellen](#) (see page 270)
- [Welche Zeichenkette soll ich bei Token-Based Load Balancing eingeben?](#) (see page 273)
- [RDP Fabulatech Scanner Redirection](#) (see page 274)
- [RDP RemoteApp Parametereinstellungen](#) (see page 276)
- [RDP-Leistung verbessern](#) (see page 277)
- [RDPSND\\_NEGOTIATE-Fehler in RDP-Sitzung](#) (see page 279)
- [Knackgeräusche und Audio-Aussetzer in RDP-Sitzungen](#) (see page 280)
- [Anmeldung fehlgeschlagen aufgrund des abgelaufenen AD-Passworts](#) (see page 282)
- [Benutzer muss Anmeldeinformationen für die RDP-Anmeldung doppelt angeben](#) (see page 284)

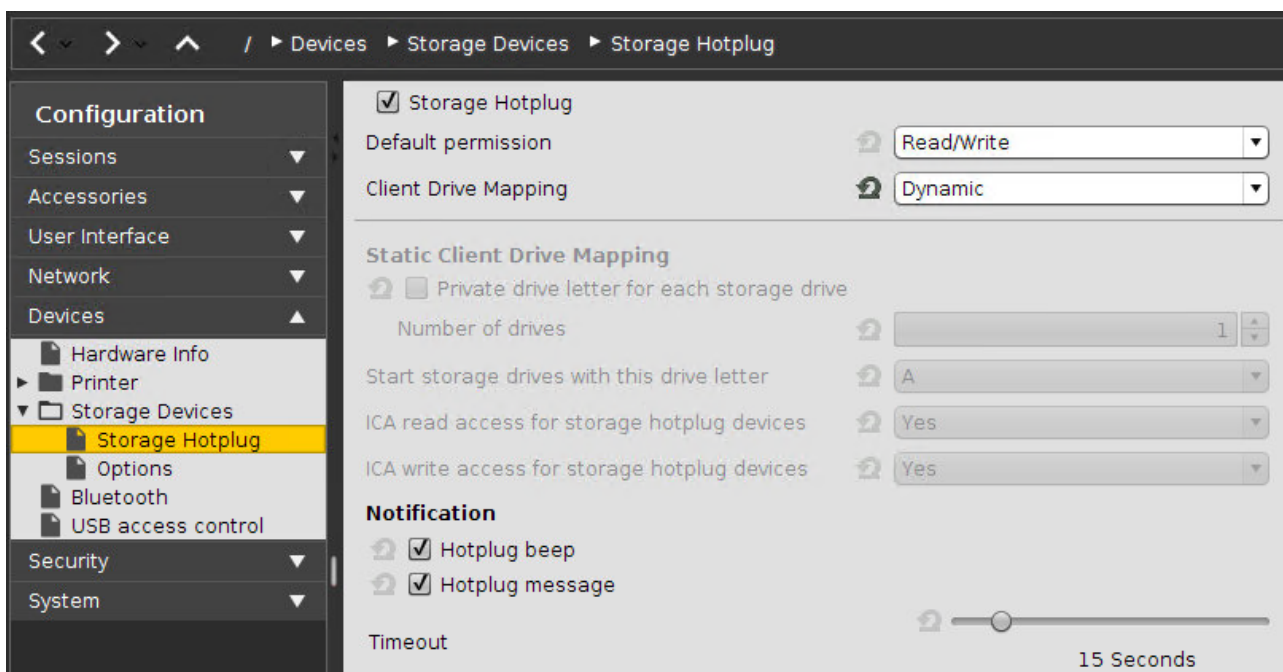
## USB-Speichergeräte in RDP-Sitzungen bereitstellen

In diesem How-to erfahren Sie, wie Sie an den Thin Client angeschlossene USB-Speichergeräte in RDP-Sitzungen bereitstellen.

### Lösung

**i** Die Bereitstellung von USB-Speichergeräten ist für Geräte der Klasse "usb mass storage class" möglich. Der Zugriff auf den Speicher von Smartphones oder Digitalkameras erfolgt normalerweise über das MTP-Protokoll. Das MTP-Protokoll wird ab IGEL OS 10.04.100 unterstützt, siehe [Mobilgeräte-Zugriff verwenden](#) (see page 773).

### Grundkonfiguration des Clients



In IGEL Setup oder einem UMS-Profil müssen Sie folgende Parameter konfigurieren:

► Aktivieren Sie **Geräte > Speichergeräte > Speicher-Hotplug > Zuordnung der Client-Laufwerke > Dynamisch**. Diese Option aktiviert die dynamische Zuordnung von Client-Laufwerken. Neue Speichermedien werden beim Anschluss an den Thin Client automatisch erkannt. Der Thin Client piept und zeigt eine Benachrichtigung an, während er das neue Gerät einbindet. Die Speichergeräte werden automatisch auf dem Thin Client und in Citrix ICA Sitzungen nutzbar.

Die nachfolgenden Einstellungen sind nur für Sitzungen ohne dynamische Laufwerkszuordnung relevant.

⚠ Montierte Geräte müssen vor dem Entfernen abmontiert werden, um Datenintegrität zu gewährleisten. Dies kann über das **Disk Utility**, das neue **Hardware sicher entfernen**-Tool oder ein Tray-Icon erfolgen.

## Zusätzliche zu prüfende Parameter

Die folgenden Parameter sind standardmäßig eingestellt, so dass die Laufwerkszuordnung funktioniert, aber vielleicht haben Sie diese aus irgendeinem Grund geändert und müssen sie anpassen, um die Laufwerkszuordnung zu ermöglichen:

- **Sitzungen > RDP > RDP Global > Mapping > Laufwerkszuordnung > Laufwerkszuordnung aktivieren (Haken setzen)**
- **Sitzungen > RDP > RDP Global > Native USB Redirection > Native USB Redirection (Haken rausnehmen)**
- **Sitzungen > RDP > RDP Global > Fabulatech USB Redirection > Fabulatech USB Redirection (Haken rausnehmen)**
- **Geräte > USB-Zugriffskontrolle > Aktiviert (Haken rausnehmen)**
- **Sitzungen > RDP > RDP-Sitzungen > [session name] > USB Redirection > Native USB Redirection (Globale Einstellung)**
- **Sitzungen > RDP > RDP-Sitzungen > [session name] > Mapping > Laufwerkszuordnung aktivieren (Globale Einstellung)**

## Zuweisen eines Laufwerksbuchstaben innerhalb der Sitzung (optional)

Wenn Sie nicht nur das Laufwerk in der Sitzung wie z. B. "A auf IGEL-123456789" sehen möchten, sondern das Laufwerk innerhalb der Sitzung mit einem echten Laufwerksbuchstaben ansprechen möchten, können Sie einen dieser Befehle ausführen:

```
subst T: \\tsclient\t
```

or

```
net use T: \\tsclient\t
```

In diesem Beispiel wird "T auf IGEL-123456789" dem Laufwerksbuchstaben T: innerhalb der Sitzung zugewiesen. Sie können das zugeordnete Laufwerk auch einem anderen Laufwerksbuchstaben zuweisen, der im Namen verwendet wird.

## Konfiguration auf der Serverseite

Auf der Serverseite, z.B. bei Windows Server 2008R2, hat ein Benutzer in der Gruppe "Benutzer" mit Zugriff auf den Terminalserver standardmäßig die Zuordnung. Dies gilt für einen neu installierten Server. Aber das Mapping kann durch eine Änderung der Richtlinien verhindert werden.

**i Do not allow drive redirection** - Gibt an, ob die Zuordnung von Client-Laufwerken in einer Remote Desktop Services-Sitzung verhindert werden soll (Laufwerksumleitung). Standardmäßig ordnet ein RD Session Host-Server Client-Laufwerke automatisch nach der Verbindung zu. Zugeordnete Laufwerke erscheinen im Sitzungsordnerbaum des Windows Explorers oder Computers im Format[Laufwerksbuchstabe] auf[Computername]. Mit dieser Einstellung können Sie dieses Verhalten außer Kraft setzen. Quelle: <https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx>Source: <https://technet.microsoft.com/de-de/library/ee791794%28v=ws.10%29.aspx>



## Welche Zeichenkette soll ich bei Token-Based Load Balancing eingeben?

### Umgebung

Token-Based Load Balancing wird als Methode zur Lastverteilung verwendet. Dieses Dokument ist nicht auf andere Load-Balancing-Methoden anwendbar.

### Frage

Welche Zeichenkette muss in **Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > Optionen** eingegeben werden, damit das Token-Based Load Balancing funktioniert?

### Antwort

IGEL OS 10.05.700 oder höher, IGEL OS 11.01.110 oder höher

► Geben Sie unter **Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > Optionen > Sammlung** einfach den Namen Ihrer RDS-Sammlung (Collection) ein. Der Name der Sammlung wurde vom Serveradministrator festgelegt.

IGEL OS 10.01 bis 10.05.500, 11.01.100

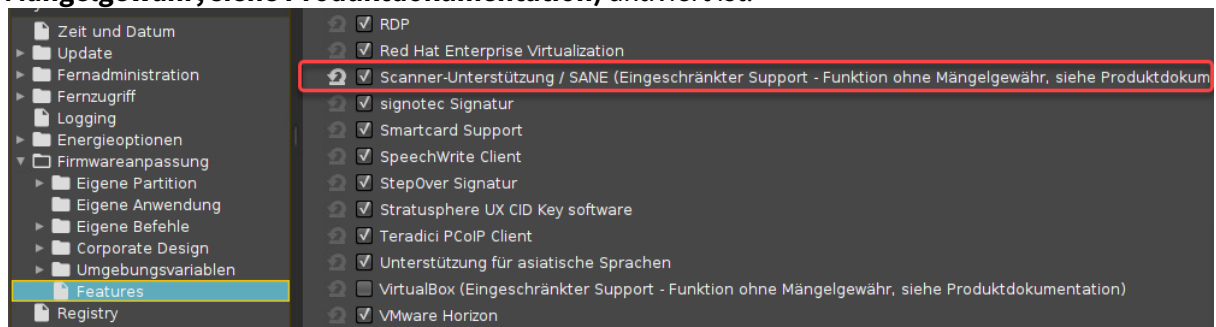
► Geben Sie unter **Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > Optionen > Routing Token für Load Balancer** die Zeichenkette `tsv://MS TerminalServices Plugin.1.[Name der Sammlung]` ein, wobei

- `tsv://MS TerminalServices Plugin.1.` das Routing Token ist und
- `[Name der Sammlung]` der Name der RDS-Sammlung (Collection); dieser wurde vom Serveradministrator festgelegt.

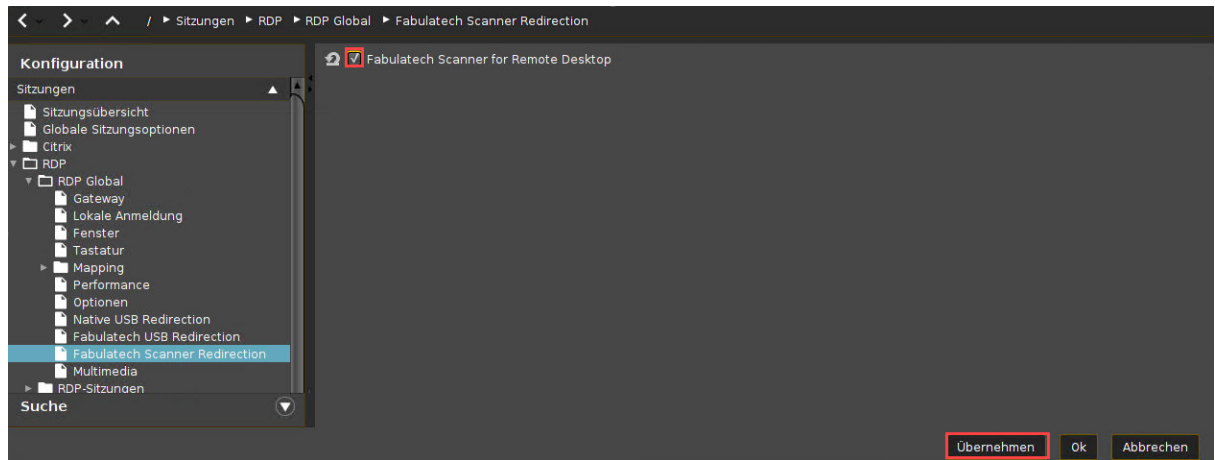
## RDP Fabulatech Scanner Redirection

### Fabulatech Scanner Redirection aktivieren

1. Gehen Sie im IGEL Setup auf **System > Firmwareanpassung > Features** und stellen Sie sicher, dass **Scanner-Unterstützung / SANE (Eingeschränkter Support - Funktion ohne Mängelgewähr, siehe Produktdokumentation)** aktiviert ist.



- Wenn die Option bereits aktiviert ist, fahren Sie mit Schritt 2 fort.
  - Wenn die Option noch nicht aktiviert war, muss die Softwarekomponente erst heruntergeladen werden. Stellen Sie hierzu sicher, dass die Quelle der aktuellen Firmware korrekt gesetzt ist:
    - Wenn Sie Universal Firmware Update nutzen, stellen Sie sicher, dass das Gerät der aktuellen Firmware zugewiesen ist. Die Einzelheiten finden Sie unter Universal Firmware Update und Updates zuweisen.
    - Wenn Sie Universal Firmware Update nicht nutzen, stellen Sie sicher, dass **System > Update > Firmwareupdate** auf die Quelle der aktuellen Firmware gesetzt ist. Die Einzelheiten finden Sie unter Firmwareupdate-Einstellungen für IGEL OS.
  - Nachdem Sie **OK** geklickt haben, um Ihre Änderungen zu speichern, müssen Sie das System neu starten.
2. Gehen Sie im IGEL Setup unter **Sitzungen > RDP > RDP Global > Fabulatech Scanner Redirection**.
  3. Setzen Sie einen Haken bei **Fabulatech Scanner for Remote Desktop**.



4. Klicken Sie **Übernehmen** oder **Ok**, um die Einstellungen zu übernehmen.

## RDP RemoteApp Parametereinstellungen

### Symptom

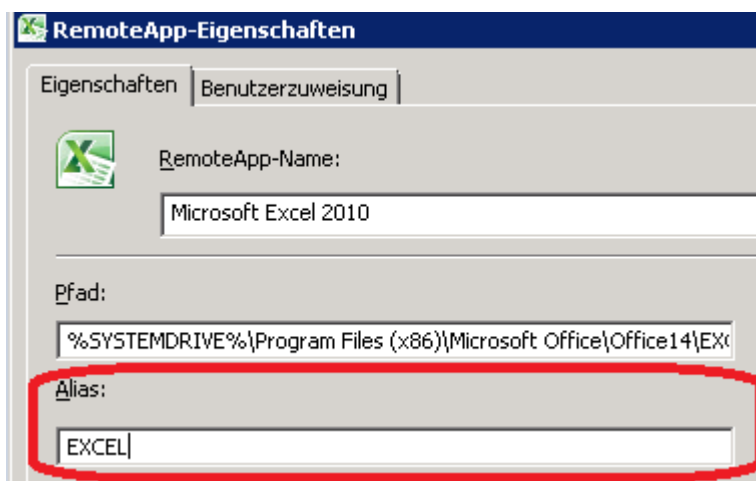
Die RemoteApp öffnet oder schließt sich nicht unmittelbar nach einer Anmeldung.

### Problem

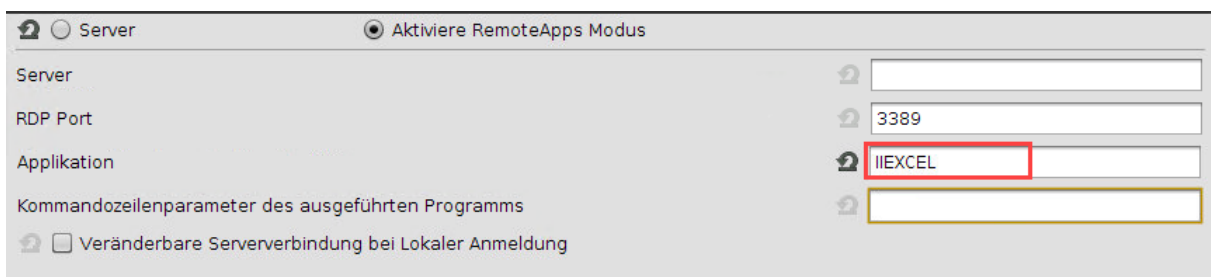
Sitzungseinstellungen auf dem Server oder Gerät sind fehlerhaft oder unvollständig.

### Lösung

1. Stellen Sie mit der **RemoteApp Management Console** auf dem Terminalserver einen ALIAS für die RemoteApp ein.



2. Verwenden Sie den ALIAS-Wert in der Geräteeinstellung **Setup > Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > Server > Applikation**



**i** Fügen Sie zwei Pipe-Zeichen ( || ) am Anfang des ALIAS-Wertes hinzu.

## RDP-Leistung verbessern

### Symptom

RDP-Benutzer haben Leistungsprobleme (schlechte Benutzererfahrung)

Beispiel:

- Maus ist verzögert
- Bildschirm baut sich sehr langsam auf
- Sitzung nutzt hohe Bandbreite
- Verschiedene andere Leistungsprobleme

### Problem

Es gibt viele verschiedene Ursachen, die zu einer verminderten Leistung führen können.

### Lösung

Die folgenden Einstellungen können sowohl einzeln als auch in Kombination verwendet werden

#### Grundlagen

- Die Farbtiefe sollte auf dem Server, dem Gerät und in der Sitzung gleich sein (am besten: 32 Bit).
- Setzen Sie im BIOS den gemeinsamen VGA-Speicher (VGA shared memory) auf 64 MB oder mehr.

#### Optimierungen für eine LAN-Umgebung

- Ändern Sie unter **Sitzungen > RDP > RDP Global > Performance** die Einstellungen wie folgt:
  - Deaktivieren Sie **Komprimierung**. (Erhöht die Performanz, erzeugt etwa 30% mehr Netzwerkverkehr.)
  - Wenn RemoteFX 8 verfügbar ist, schalten Sie **RemoteFX aktivieren** ein.
  - Wenn RemoteFX 8 verfügbar ist, setzen Sie **RemoteFX-Codec-Modus** auf "Optimiert für LAN".
- Wenn Windows Server 2012r2 oder niedriger bzw. Windows 8.1 oder niedriger verwendet wird: Aktivieren Sie unter **Sitzungen > RDP > RDP Global > Multimedia** die Option **Video Redirection**.

#### Optimierungen für eine WAN-Umgebung

- Ändern Sie unter **Sitzungen > RDP > RDP Global > Performance** die Einstellungen wie folgt:
  - Aktivieren Sie **Komprimierung**. (Erzeugt etwa 30% weniger Netzwerkverkehr, verbraucht mehr lokale Ressourcen.)
  - Wenn RemoteFX 8 verfügbar ist, schalten Sie **RemoteFX aktivieren** ein.

- Wenn RemoteFX 8 verfügbar ist, setzen Sie **RemoteFX-Codec-Modus** auf "Optimiert für WAN".

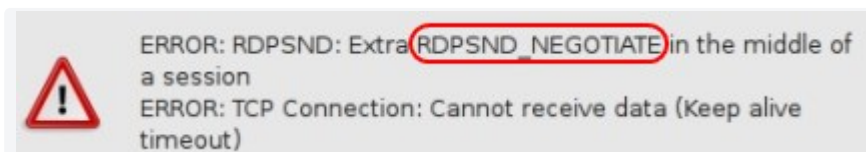
## RDPSND\_NEGOTIATE-Fehler in RDP-Sitzung

### Symptom

Bei der Wiedergabe eines Sounds wird die RDP-Verbindung auf einigen Geräten mit einer Fehlermeldung abgebrochen:

```
ERROR: RDPSND: Extra RDPSND_NEGOTIATE in the middle of a session
```

```
ERROR: TCP Connection: Cannot receive data (Keep alive timeout)
```



### Problem

Dies kann passieren, wenn während der Datenübertragung die Verbindung ausfällt.

### Lösung

Probieren Sie einen anderen Audiotreiber für die RDP-Sitzung:

1. Gehen Sie unter **System > Registry > rdp.winconnect.sound-driver**
2. Wählen Sie **OSS** oder **ALSA**

## Knackgeräusche und Audio-Aussetzer in RDP-Sitzungen

### Symptom

Die Benutzererfahrung bei RDP-Sitzungen wird durch Knackgeräusche und Aussetzer beeinträchtigt.

### Umgebung

- Gerät mit einer Soundkarte, die einen kleinen Puffer hat, z. B. IGEL UD3 (M340C)
- Für die Lösung benötigt: IGEL OS 11.03.500 oder höher

### Problem

Die Knackgeräusche oder Audio-Aussetzer entstehen, wenn der Puffer leerläuft (buffer underrun). Dies geschieht, wenn neue Audiodaten nicht schnell genug geliefert werden und der Puffer der Soundkarte keine Audiodaten mehr zum Abspielen übrig hat. Somit kann die Lücke in der Wiedergabe nicht gefüllt werden. Dies passiert besonders leicht bei Soundkarten mit relativ kleinem Puffer.

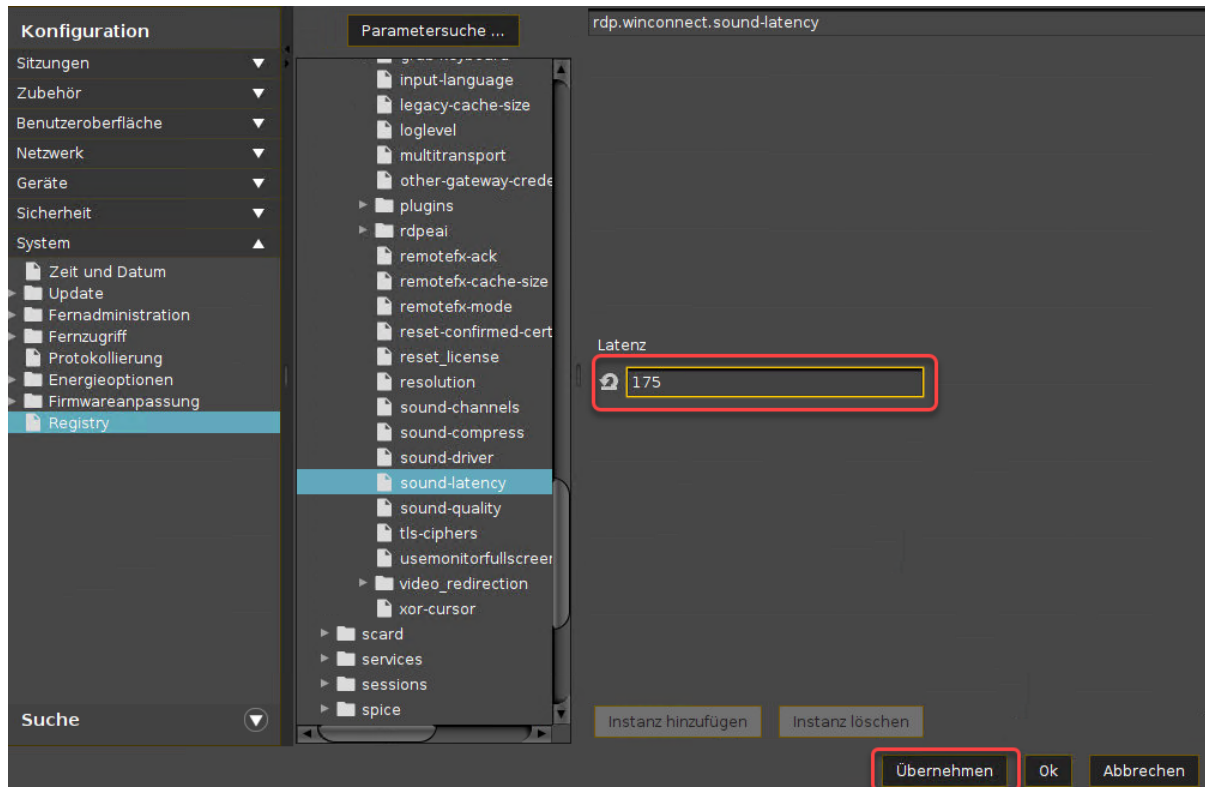
### Lösung

Um dem Gerät zu ermöglichen, größere Lücken zu füllen, muss Pufferkapazität hinzugefügt werden. Dies kann erreicht werden, indem man den Puffer des RDP-Clients erhöht, wodurch zugleich die Latenz erhöht wird. Allerdings kann eine hohe Latenz ein Problem bei interaktiven Anwendungen darstellen, etwa bei Telefonaten oder Videokonferenzen.

Um die Latenz des RDP-Clients zu erhöhen:

1. Öffnen Sie das Setup des Geräts und gehen Sie zu **System > Registry > rdp > winconnect > sound-latency** (Registry Key: `rdp.winconnect.sound-latency`).
2. Erhöhen Sie die Latenz um ungefähr 50 Millisekunden (empfohlen) und klicken Sie **Übernehmen**.





3. Starten Sie die RDP-Sitzung neu und testen Sie die Audiowiedergabe.
4. Wenn die Audioqualität gut ist, klicken Sie **Ok**, um das Setup zu schließen. Wenn immer noch Knackgeräusche auftreten, wiederholen Sie Schritt 2 und 3, bis die Audioqualität akzeptabel ist.

## Anmeldung fehlgeschlagen aufgrund des abgelaufenen AD-Passworts

Wenn Sie versuchen, sich bei einer **RDP**-Sitzung anzumelden, erhalten Sie die Fehlermeldung "Anmeldung fehlgeschlagen!", da Ihr Active Directory-Passwort abgelaufen ist.

Sie können Ihr Passwort nicht ändern, da das lokale Login keine Option dafür bietet.

**i** Bevor Sie diesen Anweisungen folgen, überprüfen Sie, ob die Ports offen sind, vielleicht können Sie das Problem dadurch beheben:

- Anmeldung auf dem Client -> Port: 88
- Passwort ändern -> Port: 464

Hier finden Sie eine Übersicht über die Ports des Domain Controllers: [Required Ports to Communicate with Domain Controller](https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS)<sup>29</sup>

## Lösung

Aktivieren Sie die **Active Directory/Kerberos** Authentifikation für die **RDP**-Sitzung. Beim nächsten Versuch, sich im IGEL OS anzumelden, werden Sie aufgefordert Ihr Passwort zu ändern.

## Ändern eines abgelaufenen Active Directory Passworts

**!** Bei der Verwendung von Sitzungen mit Passthrough-Authentifizierung ist es wichtig, dass Sie den Bildschirm Ihres Geräts sperren, wenn es unbeaufsichtigt bleibt.

### Active Directory/Kerberos-Authentifizierung für RDP-Sitzungen aktivieren

1. Gehen Sie im IGEL Setup unter **Security > Anmeldung > Active Directory/Kerberos**.
2. Aktivieren Sie **Anmeldung an Active-Directory-Domäne**.
3. Gehen Sie unter **Sicherheit > Active Directory/Kerberos**.
4. Setzen Sie ein Häkchen bei **Aktivieren**.
5. Geben Sie die **Standarddomäne (vollständiger Domänenname)** ein.
6. Gehen Sie unter **Sitzungen > RDP > RDP Sitzung > [RDP-Sitzung] > Anmeldung**.
7. Aktivieren Sie **Passthrough-Authentifizierung verwenden**.
8. Klicken Sie **Übernehmen** oder **Ok**.

**i** Bitte beachten Sie, dass das Gerät nun lokal und nicht mehr in der Sitzung gesperrt sein muss, um zu verhindern, dass eine andere Person über den Passthrough ohne Angabe des Passworts in die Sitzung gelangt.

<sup>29</sup> <https://social.technet.microsoft.com/Forums/windows/en-US/1c6a59de-c1fe-4946-bb4e-1fe36fd40b08/required-ports-to-communicate-with-domain-controller?forum=winserverDS>

## Bildschirmsperre aktivieren

1. Gehen Sie im IGEL Setup unter **Benutzeroberfläche > Bildschirmsperre/-schoner**.
2. Aktivieren Sie **Hotkey**.
3. Wählen Sie **Win** unter **Steuertasten**.
4. Geben Sie "L" ein unter **Hotkey**.
5. Gehen Sie auf **Benutzeroberfläche > Bildschirmsperre/-schoner > Optionen**.
6. Aktivieren Sie **Benutzerpasswort**.

Der Hotkey "Win + L" sperrt nun das IGEL-Gerät anstelle des Sitzungsdesktops.

Zur Aktivierung der IGEL-Geräte muss das AD-Passwort eingegeben werden.

## Benutzer muss Anmeldeinformationen für die RDP-Anmeldung doppelt angeben

### Problem

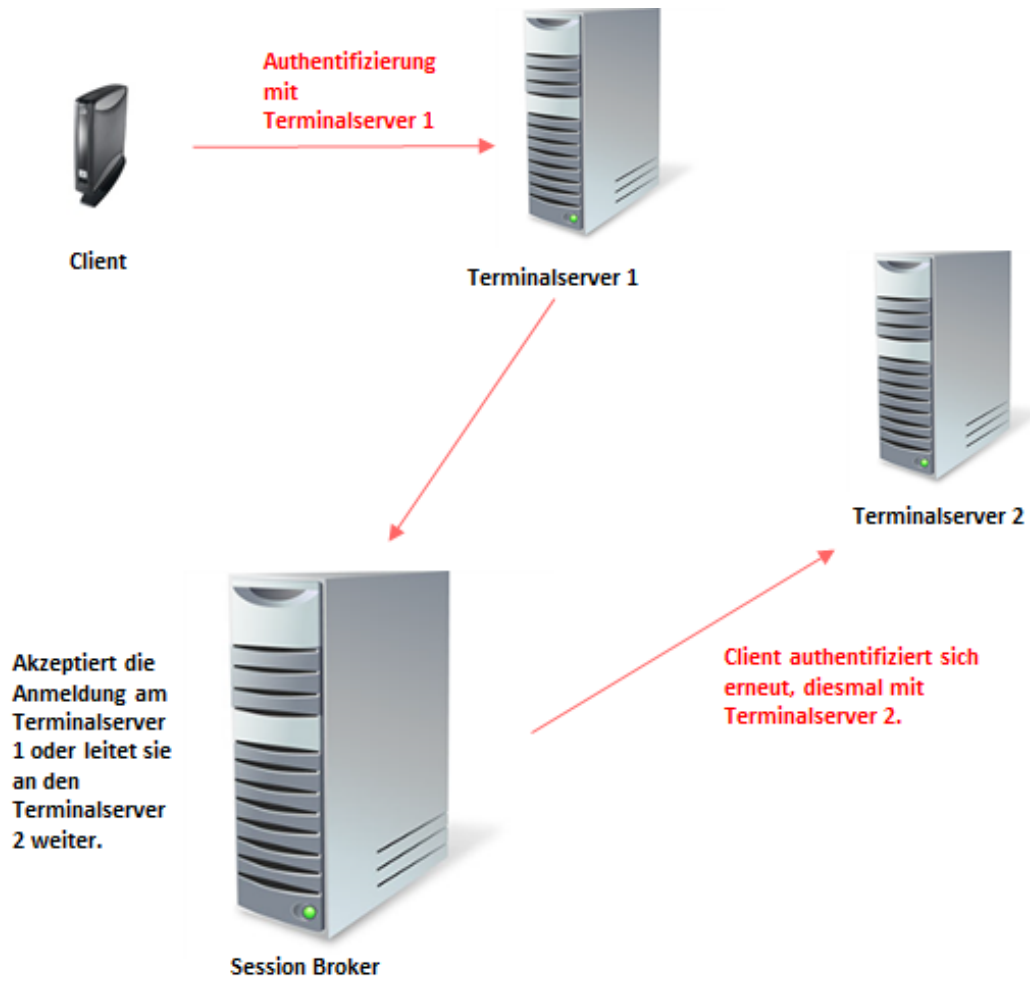
Wenn Sie sich mit einem Windows-Terminalserver verbinden, werden Sie aufgefordert, Ihre Anmeldeinformationen zweimal einzugeben.

### Ursache

Dieses Verhalten wird durch die Funktionsweise des RDS-Lastausgleichs verursacht. Das Problem ist, dass der Terminalserver nicht direkt mit dem Session Broker kommuniziert.

Stattdessen ist das Szenario wie folgt:

1. Der Client verbindet sich mit dem Terminalserver 1 und authentifiziert sich mit dem Terminalserver 1. Dies ist das erste Mal, dass der Benutzer nach seinen Zugangsdaten gefragt wird.
2. Da wir ein Load Balancing-Setup haben, wird Terminalserver 1 mit dem Session Broker sprechen und fragen, ob der Client Terminalserver 1 verwenden kann oder ob er auf einen anderen Terminalserver umgeleitet werden soll.
3. Wenn eine Umleitung stattfindet, muss sich der Client auch bei dem Terminalserver authentifizieren, auf den der Client umgeleitet wurde (Terminalserver 2 in der folgenden Abbildung). Dies ist das zweite Mal, dass der Benutzer nach seinen Zugangsdaten gefragt wird.



## Lösung

Das Problem kann durch Aktivieren der Kerberos/Active Directory Authentifizierung behoben werden. Weitere Informationen finden Sie unter Active Directory/Kerberos v10.04.

## VMware Horizon

- [VMware Blast für Horizon Client-Sitzungen aktivieren \(see page 287\)](#)
- [NLA für die Anmeldung mit Horizon Client-Sitzungen verwenden \(see page 288\)](#)
- [Workaround für Hotkeys in Horizon Sitzungen \(see page 289\)](#)
- [Multimedia-Beschleunigung mit VMware Horizon View im VESA-Modus \(see page 290\)](#)
- [Horizon Feature Matrix \(see page 291\)](#)
- [Troubleshooting the Horizon Client \(see page 292\)](#)
- [VMware Horizon Authentifizierungsprobleme \(Zertifikatswiderrufsliste\) \(see page 293\)](#)

## VMware Blast für Horizon Client-Sitzungen aktivieren

### Voraussetzungen

- Gerät mit Hardware-Videobeschleunigung, siehe das FAQ [Hardware-Videobeschleunigung auf IGEL OS \(see page 853\)](#)
- VMware Horizon 7 Server  
Weitere Informationen zur Serverkonfiguration finden Sie auf der Webseite von VMware in der Dokumentation zu VMware Horizon 7: <https://docs.vmware.com/de/VMware-Horizon-7/index.html>

### VMware Blast aktivieren

1. Gehen Sie in IGEL Setup zu **System > Firmwareanpassung > Features**.
2. Aktivieren Sie **Hardware-Videobeschleunigung**.
3. Gehen Sie zu **Sitzungen > Horizon Client > Horizon Client Global > Serveroptionen**.
4. Setzen Sie **Bevorzugtes Verbindungsprotokoll** auf **VMware Blast**.
5. Klicken Sie **Übernehmen** oder **Speichern**.

## NLA für die Anmeldung mit Horizon Client-Sitzungen verwenden

Das Starten einer Sitzung, auch wenn nur ein Anmeldebildschirm angezeigt wird, hat erhebliche Auswirkungen auf die Ressourcen. Jedes Mal wenn ein Benutzer versucht sich anzumelden, werden Prozesse auf dem Remote-Computer gestartet, unabhängig davon ob die Anmeldeinformationen des Benutzers gültig sind oder nicht. Mit dem Network Layer Authentication (NLA) können Sie Ressourcen sparen und Denial of Service (DoS)-Angriffe verhindern. NLA prüft, ob ein Benutzer die richtige Person ist, bevor ein Anmeldevorgang gestartet wird.

Weitere Informationen zu NLA, finden Sie unter <https://technet.microsoft.com/en-us/magazine/hh750380.aspx>.

NLA für Horizon Client-Sitzungen ist ab IGEL Linux Version 5.08.100 verfügbar.

Um NLA für Horizon Client-Sitzung zu verwenden:

1. Öffnen Sie Setup und gehen Sie zu **Sitzungen > Horizon Client > Horizon Client-Sitzungen > [Sitzungsname] > Optionen**
2. Aktivieren Sie **Authentifizierung auf Netzwerkebene**.



## Workaround für Hotkeys in Horizon Sitzungen

### Problem

Sie möchten mit der Tastenkombination [Strg] + [Windows] + [D] aus der VMware Horizon Sitzung auf den IGEL Desktop wechseln. Während die Tastenkombination [Strg] + [Windows] + [D] bei IGEL OS 11.01.100 oder niedriger (Horizon Client 4.x) realisiert werden kann, ist dies bei IGEL OS 11.01.110 oder höher (Horizon Client 5.x) nicht möglich.

### Lösung

1. Drücken Sie [Strg] + [Alt] und lassen Sie die Tasten los.  
Der Fokus wird von der VMware Horizon Sitzung auf das lokale System umgeschaltet.
2. Drücken Sie [Strg] + [Windows] + [D], um auf den IGEL Desktop zu wechseln.
3. Um den Fokus wieder auf die VMware Horizon Sitzung zu setzen, klicken Sie in das Fenster der VMWare Horizon Sitzung.

## Multimedia-Beschleunigung mit VMware Horizon View im VESA-Modus

### Symptom

Sie haben IGEL Universal Desktop OS 2 auf nicht vollständig unterstützter Hardware mit IGEL Universal Desktop Converter 2 installiert. Die Multimedia-Beschleunigung funktioniert innerhalb einer VMware Horizon View-Sitzung nicht.

### Problem

Der Grafikchip Ihrer Hardware wird nicht unterstützt und als Fallback wird der VESA-Modus verwendet.

### Lösung


Es gibt keine andere Lösung für das Problem, als die Verwendung vollständig unterstützter Hardware. Informationen zur unterstützten Hardware finden Sie im UDC2-Handbuch.

Sie können auch auf [IGEL's 3rd party hardware support database](https://www.igel.com/linux-3rd-party-hardware-database/)<sup>30</sup> zugreifen, um vollständig unterstützte Grafikchips zu finden.


---

<sup>30</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

## Horizon Feature Matrix

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## Troubleshooting the Horizon Client

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## VMware Horizon Authentifizierungsprobleme (Zertifikatswiderrufsliste)

Neuere Versionen von VMware Horizon Client für Linux versuchen, eine Zertifikatswiderrufsliste (Certificate Revocation List, CRL) für alle Zertifikate herunterzuladen, die für die Verbindung mit einer VMware Horizon Umgebung verwendet werden. Manchmal kann dies auf Geräten mit niedrigerem Stromverbrauch oder auf Geräten, die keinen Zugriff auf eine CRL-Adresse haben, ein Problem verursachen.

Der folgende Artikel erklärt, wie Sie den CRL-Download deaktivieren können, wenn Sie Probleme mit der Authentifizierung für VMware Horizon Sitzungen in IGEL OS haben.

---

### Problem

Sie stoßen auf die folgenden Probleme:

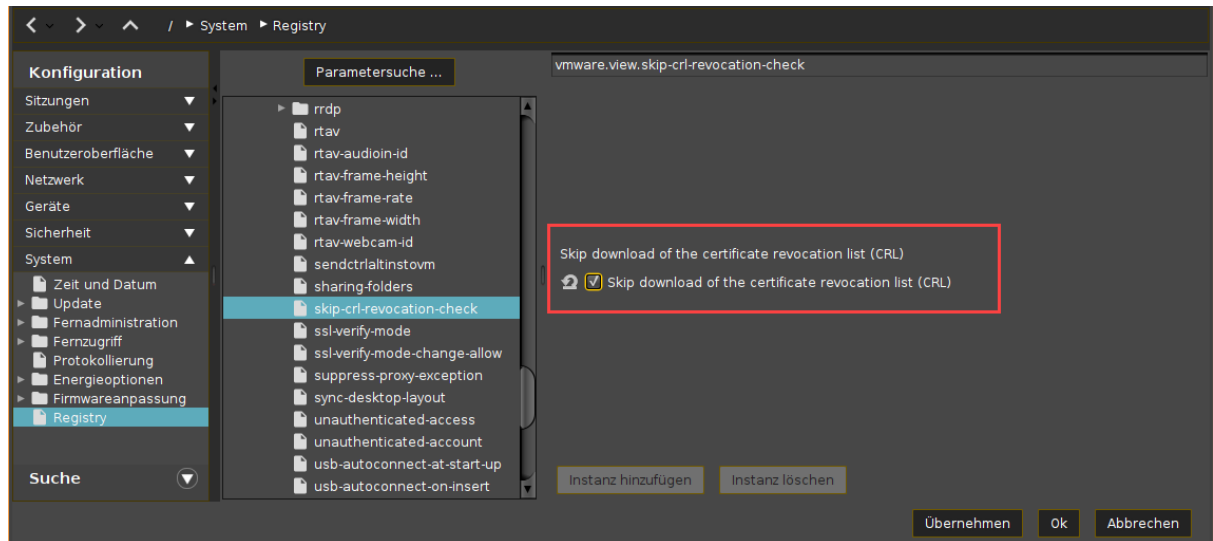
- Der VMware Horizon Client "hängt" während der Authentifizierung.  
ODER
- Der VMware Horizon Client benötigt viel Zeit für die Authentifizierung (in einigen Fällen über 1 Minute).  
ODER
- Sie verwenden ein Zertifikat, das von der Zertifizierungsstelle (CA) für die Domäne ausgestellt wurde, und erhalten die folgende Fehlermeldung:  
"Failed to connect to the connection server. The server provided an invalid certificate. Unsupported URI in CRL distribution points extension, only http/https are supported."

### Lösung

Diese Probleme entstehen normalerweise aufgrund der Standardeinstellung für das Herunterladen von CRLs für den VMware Client für Linux. Wenn die oben genannten Probleme auftreten, wird empfohlen, das Herunterladen der CRL zu deaktivieren.

Um den Download der CRL zu deaktivieren, gehen Sie wie folgt vor:

1. Gehen Sie im IGEL Setup oder im Konfigurationsdialog in der UMS zu **System > Registry**.
2. Aktivieren Sie den Registry Key `vmware.view.skip-crl-revocation-check`, d.h. **Skip download of the certificate revocation list (CRL)**.



3. Übernehmen Sie die Einstellungen. Wenn Sie ein Profil erstellt haben, weisen Sie das Profil den erforderlichen Geräten zu.
4. Starten Sie die Geräte neu und testen Sie noch einmal die Verbindung.

## Evidian

- [Authentifizierung mit dem Evidian Authentication Manager \(see page 296\)](#)

## Authentifizierung mit dem Evidian Authentication Manager


Mit dem Evidian Authentication Manager (AuthMgr) können Sie sich mit Citrix-, RDP- und VMware Horizon-Roaming-Sitzungen über RFID-Badges verbinden. Benutzerdefinierte Befehle werden ebenfalls unterstützt.

### Voraussetzungen

- IGEL Universal Desktop Linux 5.06.100 oder neuer auf dem Gerät.
- Ein installierter und laufender Evidian SSO Controller, Version 10.0 oder höher
- Bei Verwendung von HTTPS (IGEL Linux 5.07.100 oder neuer) wird das CA-Root-Zertifikat des User Access Servers lokal auf dem Gerät gespeichert.
- Das Gerät und der/die Server müssen Teil derselben Active Directory-Domäne sein.
- Ein unterstütztes RFID-Lesegerät (z. B. OMNIKEY 5022 CL, OMNIKEY 5421), das an den Endpoint angeschlossen ist.
- RFID-Badges, die bereits registriert sind.

### Konfigurieren einer Evidian Authentication Manager-Sitzung

1. Gehen Sie im Setup des Geräts zu **Sitzungen > Evidian AuthMgr > Evidian AuthMgr Sitzungen**.
2. Fügen Sie eine neue Sitzung hinzu.
3. Gehen Sie zu **Sitzungen > Evidian AuthMgr > Evidian AuthMgr Sitzungen > [Sitzungsname] > Verbindung**.
4. Wählen Sie das **Protokoll**, das für den User Access Service verwendet wird (z. B. HTTP).
5. Geben Sie unter **Server** die IP-Adresse oder den DNS-Namen an, der für den User Access Service verwendet wird.
6. Wählen Sie den **Port** für den User Access Service aus (z. B. 9764).
7. Geben Sie unter **Servicepfad** den Pfad für den User Access Service an (z. B. `/soap`).
8. Geben Sie unter **Stammzertifikat** den Pfad zum Stammzertifikat mit Dateiname, zum Beispiel `/wfs/ca-certs/ca.crt`. Das Zertifikat wird für HTTPS-Verbindungen benötigt.
9. Geben Sie das **Roamingsitzung-Passwort** an.
10. Wenn Sie HTTPS verwenden, wählen Sie das **CA-Root-Zertifikat** des User Access Servers auf dem Gerät als Stammzertifikat aus.
11. Gehen Sie zu **Sitzungen > Evidian AuthMgr > Evidian AuthMgr Sitzungen > [Sitzungsname] > Optionen** und wählen Sie den gewünschten **Sitzungstyp** aus.  
Der hier ausgewählte Sitzungstyp, z. B. RDP, wird vom Evidian Authentication Manager als erste konfigurierte Sitzung verwendet. Stellen Sie sicher, dass eine Sitzung konfiguriert ist.

 Wenn Sie benutzerdefinierte Befehle wählen, müssen Sie die Befehle bereitstellen; siehe [Custom Commands](#) (see page 298). Weitere Optionen finden Sie unter Optionen im IGEL OS Referenzhandbuch.

12. Starten Sie die neue Sitzung, indem Sie auf das Symbol im **Startmenü** klicken. Alternativ können Sie das Gerät neu starten. In der standardmäßigen Autostarteneinstellung startet der Evidian

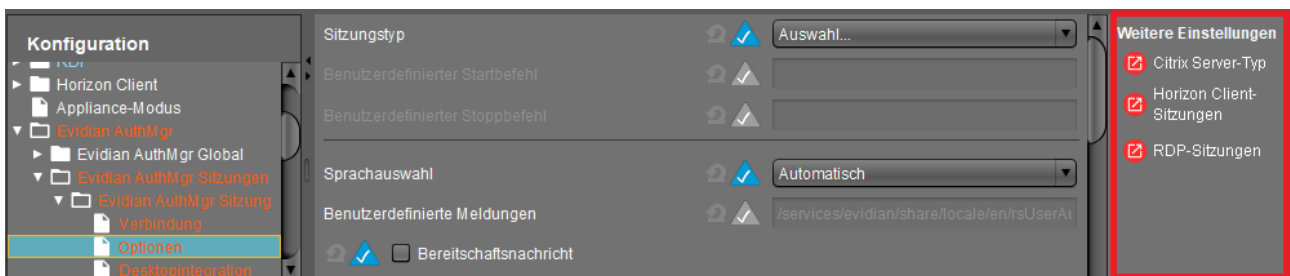


Authentication Manager für Ihre Sitzung automatisch und wartet darauf, dass ein RFID-Badge auf dem Lesegerät angebracht wird.

 Sie können nur eine einzelne Instanz einer Evidian Authentication Manager-Sitzung starten.

## Citrix/RDP/VMware Horizon Sitzung konfigurieren

► Konfigurieren Sie die Sitzung, die Sie mit dem Evidian Authentication Manager verwenden möchten, als erste Sitzung dieser Art. Die Verknüpfungen zu den Sitzungseinstellungen sind im Setup-Bereich **Weitere Einstellungen** zu finden:



### Eine benutzerdefinierte Konfigurationsdatei verwenden

Anstatt die Einstellungen des IGEL Setups zu verwenden, können Sie unter **Sitzungen > Evidian AuthMgr > Evidian AuthMgr Sitzungen > [Sitzungsname] > Optionen > Verwende benutzerdefinierte Konfigurationsdatei** eine benutzerdefinierte Konfigurationsdatei aktivieren. Dann werden alle anderen Sitzungseinstellungen ignoriert. Eine kommentierte Vorlage für die Konfigurationsdatei finden Sie unter `/etc/rsUserAuth/rsUserAuth.ini`.

### Mit Evidian Authentication Manager anmelden

1. Platzieren Sie Ihren RFID-Badge auf dem RFID-Lesegerät (oder tippen Sie damit auf das Lesegerät, wenn Sie den **Tapping-Modus** konfiguriert haben).
2. Ihre Citrix/RDP/VMware Horizon-Sitzung wird geöffnet, wenn bereits eine aktive Roamingsitzung für Ihren Benutzer existiert. Wenn dies nicht der Fall ist, wird Ihnen eine Passwortabfrage für das Active Directory-Passwort des Benutzers angezeigt.
3. Entfernen Sie Ihren RFID-Ausweis (oder tippen Sie erneut auf das Lesegerät), um die Verbindung zur Sitzung zu trennen.

## Custom Commands

Die folgenden einfachen Shell-Skripte veranschaulichen, wie man benutzerdefinierte Befehle schreibt, die Benutzernamen und Domäne als Parameter aus dem Evidian Authentication Manager empfangen.

Um sie zu verwenden

1. Speichern Sie die Skripte in `/wfs/` .
2. Führen Sie sie aus mit `chmod a+x [Dateiname]` .
3. Geben Sie den vollständigen Pfad (z.B. `/wfs/start.sh` ) unter **Sitzungen > Evidian > [Sitzungsname] > Optionen** ein.

### Start-Skript

```
#!/bin/sh
# Sample start script
if [ $# -eq 3 ] ; then
    # Start "session"
    gtkmessage -t "Evidian Authentifcation Manager Login" -m "Login as user '$1'
with domain '$3'."
else
    exit 1
fi
exit 0
```


### Stop-Skript

```
#!/bin/sh
# Sample stop script
# Close running "session"
pkill gtkmessage
gtkmessage -t "Evidian Authentication Manager Logout" -s 5 -S -m "Logout user
'$1'."
exit 0
```

## Debugging und Fehlerbehebung

### Debugging

1. Aktivieren Sie im Setup den **Debugmodus** in **Sitzungen > Evidian > [Session Name] > Optionen** und stellen Sie den Detaillierungsgrad unter **Trace-Level** ein.
2. Beenden Sie den Prozess **Evidian Authentication Manager** (siehe Weitere Fehlerbehebung).
3. Starten Sie die gewünschte Evidian-Sitzung aus dem Startmenü.
4. Beobachten Sie die Ausgabe mit `tail -F /var/log/user/rsuserauth[Session Number].debug` im lokalen Terminal. Alternativ können Sie die Datei auch dem **System Log Viewer** hinzufügen.

 Die Sitzungsnummer beginnt mit 0, nicht mit 1. Um die Ausgabe der ersten konfigurierten Sitzung zu sehen, verwenden Sie `tail -F /var/log/user/rsuserauth0.debug`.

### Weitere Fehlerbehebung

1. Öffnen Sie das lokale **Terminal**.
2. Geben Sie `ps fax | grep rsuserauth | grep -v grep` ein, um nach Prozessen des Evidian Authentication Manager zu suchen.
3. Verwenden Sie die **Evidian AuthMgr Neustart**-Sitzung, um bei Bedarf alle Evidian-Sitzungen neu zu starten.  
ODER unerwünschte Prozesse durch Eingabe von `kill[process ID]` im Terminal beenden, gewünschte Prozesse über die Evidian-Einträge im **Startmenü** starten.

## IBM iAccess

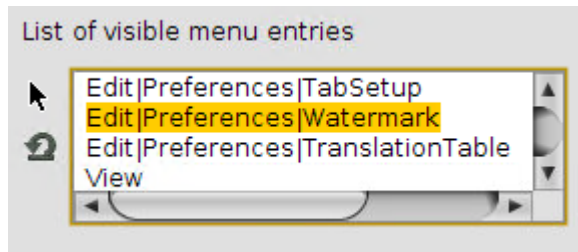
- [Die Liste der sichtbaren Menüeinträge für IBM iAccess bearbeiten \(see page 301\)](#)
- [Tastenbelegung für IBM iAccess Client \(see page 303\)](#)

## Die Liste der sichtbaren Menüeinträge für IBM iAccess bearbeiten


Sie können das Menü einer IBM iAccess-Client-Sitzung vereinfachen, indem Sie Elemente aus der Menüstruktur entfernen. Sie können auch das ursprüngliche Menü wiederherstellen.

### Menüpunkte entfernen

1. Gehen Sie im IGEL-Setup auf den Registry Key `session.iaccess[NUMBER].options.deletemenus` unter **System > Registry > Sessions > iaccess[NUMBER] > options > deletemenus**. [NUMBER] ist die Instanznummer der Sitzung, die Sie konfigurieren möchten; 0 steht beispielsweise für die erste Sitzung, 1 für die zweite Sitzung usw.
2. Markieren Sie in der **List of visible menu entries** mit der Maus die Zeile mit dem Eintrag, den Sie löschen möchten:



3. Drücken Sie die Return- oder die Entf-Taste.
4. Der Menüpunkt ist gelöscht.

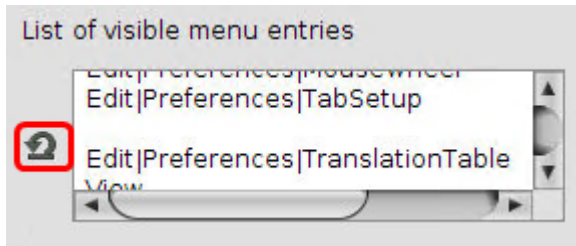
 Wenn Sie einen Menüpunkt mit Unterpunkten löschen, sind die Unterpunkte ebenfalls unsichtbar.

1. Um weitere Menüpunkte zu entfernen, wiederholen Sie die Schritte 2 und 3.
2. Klicken Sie auf **Übernehmen** oder **Ok**.
3. Starten oder starten Sie den IBM iAccess Client neu, um Ihre Änderungen zu überprüfen.

### Das Originalmenü wieder herstellen

1. Gehen Sie im IGEL-Setup auf den Registry Key `session.iaccess[NUMBER].options.deletemenus` unter **System > Registry > Sessions > iaccess[NUMBER] > options > deletemenus**.

2. Klicken Sie in der **List of visible menu entries** auf das folgende Symbol:



3. Das ursprüngliche Menü wird wiederhergestellt.  
Klicken Sie auf **Übernehmen** oder **Ok**.

## Tastenbelegung für IBM iAccess Client

### Problem

Wenn Sie die Tastenbelegung im IBM iAccess Client ändern, werden die Änderungen bei einem Neustart nicht übernommen.

Die Übernahme der Änderungen über das IGEL Setup ist nicht möglich.

### Umgebung/Voraussetzung

- IGEL OS 10.05.100 oder höher
- UMS 5.09.110 oder höher
- IBM iAccess Client Sitzung ist eingerichtet

### Lösung

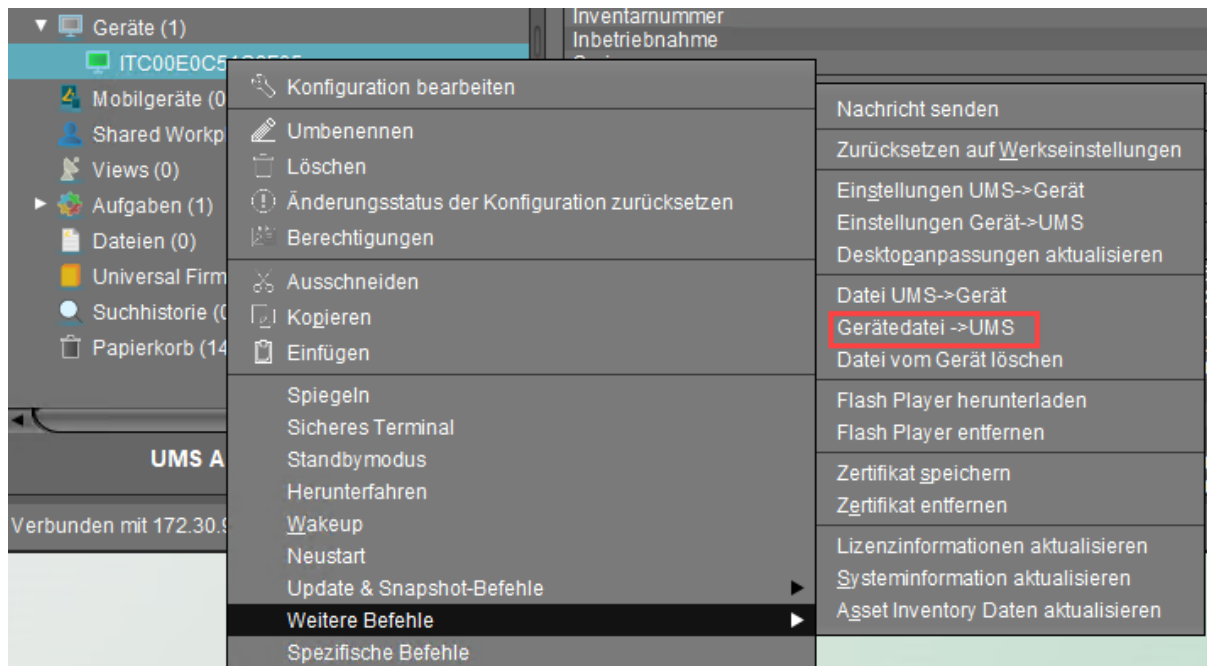
Speichern Sie die im IBM iAccess Client vorgenommenen Einstellungen in einer Datei und verteilen Sie diese Datei über die UMS.

### Tastenbelegungen bearbeiten

1. Öffnen Sie die IBM iAccess-Sitzung und melden Sie sich an Ihrer Remote-Umgebung an.
2. Gehen Sie im IBM iAccess Client unter **Bearbeiten > Einstellungen > Tastatur**.
3. Unter **Tastenbelegung**, erstellen Sie die gewünschten Tastenbelegungen.
4. Klicken Sie auf **Speichern unter...**
5. Wählen Sie im Speicherdialog **Datei** und bearbeiten Sie den Dateipfad wie folgt: `/userhome/IBM/iAccessClient/Emulator/IBMi.kmp`
6. Klicken Sie **Ok**.  
Der IBM iAccess-Client erkennt die Datei `IBMi.kmp` als Standardschlüssel.

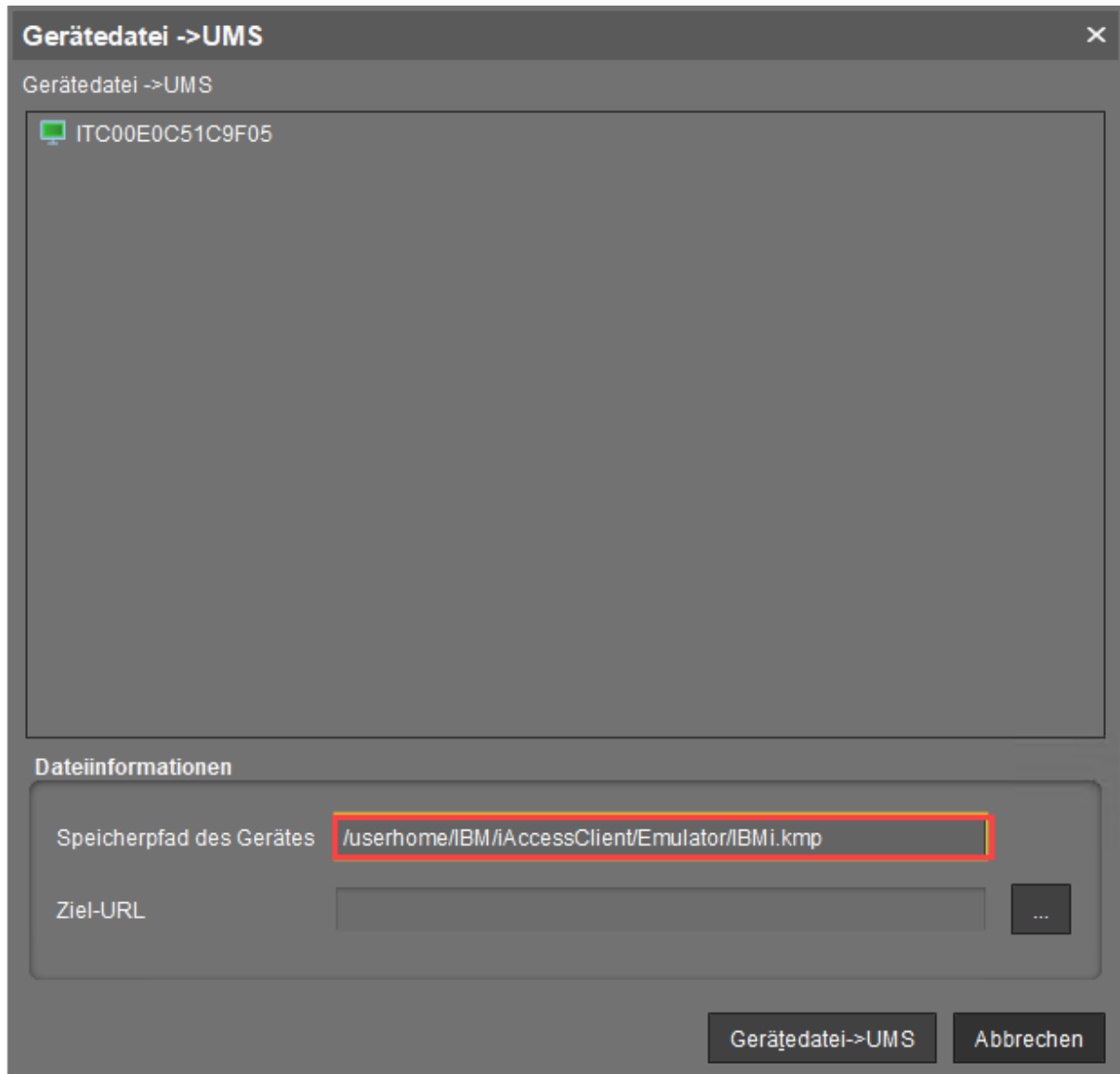
### Die Konfigurationsdatei in die UMS importieren

1. Öffnen Sie die UMS.
2. Suchen Sie im Navigationsbaum das Gerät mit der Datei `IBMi.kmp` und wählen Sie die Option **Weitere Befehle > Gerätedatei > UMS** im Kontextmenü.

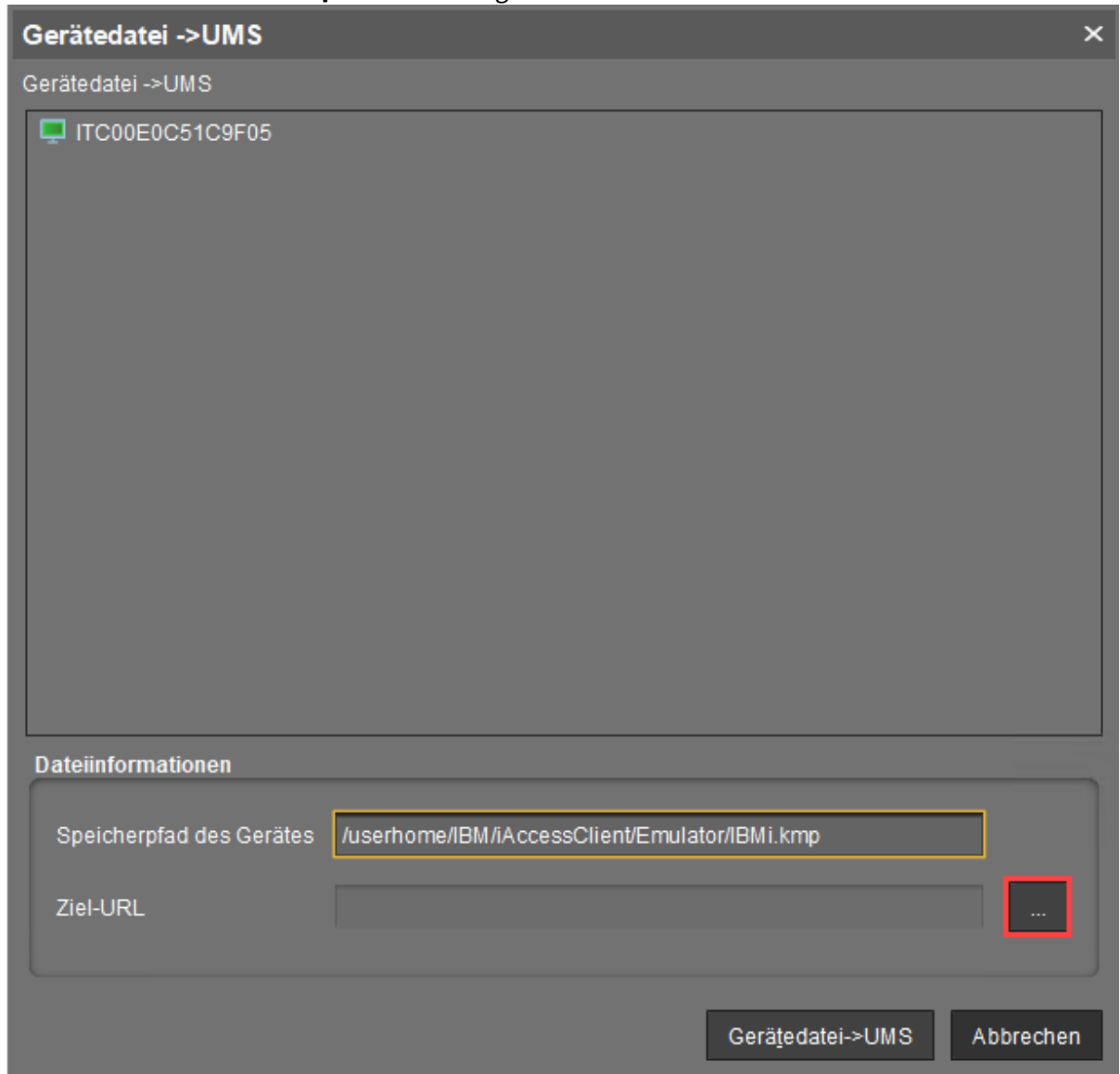


3. Geben Sie unter **Speicherpfad des Gerätes** `/userhome/IBM/iAccessClient/Emulator/IBMi.kmp` ein.

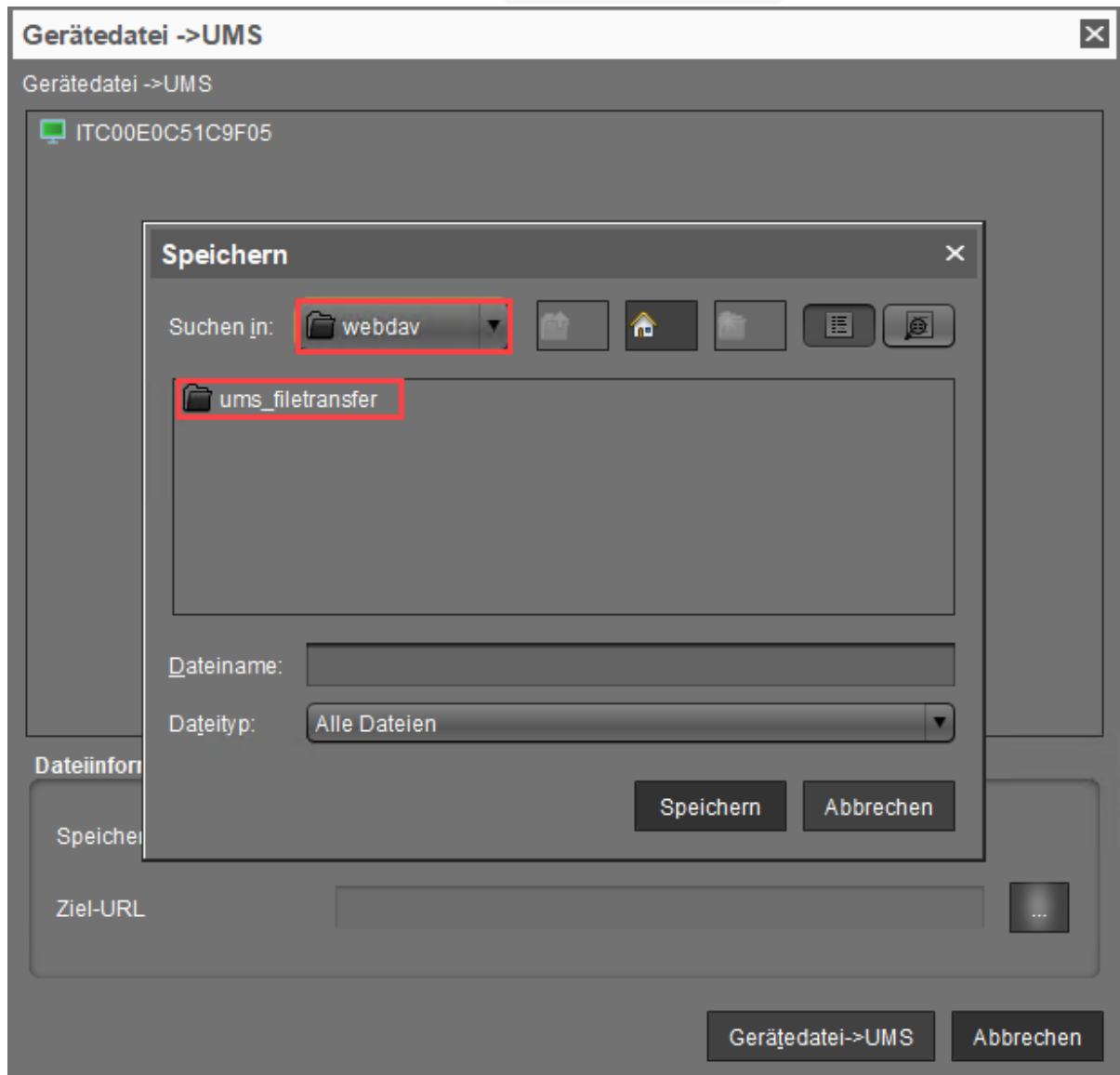




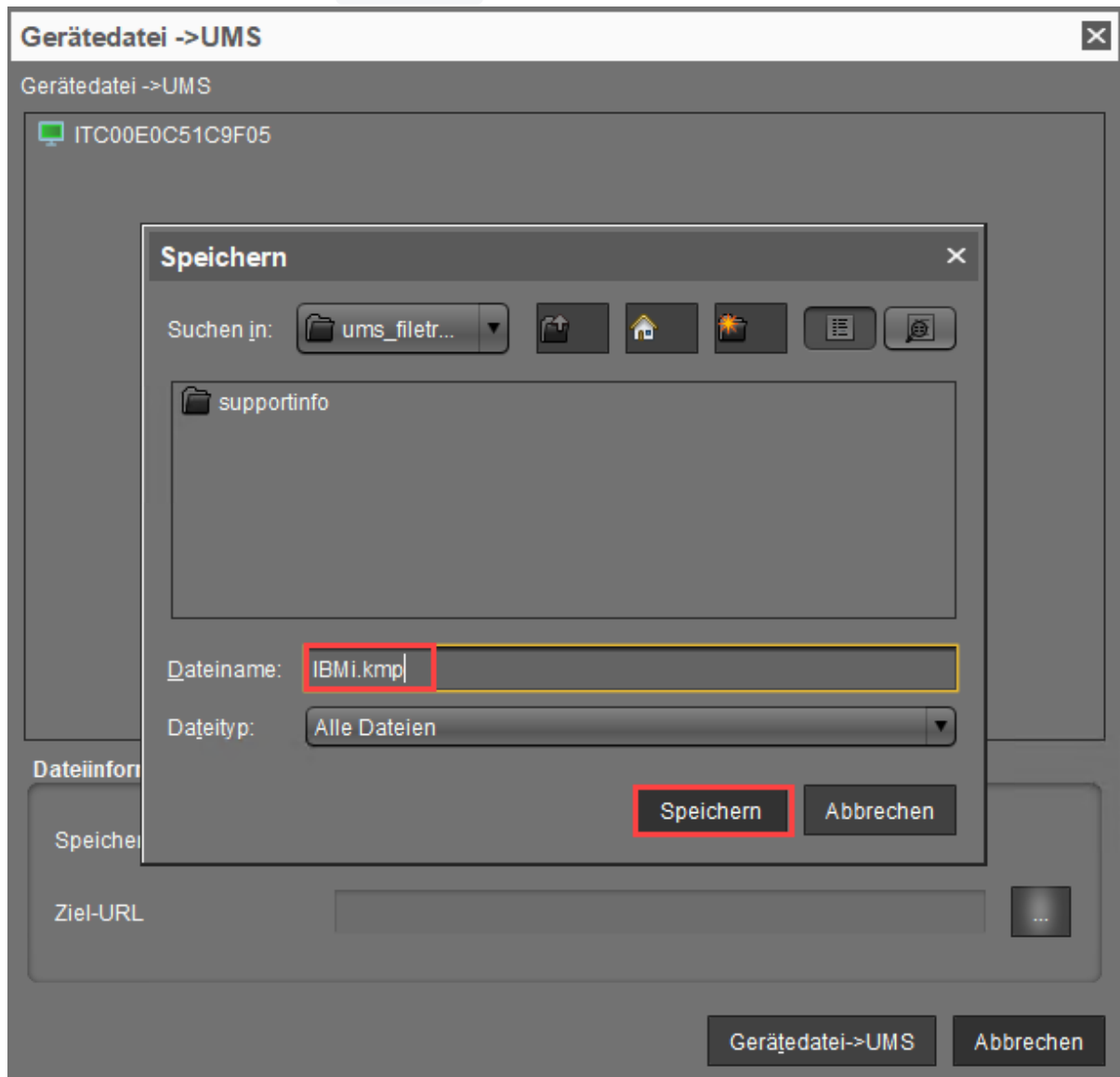
4. Klicken Sie  um den **Speichern**-Dialog zu öffnen.

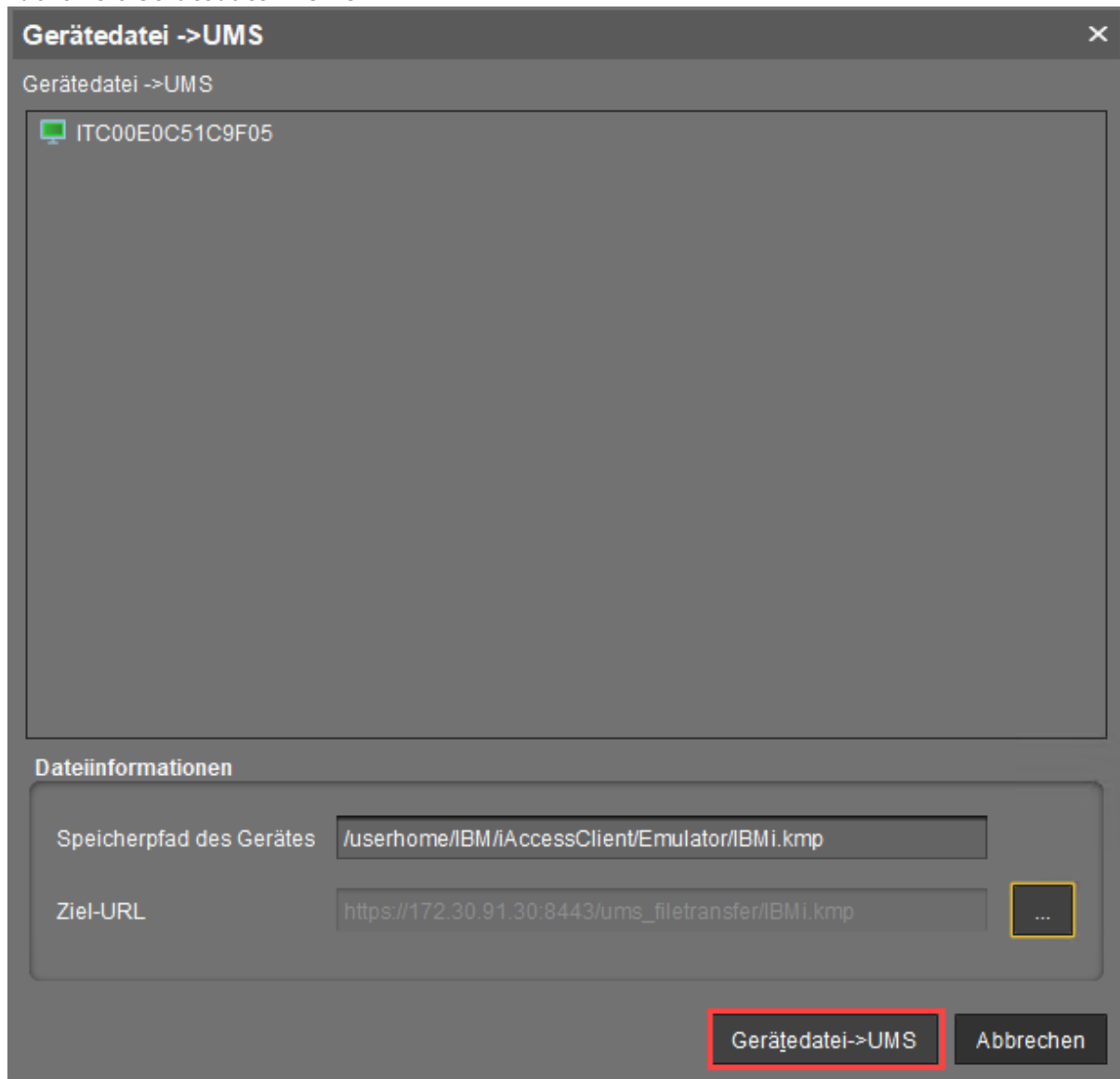


5. Wählen Sie einen Speicherort innerhalb des `ums_filetransfer` Ordners.



6. Unter **Dateiname**, geben Sie `IBMi.kmp` ein und klicken Sie **Speichern**.

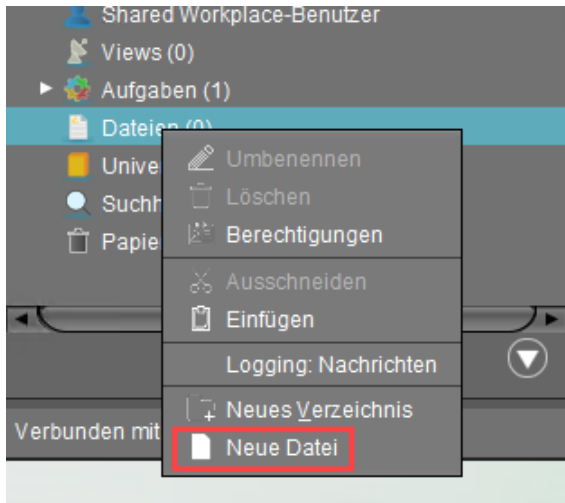


7. Klicken Sie **Gerätefile** → **UMS**

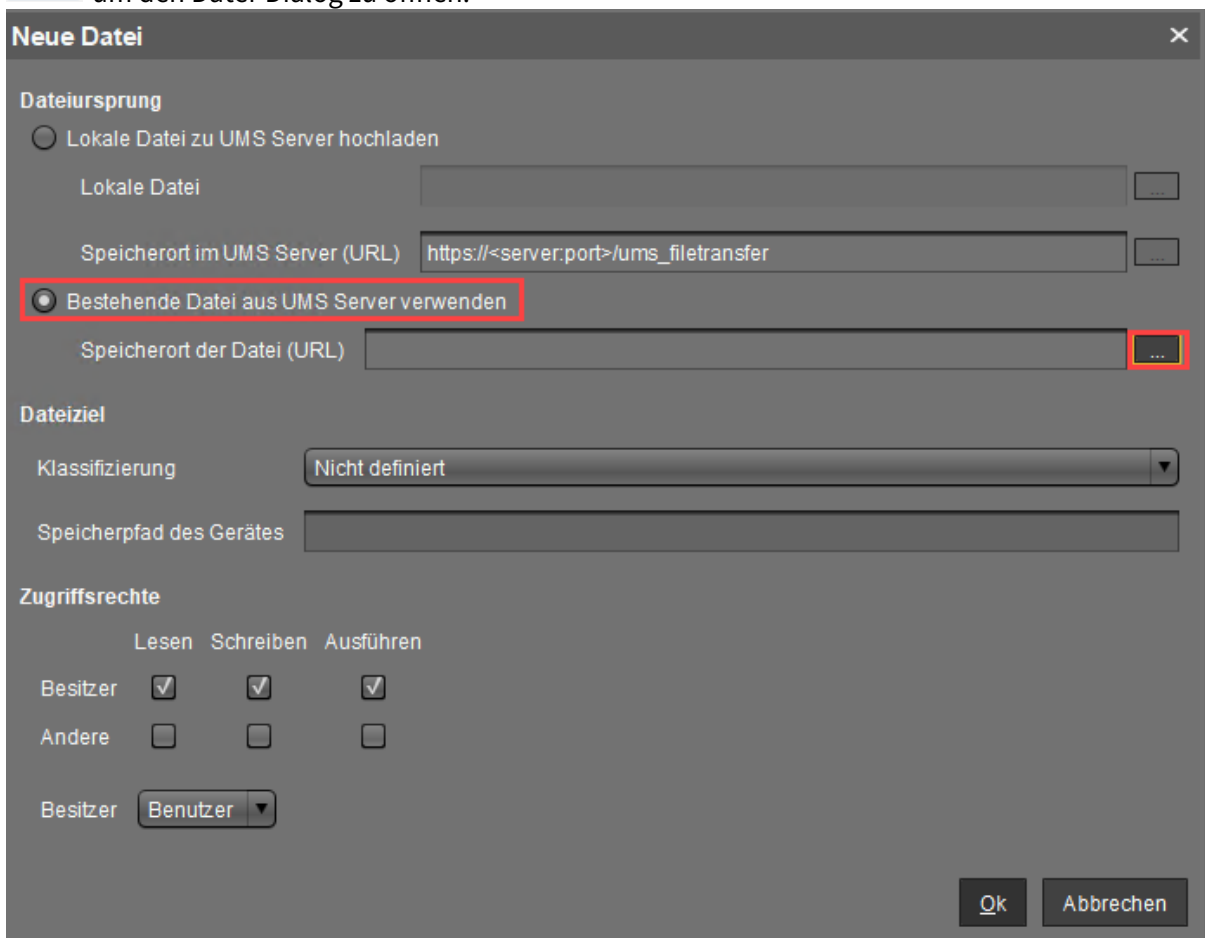
Die Datei wird im UMS gespeichert. Als nächstes stellen wir sie als Objekt zur Verfügung.

## Das Datei-Objekt in der UMS erstellen

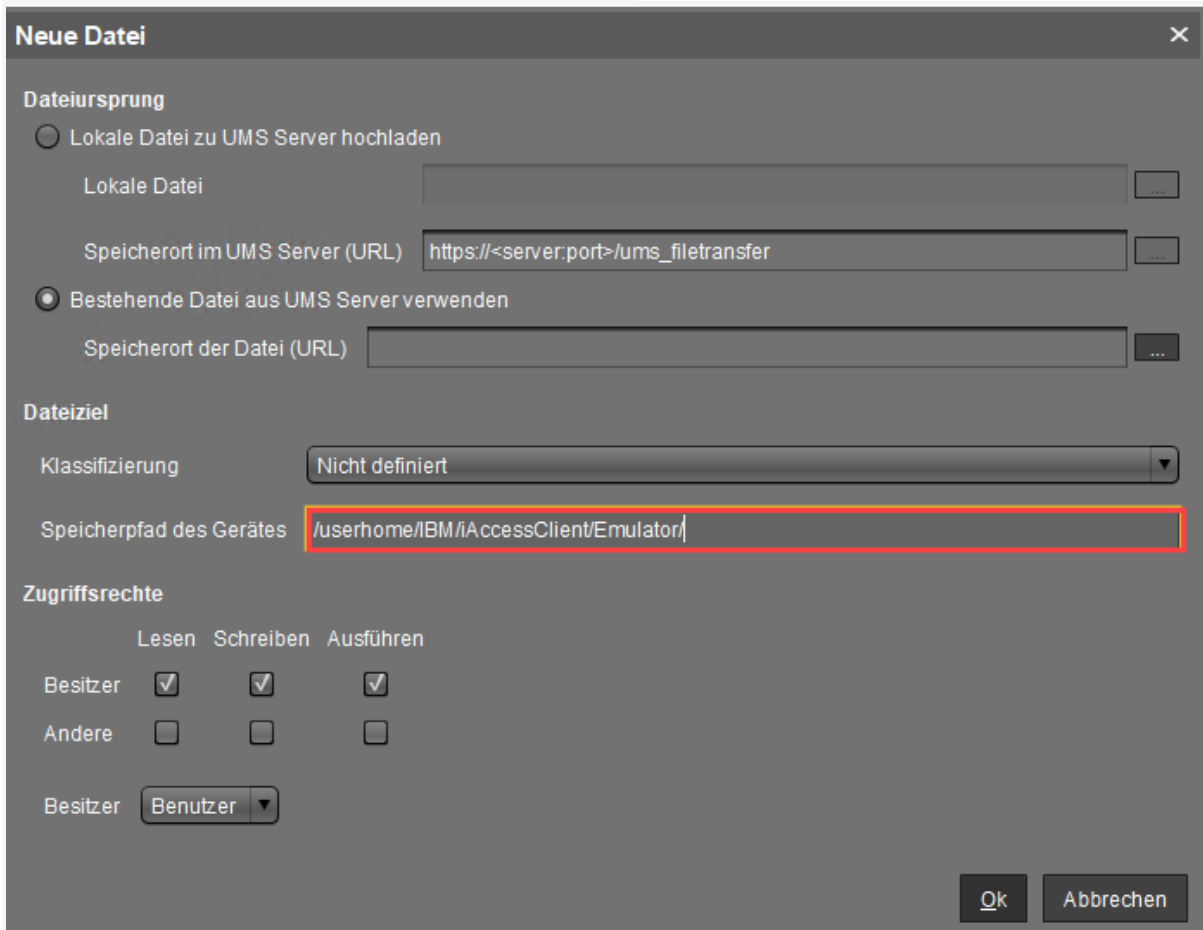
1. Gehen Sie im Navigationsbaum unter **Dateien**, öffnen Sie das Kontextmenü und wählen Sie **Neue Datei**.



- Wählen Sie **Bestehende Datei aus UMS Server verwenden** im **Neue Datei**-Dialog und klicken Sie  um den Datei-Dialog zu öffnen.



- Suchen Sie im Datei-Dailog die Datei `IBMi.kmp` die Sie zuvor erstellt haben, und klicken Sie auf **Öffnen**.
- Zurück im **Neue Datei**-Dialog, geben Sie den **Speicherpfad des Gerätes** wie folgt ein: `/userhome/IBM/iAccessClient/Emulator/`



**Neue Datei**

**Dateiursprung**

Lokale Datei zu UMS Server hochladen

Lokale Datei

Speicherort im UMS Server (URL)

Bestehende Datei aus UMS Server verwenden

Speicherort der Datei (URL)

**Dateiziel**

Klassifizierung

Speicherpfad des Gerätes

**Zugriffsrechte**

	Lesen	Schreiben	Ausführen
Besitzer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Andere	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Besitzer

- Stellen Sie sicher, dass die **Zugriffsrechte** und der **Besitzer** wie folgt eingestellt sind:
  - Besitzer-Rechte: Lesen, Schreiben, Ausführen**

- **Besitzer:"Benutzer"**

**Neue Datei** ✕

**Dateiursprung**

Lokale Datei zu UMS Server hochladen

Lokale Datei

Speicherort im UMS Server (URL)

Bestehende Datei aus UMS Server verwenden

Speicherort der Datei (URL)

**Dateiziel**

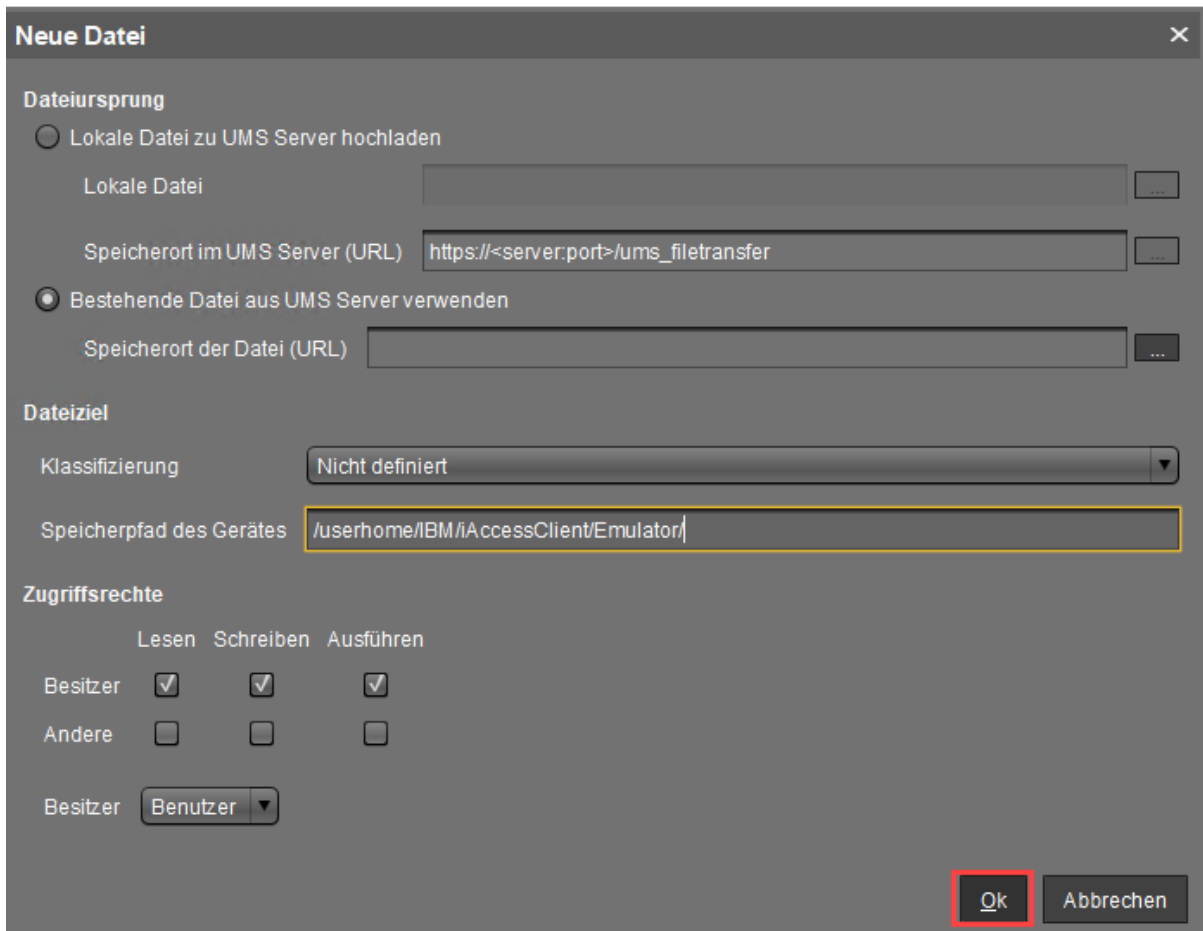
Klassifizierung

Speicherpfad des Gerätes

**Zugriffsrechte**

	Lesen	Schreiben	Ausführen
Besitzer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Andere	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Besitzer	<input style="width: 100%;" type="text" value="Benutzer"/>		



6. Klicken Sie **Ok**.


**Neue Datei**

**Dateiursprung**

Lokale Datei zu UMS Server hochladen

Lokale Datei

Speicherort im UMS Server (URL)

Bestehende Datei aus UMS Server verwenden

Speicherort der Datei (URL)

**Dateiziel**

Klassifizierung

Speicherpfad des Gerätes

**Zugriffsrechte**

	Lesen	Schreiben	Ausführen
Besitzer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Andere	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Besitzer

Das Dateiojekt "IBMi.kmp" wurde erstellt.

## Das Dateiojekt den Geräten zuordnen

1. Wählen Sie im Navigationsbaum das Dateiojekt "IBMi.kmp" und klicken Sie im Bereich **Zugeordnete Objekte** (oben rechts).
2. Wählen Sie im Dialog **Zuweisbare Objekte auswählen**, die Geräte aus, denen Sie das neue Key Mapping zuordnen möchten, und fügen Sie sie dem Bereich **Ausgewählte Objekte** hinzu.
3. Klicken Sie **Ok**.
4. Wählen Sie im **Update Zeitpunkt** Dialog, ob die Datei den Geräten beim nächsten Neustart zugeordnet werden soll oder sofort; dann klicken Sie **Ok**.

Die Datei wird auf die Geräte übertragen.

## Imprivata

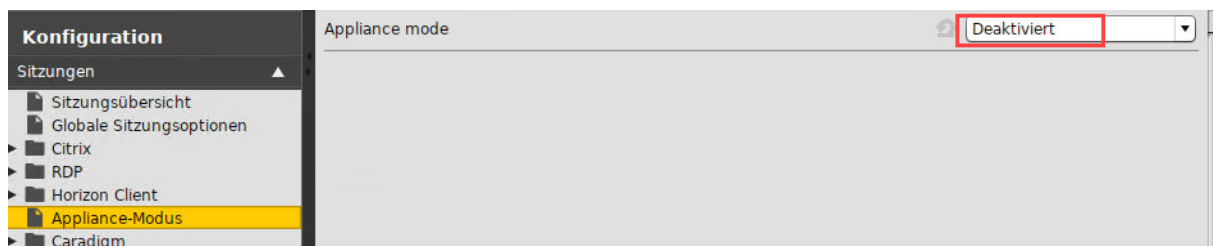
- [Imprivata: Imprivata Datenpartition löschen](#) (see page 315)
- [Imprivata: Kundenspezifische Anpassung der Sitzung](#) (see page 316)

## Imprivata: Imprivata Datenpartition löschen

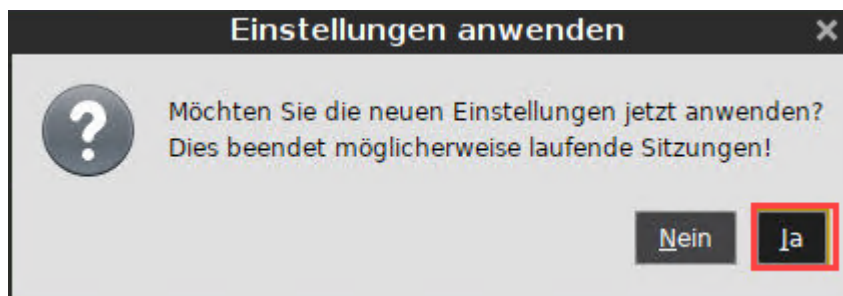
Die Funktion, die die Imprivata Datenpartition explizit löscht, wurde entfernt. Sie können diese Funktion jedoch einfach emulieren, indem Sie den Imprivata Appliance-Modus deaktivieren und wieder aktivieren.

Wenn Sie bereits eine gültige Appliance im Einsatz haben und die Imprivata Datenpartition löschen möchten, führen Sie die folgenden Schritte aus:

1. Gehen Sie im IGEL Setup zu **Sitzungen > Appliance-Modus**.
2. Setzen Sie **Appliance mode** auf "**Deaktiviert**".

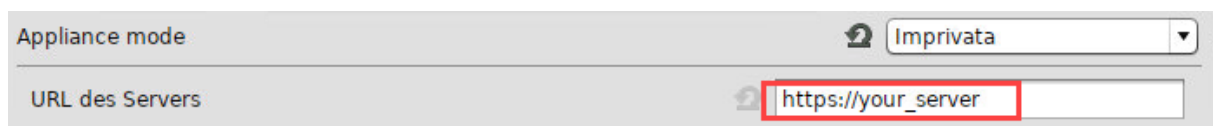


3. Klicken Sie **Ok**, um die Einstellung zu speichern.
4. Klicken Sie **Ja**, um den Dialog **Einstellungen anwenden** zu bestätigen.



Der normale Desktop-Modus ist aktiv. Die Imprivata Datenpartition ist nun leer.

5. Gehen Sie im IGEL Setup zu **Sitzungen > Appliance-Modus**.
6. Setzen Sie **Appliance mode** auf "**Imprivata**".
7. Geben Sie unter **URL des Servers** die neue Server-Adresse ein.



8. Klicken Sie **Ok** und bestätigen Sie den Dialog **Einstellungen anwenden**. Jetzt haben Sie einen neuen Imprivata Appliance-Modus ohne Altdateien.

## Imprivata: Kundenspezifische Anpassung der Sitzung

Sie können in den Sitzungen **IMPRIVATA\_RDP** (**IGEL Setup > RDP > RDP-Sitzungen > Imprivata\_RDP**) und **IMPRIVATA\_VMware** (**IGEL Setup > Horizon Client > Horizon Client-Sitzungen > IMPRIVATA\_VMware**) die gleichen Einstellungen vornehmen wie in den Standardsitzungen (siehe die Beschreibungen für RDP-Sitzung und Horizon Client Sitzung).

**i** **IMPRIVATA\_RDP** und **IMPRIVATA\_VMware** erscheinen im Setup, wenn **Appliance-Modus** auf **Imprivata** gesetzt ist, siehe Imprivata.

Änderungen unter den folgenden Unterkategorien werden jedoch ignoriert:

### Imprivata\_VMware Sitzung

- **Verbindungseinstellungen**

**i** Sie können auch das von der Imprivata Appliance ausgewählte VMware Protokoll ignorieren, indem Sie den Registry Key **imprivata.ignore\_horizon\_protocol** unter **System > Registry** aktivieren. Stattdessen wird die lokale Auswahl unter **Horizon Client > Horizon Client Global > Serveroptionen > Bevorzugtes Verbindungsprotokoll** verwendet.

### Imprivata\_RDP-Sitzung

- **Server**
- **Anmeldung**

## Microsoft Azure Virtual Desktop (AVD)

Dieses IGEL Release ist ein Build von IGEL OS, der den AVD Client als konfigurierbare Methode zur Verbindung mit Azure Virtual Desktops enthält.

- [Feature Matrix: AVD \(RDP3\) for IGEL OS 11 \(see page 318\)](#)
- [IGEL OS mit Azure Virtual Desktop verbinden \(see page 319\)](#)
- [Keeping Your Firmware Up-To-Date for Azure Virtual Desktop \(AVD\) \(see page 323\)](#)
- [Microsoft Teams Feature Comparison for IGEL OS \(see page 324\)](#)
- [Authentication Issue with Microsoft Azure Virtual Desktop on IGEL OS](#)

## Feature Matrix: AVD (RDP3) for IGEL OS 11

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## IGEL OS mit Azure Virtual Desktop verbinden


### Schnellstartanleitung

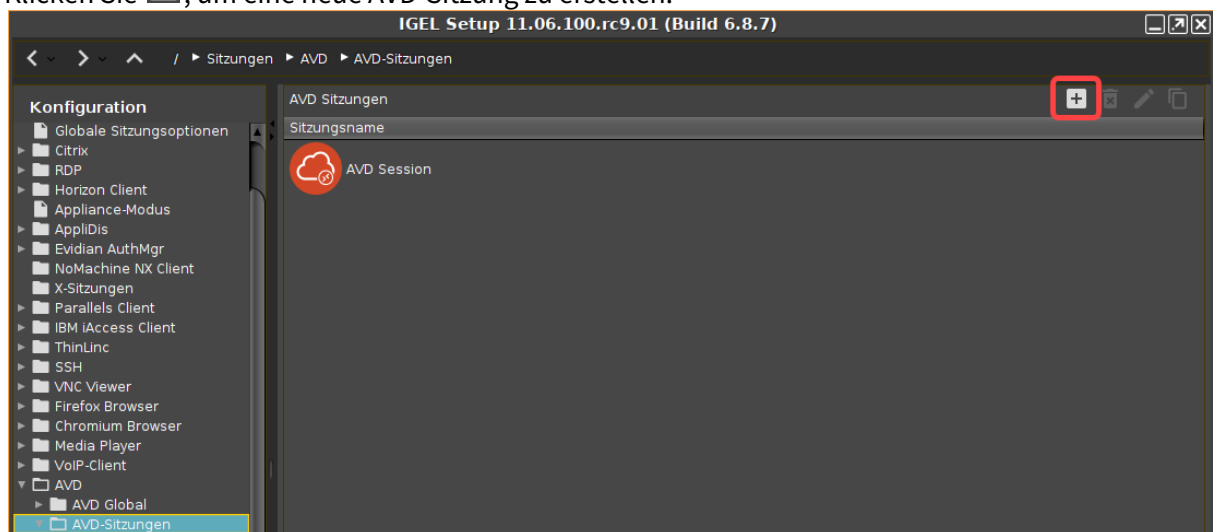
Dieser Abschnitt beschreibt die Einrichtung einer Azure Virtual Desktop (AVD)-Sitzung (ehemals Windows Virtual Desktop, WVD) über den IGEL AVD-Client, der auf Microsofts RD Core SDK für Linux basiert und für die Verbindung mit einer AVD-Bereitstellung verwendet werden kann.

### Anforderungen

- Gerät mit IGEL OS 11.03.261 oder höher; Herunterladen der neuesten Version unter [igel.com/avd](http://igel.com/avd)<sup>31</sup>
- Bereitstellung von Azure Virtual Desktop

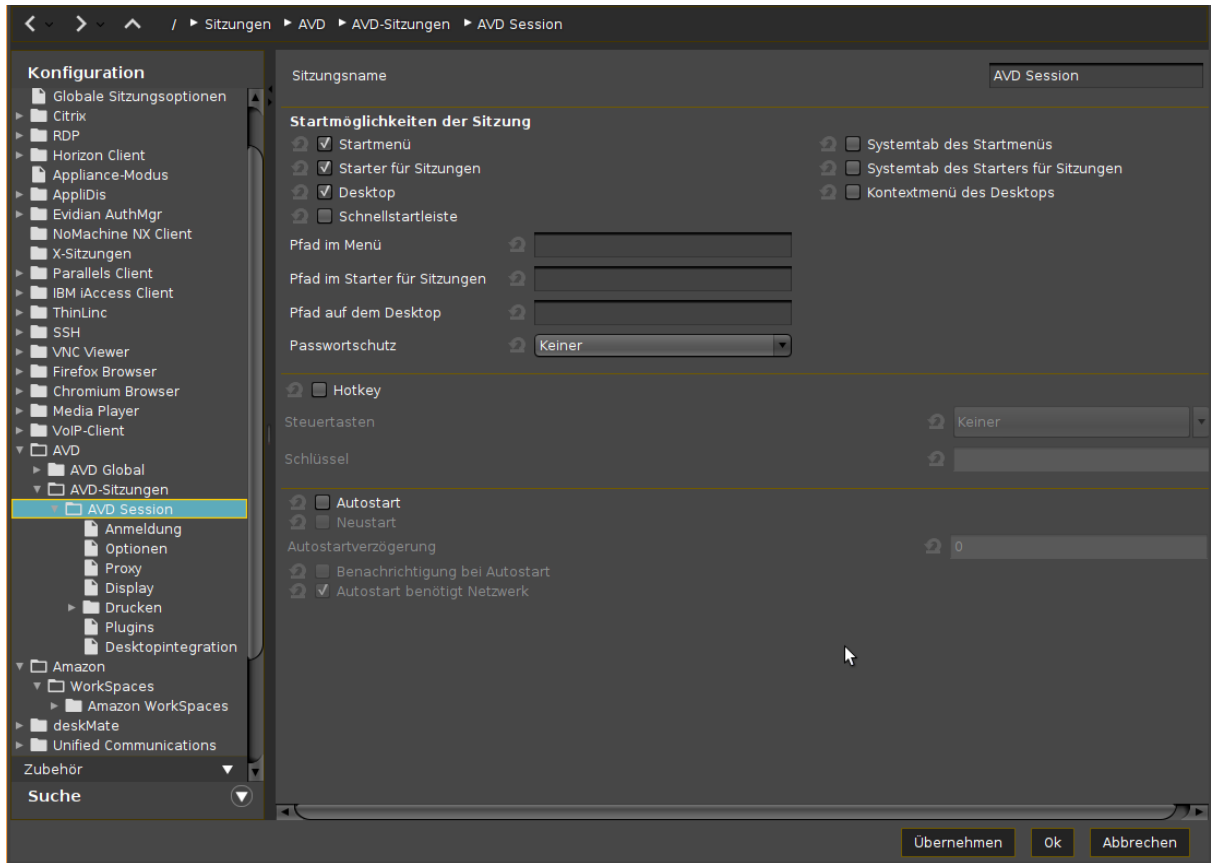
### Anweisungen

1. Öffnen Sie das Setup oder den Konfigurationsdialog in der UMS und gehen Sie zu **Sitzungen > AVD > AVD-Sitzungen**.
2. Klicken Sie , um eine neue AVD-Sitzung zu erstellen.



<sup>31</sup> <http://igel.com/avd>

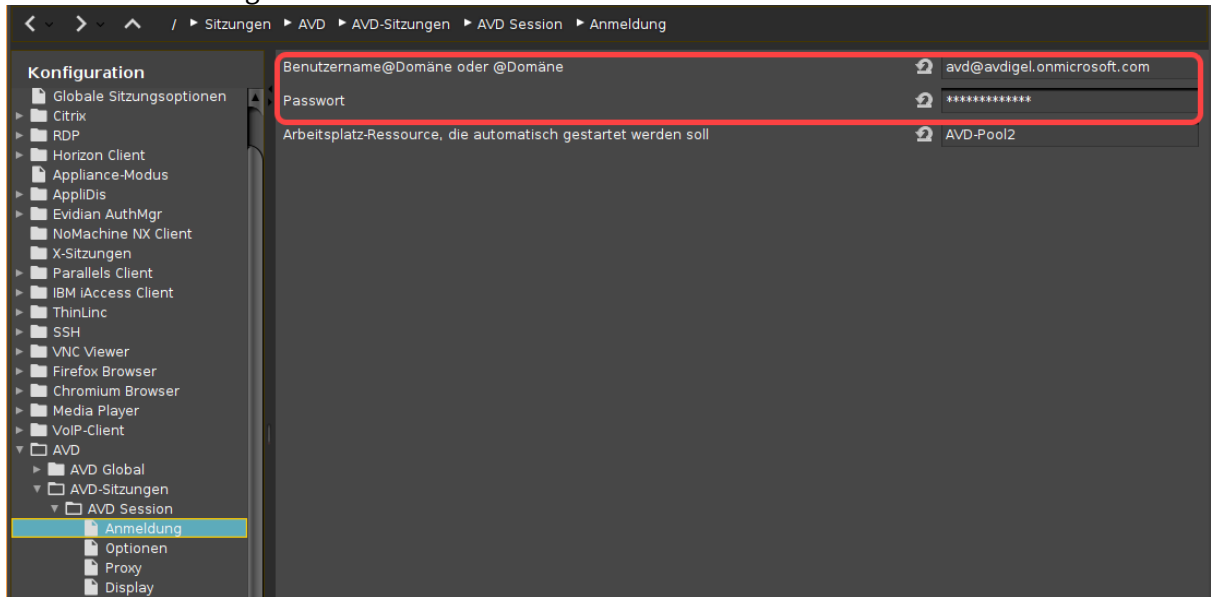
3. Geben Sie einen **Sitzungsname** ein und konfigurieren Sie die Startmöglichkeiten nach Ihren Bedürfnissen.



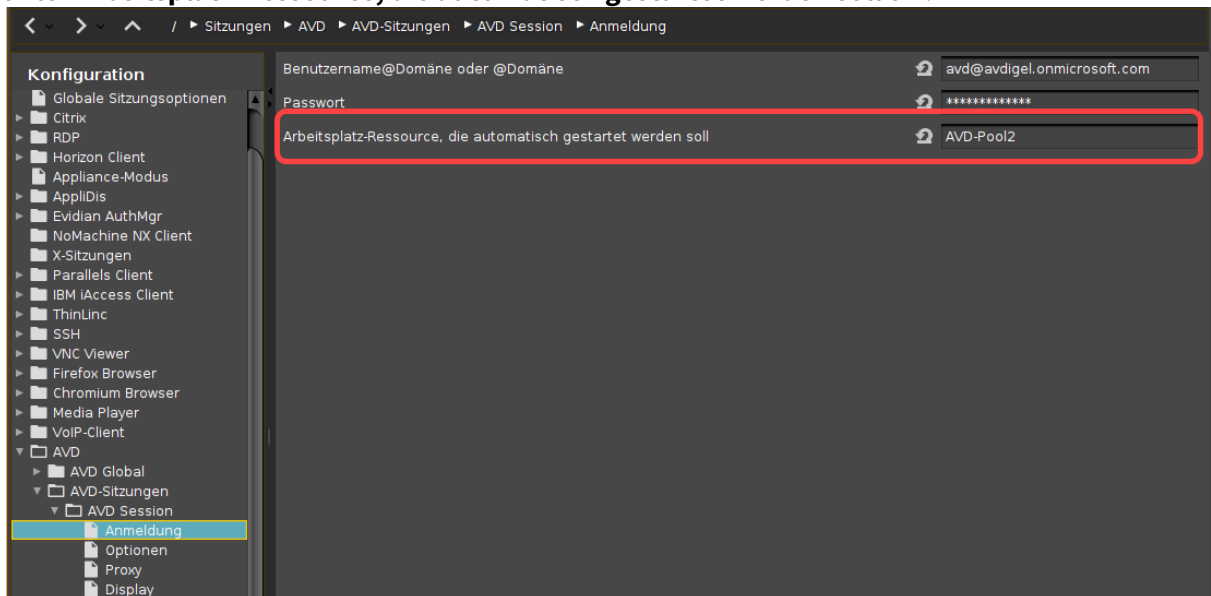
4. Wenn die Anmeldung beim Sitzungsstart automatisch gestartet werden soll, gehen Sie zu **Sitzungen > AVD > AVD-Sitzungen > [Sitzungsname] > Anmeldung** und geben Sie Ihre Anmeldedaten unter **Benutzername@Domäne oder @Domäne** und **Passwort** ein. Details finden



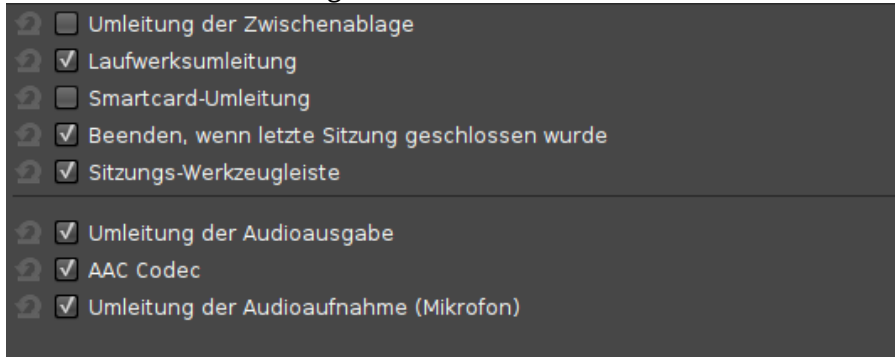
Sie unter Anmeldung.



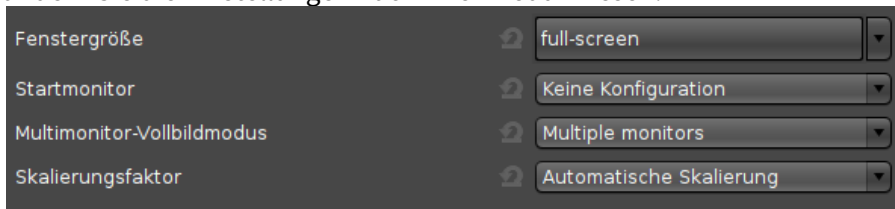
5. Wenn eine bestimmte Ressource automatisch gestartet werden soll, geben Sie deren Namen unter **Arbeitsplatz-Ressource, die automatisch gestartet werden soll** ein.



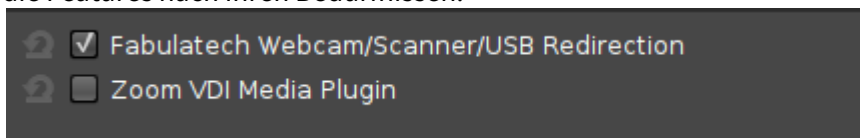
6. Gehen Sie zu **Sitzungen > AVD > AVD-Sitzungen > [Sitzungsname] > Optionen** und (de)aktivieren Sie Features und Umleitungen nach Ihren Bedürfnissen.



7. Wenn Sie den AVD-Client nicht auf allen verfügbaren Bildschirmen im Vollbildmodus ausführen möchten, gehen Sie zu **Sitzungen > AVD > AVD-Sitzungen > [Sitzungsname] > Display** und ändern Sie die Einstellungen nach Ihren Bedürfnissen.



8. Gehen Sie zu **Sitzungen > AVD > AVD-Sitzungen > [Sitzungsname] > Plugins** und aktivieren Sie die Features nach Ihren Bedürfnissen.




9. Klicken Sie **Übernehmen** oder **OK**.  
Die AVD-Sitzung ist konfiguriert und kann mit den Startmöglichkeiten, die Sie in Schritt 3 konfiguriert haben, gestartet werden.


Wenn Sie weitere AVD-Sitzungen konfigurieren möchten, beginnen Sie wieder bei Schritt 2.

Siehe auch das Kapitel AVD-Sitzung im Referenzhandbuch.

## Keeping Your Firmware Up-To-Date for Azure Virtual Desktop (AVD)

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Microsoft Teams Feature Comparison for IGEL OS

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## SSH

- [Schwächere Algorithmen im eingebauten OpenSSH-Dienst aktivieren \(see page 326\)](#)
- [Schwächere Algorithmen im SSH-Client aktivieren \(see page 327\)](#)
- [SSH: Veraltete schwache Algorithmen ab IGEL Linux 10.04.100 \(see page 328\)](#)

## Schwächere Algorithmen im eingebauten OpenSSH-Dienst aktivieren

### Problem

Sie versuchen, eine Verbindung zum eingebauten OpenSSH-Server von IGEL OS mit einem SSH-Client herzustellen, der die starken Algorithmen des Servers nicht unterstützt.

### Lösung

Um die schwächeren Algorithmen zu aktivieren, gehen Sie wie folgt vor:

1. Gehen Sie im Setup unter **System > Registry > network > ssh\_server**.
2. Ändern Sie die Einstellungen nach Ihren Wünschen:
  - **disable\_weak\_encryption**: Deaktivieren Sie diese Option, um eine schwächere Verschlüsselung zu aktivieren.
  - **disable\_weak\_hostkey\_algos**: Deaktivieren Sie diese Option, um schwächere Host-Key-Algorithmen zu aktivieren.
  - **disable\_weak\_kexalgorithms**: Deaktivieren Sie diese Option, um schwächere Schlüsselaustauschalgorithmen zu aktivieren.
  - **disable\_weak\_macs**: Deaktivieren Sie diese Option, um schwächere MACs zu aktivieren.
  - **minimal\_encryption\_level**: Die minimale Verschlüsselungsstufe

## Schwächere Algorithmen im SSH-Client aktivieren

### Voraussetzung

IGEL Linux 10.04.100 oder höher

### Problem

Sie versuchen, sich mit einem SSH-Server zu verbinden, der die starken Algorithmen, die standardmäßig im SSH-Client aktiviert sind, nicht unterstützt.

### Lösung

Um schwächere Algorithmen zu aktivieren, gehen Sie wie folgt vor:

1. Gehen Sie im Setup unter **System > Registry > network > ssh\_client**.
2. Ändern Sie die Einstellungen nach Ihren Wünschen:
  - **disable\_weak\_encryption**: Deaktivieren Sie diese Option, um eine schwächere Verschlüsselung zu aktivieren.
  - **disable\_weak\_hostkey\_algos**: Deaktivieren Sie diese Option, um schwächere Host-Key-Algorithmen zu aktivieren.
  - **disable\_weak\_kexalgorithms**: Deaktivieren Sie diese Option, um schwächere Schlüsselaustauschalgorithmen zu aktivieren.
  - **disable\_weak\_mac**: Deaktivieren Sie diese Option, um schwächere MACs zu aktivieren.
  - **minimal\_encryption\_level**: Die minimale Verschlüsselungsstufe

## SSH: Veraltete schwache Algorithmen ab IGEL Linux 10.04.100

Ab IGEL Linux 10.04.100 sind bestimmte ältere, weniger sichere Algorithmen sowohl im SSH-Client als auch im Server veraltet.

Die folgende Tabelle zeigt die ab IGEL Linux Version 10.04.100 standardmäßig aktivierten Algorithmen.

Key exchange algorithms	<ul style="list-style-type: none"> <li>• curve25519-sha256@libssh.org</li> <li>• ecdh-sha2-nistp521</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp256</li> <li>• diffie-hellman-group-exchange-sha256</li> </ul>
Message authentication codes (MACs)	<ul style="list-style-type: none"> <li>• hmac-sha2-512-etm@openssh.com</li> <li>• hmac-sha2-256-etm@openssh.com</li> <li>• umac-128-etm@openssh.com</li> <li>• hmac-sha2-512</li> <li>• hmac-sha2-256</li> <li>• umac-128@openssh.com</li> </ul>
Host keys	<ul style="list-style-type: none"> <li>• ssh-ed25519-cert-v01@openssh.com</li> <li>• ssh-rsa-cert-v01@openssh.com</li> <li>• ssh-ed25519</li> <li>• ssh-rsa</li> <li>• ecdsa-sha2-nistp521-cert-v01@openssh.com</li> <li>• ecdsa-sha2-nistp384-cert-v01@openssh.com</li> <li>• ecdsa-sha2-nistp256-cert-v01@openssh.com</li> <li>• ecdsa-sha2-nistp521</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp256</li> </ul>

Wenn Sie schwächere Algorithmen aktivieren müssen, lesen Sie bitte unter [Schwächere Algorithmen im SSH-Client aktivieren](#) (see page 327) und/oder [Schwächere Algorithmen im eingebauten OpenSSH-Dienst aktivieren](#) (see page 326).



## Amazon WorkSpaces mit dem HP Anyware PCoIP Client verwenden

Sie können eine Amazon WorkSpaces-Sitzung unter **Sitzungen > Amazon > WorkSpaces > Amazon WorkSpaces Sitzung** konfigurieren, siehe Amazon WorkSpaces.

Alternativ können Sie Amazon WorkSpaces auch über HP Anyware PCoIP nutzen. Dies ist in den folgenden Artikeln beschrieben.

- [IGEL OS Geräte über den HP Anyware PCoIP Client mit Amazon WorkSpaces verbinden \(see page 330\)](#)
- [Ihren HP Anyware Client für Amazon WorkSpaces in IGEL OS konfigurieren \(see page 334\)](#)
- [Brokertypen, um Amazon WorkSpaces mit dem HP Anyware Client in IGEL OS zu verbinden \(see page 336\)](#)
- [Wie kann ich die H.264-Beschleunigung in einer HP Anyware PCoIP-Sitzung verwenden? \(see page 337\)](#)

## IGEL OS Geräte über den HP Anyware PCoIP Client mit Amazon WorkSpaces verbinden

Sie können IGEL OS Geräte über PCoIP mit Amazon WorkSpaces einrichten und nutzen. Der HP Anyware PCoIP Client ist eine Alternative zum Amazon Workspaces Client.

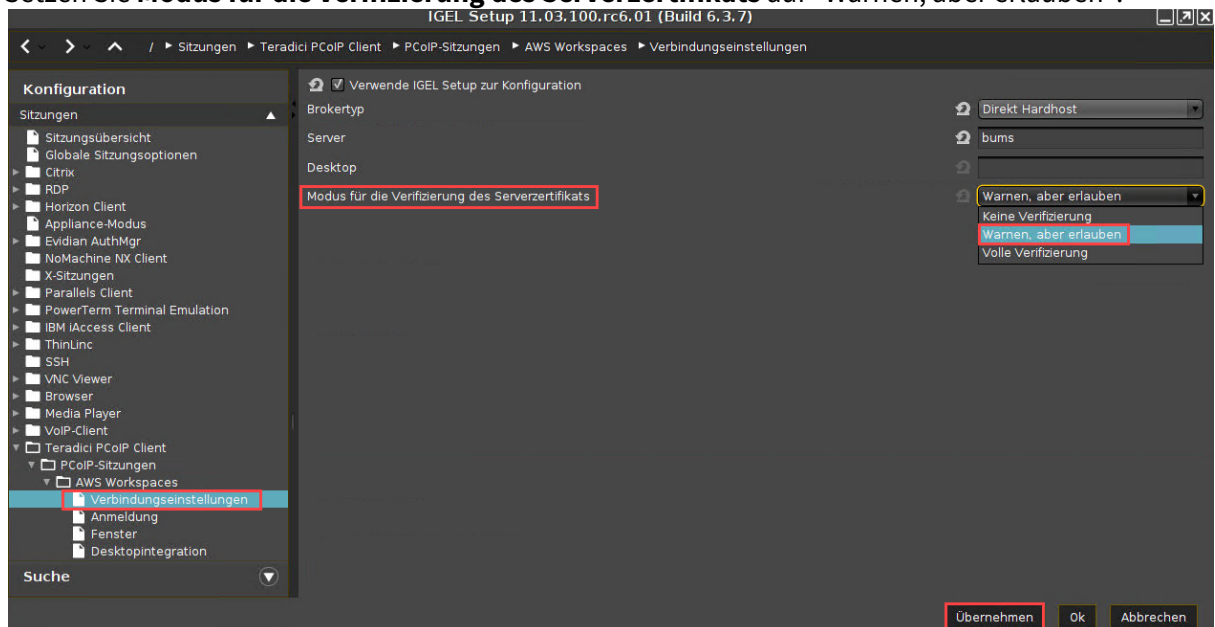
### Geräteverbindung einrichten

Bevor Sie das Gerät zum ersten Mal mit den Amazon WorkSpaces verbinden, müssen Sie möglicherweise einige Einstellungen ändern. Ihr Amazon WorkSpace Administrator kann Ihnen zusätzliche Installationsanweisungen zur Verfügung stellen, die für Ihre spezielle Umgebung erforderlich sind.

### Sitzungsverbindung

So stellen Sie die Sitzungsverbindung ein:

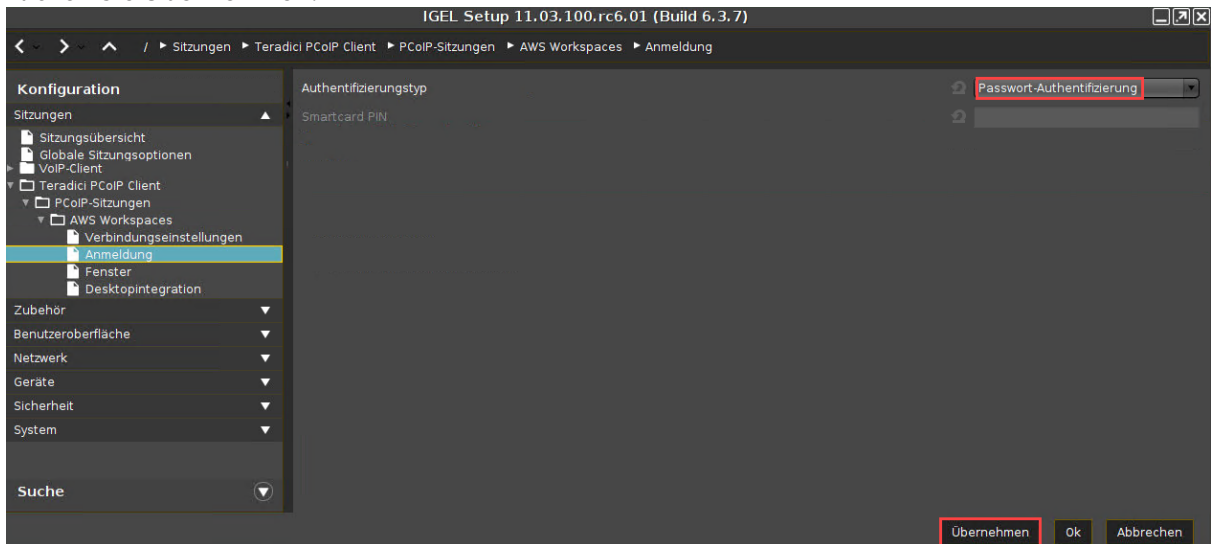
1. Gehen Sie im IGEL Setup zu **Sitzungen > HP Anyware PCoIP Client > PCoIP-Sitzungen**.
2. Klicken Sie auf **+**, um eine neue Sitzung zu erstellen.
3. Gehen Sie zu **Verbindungseinstellungen**.
4. Setzen Sie **Modus für die Verifizierung des Serverzertifikats** auf "Warnen, aber erlauben".



**i** Wenn Sie **Verwende IGEL Setup zur Konfiguration** nicht aktivieren, müssen Sie die Host-Adresse oder den Host-Code im Anmeldefenster des HP Anyware PCoIP Clients eingeben. Siehe den Screenshot unter "Mit Amazon WorkSpaces verbinden".  
Wenn Sie **Verwende IGEL Setup zur Konfiguration** aktivieren, lesen Sie [Ihren HP Anyware Client für Amazon WorkSpaces in IGEL OS konfigurieren](#) (see page 334).

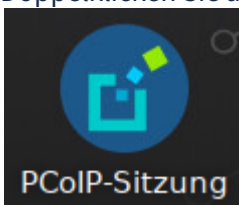
**i** Weitere Informationen zur Verbindung mit den **Brokertypen** "PCoIP Broker" und "Direkt Hardhost" finden Sie unter [Brokertypen,, umum Amazon WorkSpaces mit dem HP Anyware Client in IGEL OS zu verbinden mit dem HP Anyware Client in IGEL OS zu verbinden](#) (see page 336).

5. Klicken Sie **Übernehmen**.
6. Gehen Sie zu **Anmeldung** und setzen Sie **Authentifizierungstyp** auf "Passwort-Authentifizierung". Klicken Sie **Übernehmen**.



## Mit Amazon WorkSpaces verbinden

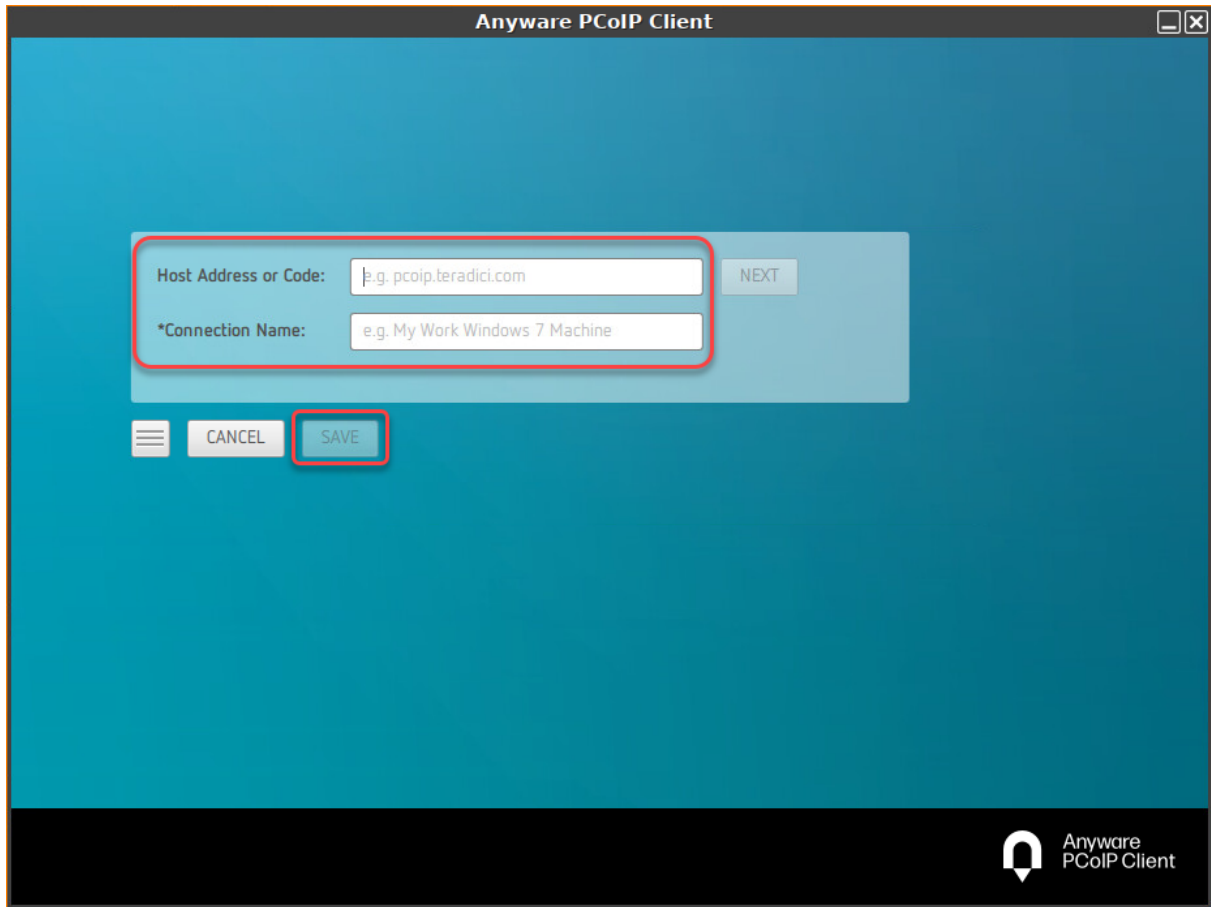
1. Doppelklicken Sie auf Ihrem Desktop das Symbol der PCoIP-Sitzung.



Das Fenster **Anyware PCoIP Client** öffnet sich.

2. Geben Sie die **Host Address or Code** ein, die Ihnen in der Willkommens-E-Mail von Amazon WorkSpaces gesendet wurde.

3. Geben Sie den **Connection Name** ein und klicke Sie **SAVE**.



4. Geben Sie Ihre Amazon WorkSpaces-Anmeldeinformationen ein.
5. Geben Sie den **Multi-Factor Authentication (MFA) Token** ein.

Multi-Faktor-Authentifizierung ist ein Identitätsnachweis für Benutzer, der zwei verschiedene und voneinander unabhängige Komponenten (Faktoren) verwendet.

Wenn Sie keine Multi-Faktor-Authentifizierung verwenden, müssen Sie trotzdem etwas in das MFA-Feld eingeben, auch wenn es nur eine Zahl oder "1234" ist. Ansonsten kann keine Verbindung zu Amazon WorkSpaces hergestellt werden.

6. Klicken Sie **Ok**.  
Der Amazon WorkSpaces Bildschirm wird angezeigt.

Sehen Sie auch unsere Videobeschreibung auf youtube:



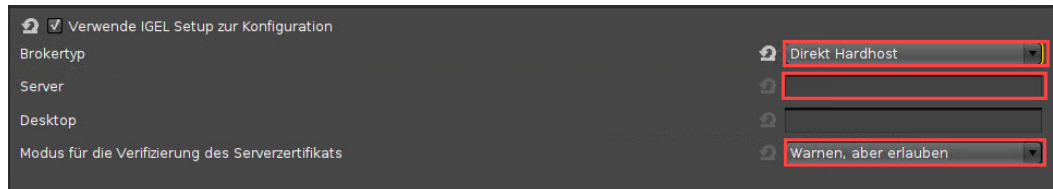
Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:  
<https://www.youtube.com/watch?v=NDQxTEKLPZE>

## Ihren HP Anyware Client für Amazon WorkSpaces in IGEL OS konfigurieren

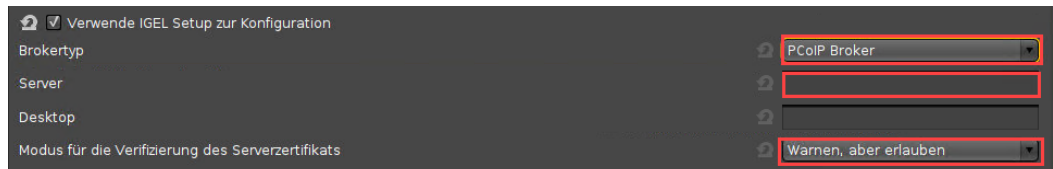
### Im IGEL Setup konfigurieren

Wenn Sie das IGEL Setup für die Konfiguration verwenden möchten, gehen Sie wie folgt vor:

1. Aktivieren Sie **Verwende IGEL Setup zur Konfiguration**.
2. Wählen Sie den **Brokertyp**, über den Sie sich mit Amazon WorkSpaces verbinden möchten.
  - a. Brokertyp: **Direkt Hardhost**
    - Geben Sie den AWS WorkSpaces Registrierungs-Code als **Server** ein.
    - Setzen Sie **Modus für die Verifizierung des Serverzertifikats** auf "Warnen, aber erlauben".



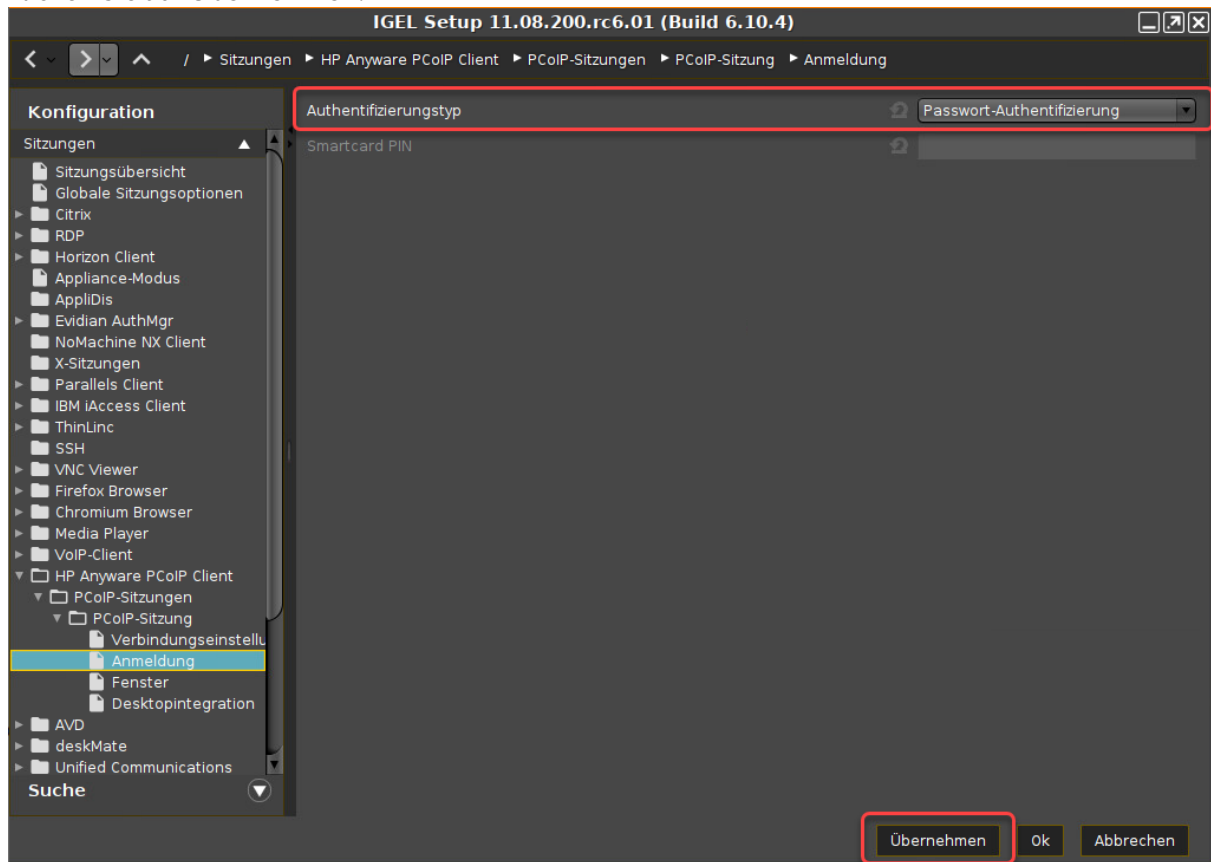
- b. Brokertyp: **PCoIP Broker**
  - Geben Sie den Server des PCoIP Brokers als **Server** ein.
  - Setzen Sie **Modus für die Verifizierung des Serverzertifikats** auf "Warnen, aber erlauben".



 Für weitere Informationen über die Brokertypen, siehe [Brokertypen, um Amazon WorkSpaces mit dem HP Anyware Client in IGEL OS zu verbinden](#) (see page 336).

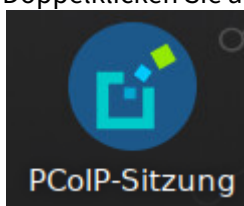
3. Klicken Sie **Übernehmen**.
4. Gehen Sie auf **Anmeldung** und setzen Sie **Authentifizierungstyp** auf "Passwort-Authentifizierung".

5. Klicken Sie auf **Übernehmen**.



### Mit Amazon WorkSpaces verbinden

1. Doppelklicken Sie auf Ihrem Desktop das Symbol Ihrer PCoIP-Sitzung.



2. Die Anmeldemaske des HP Anyware PCoIP Client übernimmt die von Ihnen im IGEL Setup eingegebenen Informationen.
3. Klicken Sie **SAVE**.
4. Geben Sie Ihre Amazon Workspace-Anmeldeinformationen ein.  
Für den weiteren Verlauf des Verfahrens gehen Sie auf [aws.amazon.com/de/](https://aws.amazon.com/de/)<sup>32</sup>.

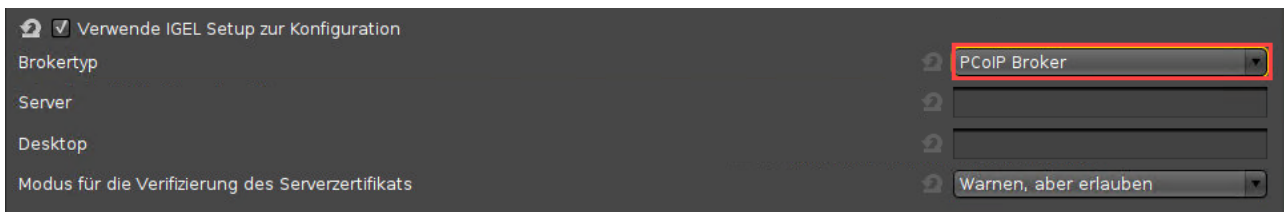
<sup>32</sup> <https://aws.amazon.com/de/>

## Brokertypen, um Amazon WorkSpaces mit dem HP Anyware Client in IGEL OS zu verbinden

Sie können zwischen zwei Brokertypen wählen, mit denen Sie sich mit Amazon WorkSpace verbinden.

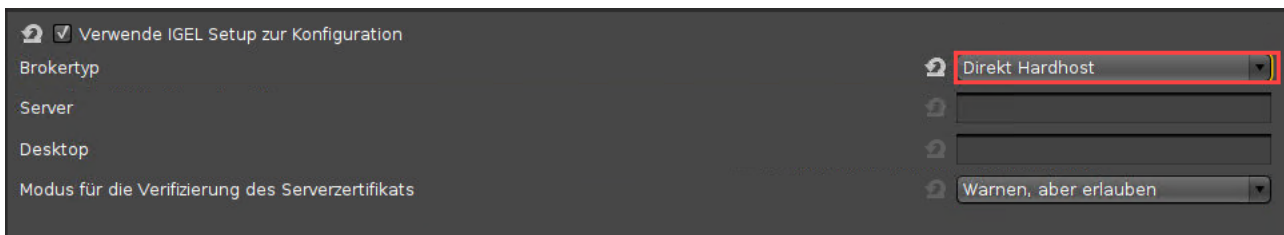
### PCoIP Broker

PCoIP Broker ist ein Ressourcenmanager, der Host-PCs dynamisch Null-Clients zuweist, basierend auf der Identität des Benutzers, der sich vom Null-Client aus einrichtet. Verbindungsbroker werden auch verwendet, um einen Pool von Hosts einer Gruppe von Null-Clients in einer PCoIP-Bereitstellung zuzuordnen. Sie sind so konfiguriert, dass sie sich immer mit demselben Host verbinden (d. h. eine statische Eins-zu-Eins-Verbindung), dann ist ein Verbindungsbroker nicht erforderlich.



### Direkt Hardhost

Ein direkter Hardhost ist eine direkte Verbindung zwischen einem Zero Client und einer entfernten Arbeitsstation, die eine PCoIP Remote Workstation Karte enthält. Sie können den DNS-Namen oder die IP-Adresse eines Hosts angeben oder Clients so konfigurieren, dass sie das Service Location Protocol (SLP) verwenden, um einen Host zu ermitteln. Sie können auch Clients so konfigurieren, dass sie sich automatisch wieder mit einem Host verbinden, wenn eine Sitzung verloren geht.





## Wie kann ich die H.264-Beschleunigung in einer HP Anyware PCoIP-Sitzung verwenden?

### Frage

Wie muss ich den Client und den Server konfigurieren, um in einer HP Anyware PCoIP-Sitzung H.264-Beschleunigung zu erhalten?

### Umgebung

Dieser Artikel ist für die folgende Umgebung gültig:

- IGEL OS 11.04 oder höher

 Mit IGEL OS 11.08.200 wurde der Client von "Teradici PCoIP" zu "HP Anyware PCoIP" umbenannt.

- UMS 6.04 oder höher
- HP Anyware PCoIP-Grafikagent für Windows 20.04

### Antwort

#### Serverseitig

1. Öffnen Sie den Group Policy Editor ( `gpedit.msc` ).
2. Gehen Sie zu **Local Computer Policy > Administrative Templates > PCoIP Session Variables > Overridable Administrator Defaults**.
3. Bearbeiten Sie die Einstellungen wie folgt:
  - Setzen Sie **Configure PCoIP image quality levels** auf "Enabled".
  - Setzen Sie **Configure PCoIP image quality levels > YUV chroma subsampling** auf "4:2:0".
  - Setzen Sie **Enable PCoIP Ultra GPU optimization** auf "Enabled".

#### Client-seitig

1. Öffnen Sie das Setup oder den Konfigurationsdialog der UMS.
2. Gehen Sie zu **System > Registry > pcoip > codec\_h264** und aktivieren Sie **H.264 codec** (Registry-Parameter: `pcoip.codec_h264` ).
3. Speichern Sie Ihre Einstellungen.

## Konfiguration von Login Enterprise

Mit dem Login Enterprise Launcher (früher Login PI) können Sie Änderungen testen, die sich auf die Leistung von Desktop- und Anwendungsanmeldungen und bestimmten Aufgaben innerhalb einer bestimmten Anwendung auswirken, bevor Sie sie auf realen Geräten implementieren.

- [Login Enterprise Launcher in IGEL OS \(see page 339\)](#)
- [Den geheimen Schlüssel \(Secret\) für den Login Enterprise Launcher erhalten \(see page 344\)](#)
- [Login Enterprise Launcher innerhalb einer VMware Horizon Sitzung verwenden \(see page 347\)](#)


## Login Enterprise Launcher in IGEL OS

### Voraussetzungen

- IGEL OS 11.03.100 oder höher

### Das SSL-Zertifikat hochladen

Um den Login Enterprise Launcher (früher Login PI) nutzen zu können, müssen Sie zuerst das SSL-Zertifikat von Ihrem Login Enterprise Server herunterladen: `https://IhreServerURL/contentDelivery/content/CA.crt`. Klicken Sie auf **Weiter zur Webseite**. Laden Sie das Zertifikat herunter.

 Sie müssen den Dateinamen von `CA.crt` in `LoginPI.crt` umbenennen.

← → ↻ ⓘ loginpi. /contentDelivery/content/CA.crt



#### Dies ist keine sichere Verbindung

Hacker könnten versuchen, Ihre Daten von ██████████ zu stehlen, zum Beispiel Passwörter, Nachrichten oder Kreditkartendaten. [Weitere Informationen](#)

NFT:FRR\_CFRT\_AUTHORITY\_INVALID

Dabei helfen, die Sicherheit von Chrome zu verbessern. Hierfür werden [die URLs einiger von Ihnen besuchter Seiten, bestimmte Systeminformationen und einige Seiteninhalte](#) an Google gesendet. [Datenschutzklärung](#)

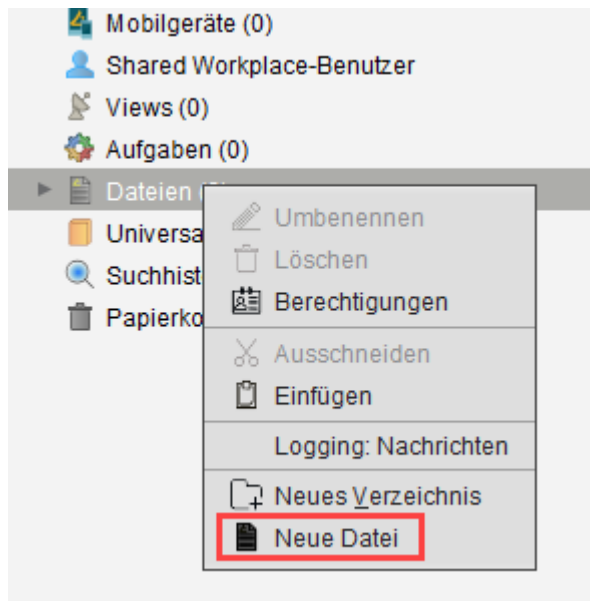
Erweiterte Informationen ausblenden

Zurück zu sicherer Website

Dieser Server konnte nicht beweisen, dass er ██████████ ist. Sein Sicherheitszertifikat wird vom Betriebssystem Ihres Computers als nicht vertrauenswürdig eingestuft. Mögliche Gründe sind eine fehlerhafte Konfiguration oder ein Angreifer, der Ihre Verbindung abfängt.

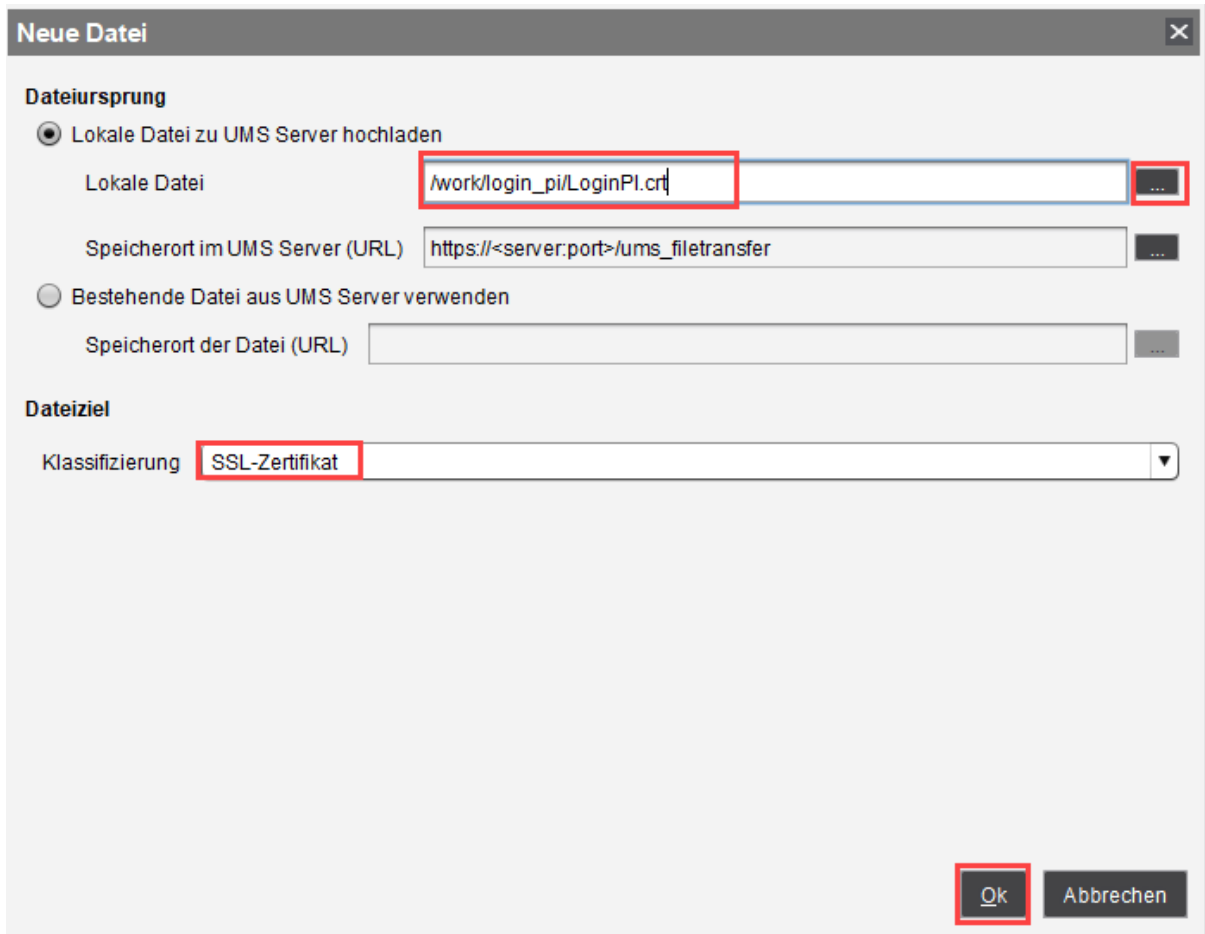
Weiter zu ██████████ (unsicher)

1. Öffnen Sie die **UMS Konsole**.
2. Wählen Sie **Neue Datei** im Kontextmenü von **Dateien**.



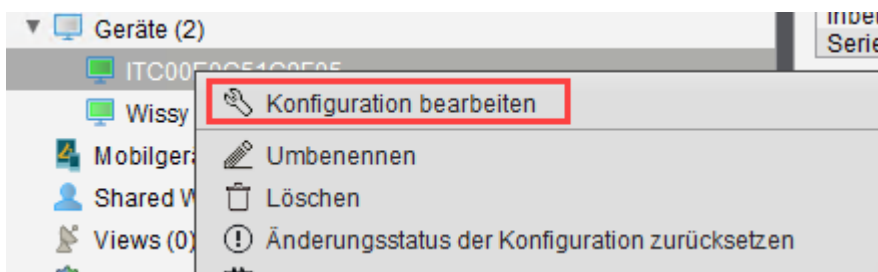
Das Fenster **Neue Datei** öffnet sich.

3. Wählen Sie die **Lokale Datei** unter **Lokale Datei zu UMS Server hochladen** aus.
4. Wählen Sie **SSL-Zertifikat** als **Klassifizierung** und klicken Sie **Ok**.



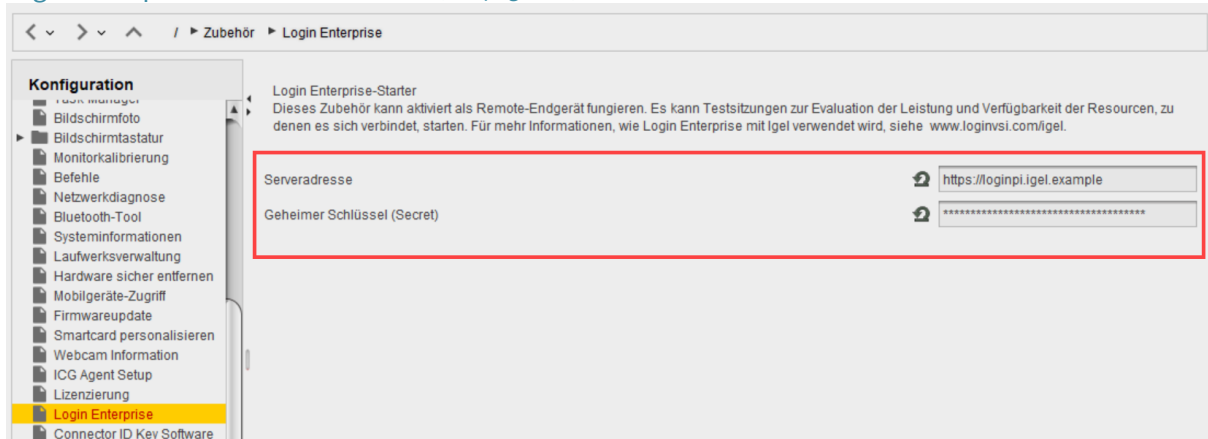
## Login Enterprise Launcher konfigurieren

1. Wählen Sie unter **Geräte** im UMS Strukturbaum das Gerät aus und klicken Sie im Kontextmenü des Geräts auf **Konfiguration bearbeiten**. Oder Sie können unter **Profile** ein neues Profil mit den erforderlichen Einstellungen erstellen und es dem Gerät zuweisen, siehe Profile erstellen.



2. Gehen Sie unter **Zubehör > Login Enterprise**.
3. Geben Sie unter **Serveradresse** die URL Ihres Login Enterprise Servers ein.

4. Geben Sie den **Geheimen Schlüssel (Secret)** ein, siehe [Den geheimen Schlüssel \(Secret\) für den Login Enterprise Launcher erhalten](#) (see page 344).



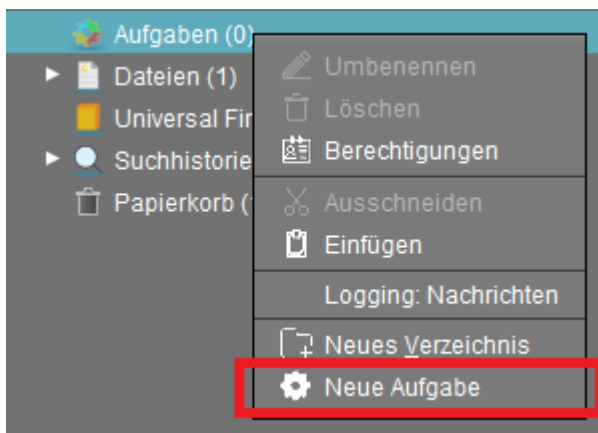
5. Speichern Sie die Einstellungen.

⚠ Wenn Sie den Login Enterprise Launcher innerhalb einer VMware Sitzung verwenden möchten, siehe [Login Enterprise Launcher innerhalb einer VMware Horizon Sitzung verwenden](#) (see page 347).

## Login Enterprise Launcher aus der UMS starten

Nachdem der Login Enterprise Server konfiguriert wurde, können Sie eine Aufgabe in der UMS erstellen, damit der Login Enterprise Launcher automatisch in einer definierten Zeit startet.

1. Im UMS Strukturbaum gehen Sie unter **Aufgaben** > [Kontextmenü] > **Neue Aufgabe**.



Das Fenster **Neue Aufgabe** öffnet sich.

2. Unter **Name** geben Sie einen Namen für die Aufgabe ein, z. B. "Login Enterprise".
3. Unter **Befehl** wählen Sie **Start Login Enterprise Launcher** aus.

**Neue Aufgabe** ✕

**Details**

Name

Befehl

Ausführungszeit  Start Datum   Aktiv

Kommentar

**Optionen**

Ergebnisse sichern  Beim Booten neu versuchen

Max. Prozesse  Verzögerung  Sekunden

Zeitlimit

**Aufgaben-Info**

Aufgaben-ID

Nächste Laufzeit

Benutzer

4. Wählen Sie die **Ausführungszeit** und das **Start Datum** aus.
5. Klicken Sie **Weiter** und weisen Sie die Geräte zu.
6. Klicken Sie **Fertig**, um die Aufgabe zu speichern.

Mehr Informationen über die Verwendung von Login Enterprise mit IGEL finden Sie unter <https://www.loginvsi.com/igel/> und im folgenden Webinar:



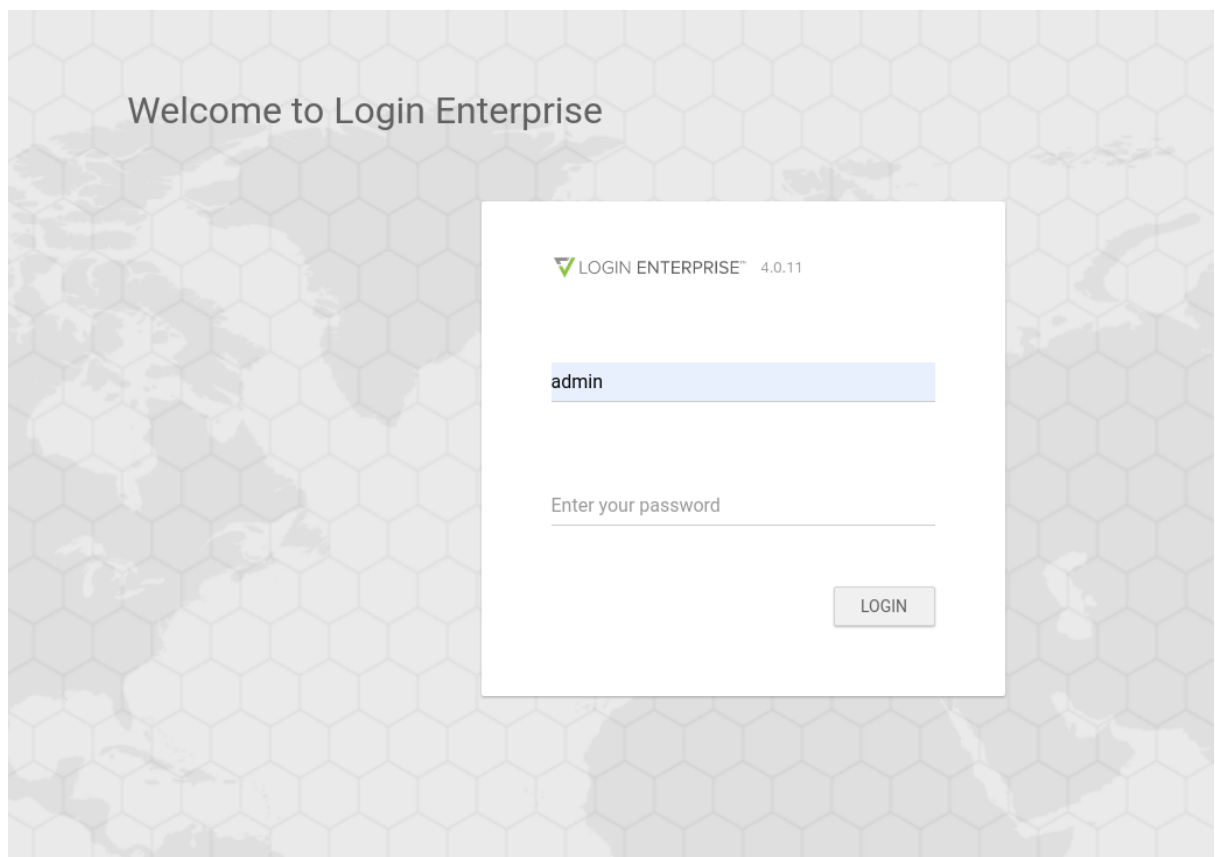
Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=N2L6z4nk8zQ>

## Den geheimen Schlüssel (Secret) für den Login Enterprise Launcher erhalten

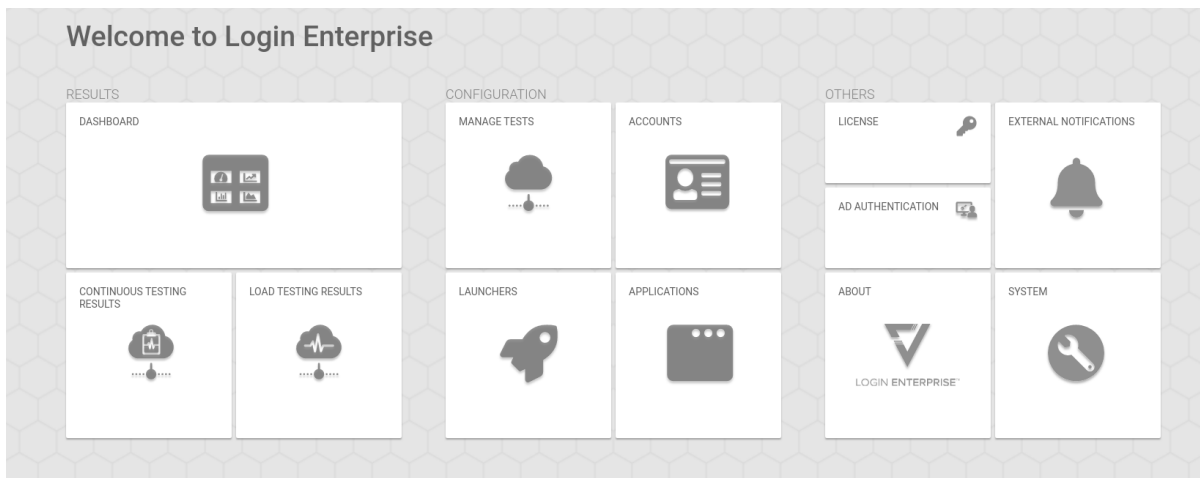
Die folgenden Schritte zeigen Ihnen, wie Sie den [geheimen Schlüssel \(Secret\)](#) (see page 342) erhalten, um den Login Enterprise Launcher zu konfigurieren.

1. Gehen Sie unter `https://IhreServerURL` .  
Geben Sie als Benutzername und Passwort `admin` ein und klicken Sie **LOGIN**.

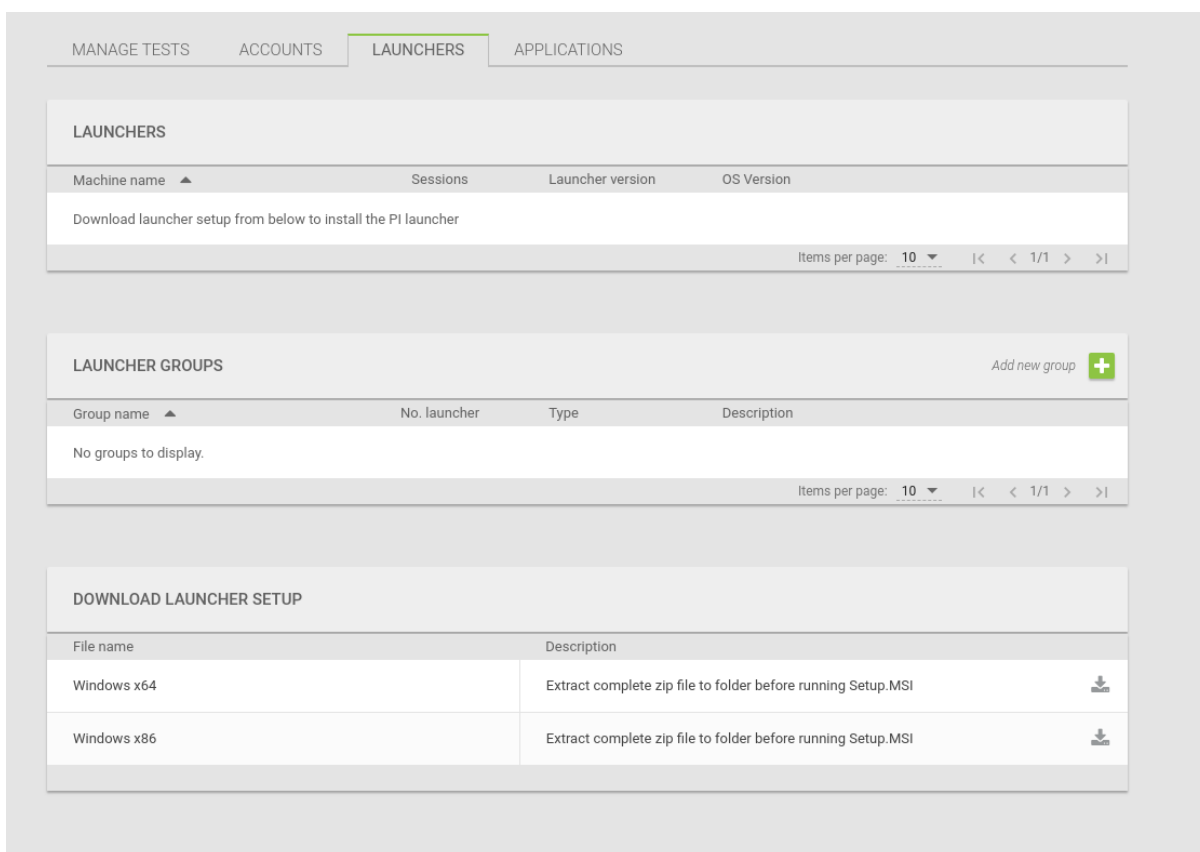


2. Gehen Sie unter **Launchers**.





3. Laden Sie eine notwendige `.zip` Datei unter **Download Launcher Setup** herunter und entpacken Sie diese.




4. Öffnen Sie die Datei `appsettings.json` im Editor.

Name	Typ
 appsettings	JSON-Datei
 Setup	CAB-Datei
 Setup	Windows Installer-Paket

Hier finden Sie den geheimen Schlüssel (**Secret**) für Ihren Login Enterprise Launcher.

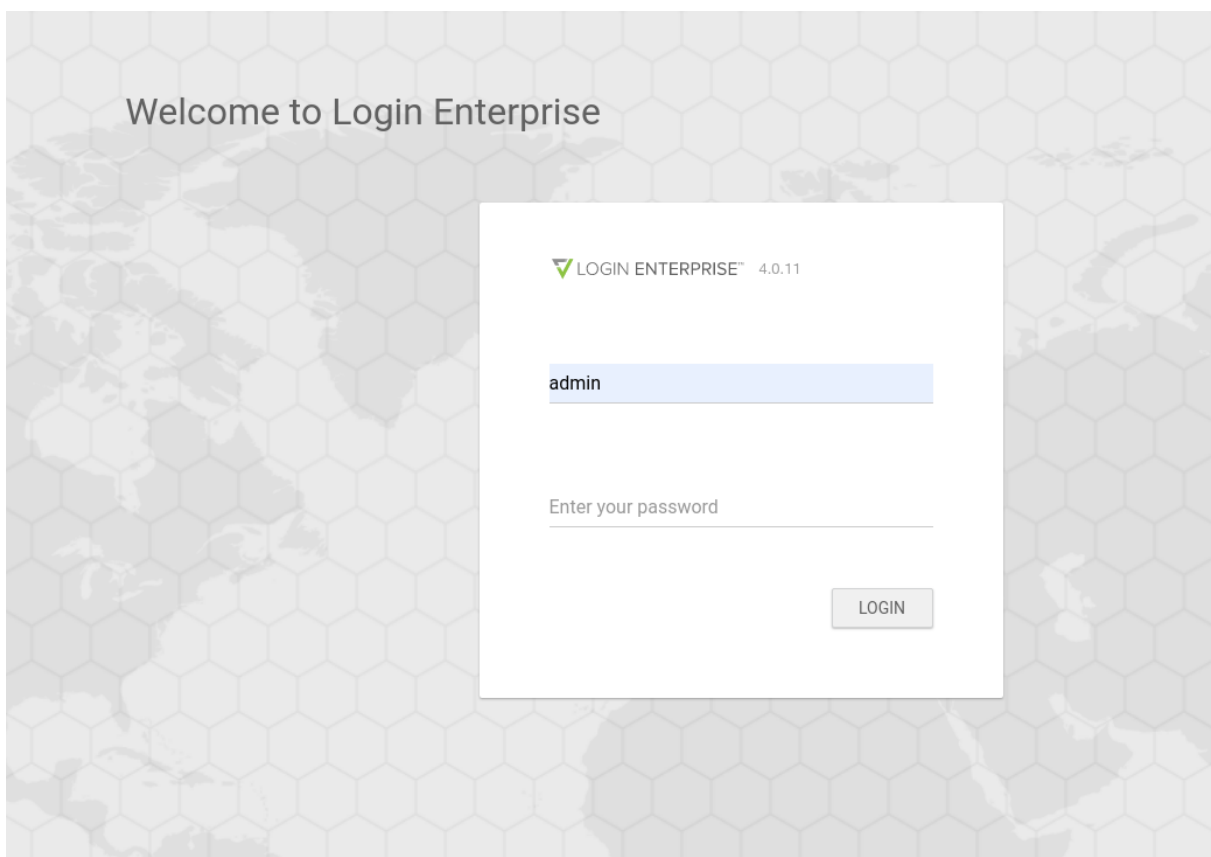
```
},  
"ServerUrl": "https://loginpi.██████████",  
"IdentityProvider": {  
  "ClientId": "Launcher",  
  "Scope": "microservice",  
  "Authority": "{ServerUrl}/identityServer",  
  "Secret": "885F0D83DB88C7F840288F██████████"  
},  
"Services": {  
  "LaunchersUrl": "{ServerUrl}/launchers",  
  "AccountsUrl": "{ServerUrl}/accounts",  
  "EnvironmentsUrl": "{ServerUrl}/environments",  
  "SessionRequestsUrl": "{ServerUrl}/sessionRequests"
```

 Verwenden Sie den geheimen Schlüssel (**Secret**) ohne Anführungszeichen "".

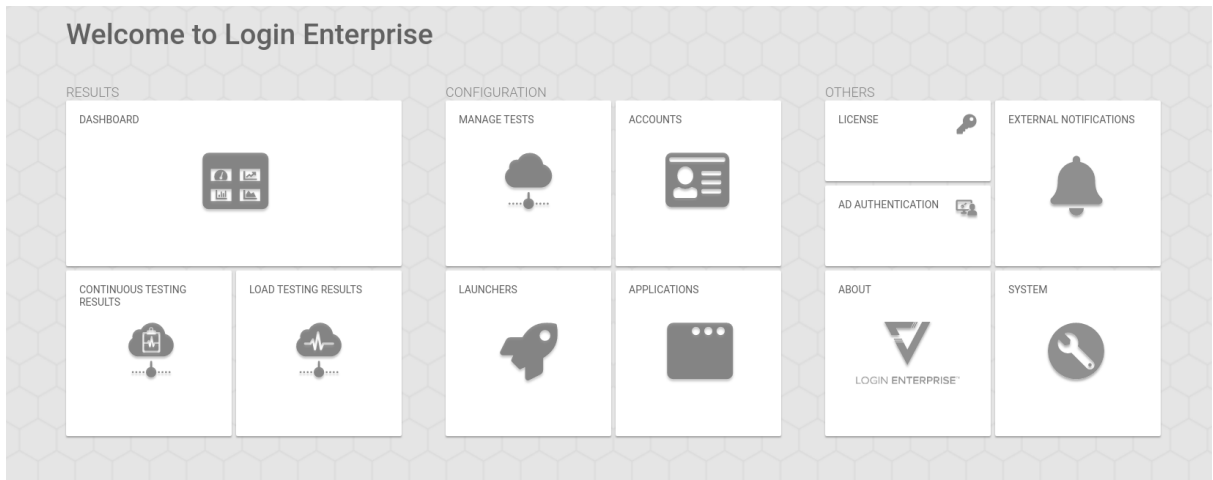
## Login Enterprise Launcher innerhalb einer VMware Horizon Sitzung verwenden

Wenn Sie den Login Enterprise Launcher innerhalb einer VMware Horizon Sitzung auf Ihrem IGEL OS Gerät verwenden möchten, müssen Sie folgendes beachten:

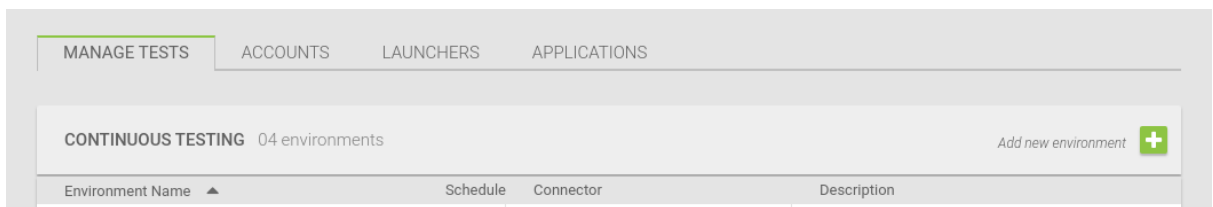
1. Gehen Sie unter `https://IhreServerURL` und melden Sie sich an.



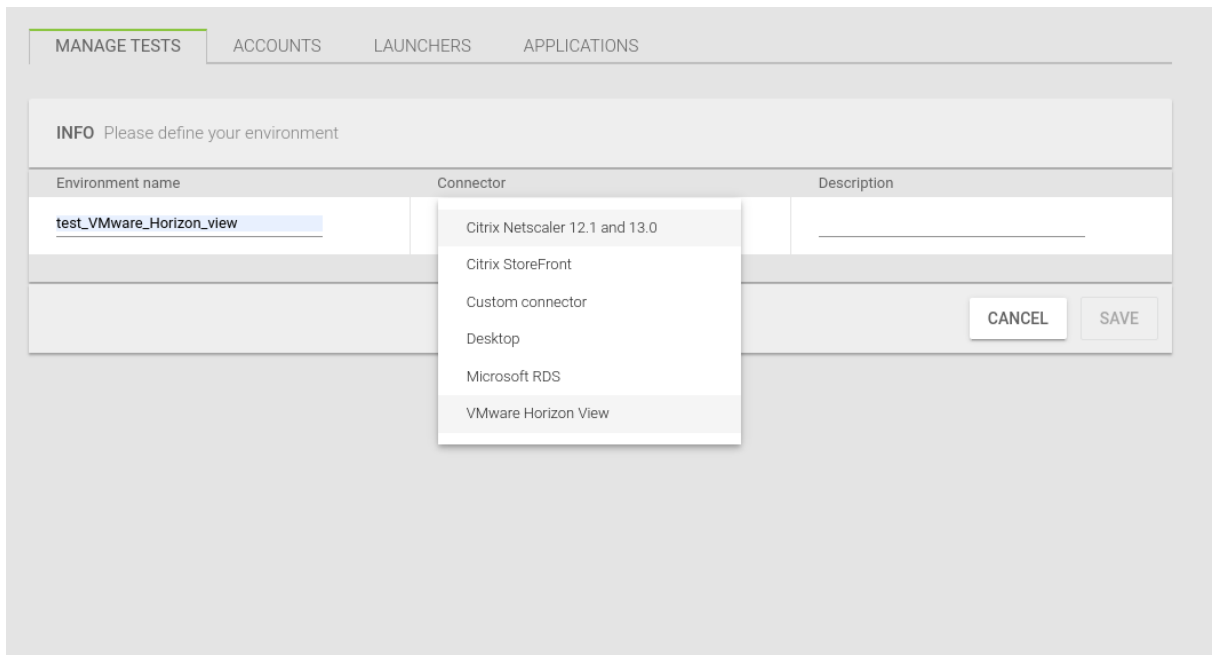
2. Gehen Sie unter **Manage Tests**.



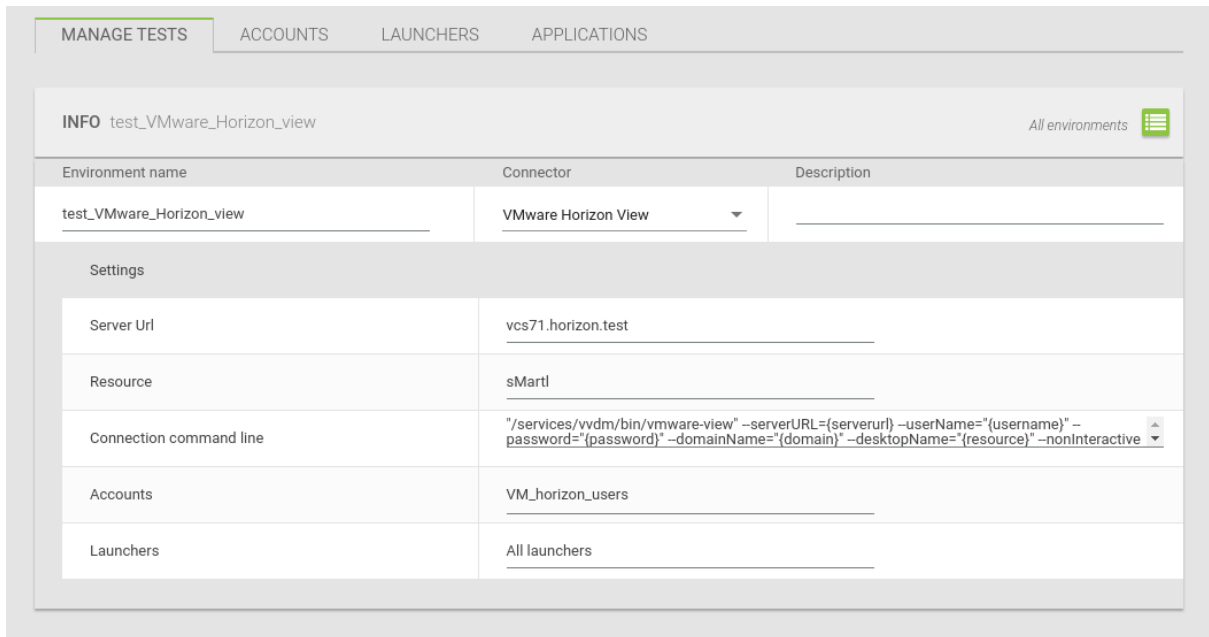
3. Klicken Sie auf **Add new environment**.



- 4. Geben Sie einen Namen unter **Environment name** ein.
- 5. Wählen Sie **VMware Horizon View** unter **Connector**.



6. Geben Sie die **Server URL** und die **Resource** ein.



The screenshot shows the 'MANAGE TESTS' tab in the IGEL configuration interface. The environment name is 'test\_VMware\_Horizon\_view'. The connector is 'VMware Horizon View'. The settings are as follows:

Environment name	Connector	Description
test_VMware_Horizon_view	VMware Horizon View	

Settings:


Server Url	vcs71.horizon.test
Resource	sMartl
Connection command line	"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --username="{username}" --password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive
Accounts	VM_horizon_users
Launchers	All launchers

7. Kopieren Sie Folgendes:

```
"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --
username="{username}" --password="{password}" --
domainName="{domain}" --desktopName="{resource}" --nonInteractive
```

und fügen Sie dies unter **Connection command line** ein.


MANAGE TESTS   ACCOUNTS   LAUNCHERS   APPLICATIONS

INFO test\_VMware\_Horizon\_view All environments 

Environment name	Connector	Description
test_VMware_Horizon_view	VMware Horizon View	

Settings

Server Url	vcs71.horizon.test
Resource	sMartl
Connection command line	"/services/vvdm/bin/vmware-view" --serverURL={serverurl} --userName="{username}" --password="{password}" --domainName="{domain}" --desktopName="{resource}" --nonInteractive
Accounts	VM_horizon_users
Launchers	All launchers

 Dies ist wichtig, wenn Sie den Login Enterprise Launcher für IGEL OS Geräte verwenden möchten!

Mehr Informationen über die Konfiguration finden Sie unter <http://www.loginvsi.com>.

## Nutanix

Nutanix ermöglicht IT-Teams den Aufbau und den Betrieb von leistungsstarken Multi-Cloud-Architekturen. Die Enterprise Cloud OS Software kombiniert private, öffentliche und verteilte Cloud-Betriebsumgebungen und bietet eine zentrale Steuerung zur Verwaltung von IT-Infrastrukturen und Anwendungen jeder Größe.

Die Lösungen von Nutanix sind zu 100 % softwarebasiert und nutzen die in der Industrie populärste hyper-konvergente Infrastruktur (HCI) Technologie.

### **Hyper-konvergente Infrastruktur**

Hyper-konvergente Infrastrukturen sind eine Weiterentwicklung von konvergenten Infrastrukturen, in denen auch Hard- und Software gebündelt sind.

Sie bieten einen kompletten Infrastruktur-Stack, der Computing, Virtualisierung, Speicher, Netzwerk und Sicherheit kombiniert, um jede Anwendung jeder Größe auszuführen.

Die Software läuft in mehreren Cloud-Umgebungen, um den IT-Betrieb zu harmonisieren und die reibungslose Mobilität aller Anwendungen zu gewährleisten. Weitere Informationen finden Sie unter [nutanix.com](https://www.nutanix.com)<sup>33</sup>.


## Frame auf Nutanix

Frame ist der einfachste Weg, um virtuelle Anwendungen und Desktops auf einer Infrastruktur Ihrer Wahl zu betreiben.

Es ist eine neue Möglichkeit, Frame Desktop-as-a-Service (DaaS) mit Apps, Desktops und Benutzerdaten zu nutzen, die auf Ihrer Nutanix (AHV) Infrastruktur gehostet werden.

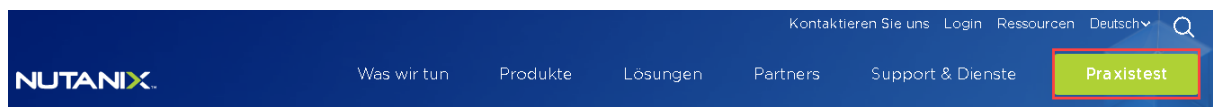
Dazu müssen Sie ein Browser-Profil erstellen und die Adresse Ihres Frame Brokers eingeben.

## Einrichten der Frameverbindung

1. Gehen Sie im IGEL Setup unter **Sitzungen > Firefox Browser > Firefox Browsersitzungen**.
2. Klicken Sie , um eine Browsersitzung hinzuzufügen.  
Für mehr Informationen über die Einrichtung, siehe Firefox Browsersitzung.

## Durchführung der Nutanix-Praxistest auf IGEL

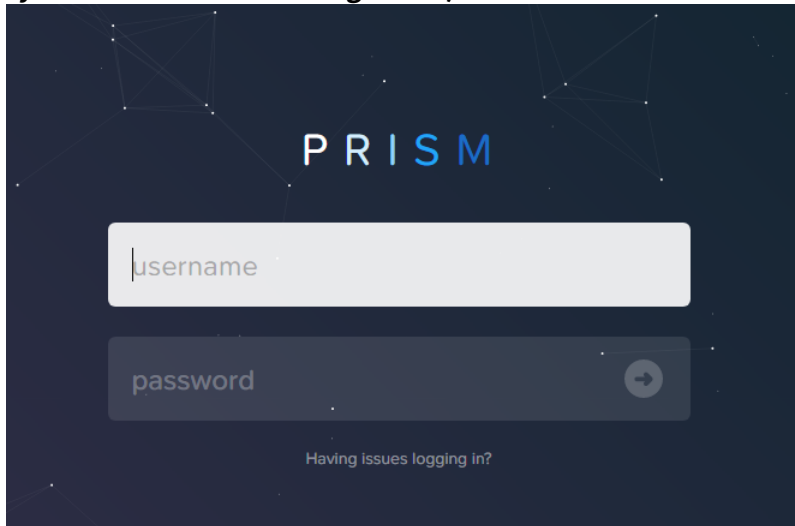
1. Öffnen Sie den Firefox Browser.
2. Geben Sie <https://www.nutanix.com/de> ein.
3. Klicken Sie **Praxistest**.



4. Geben Sie die erforderlichen Daten ein.

<sup>33</sup> <https://www.nutanix.com/de>

5. Klicken Sie auf **Launch Test Drive**.
6. Ihre **Nutanix Test Drive Informationen** werden angezeigt.
7. Klicken Sie **Test Drive starten**.
8. Geben Sie Ihre Anmeldedaten im **PRISM (Planning tool for Resource Integration, Synchronization and Management)** ein.




Für die nächsten Schritte folgen Sie den Anweisungen von Nutanix.



## Browser

- [How Can Chromium and Firefox Browsers Use H.264 Hardware Acceleration on IGEL OS Endpoint Devices? \(see page 354\)](#)
- [Mehrere Startseiten für Ihren Browser festlegen \(see page 355\)](#)
- [Touchscreen: Multitouch/Gesture Support for Firefox](#)
- [Erweiterte Benutzereinstellungen für den Browser festsetzen \(see page 356\)](#)
- [Den Firefox-Browser im Kiosk-Modus verwenden \(see page 358\)](#)
- [SSL/TLS-Fehler bei Firefox im Appliance-Modus \(see page 366\)](#)
- [Browser kann keine Dateien herunterladen \(see page 367\)](#)
- [Manche PDFs können nicht von Firefox geöffnet werden \(see page 368\)](#)
- [Kann ich Firefox Erweiterungen installieren? \(see page 370\)](#)
- [Troubleshooting: Outlook-E-Mail-Anhänge Können Nicht Heruntergeladen Werden \(see page 371\)](#)
- [Troubleshooting: Anmeldung bei MS Teams im Chromium-Browser nicht möglich \(see page 372\)](#)

## How Can Chromium and Firefox Browsers Use H.264 Hardware Acceleration on IGEL OS Endpoint Devices?

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

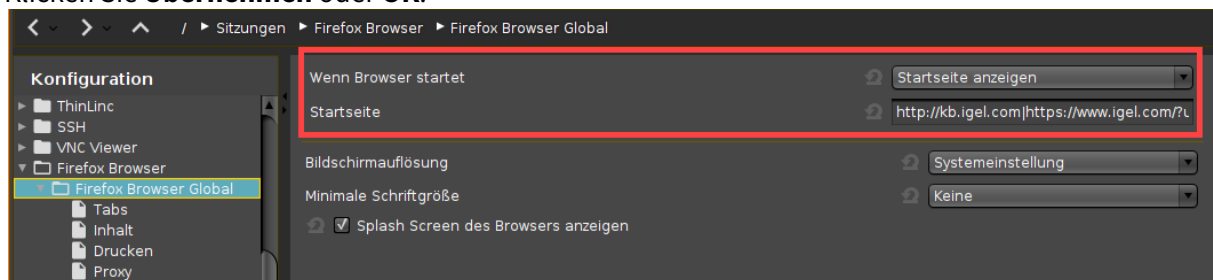
## Mehrere Startseiten für Ihren Browser festlegen

In manchen Fällen kann sich ein fester Satz von Startseiten, die in separaten Registerkarten angezeigt werden, als nützlich erweisen. Zum Beispiel, wenn der Browser im Kiosk-Modus arbeitet, ist die Wiederverwendung einer Reihe von Registerkarten aus einer früheren Sitzung keine Option.

Im Folgenden wird beschrieben, wie Sie mehrere Startseiten festlegen, die beim Start des Browser geöffnet werden.

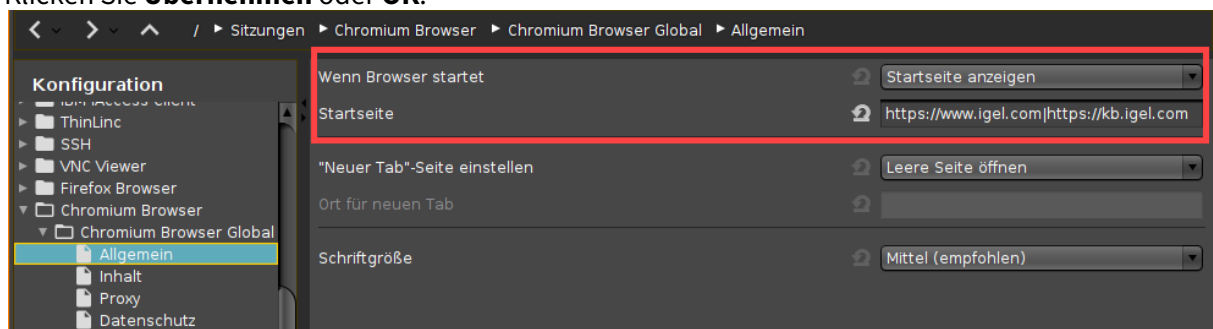
### Firefox

1. Öffnen Sie IGEL Setup und gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global**.
2. Setzen Sie **Wenn Browser startet** auf **Startseite anzeigen**.
3. Legen Sie unter **Startseite** die URLs fest, die beim Browserstart geöffnet werden sollen. Verwenden Sie "|" als Trennzeichen.
4. Klicken Sie **Übernehmen** oder **OK**.



### Chromium

1. Öffnen Sie IGEL Setup und gehen Sie zu **Sitzungen > Chromium Browser > Chromium Browser Global > Allgemein**.
2. Setzen Sie **Wenn Browser startet** auf **Startseite anzeigen**.
3. Legen Sie unter **Startseite** die URLs fest, die beim Browserstart geöffnet werden sollen. Verwenden Sie "|" als Trennzeichen.
4. Klicken Sie **Übernehmen** oder **OK**.



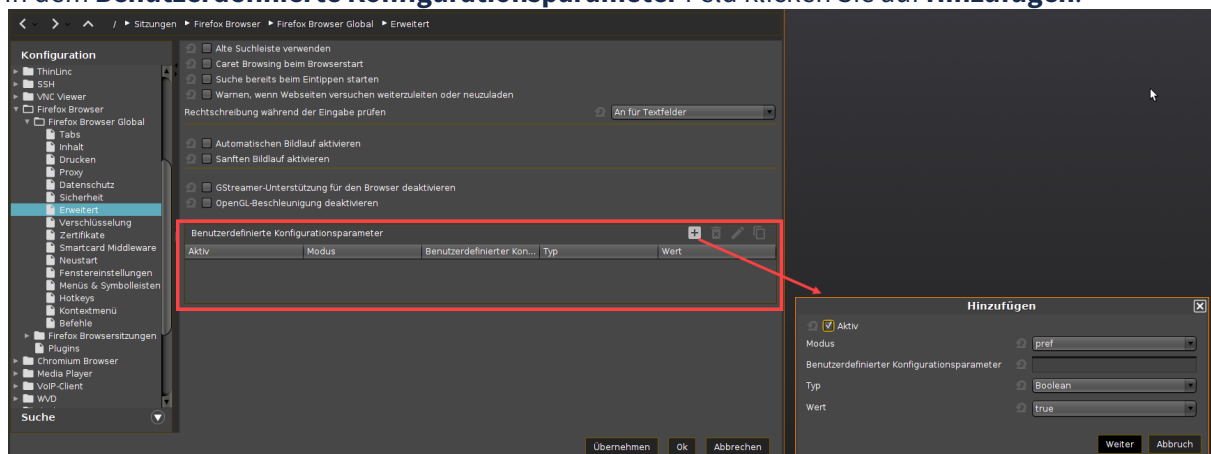
## Erweiterte Benutzereinstellungen für den Browser festsetzen

Der in IGEL OS integrierte Browser Mozilla Firefox bietet eine Vielzahl von Konfigurationsmöglichkeiten. Sie reichen von der Sortierreihenfolge über Verschlüsselungsalgorithmen bis hin zur Behebung von Fehlern in Webanwendungen, die für Sie von Bedeutung sind. Insgesamt sind es zu viele, um sie im IGEL Setup als einzelne Elemente darzustellen. Ab IGEL Linux Version 5.09.100 können Sie jedoch alle Browser-Benutzereinstellungen im IGEL Setup generisch festlegen.

⚠ Änderungen an den erweiterten Firefox-Browsereinstellungen können die Stabilität, Sicherheit und Geschwindigkeit beeinträchtigen. IGEL Support ist nicht verantwortlich für Probleme, die durch eine Änderung der Browserkonfiguration entstehen, auch wenn die Browserkonfiguration im IGEL Setup geändert wurde.

Informationen zu den Konfigurationsparametern für Firefox finden Sie in der MozillaZine Knowledge Base unter [Firefox About:config entries](http://kb.mozillazine.org/About:config_entries)<sup>34</sup>.

1. Gehen Sie in Setup unter **Sitzungen > Firefox Browser > Firefox Browser Global > Erweitert**.
2. In dem **Benutzerdefinierte Konfigurationsparameter** Feld klicken Sie auf **Hinzufügen**.



3. Geben Sie in der Option **Aktiv** an, ob der Konfigurationsparameter aktiv sein soll.
4. Geben Sie den **Modus** des Konfigurationsparameters an - in vielen Fällen reicht **pref**.
5. Geben Sie unter **Benutzerdefinierter Konfigurationsparameter** den Namen des Konfigurationsparameters an. Beispiel: `ui.textSelectBackground`
6. Geben Sie den **Typ** des Konfigurationsparameters an.  
Mögliche Werte:
  - **String:** Dieser Wert ist eine Zeichenkette.
  - **Integer:** Dieser Wert ist eine ganze Nummer.
  - **Boolean:** Dieser Wert ist ein Wahrheitswert, z. B. `true` oder `false`.
7. Geben Sie den **Wert** des Konfigurationsparameters an. Die Eingabemöglichkeiten sind abhängig vom gewählten **Typ**.
8. Klicken Sie **Ok**.  
Der Konfigurationsparameter wird beim nächsten Start des Browsers wirksam.

<sup>34</sup> [http://kb.mozillazine.org/About:config\\_entries](http://kb.mozillazine.org/About:config_entries)

Weitere Informationen zur Browserkonfiguration finden Sie im IGEL OS Referenzhandbuch unter Firefox Browser Global.

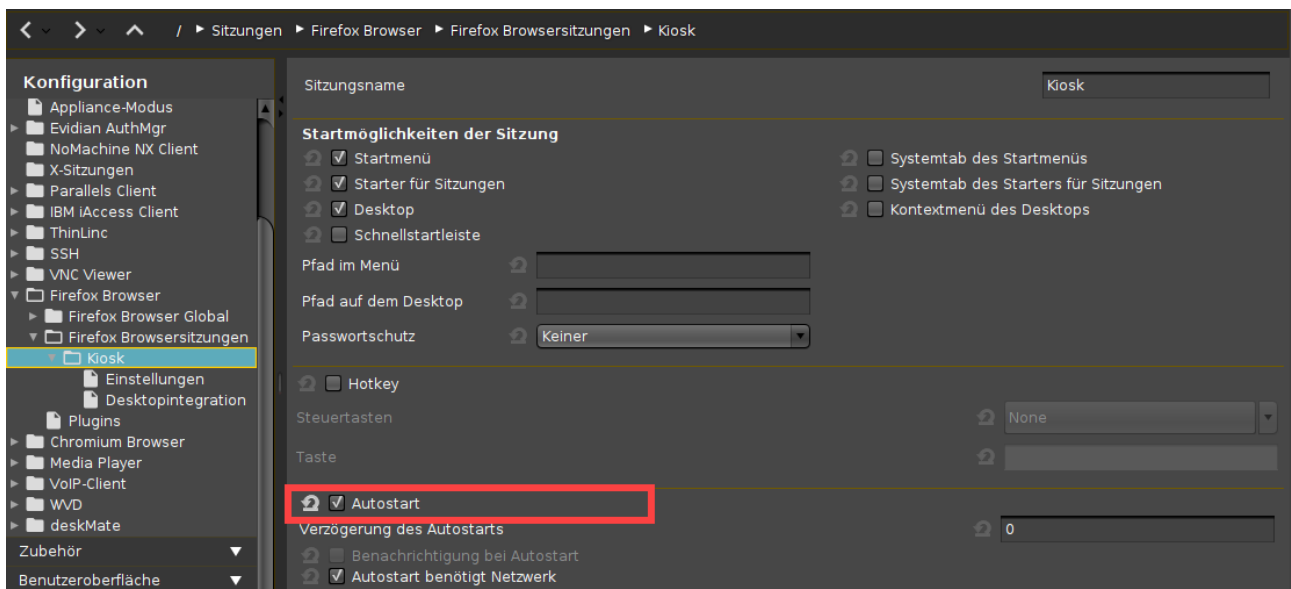
## Den Firefox-Browser im Kiosk-Modus verwenden

Der Browser-Kiosk-Modus ist eine Option für ein beliebiges öffentliches Terminal mit anonymem Zugriff betreiben, z. B.:

- Bildungsservice in einem Museum
- Service-Terminals oder Ticketautomaten für den öffentlichen Verkehr
- Eingangsportale für ein Firmen-Intranet

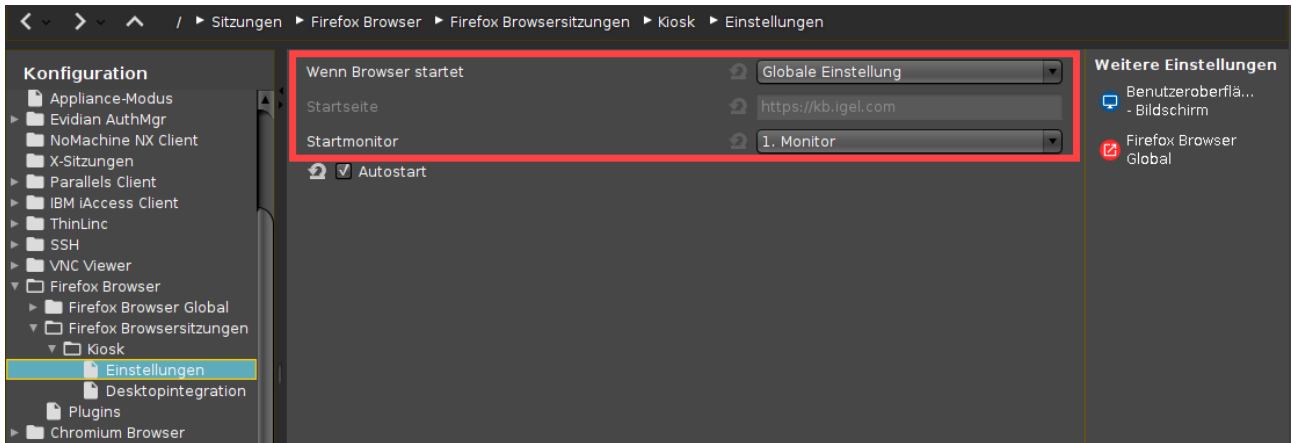
Auch wenn die Konfiguration eines IGEL OS-Geräts für den Browser-Kiosk-Modus recht umfangreich erscheint, haben Sie die Möglichkeit, Ihren eigenen Geschmack des Kiosk-Modus zu definieren. Berücksichtigen Sie die folgenden Einstellungen.

### Einstellungen unter Sitzungen > Firefox Browser > Firefox Browsersitzungen > [Sitzungsname]



- ▶ Aktivieren Sie **Autostart**.

Einstellungen unter Sitzungen > Firefox Browser > Firefox Browsersitzungen > [Sitzungsname] > Einstellungen



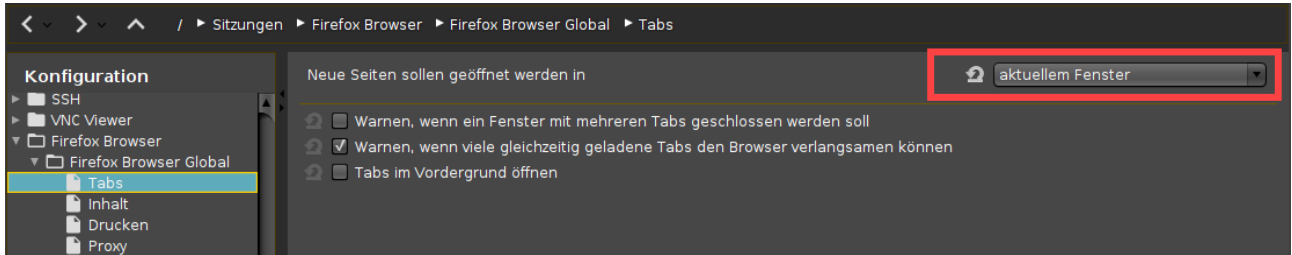
- ▶ Setzen Sie die Einstellung **Wenn Browser startet** auf **Globale Einstellung**.
- ▶ Falls notwendig, wählen Sie den **Startmonitor**.

Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global



- ▶ Setzen Sie die Einstellung **Wenn Browser startet** auf **Startseite anzeigen**.
- ▶ Geben Sie unter **Startseite** die gewünschte Startseite ein.

## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Tabs



- ▶ Setzen Sie die Einstellung **Neue Seiten sollen geöffnet werden in** auf **aktuellem Fenster** oder **neuem Tab**.

## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Inhalt



- ▶ Falls zutreffend, aktivieren Sie **Popups blockieren**.
- ▶ Aktivieren Sie **Bilder automatisch laden**.
- ▶ Aktivieren Sie bei Bedarf **JavaScript aktivieren** und passen Sie die für JavaScript zulässigen Aktionen Ihren Bedürfnissen an.

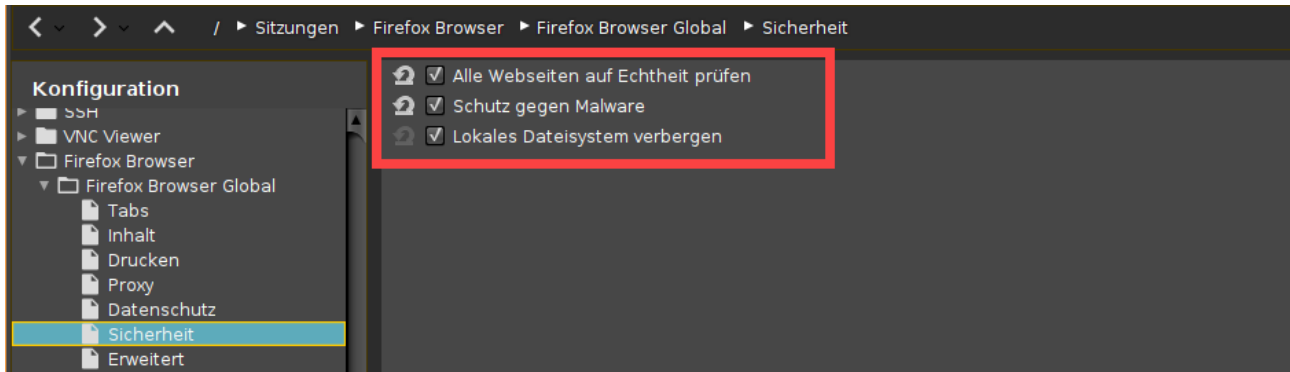


## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Datenschutz



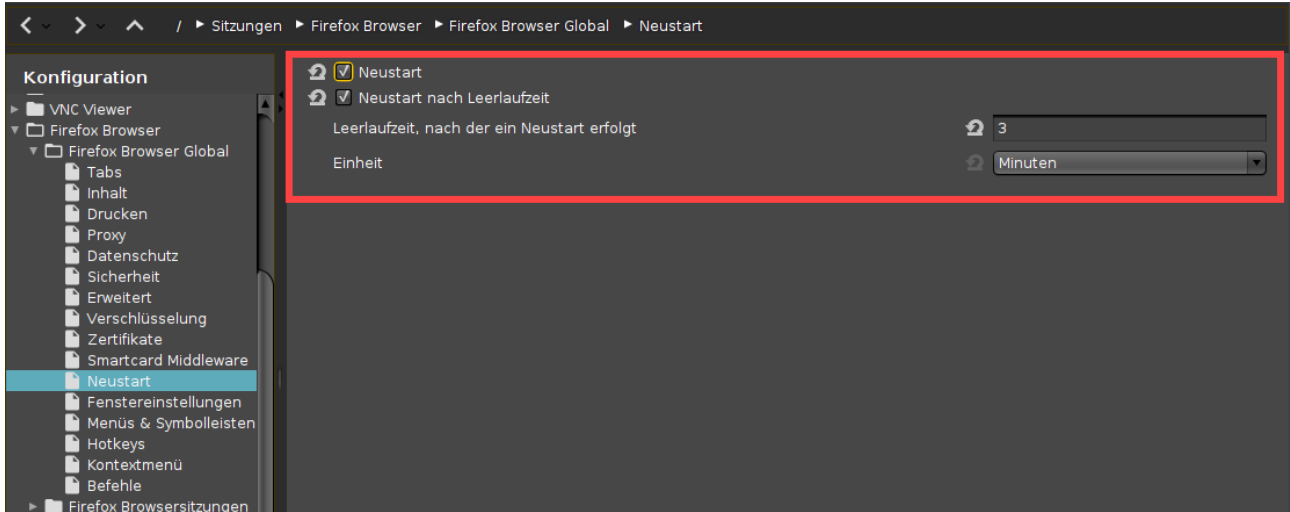
- ▶ Wählen Sie in **Browserchronik abspeichern (in Tagen)** die Einstellung **Chronik nicht abspeichern**.
- ▶ Deaktivieren Sie **Eingaben in Formulare und Suchleisten speichern**.
- ▶ Deaktivieren Sie **Passwörter speichern**.
- ▶ Aktivieren Sie **Private Daten löschen, sobald Browser beendet wurde**.
- ▶ Aktivieren Sie alle Elemente im Bereich **Welche privaten Daten sollen gelöscht werden?**
- ▶ Wenn Sie das Tracking der Aktivitäten des Benutzers unterdrücken möchte, aktivieren Sie **Privaten Browsermodus erlauben** und **Browser standardmäßig im privaten Modus starten**.
- ▶ Falls zutreffend, aktivieren Sie **Nicht-Verfolgen-Funktion einschalten**.
- ▶ Um den Browser dazu zu bringen, Domänen und Websites zu blockieren, aktivieren Sie **Tracking-Schutz aktivieren**.

## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Sicherheit



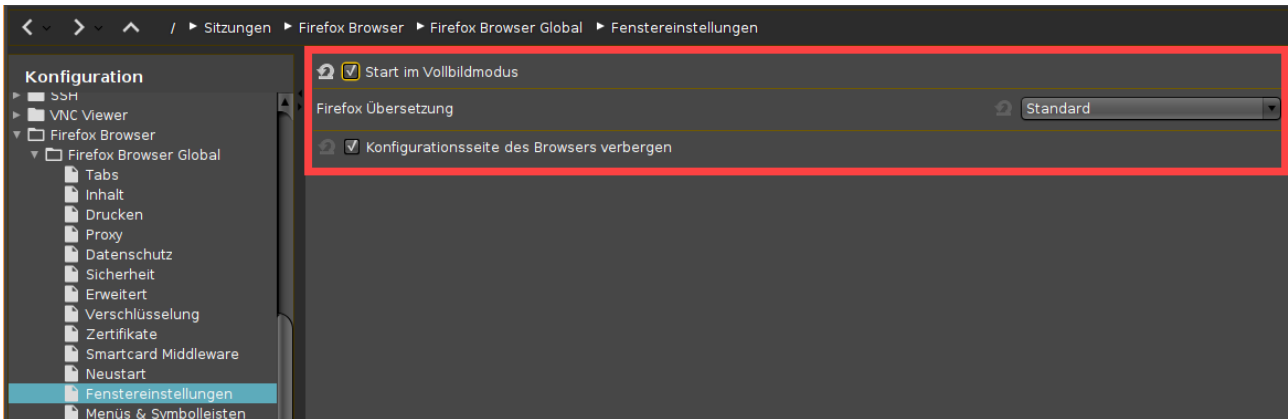
- ▶ Um den Schutz vor Phishing zu aktivieren, aktivieren Sie **Alle Webseiten auf Echtheit prüfen**.
- ▶ Um den Schutz vor bösartigen Downloads zu aktivieren, aktivieren Sie **Schutz gegen Malware**.
- ▶ Aktivieren Sie **Lokales Dateisystem verbergen**.

## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Neustart



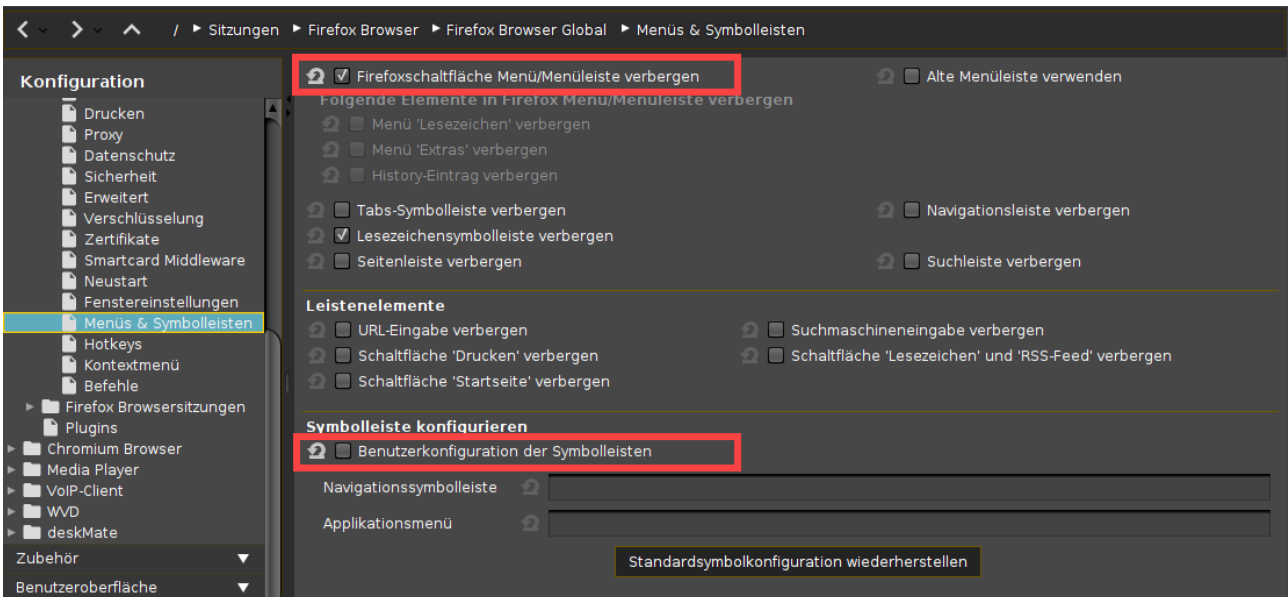
- ▶ Aktivieren Sie **Neustart**. Der Browser wird automatisch neu gestartet, wenn der Benutzer das Browser-Fenster schließt.
- ▶ Wenn Sie möchten, dass der Browser nach einer gewissen Leerlaufzeit automatisch neu gestartet wird, aktivieren Sie **Neustart nach Leerlaufzeit** und geben Sie die **Leerlaufzeit, nach der ein Neustart erfolgt** in Minuten oder Sekunden ein.

## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Fenstereinstellungen



- ▶ Wenn der Browser in Vollbildmodus angezeigt werden soll, aktivieren Sie **Start im Vollbildmodus**.
- ▶ Aktivieren Sie **Konfigurationsseite des Browsers verbergen**.

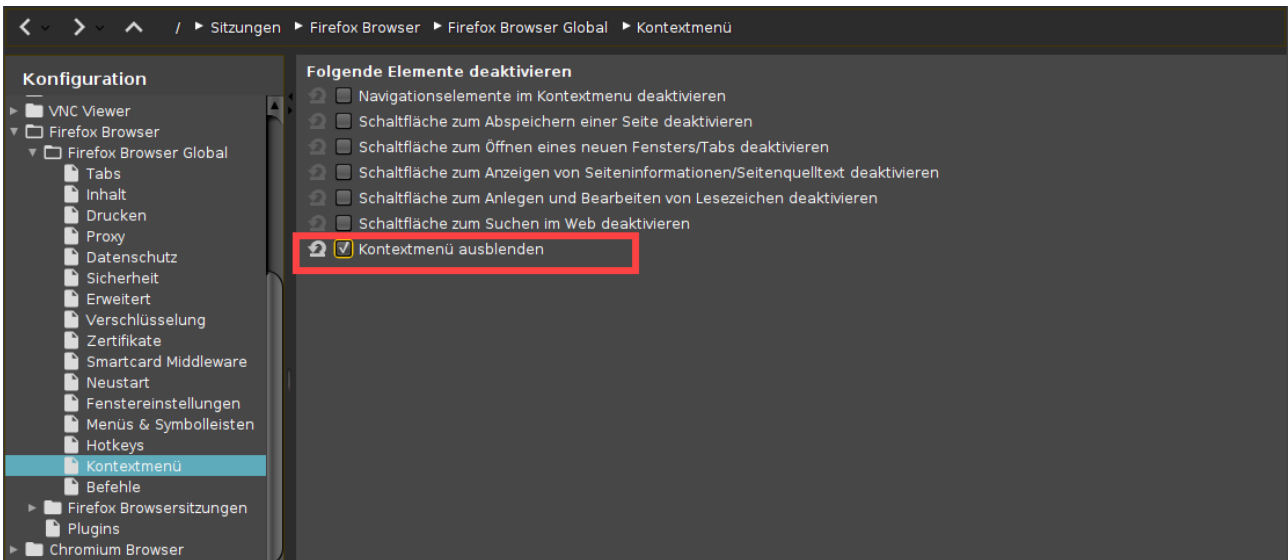
## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Menüs & Symboleisten



- ▶ Aktivieren Sie **Firefoxschaltfläche Menü/Menüleiste verbergen**.
- ▶ Wählen Sie welche Menüs und Symboleisten ausgeblendet werden sollen. Im Kiosk-Modus sind üblicherweise alle Menüs, Symbolleisten und die Adressleiste ausgeblendet.

- ▶ Deaktivieren Sie **Benutzerkonfiguration der Symbolleisten**.

## Einstellungen unter Sitzungen > Firefox Browser > Firefox Browser Global > Kontextmenü



- ▶ Aktivieren Sie **Kontextmenü ausblenden**.

## Deaktivieren des Zugriffs auf Entwickler-Tools

Um den Zugriff auf die Entwickler-Tools zu deaktivieren, fügen Sie die folgende benutzerdefinierte Einstellung hinzu.

Allgemeine Anweisungen zum Hinzufügen von benutzerdefinierten Einstellungen finden Sie unter [Erweiterte Benutzereinstellungen für den Browser festsetzen](#) (see page 356).

<b>Modus</b>	pref
<b>Benutzerdefinierte Einstellung</b>	devtools.toolbox.host
<b>Typ</b>	String
<b>Wert</b>	(lassen Sie dieses Feld leer)

## Crash-Berichte deaktivieren

Um Crash-Berichte zu deaktivieren, fügen Sie die folgenden benutzerdefinierten Einstellung hinzu.

Allgemeine Anweisungen zum Hinzufügen von benutzerdefinierten Einstellungen finden Sie unter [Erweiterte Benutzereinstellungen für den Browser festsetzen](#) (see page 356).

<b>Modus</b>	pref
<b>Benutzerdefinierte Einstellung</b>	datareporting.policy.dataSubmission
<b>Typ</b>	Boolean
<b>Wert</b>	false
<b>Modus</b>	pref
<b>Benutzerdefinierte Einstellung</b>	datareporting.healthreport.upload
<b>Typ</b>	Boolean
<b>Wert</b>	false
<b>Modus</b>	pref
<b>Benutzerdefinierte Einstellung</b>	toolkit.telemetry
<b>Typ</b>	Boolean
<b>Wert</b>	false

## SSL/TLS-Fehler bei Firefox im Appliance-Modus

### Symptom

Firefox auf IGEL Linux 5.07.100 warnt vor einem SSL/TLS-Fehler im Appliance-Modus, der im normalen Fenstermodus nicht auftritt. Der Fehlercode ist `ssl_error_unsupported_version`. Dies ist bei IGEL Linux 5.06.x nicht der Fall.

### Problem

Sie können sich nicht mit dem betroffenen HTTPS-Dienst verbinden.

### Lösung

Als Workaround können Sie Firefox anweisen, Probleme mit SSL/TLS-Versionen zu ignorieren:

1. Gehen Sie unter IGEL Setup auf **System > Firmwareanpassung > Eigene Kommandos > Basis**
2. Geben Sie folgendes Kommando in das Eingabefeld **Nach der Sitzungskonfiguration** ein:

```
echo "clearPref(\"security.tls.version.min\");" >> /services/fbrw/  
firefox/firefox.cfg
```

Es gibt auch einen IGEL Linux Privatanbieter, der dieses Problem löst.

## Browser kann keine Dateien herunterladen

### Symptom

Sie versuchen, mit dem Browser eine Datei anzusehen oder herunterzuladen, bekommen aber stattdessen eine Fehlermeldung.

### Problem

Der Browser hat keine Erlaubnis für den Dateipfad, den Sie für das Herunterladen ausgewählt haben. Dies liegt daran, dass der Browser aus Sicherheitsgründen von AppArmor überwacht wird.

### Lösung

Prüfen Sie, ob eine der folgenden Möglichkeiten anwendbar/verfügbar ist:

- Hotplug-Speichergerät, das in `/media/[device name]` oder `/userhome/media/[device name]` eingehängt ist  
Zur Konfiguration von Hotplug-Speichergerät siehe Hotplug-Speichergerät.
- Netzlaufwerk, das unter `/mnt/[folder name]` eingehängt ist
- Ordner `/userhome` im lokalen Dateisystem; nicht persistent

## Manche PDFs können nicht von Firefox geöffnet werden

### Symptom

Beim Öffnen einiger PDFs aus dem Internet öffnet der Browser Mozilla Firefox ein neues Fenster oder eine neue Registerkarte, zeigt aber den PDF-Inhalt nicht an.

### Problem

Dies kann auf eine Fehlfunktion der Firefox-Komponente des Mozpluggers zurückzuführen sein.

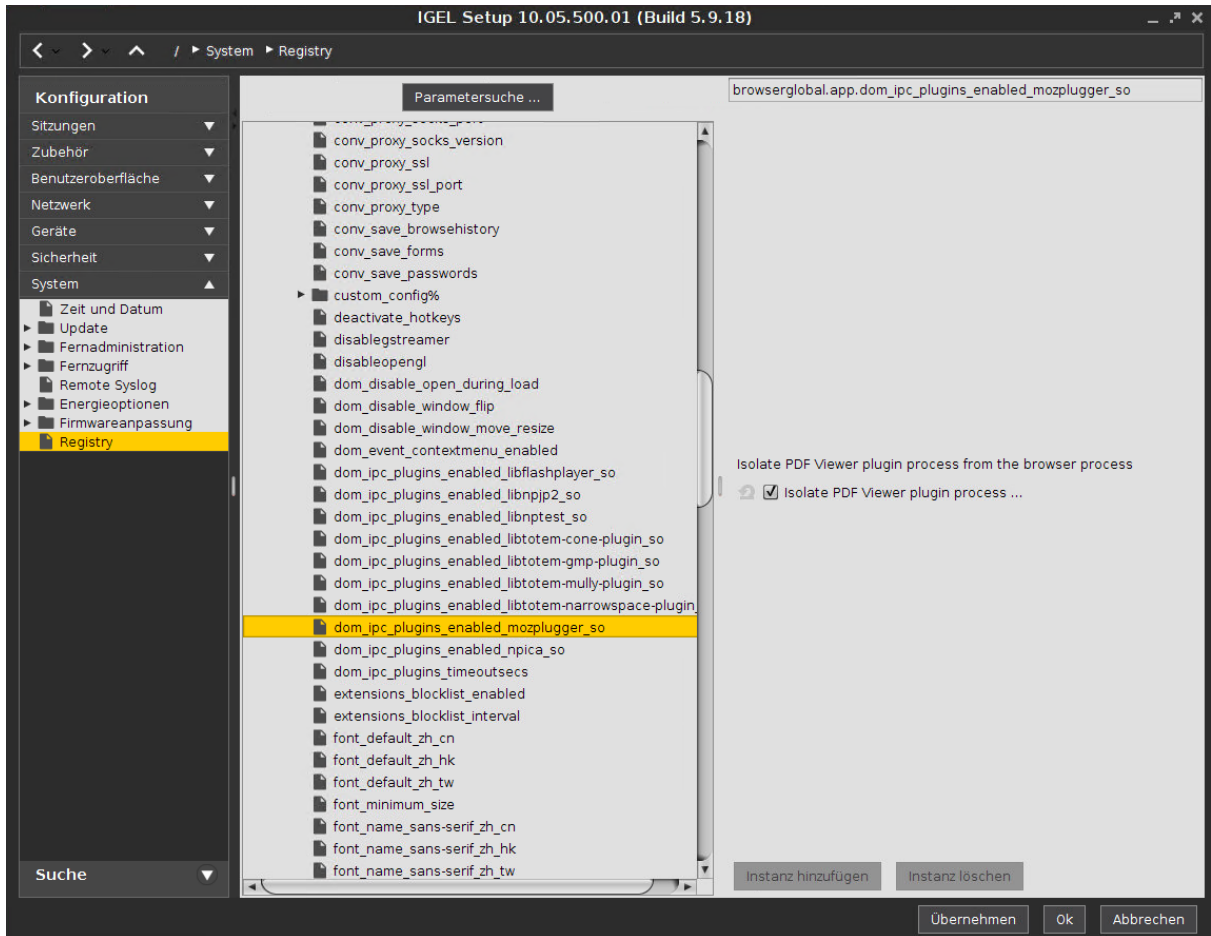
### Lösung

Deaktivieren Sie den Mozplugger. Firefox lädt das PDF-Dokument herunter und öffnet es mit einer lokalen Anwendung (IGEL Linux 5.07.100 oder neuer):

1. Gehen Sie im IGEL Setup auf **System > Registry**.
2. Verwenden Sie **Parametersuche...** um den Parameter `browserglobal.app.dom_ipc_plugins_enabled_mozplugger_so` zu finden.
3. Aktivieren Sie das Kontrollkästchen **Mozplugger deaktivieren**.
4. Bestätigen Sie die Einstellung mit **Übernehmen** oder **Ok**.



5. Starten Sie Firefox neu.



## Kann ich Firefox Erweiterungen installieren?

### Frage

Können Firefox Erweiterungen installiert werden?

### Antwort

Das Installieren von Firefox Erweiterungen ist nicht möglich. Dies gilt für alle Versionen von IGEL Linux v5.x und IGEL OS.

## Troubleshooting: Outlook-E-Mail-Anhänge Können Nicht Heruntergeladen Werden

### Problem

Wenn man versucht, einen Anhang von E-Mails in Outlook in Chromium Browser herunterzuladen, lädt Chromium nur eine Datei mit einer uid herunter.

### Lösung

Deaktivieren Sie den Dialog zum Annehmen von Downloads, durch Deaktivieren des folgenden Registrierungsschlüssels:

Parameter	<b>IGEL Download-Dialog aktivieren</b>
Pfad	<b>System &gt; Registry</b>
Registry	<code>chromiumglobal.app.enable_download_dialog</code>
Wert	<b>aktiviert</b> (default) / <b>deaktiviert</b>

## Troubleshooting: Anmeldung bei MS Teams im Chromium-Browser nicht möglich

### Problem

Wenn Sie versuchen, sich bei Microsoft Teams im Chromium-Browser anzumelden, wird die Website in einer Endlosschleife angezeigt, und Sie können sich nicht anmelden.

Weitere Informationen finden Sie unter <https://learn.microsoft.com/en-us/microsoftteams/troubleshoot/teams-sign-in/sign-in-loop#resolution>.

### Lösung

Damit Microsoft Teams in Chromium Browser funktioniert, müssen Sie die Verwendung von Cookies zulassen. Sie können die Verwendung aller Cookies von Drittanbietern in Chromium Browser zulassen, indem Sie den Parameter **Blocke Cookies von Drittanbietern** unter **Sitzungen > Chromium Browser > Chromium Browser Global > Datenschutz** deaktivieren.

Sie können auch Cookie-Ausnahmen konfigurieren, während Cookies von Drittanbietern blockiert bleiben, indem Sie eine benutzerdefinierte Richtlinie hinzufügen:

1. Gehen Sie zu **Sitzungen > Chromium Browser > Chromium Browser Global > Benutzerdefiniertes Setup > Policies**.
2. Klicken Sie auf  **Hinzufügen**, um eine Richtlinie zu erstellen.
3. Geben Sie als **Name der Richtlinie** ein: `CookiesAllowedForUrLs`
4. Geben Sie in das Feld **Wert der Richtlinie** die folgende Liste von URLs ein:  
`[[*.]microsoft.com; [*.]microsoftonline.com; [*.]teams.skype.com;  
[*.]teams.microsoft.com; [*.]sfbassets.com;  
[*.]skypeforbusiness.com]`
5. Speichern Sie die Änderungen.

## System

- [Zurücksetzen eines Geräts mit unbekanntem Administratorpasswort \(see page 374\)](#)
- [Fehler: "Unknown filesystem..." \(see page 376\)](#)
- [Custom Boot Commands sind nach Zurücksetzen auf Werkseinstellung weiterhin aktiv \(see page 377\)](#)
- [Lösen von Problemen mit signierten Partitionen \(see page 378\)](#)
- [Bootmodus von IGEL OS überprüfen \(see page 385\)](#)
- [IGEL OS Features zur Reduzierung der Firmware-Größe deaktivieren \(see page 386\)](#)
- [Fabulatech Umleitung-Server-Komponente \(see page 388\)](#)
- [Welche Features von IGEL OS sind betroffen, wenn die UMS ausfällt? \(see page 389\)](#)

## Zurücksetzen eines Geräts mit unbekanntem Administratorpasswort

### Symptom

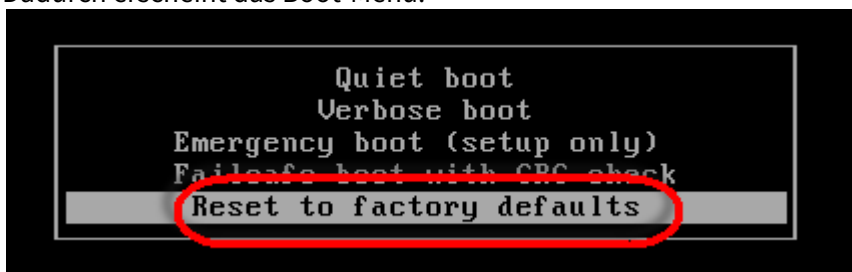
Auf IGEL OS wurde ein Administratorpasswort festgelegt (über **Setup > Sicherheit > Passwort > Administrator**), das jedoch verloren gegangen ist.

### Problem

Ohne das Passwort ist das lokale Setup nicht zugänglich. Außerdem scheint es unmöglich, das Gerät auf die Werkseinstellungen zurückzusetzen.

### Lösung

- Ändern Sie das Administratorpasswort mit IGEL UMS über **Setup > Sicherheit > Passwort > Administrator** oder
  - Setzen Sie das Gerät mit IGEL UMS zurück über **Geräte > Weitere Befehle > Zurücksetzen auf Werkseinstellungen** im UMS Menü oder
  - Setzen Sie das Gerät lokal mit einem von IGEL bereitgestellten Schlüssel auf die Werkseinstellungen zurück:
1. Drücken Sie in kurzem Abstand wiederholt die [ESC]-Taste während das Gerät neu startet. Dadurch erscheint das Boot-Menü.



2. Wählen Sie **Reset to factory defaults** und drücken Sie [Enter].

Folgendes wird angezeigt:

```
Loading "German" keyboard layout.  
The Administrator Password is required to reset the terminal settings.  
If your Administrator Password is not available anymore, enter 3 times return.  
  
Password:  
Authentication: Authentication failure  
Password:  
Authentication: Authentication failure  
Password: _
```

- Drücken Sie dreimal [Enter] ohne Angabe eines Passworts.

```
Enter <r> if you want to reboot and type the password again.
Enter <c> if you want to continue and reset the terminal settings
in case your Administrator Password is not available anymore.
<r> or <c>: _
```

- Geben Sie [c] ein und drücken Sie [Enter].  
Die Software zeigt daraufhin den Terminalschlüssel an. Notieren Sie ihn sich, da Sie ihn benötigen, den Schlüssel zum Zurücksetzen auf Werkseinstellungen von IGEL zu erhalten.
- Fordern Sie von IGEL Schlüssel für das zurücksetzen auf Werkseinstellung an. Schreiben Sie eine E-Mail an [license@igel.com](mailto:license@igel.com)<sup>35</sup> mit folgendem Inhalt
  - Ihren Terminalschlüssel
  - Ihre E-Mail-Adresse, mit der Sie beim IGEL Support registriert sind
  - Ihre Firmenadresse
  - Ihre Telefonnummer
- IGEL sendet Ihnen den Schlüssel zu.
- Geben Sie in der aktuellen Sitzung [e] ein und drücken Sie [Enter], um das Gerät herunterzufahren.
- Wiederholen Sie nach dem Zurücksetzen auf die Werkseinstellung die Schritte 1 bis 3, um das Gerät mit dem gleichen Terminalschlüssel zu starten.
- Geben Sie [e] ein und drücken Sie [Enter]. Sie werden aufgefordert, den Schlüssel zum Zurücksetzen auf Werkseinstellungen einzugeben.

```
3) enter now the "reset to defaults key", you got by the service team
for "terminal key" 39099-53083-29440-48934 and firmware version 5.03.100.01
(you have only three tries to enter the key correctly) :
1. Try: _
```

- Geben Sie den Schlüssel zum Zurücksetzen auf Werkseinstellungen ein. Geben Sie `yes` ein und drücken Sie [Enter] um das Zurücksetzen des Geräts zu bestätigen. Alle lokalen Geräteeinstellungen gehen dabei verloren.

Wenn Sie den falschen Schlüssel eingeben oder sich vertippen, müssen Sie mit Schritt 1 fortfahren.

<sup>35</sup> <mailto:license@igel.com>

## Fehler: "Unknown filesystem..."

### Symptom

Der Bootvorgang wird in einem frühen Stadium abgebrochen; die Fehlermeldung lautet "Unbekanntes Dateisystem". Konnte keine gültige IGEL-Partition finden..."

### Umgebung

- IGEL OS (egal, welche Version)

### Problem

Eine oder mehrere Systempartitionen konnten nicht gefunden werden oder sind nicht gültig.

### Lösung

► Installieren Sie mit IGEL OS Creator (OSC) das IGEL OS neu auf ein Gerät. Für eine Anleitung siehe das Kapitel Installation im IGEL OS Creator Referenzhandbuch.

#### **Bewahren Sie Ihre Einstellungen**

Um zu verhindern, dass die Einstellungen des Geräts gelöscht werden, stellen Sie sicher, dass **Alte Einstellungen migrieren** in den Installationseinstellungen aktiviert ist; siehe Installationsvorgang.

#### **Daten, die verloren gehen**

Bei einer Neuinstallation von IGEL OS gehen die folgenden Daten verloren:

- Alle Daten auf der beschreibbaren Partition /wfs
- Alle Daten, die seit ihrer Bereitstellung in einer benutzerdefinierten Partition gespeichert wurden; benutzerdefinierte Partitionen werden in ihren ursprünglichen Zustand zurückgesetzt.

#### **Lizenzen gehen verloren**

In diesem Szenario gehen die auf dem Gerät gespeicherten Lizenzen verloren. Die Lizenzen werden jedoch in der UMS zwischengespeichert, so dass sie wiederhergestellt werden, wenn sich das Gerät in der UMS registriert.



## Custom Boot Commands sind nach Zurücksetzen auf Werkseinstellung weiterhin aktiv

### Symptom

Sie haben Ihr Gerät auf die Werkseinstellungen zurückgesetzt, aber die Custom Boot Commands sind weiterhin aktiv.

### Problem

Nach dem Zurücksetzen des Geräts auf die Werkseinstellungen sind die folgenden Einstellungen weiterhin verfügbar:

- `boot_id`
- `uptime_total`
- `product`
- `force_Legacy`
- der Bootreg Eintrag `Splash` wird auf `1` gesetzt

### Lösung

Sie können diese Einstellungen manuell mit dem folgenden Kommando löschen:

1. Öffnen Sie eine lokales Terminal und melden Sie sich als root an.
2. Geben Sie das folgende Kommando ein um die Einstellungen zu löschen:

```
bootreg delete /dev/igfdisk boot_cmd
```

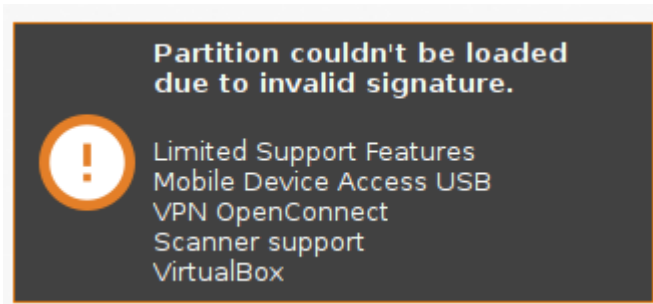
Weitere Informationen zu Custom Boot Commands finden Sie unter Custom Boot Command.

## Lösen von Problemen mit signierten Partitionen

## Fehler: "Partition couldn't be loaded due to invalid signature"

### Symptom

Während des Betriebs erscheint eine Systemmeldung wie diese:



### Umgebung

- IGEL OS 11.03 oder höher

### Problem

Eine Systempartition wurde ungültig gemacht, wodurch das Laden von Systemkomponenten verhindert wird.

### Lösung

1. Stellen Sie sicher, dass eine gültige Update-Quelle unter **System > Update > Firmware-Update** konfiguriert ist und die richtige Firmware auf dem Server gespeichert ist. (Detaillierte Informationen finden Sie unter Firmware-Update.) Wenn das lokale Setup nicht zugänglich ist, verwenden Sie das UMS.
2. Starten Sie das Gerät neu.  
Das Gerät holt sich die gültige Partition von der Updatequelle.

## Fehler: Gerät gibt einen Piepton ab, anstatt zu booten

### Symptom

Der Bootvorgang schlägt fehl, und es wird ein Pieptoncode abgespielt. Zwei Piep-Codes sind möglich:

- 3 kurze und 1 langer Piepton, 2 Mal wiederholt (die gesamte Sequenz wiederholt sich bis zu 1 Minute)
- Langer Piepton wird 1,1 Sekunden lang abgespielt, dann 2,9 Sekunden Pause (Wiederholungen bis zu 1 Minute)

### Umgebung

- IGEL OS 11.03 oder höher

### Problem

- 3 kurze und 1 langer Piepton, 2 Mal wiederholt (die gesamte Sequenz wiederholt sich bis zu 1 Minute): Die Signatur der gefundenen Systempartition ist ungültig.
- Langer Piepton wird 1,1 Sekunden lang abgespielt, dann 2,9 Sekunden Pause (wiederholt sich bis zu 1 Minute): Nach bis zu 120 Versuchen wurde überhaupt keine passende Systempartition gefunden.

### Diagnose

Um weitere Einzelheiten zu erhalten:

1. Starten Sie das Gerät neu und drücken Sie wiederholt [ESC].
2. Wählen Sie **Verbose Boot**.  
Wenn die Signatur der gefundenen Systempartition ungültig ist, sieht die Ausgabe wie folgt aus:



## Lösung

► Installieren Sie mit IGEL OS Creator (OSC) das IGEL OS neu auf ein Gerät. Für eine Anleitung siehe das Kapitel Installation im IGEL OS Creator Referenzhandbuch.

### **Bewahren Sie Ihre Einstellungen**

Um zu verhindern, dass die Einstellungen des Geräts gelöscht werden, stellen Sie sicher, dass **Alte Einstellungen migrieren** in den Installationseinstellungen aktiviert ist; siehe Installationsvorgang.

### **Daten, die verloren gehen**

Bei einer Neuinstallation von IGEL OS gehen die folgenden Daten verloren:

- Alle Daten auf der beschreibbaren Partition /wfs
- Alle Daten, die seit ihrer Bereitstellung in einer benutzerdefinierten Partition gespeichert wurden; benutzerdefinierte Partitionen werden in ihren ursprünglichen Zustand zurückgesetzt.

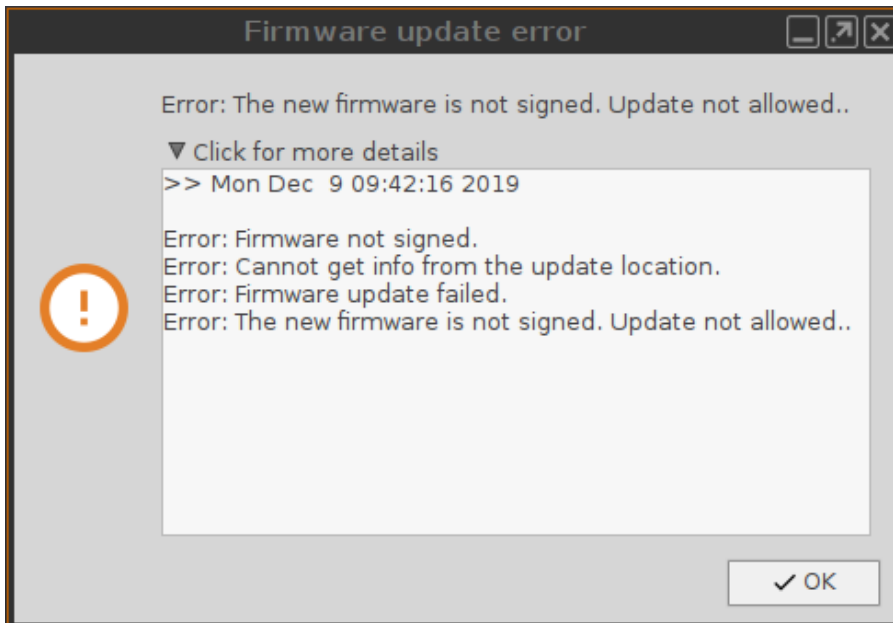
### **Bewahrung von Lizenzen**

Bei einer Neuinstallation von IGEL OS bleiben alle auf dem Gerät gespeicherten Lizenzen erhalten, sofern die entsprechende Partition gültig ist.

Fehler: "The new firmware is not signed. Update not allowed."

## Symptom

Während des Aktualisierungsvorgangs werden die folgenden Fehlermeldungen angezeigt:



## Umgebung

- IGEL OS 11.03 oder höher

## Problem

Das System erwartet signierte Systempartitionen, aber die Partitionen der Updatequelle sind nicht signiert. Dies tritt auf, wenn Sie versucht haben, ein Downgrade von IGEL OS 11.03 oder höher auf eine ältere Version von IGEL OS 11 durchzuführen.

## Lösung

- ▶ Wenn Sie ein Downgrade von IGEL OS 11.03 auf IGEL OS 11.02 durchführen möchten, z. B. weil Sie bestimmte ältere Client-Versionen benötigen, setzen Sie die Update-Quelle auf IGEL OS 11.02.200.

IGEL OS 11.02.200 ist eine spezielle Variante von IGEL OS 11.02, die über signierte Partitionen verfügt; diese Version ist nur über das IGEL Support-Team erhältlich.

## Fehler: "Invalid signature - Failed to read from partition"

### Symptom

Während des Betriebs erscheint eine Systemmeldung wie diese:



### Umgebung

- IGEL OS 11.03 oder höher

### Problem

Eine Systempartition wurde ungültig gemacht, wodurch das Laden von Systemkomponenten verhindert wird.

### Lösung

1. Stellen Sie sicher, dass eine gültige Update-Quelle unter **System > Update > Firmware-Update** konfiguriert ist und die richtige Firmware auf dem Server gespeichert ist. (Detaillierte Informationen finden Sie unter Firmware-Update.) Wenn das lokale Setup nicht zugänglich ist, verwenden Sie das UMS.
2. Starten Sie das Gerät neu.  
Das Gerät holt sich die gültige Partition von der Updatequelle.



## Bootmodus von IGEL OS überprüfen

So überprüfen Sie den Bootmodus von IGEL OS:

1. Öffnen Sie das IGEL Startmenü.
2. Klicken Sie das i-Icon.  
Der Dialog **Informationen** öffnet sich.
3. Den **Bootmodus** finden Sie im Abschnitt **Hardware**.  
Beispiel: BIOS

## IGEL OS Features zur Reduzierung der Firmware-Größe deaktivieren

Sie möchten Ihre IGEL OS Firmware auf eine höhere Version aktualisieren, aber das Firmware-Update benötigt mehr Festplattenspeicher. Das Aktualisieren von Geräten mit weniger Festplattenspeicher führt zu einem Fehler: `Not enough space on local drive`.

### Problem

Die Größe der neue Firmware


- mit allen aktivierten Softwarefunktionen inklusive
- mit dem NVIDIA Grafiktreiber
- mit der Firefox Profil Erweiterung
- eventuell mit einer benutzerdefinierten Partition
- eventuell mit individuellem Hintergrundbild und Bootsplash

überschreitet den Festplattenspeicher des Geräts (z.B. 2 GB).

### Lösung

Deaktivieren Sie Firmware-Features, die für den produktiven Betrieb nicht erforderlich sind, um die Größe der Firmware zu reduzieren:

1. Gehen Sie in IGEL Setup unter **System > Firmwareanpassung > Features**.
2. Deaktivieren Sie Features, die in Ihrer Umgebung nicht benötigt werden.
3. Speichern Sie Ihre Einstellungen mit **Übernehmen** oder **Ok**.
4. Starten Sie das Gerät neu.
5. Aktualisieren Sie das Gerät.

 Verwenden Sie Profile, um Features auf einer Gruppe von Geräten zu deaktivieren. Detaillierte Informationen über Profile finden Sie unter Profile.



#### **Alternative Methode zur Reduzierung des Feature-Umfangs ab IGEL OS 11.04**

Wenn Sie auf IGEL OS 11.04 oder höher aktualisieren, können Sie als Alternative die unter [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher \(see page 212\)](#) beschriebene Methode verwenden. Im Vergleich zur Deaktivierung von Features über das IGEL Setup hat diese Methode den Vorteil, dass Sie die deaktivierten Features nicht erneut deaktivieren müssen, falls Sie das Endgerät auf die Werkseinstellungen zurücksetzen (siehe Reset to Factory Defaults).

## IGEL Tech Video



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=KmcCdoGbNM>

## Fabulatech Umleitung-Server-Komponente

Für die Fabulatech USB-Umleitung muss eine spezielle Fabulatech-Serverkomponente auf dem Citrix- oder RDP-Server installiert sein (USB für Remote Desktop IGEL Edition).

---

Auf der Partnerseite von Fabulatech<sup>36</sup> finden Sie nähere Informationen zur Funktion und können die Serverkomponente herunterladen.

Aktuelle Versionen sind:

- USB Redirection: [https://www.fabulatech.com/usb-for-remote-desktop-download.html#tab\\_usbrdp-lin-linux-current](https://www.fabulatech.com/usb-for-remote-desktop-download.html#tab_usbrdp-lin-linux-current)
- Scanner Redirection: <https://www.usb-over-network.com/partners/igel/scanner-for-remote-desktop-download.html>

Weitere Informationen zu Fabulatech Redirections in IGEL OS finden Sie in den folgenden Artikeln:

- Citrix: Fabulatech USB Redirection für Citrix and Fabulatech Scanner Redirection
- RDP: Fabulatech USB Redirection für RDP and Fabulatech Scanner Redirection
- Horizon: Fabulatech USB Redirection für IGEL OS and Fabulatech Scanner Redirection
- AVD: Fabulatech USB Redirection für AVD

---

<sup>36</sup> <http://www.usb-over-network.com/partners/igel/>

## Welche Features von IGEL OS sind betroffen, wenn die UMS ausfällt?

### Überblick

Im Allgemeinen arbeitet IGEL OS unabhängig von der Unified Management Suite (UMS). Das schließt beispielsweise alle Remote-Desktop-Clients ein, wie Citrix, RDP oder VMware Horizon, sowie Browser.

Alle mit der UMS vorgenommenen Konfigurationsänderungen werden auf dem Gerät gespeichert und bleiben daher bei einem Ausfall der UMS stabil.

Das Feature Shared Workplace (SWP) sowie Verwaltungsfunktionen sind jedoch von einem Ausfall der UMS betroffen.

In den folgenden Abschnitten werden die Einzelheiten aufgeführt.

### Produktivitätsfunktionen, die bei einem Ausfall der UMS betroffen sind

- Anmeldung über Shared Workplace (SWP); siehe Shared Workplace (SWP)

### Verwaltungsfunktionen, die bei einem Ausfall der UMS betroffen sind

- Konfigurationsänderungen
- Lizenzverwaltung
- Sicheres Spiegeln
- Sicheres Terminal
- Universal Firmware Update
- Firmwareanpassungen
- Übertragung von Dateien, einschließlich Custom Partitions
- Fernbefehle, etwa Wake-on-LAN oder Neustart

## Netzwerk

- [OpenVPN-Sitzungen einrichten \(see page 391\)](#)
- [Running the OpenVPN Client with a Preconfigured Configuration File \(see page 403\)](#)
- [How Can I Configure OpenVPN with an .ovpn or .conf File? \(see page 404\)](#)
- [WLAN-Roaming konfigurieren \(see page 405\)](#)
- [Eine Verbindung zu einem WLAN-Netzwerk mit versteckter SSID herstellen \(see page 407\)](#)
- [WiFi-Konnektivität verbessern \(see page 408\)](#)
- [Speicherung von WLAN-Zugangsdaten und Netzwerkschlüssel verhindern \(see page 412\)](#)
- [WPA Enterprise / WPA2 Enterprise mit TLS Client-Zertifikaten verwenden \(see page 413\)](#)
- [IPv6-Einstellungen \(see page 417\)](#)
- [Erweitertes Logging mit Syslog, Tcpdump und Netlog \(see page 420\)](#)
- [Eine Telnet-Verbindung von IGEL Linux aus herstellen \(see page 434\)](#)
- [Dynamische DNS-Aktualisierung via DDNS konfigurieren \(see page 435\)](#)
- [Ändern der SMB-Protokollversion \(see page 437\)](#)
- [Wie starte ich den WiFi-Manager in IGEL OS, wenn die Taskleiste ausgeblendet ist? \(see page 438\)](#)

## OpenVPN-Sitzungen einrichten

Dieses Dokument beschreibt die Einrichtung des OpenVPN Clients unter IGEL OS.

### Voraussetzungen


- Ein konfigurierter und laufender OpenVPN 2.x-Server
- Informationen über die OpenVPN-Serverkonfiguration (z. B. Authentifizierungsmethode)
- Ein Thin Client mit IGEL OS 10.01.100 oder höher
- Das Zertifikat und die privaten Schlüsseldateien für den Client, zusammen mit dem Stammzertifikat der CA, die die Client- und Serverzertifikate signiert hat.
- Optional eine Smartcard oder ein eToken, die von IGEL Linux unterstützt werden.

Wie Sie Schlüssel und Zertifikate auf den Thin Clients verteilen, erfahren Sie im How-To "[Sicheres Verteilen von Schlüsseln und Zertifikaten](#) (see page 402)".

- 
- [Authentifizierung mit TLS-Zertifikaten](#) (see page 392)
  - [Authentifizierung mit Name/Passwort](#) (see page 393)
  - [Authentifizierung mit Name/Passwort und Zertifikat](#) (see page 394)
  - [Authentifizierung mit statischem Schlüssel](#) (see page 395)
  - [Optionen und TLS-Optionen](#) (see page 396)
  - [DNS und Routing](#) (see page 397)
  - [Proxy](#) (see page 398)
  - [VPN-Verbindung überprüfen](#) (see page 399)
  - [VPN beim Booten automatisch starten](#) (see page 400)
  - [Weitere Informationen](#) (see page 401)
  - [Sicheres Verteilen von Schlüsseln und Zertifikaten](#) (see page 402)

## Authentifizierung mit TLS-Zertifikaten

1. Gehen Sie in IGEL Setup zu **Netzwerk > VPN > OpenVPN**.
2. Erstellen Sie eine neue Sitzung.
3. Geben Sie im Bereich **Sitzung** der neuen Sitzung den Namen oder die öffentliche IP-Adresse des OpenVPN-Servers ein.
4. Wählen Sie bei **Authentifizierungsdienst** die Option **TLS-Zertifikate**.
5. Geben Sie bei **Benutzerzertifikats-Datei** den Namen des Client-Zertifikats ein.
6. Geben Sie bei **Dateiname des CA Zertifikats** den Namen des Stammzertifikats der CA ein.
7. Geben Sie bei **Dateiname des privaten Schlüssels** den Namen der Datei mit dem privaten Schlüssel des Clients ein. Wenn der Schlüssel mit einem Passwort geschützt ist, geben Sie dieses bei **Passwort für privaten Schlüssel** ein.
8. Klicken Sie auf das Startsymbol für die neu erstellte Sitzung (z. B. im Startmenü), um die Verbindung herzustellen.

 Wenn eine PKCS12-Datei verfügbar ist, die das Client-Zertifikat, die Zertifizierungsstelle und den privaten Schlüssel enthält, müssen Sie nur den PKCS12-Dateinamen in die drei entsprechenden Felder eingeben. Der Vorteil ist, dass Sie nur eine einzige Datei anstelle von drei verschiedenen Dateien ausrollen müssen.




## Authentifizierung mit Name/Passwort

1. Gehen Sie zu **Netzwerk > VPN > OpenVPN** und erstellen Sie eine neue Verbindung.
2. Geben Sie im Bereich **Sitzung** der neuen Sitzung den Namen oder die öffentliche IP-Adresse des OpenVPN-Servers ein.
3. Wählen Sie bei **Authentifizierungstyp** die Option **Name/Passwort**.
4. Geben Sie im Feld **Benutzername** den Benutzernamen ein. Wenn Sie dieses Feld leer lassen, wird der Benutzer beim Verbinden nach dem Benutzernamen gefragt.
5. Aktivieren Sie **Passworteingabe notwendig**.
6. Geben Sie das **Passwort** ein. Wenn Sie dieses Feld leer lassen, wird der Benutzer beim Verbinden nach dem Passwort gefragt.
7. Geben Sie unter **Dateiname des CA Zertifikats** den Dateinamen der Zertifikatsdatei ein.
8. Klicken Sie auf ein Startsymbol für die neu erstellte Sitzung (z. B. im Startmenü), um die Verbindung herzustellen.

## Authentifizierung mit Name/Passwort und Zertifikat

1. Gehen Sie zu **Netzwerk > VPN > OpenVPN** und erstellen Sie eine neue Verbindung.
2. Geben Sie im Bereich **Sitzung** für die neue Verbindung den Namen oder die öffentliche IP-Adresse des OpenVPN-Servers ein.
3. Wählen Sie bei **Authentifizierungstyp** die Option **Name/Passwort und Zertifikat**.
4. Geben Sie unter **Benutzername** den Benutzernamen ein. Wenn Sie dieses Feld leer lassen, wird der Benutzer beim Verbinden nach dem Benutzernamen gefragt.
5. Aktivieren Sie **Passworteingabe notwendig**.
6. Geben Sie das **Passwort** ein. Wenn Sie dieses Feld leer lassen, wird der Benutzer beim Verbinden nach dem Passwort gefragt.
7. Geben Sie bei **Benutzerzertifikats-Datei** den Dateinamen des Client-Zertifikats ein.
8. Geben Sie bei **Dateiname des CA Zertifikats** den Dateinamen des CA-Zertifikats ein.
9. Geben Sie bei **Dateiname des privaten Schlüssels** den Dateinamen des privaten Schlüssels ein. Wenn der private Schlüssel mit einem Passwort geschützt ist, geben Sie dieses bei **Passwort für privaten Schlüssel** ein.
10. Klicken Sie auf das Startsymbol für die neu erstellte Sitzung (z. B. im Startmenü), um die Verbindung herzustellen.

 Wenn eine PKCS12-Datei verfügbar ist, die das Client-Zertifikat, die Zertifizierungsstelle und den privaten Schlüssel enthält, müssen Sie nur den PKCS12-Dateinamen in die drei entsprechenden Felder eingeben. Der Vorteil ist, dass Sie nur eine einzige Datei anstelle von drei verschiedenen Dateien ausrollen müssen.


## Authentifizierung mit statischem Schlüssel


1. Gehen Sie zu **Netzwerk > VPN > OpenVPN** und erstellen Sie eine neue Verbindung.
2. Geben Sie im Bereich **Sitzung** der neu erstellten Sitzung den Namen oder die öffentliche IP-Adresse des OpenVPN-Servers ein.
3. Wählen Sie bei **Authentifizierungstyp** die Option **Statischer Schlüssel**.
4. Geben Sie bei **Dateiname des privaten Schlüssels** den Dateinamen des statischen Schlüssels ein.
5. Wählen Sie bei **Schlüsselrichtung** die Option **None**.
6. Geben Sie bei **Entfernte IP-Adresse** die VPN-IP-Adresse des Servers ein.
7. Geben Sie bei **Lokale IP-Adresse** die VPN-IP-Adresse des Clients ein.
8. Klicken Sie auf ein Startsymbol für die neu erstellte Sitzung (z. B. im Startmenü), um die Verbindung herzustellen.

## Optionen und TLS-Optionen

### Optionen

Unter **Netzwerk > VPN > OpenVPN > [Sitzungsname] > Optionen** können Sie verschiedene Optionen für den OpenVPN-Client einstellen. In der Regel können Sie die Standardeinstellungen unverändert lassen. Wenn der Server eine Kompression verwendet, aktivieren Sie **LZO-Kompression**.

 Wenn der Aufbau eines Tunnels fehlschlägt, versuchen Sie es erneut mit aktivierter **LZO-Kompression**.

 Die Option **--comp-lzo** ist seit OpenVPN v2.4 veraltet und sollte nicht mehr verwendet werden. Für weitere Informationen siehe <https://community.openvpn.net/openvpn/wiki/DeprecatedOptions#Option:--comp-lzoStatus:Pendingremoval>.

 Wenn Sie einen Proxy verwenden, stellen Sie **Kommunikationsprotokoll zum Host** auf den Wert **tcp-client**.

### TLS-Optionen

Unter **Netzwerk > VPN > OpenVPN > [Sitzungsname] > TLS-Optionen** können Sie verschiedene TLS-bezogene Optionen einstellen. Insbesondere können Sie konfigurieren, ob das Remote-Peer-Zertifikat verifiziert werden soll. Für Einzelheiten zu diesen Einstellungen siehe [OpenVPN-Sitzungen einrichten \(see page 391\)](#) oder OpenVPN.

## DNS und Routing

Standardmäßig verwendet OpenVPN automatisch die Einstellungen des Servers für DNS und Routing.

Wenn Sie diese Einstellungen ändern möchten, gehen Sie zu **Netzwerk > VPN > Open VPN > [Sitzungsname] > IPv4**. Hier können Sie:

- **Automatische DNS-Konfiguration** deaktivieren
- **Eigene(r) Nameserver** hinzufügen
- **Eigene Such-Domäne(n)** hinzufügen
- **Automatisches Routing** deaktivieren
- **VPN ist die Standard-Route** deaktivieren

Zusätzlich können Sie unter **Netzwerk > VPN > Open VPN > Open VPN > [Session Name] > Route[0,1,2]** drei benutzerdefinierte Routen aktivieren. Bei jeder aktivierten Route können Sie folgende Einstellungen konfigurieren:

- Ob es sich um eine **Netzwerkroute** oder eine **Hostroute** handelt.
- **Netzwerk- oder Host-IP-Adresse**
- **Netzwerkmaske** (nur für Netzwerkroute)
- Optional: **Gateway**
- Optional: **Metrik** (eine Qualitätsbewertung, die für Routingentscheidungen verwendet wird, wobei 0 die beste ist)

## Proxy


Wenn Sie einen Proxy für Ihre VPN-Verbindung konfigurieren möchten, gehen Sie zu **Netzwerk > VPN > OpenVPN > [Sitzungsname] > Proxy**. Hier können Sie folgende Einstellungen konfigurieren:

- **Proxytyp: SOCKS oder HTTP**, standardmäßig auf **Kein** gesetzt
- **Proxy-Adresse** und **Proxyport**
- **Auf unbestimmte Zeit wiederholen, wenn Fehler auftreten**

Wenn Sie den Proxytyp **HTTP** wählen, können Sie das Folgende konfigurieren:

- **Proxy-Benutzername**
- **Proxypasswort**

 Wenn Sie einen Proxy verwenden, setzen Sie **Optionen > Kommunikationsprotokoll zum Host** auf den Wert **tcp-client**.

 Wenn es Probleme mit OpenVPN gibt, lesen Sie die Meldungen in `/var/log/messages`, z. B. mit dem Protokollbetrachter **Systemprotokolle**.

## VPN-Verbindung überprüfen

Sobald eine VPN-Verbindung hergestellt ist, wird im Panel ein Schloss-Symbol mit angeschlossenen Steckern angezeigt:



Dieses dient jedoch nur als Indikator. Um sicher zu gehen, dass die VPN-Verbindung wirklich vorhanden ist:

1. Öffnen Sie ein lokales Terminal.
2. Führen Sie den Befehl `ifconfig` aus.
3. Überprüfen Sie, ob die Ausgabe ein Gerät `tun` mit einer IP-Adresse aus dem privaten Netzwerk enthält.

```
Terminal
user@IGEL-000BCA050027:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0b:ca:05:00:27
          inet addr:172.30.91.219 Bcast:172.30.255.255 Mask:255.255.0.0
          inet6 addr: fe80::20b:caff:fe05:27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1091674 errors:0 dropped:47 overruns:0 frame:0
          TX packets:125138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:79070067 (79.0 MB) TX bytes:58744380 (58.7 MB)
          Interrupt:105 Base address:0xa000


lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:108954 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108954 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:45078307 (45.0 MB) TX bytes:45078307 (45.0 MB)

tun0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.123.10 P-t-P:192.168.123.9 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
          RX packets:23080 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48007 errors:0 dropped:74 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1266538 (1.2 MB) TX bytes:63784736 (63.7 MB)


user@IGEL-000BCA050027:~$
```

4. Überprüfen Sie zusätzlich, ob Sie mit dem Befehl `ping` die private IP-Adresse des VPN-Servers erreichen können.

## VPN beim Booten automatisch starten

 Wenn Sie die Firmware über das VPN aktualisieren möchten, müssen Sie **Automatischer Verbindungsaufbau während des Bootvorgangs** aktivieren. Die Aktivierung des Autostarts der Kontrollanwendung in IGEL Setup unter **Netzwerk > VPN > OpenVPN > [Sitzungsname]** ist nicht ausreichend!

1. Gehen Sie in IGEL Setup zu **Netzwerk > VPN > OpenVPN**.
2. Aktivieren Sie die Option **Automatischer Verbindungsaufbau während des Bootvorgangs**. Der Bereich **Liste der OpenVPN Sitzungen** wird angezeigt.
3. Selektieren Sie eine der konfigurierten Sitzungen.
4. Klicken Sie die Schaltfläche **Set Auto**. Die Sitzung wird in der Spalte **Auto** markiert.

 Das System fragt Sie bei Bedarf nach Key-Passphrasen oder nach der eToken/Smartcard-PIN.



## Weitere Informationen

Weitere Informationen zu OpenVPN finden Sie auf der Webseite des OpenVPN-Projekts:

- [OpenVPN How-To](#)<sup>37</sup>
- [OpenVPN-Handbuch](#)<sup>38</sup>

---

<sup>37</sup> <https://openvpn.net/index.php/open-source/documentation/howto.html>


<sup>38</sup> <https://openvpn.net/community-resources/reference-manual-for-openvpn-2-0/>

## Sicheres Verteilen von Schlüsseln und Zertifikaten


So verteilen Sie mit der Universal Management Suite (UMS) Schlüssel und Zertifikate auf sichere Weise an Thin Clients:

1. Wählen Sie bei **Klassifizierung** die Option **Nicht definiert**.
2. Geben Sie im Feld **Speicherpfad des Thin Clients** den Pfad `/wfs/OpenVPN/` ein.
3. Aktivieren Sie bei den Zugriffsrechten ausschließlich **Lesen** für **Besitzer**. Deaktivieren Sie alle anderen Zugriffsrechte.
4. Wählen Sie bei **Besitzer** die Option **Root**.

## Running the OpenVPN Client with a Preconfigured Configuration File

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## How Can I Configure OpenVPN with an .ovpn or .conf File?

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## WLAN-Roaming konfigurieren

### Problem

Verschiedene WLAN-Netzwerke wurden für ein mobiles Gerät konfiguriert. Das Gerät sollte automatisch auf das stärkste Netzwerk umschalten.

### Lösung

Parameter zur Konfiguration von Optionen für WLAN-Roaming finden Sie unter **Setup > System > Registry**. Diese Einstellungen sollten nur von Experten geändert werden.

- Parameter für eine bessere Kontrolle der WLAN-Roaming-Funktionen mit Access Points, die die gleiche SSID verwenden:

**network.interfaces.wirelesslan.device0.lock\_initial**

Standard: `false`

Bei `true` bleibt das Gerät an dem Zugangspunkt hängen, mit dem es verbunden ist, auch wenn Kandidaten mit besserer Signalqualität vorhanden sind.

Diesen Parameter auf `true` zu setzen ist ein letzter Ausweg für Probleme, die durch zu viel Roaming verursacht werden.

**network.interfaces.wirelesslan.devices0.bgscan.module**

Nur aktiv mit den Verschlüsselungsmethoden WPA Enterprise und WPA2 Enterprise.

Standard: `none`

Mögliche Werte:

`none` : Es wird keine Hintergrundsuche durchgeführt.

`simple` : Das WLAN-Modul versucht im Hintergrund nach einem möglich besseren Signal zu suchen.

**bgscan.module** `simple` bietet folgende Optionen:

**network.interfaces.wirelesslan.device0.bgscan.simple.signal\_strength** (Standard: `-45 dBm`)

Dies definiert einen Schwellenwert, der bestimmt, welcher der beiden folgenden Parameter wirksam sein soll.


**network.interfaces.wirelesslan.device0.bgscan.simple.short\_interval** (Standard: `30 s`)

Intervall zwischen den Hintergrundsuchvorgängen (in Sekunden), wenn der tatsächliche Signalpegel des aktuell angeschlossenen Access Points schlechter ist als die Signalstärke `signal_strength`.

**network.interfaces.wirelesslan.device0.bgscan.simple.long\_interval** (Standard: `300 s`)

Intervall zwischen den Hintergrundsuchvorgängen (in Sekunden), wenn der tatsächliche

Signalpegel des aktuell angeschlossenen Access Points besser ist als die Signalstärke `signal_strength`.

 Wenn Parameter `lock_initial` `true` ist, wird empfohlen, `bgscan.module` auf `none` zu setzen.

- Parameter zur Steuerung des WLAN-Roaming zwischen WLAN-Netzwerken mit unterschiedlichen SSIDs:

**`network.interfaces.wirelesslan.device0.mssid_check_interval`** (Standard: `10 s`)

Das Intervall in Sekunden zwischen der Überprüfung, ob ein automatisches Roaming erforderlich ist.

Dazu gehört auch das Erkennen, dass eine Verbindung verloren gegangen ist und eine neue hergestellt werden soll.

**`network.interfaces.wirelesslan.device0.mssid_quality_threshold`** (Standard: `20 s`)

Wenn der Qualitätsprozentsatz der aktuellen Verbindung unter diesem Wert liegt, wird diese Überprüfung durchgeführt, um ein möglicherweise besseres Netzwerk zu finden.

**`network.interfaces.wirelesslan.device0.mssid_quality_difference_threshold`** (Standard: `40`)

Ein Kandidat für das automatische Roaming wird nur dann berücksichtigt, wenn sein Qualitätsprozentsatz viel besser ist als die Qualität der aktuellen Verbindung.

**`network.interfaces.wirelesslan.device0.mssid_previously_used_threshold`** (Standard: `55`)

Während des Startvorgangs: Wenn der Qualitätsprozentsatz der zuvor verwendeten SSID über diesem Schwellenwert liegt, wird er bevorzugt.

**`network.interfaces.wirelesslan.device0.mssid_user_selection`** (Standard: `false`)

Wenn `true`, der Benutzer kann das Roaming in ein Netzwerk über das Kontextmenü des WLAN-Systray-Symbols einleiten (muss aktiviert sein).

Wenn das automatische Roaming die Wahl des Nutzers nicht beeinträchtigen soll, sind die folgenden Werte angemessen:

**`network.interfaces.wirelesslan.device0.mssid_quality_threshold=`** `0`

**`network.interfaces.wirelesslan.device0.mssid_quality_difference_threshold=`** `101`

**`network.interfaces.wirelesslan.device0.mssid_previously_used_threshold=`** `0`

## Eine Verbindung zu einem WLAN-Netzwerk mit versteckter SSID herstellen

### Symptom

Das Gerät verbindet sich nicht mit dem WLAN-Netzwerk mit versteckter SSID.

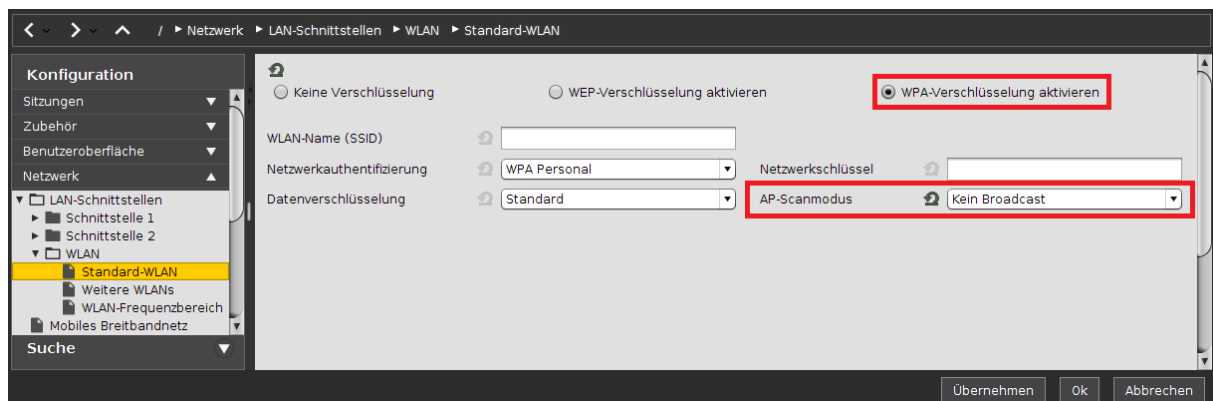
### Problem

Eine Option in der Netzwerkkonfiguration des Geräts fehlt.

### Lösung

So konfigurieren Sie versteckte Access Points:

1. Starten Sie IGEL Setup oder öffnen Sie den Konfigurationsdialog des Geräts in der UMS.
2. Gehen Sie unter **Netzwerk > LAN-Schnittstellen > WLAN > Standard-WLAN** (oder **Weitere WLANs** je nach Ihrer Konfiguration)
3. Wählen Sie **WPA-Verschlüsselung aktivieren** aus.
4. Setzen Sie den Parameter **AP-Scanmodus** auf "**Kein Broadcast**".
5. Klicken Sie **Übernehmen** oder **OK**, um die Einstellungen zu speichern.



## WiFi-Konnektivität verbessern

### Problem

Ihre WiFi-Verbindung ist instabil, schwach, oder beides.

### Voraussetzung

- UDC mit IGEL Linux v5??? oder IGEL OS??? oder höher???
- UD Pocket IGEL Linux V5??? oder IGEL OS??? oder höher???

### Mögliche Ursachen und Lösungen

Es gibt viele Umstände und Parameter, die die Qualität der WiFi-Verbindung eines Gerätes beeinflussen. Um eine geeignete Lösung für Ihr Problem zu finden, sehen Sie sich die folgende Sammlung möglicher Ursachen und Lösungsvorschläge, Workarounds und Hinweise zur Fehlerbehebung an.

#### Mehrere Access Points (APs) verwenden denselben Kanal

Wenn mehrere Access Points, die für das gerät sichtbar sind, denselben WiFi-Kanal verwenden, können Interferenzprobleme auftreten.

- ▶ Rekonfigurieren Sie den betreffenden Access Point (AP), um andere Kanäle zu verwenden.

#### Roaming innerhalb eines Netzes (dieselbe SSID)

Wenn das Gerät für das Roaming innerhalb seines Netzes konfiguriert ist, versucht er sicherzustellen, dass er den stärksten/nächsten Access Point (AP) innerhalb seines Netzes verwendet. Je nach Situation kann es sinnvoll sein, das Roaming zu deaktivieren oder zu optimieren.

Sehen Sie auch [WLAN-Roaming konfigurieren](#) (see page 405).

#### Roaming vermeiden



Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > lock\_initial** (Registry-Schlüssel: `network.interfaces.wirelesslan.device0.lock_initial`) und aktivieren Sie **Vermeiden Sie Roaming innerhalb desselben Netzes**.



Wenn Roaming deaktiviert ist, sollte **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bgscan > module** auf **keine** gesetzt werden.

Wählen Sie den Access Point mit dem besten Signal



Mit der folgenden Einstellung wählt das Gerät den Access Point aus, der beim Starten des Geräts das beste Signal sendet.

► Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bssid** (Registry-Schlüssel: `network.interfaces.wirelesslan.device0.bssid`) und geben Sie `bestsignal` in das Feld **BSSID** ein.

#### Automatisches Roaming

Automatisches Roaming ist möglich, wenn das Gerät häufig bewegt wird und mehrere Access Points verfügbar sind.

Im folgenden Beispiel ist das Gerät so konfiguriert, dass es 10 Sekunden, nachdem das Signal des aktuellen Access Points unter -78 db gefallen ist, mit der Suche nach einem anderen Access Point beginnt, während alle 60 Sekunden ein Routinescan durchgeführt wird:

1. Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bgscan > module** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module`) und wählen Sie **simple**.
2. Setzen Sie **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bgscan > module > simple > long\_interval** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module.simple.long_interval`) auf 60.
3. Setzen Sie **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bgscan > module > simple > short\_interval** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module.simple.short_interval`) auf 10.
4. Setzen Sie **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bgscan > module > simple > signal\_strength** (Registry key: `network.interfaces.wirelesslan.device0.bgscan.module.simple.signal_strength`) auf -78.

#### 40 MHz Bandbreite im 2,4-GHz-Band

Bei einigen Access Points kann es möglich sein, die 40-MHz-Bandbreite im 2,4-GHz-Band zu deaktivieren.

► Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > driver > cfg80211 > cfg80211\_disable\_40mhz\_24ghz** (Registry-Schlüssel: `network.interfaces.wirelesslan.device0.driver.cfg80211.cfg80211_disable_40mhz_24ghz`) und deaktivieren Sie **40 MHz Kanalbandbreite im 2,4-GHz-Band deaktivieren**.

#### Option für hohen Durchsatz

In manchen Umgebungen führt die in den Treiber integrierte Funktion für hohen Durchsatz möglicherweise nicht zu optimalen Ergebnissen. Sie können diese Funktion deaktivieren und prüfen, ob sich die Verbindung verbessert hat.

► Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > driver > disable\_ht** (Registry key: `network.interfaces.wirelesslan.device0.driver.disable_ht`) und klicken Sie **HT deaktivieren**.

## Nur 2,4-GHz-Band

In manchen Umgebungen kann es besser sein, nur das 2,4-GHz-Band zu verwenden.

► Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > band** (Registry key: `network.interfaces.wirelesslan.device0.band`) und wählen Sie **2,4 GHz**.

Wenn ein oder mehrere alternative WiFi-Netzwerke (SSIDs) konfiguriert sind, gehen Sie für jede alternative SSID wie folgt vor:

► Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > alt\_ssid[number] > band** (Registry key: `network.interfaces.wirelesslan.device0.alt_ssid[number].band`) und wählen Sie **2,4 GHz**.

## Frame-Aggregation

Es könnte hilfreich sein, die Frame-Aggregationsfunktion von IEEE 802.11n zu deaktivieren.

► Deaktivieren Sie die Rahmenaggregation an Ihrem Access Point (AP).

**i** Bei Ihrem Access Point kann diese Funktion einen anderen Namen haben. Beachten Sie auch, dass IGEL keine Garantie dafür übernehmen kann, dass der Access Point nach den vorgeschlagenen Konfigurationsänderungen ordnungsgemäß funktioniert.

## WiFi-Treiber scannt und wählt den Zugangspunkt aus

Standardmäßig initiiert der WPA-Antragsteller das Scannen und die Auswahl eines Zugangspunkts. Sie können dieses Verhalten ändern und diese Aufgabe dem Treiber zuweisen.

1. Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > wpa > ap\_scan** (Registry-Schlüssel: `network.interfaces.wirelesslan.device0.wpa.ap_scan`) und wählen Sie **WLAN-Treiber initiiert Scan und AP-Auswahl**.
2. Starten Sie das Gerät neu.

## Whitelist der BSSIDs

Sie können die Anzahl der zu scannenden Access Points einschränken, indem Sie eine Whitelist erstellen. Diese Whitelist enthält nur die BSSIDs derjenigen Access Points, die das Gerät scannen soll.

Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > bssid\_whitelist** (Registry-Schlüssel: `network.interfaces.wirelesslan.device0.bssid_whitelist`) und geben Sie die BSSIDs der Access Points ein, die gescannt werden sollen, getrennt durch Whitespaces.

## Debugging

Wenn keine der oben beschriebenen Methoden funktioniert, können Sie eine Protokolldatei erstellen und diese an das IGEL-Supportteam senden.

1. Gehen Sie im Setup zu **System > Registry > Netzwerk > interfaces > wirelesslan > device0 > wpa > debug** (Registry key: `network.interfaces.wirelesslan.device0.wpa.debug`) und wählen Sie **sehr umfangreich**.
2. Starten Sie das Gerät neu.
3. Senden Sie die Datei `/tmp/wpa_debug.all` an das IGEL-Supportteam.

## Speicherung von WLAN-Zugangsdaten und Netzwerkschlüssel verhindern

In diesem How-To erfahren Sie, wie Sie den WiFi-Manager so konfigurieren, dass Benutzer ihre WLAN-Zugangsdaten sowie den Netzwerkschlüssel nicht auf dem Thin Client speichern können.

1. Gehen Sie in IGEL Setup zu **System > Registry**.
2. Gehen Sie zum Parameter `network.applet.wireless.allow_storing_credentials`.
3. Deaktivieren Sie **Speichern der Anmeldedaten erlauben**. Die Einstellung ist standardmäßig aktiviert.
4. Klicken Sie **Übernehmen**.

Die Einstellungen wirken sich auf den Dialog für folgende Authentifizierungsmethoden aus:

- WPA Personal
- WPA Enterprise
- WPA2 Personal
- WPA2 Enterprise

Den Benutzern stehen ab sofort die Kontrollkästchen **Identität und Passwort permanent speichern** sowie **Netzwerkschlüssel permanent speichern** nicht mehr zur Verfügung.

## WPA Enterprise / WPA2 Enterprise mit TLS Client-Zertifikaten verwenden

Dieses Dokument beschreibt, wie Sie mit UMS WLAN-Verbindungen auf IGEL OS mit WPA Enterprise / WPA2 Enterprise und TLS-Client-Zertifikaten konfigurieren.

Es gibt zwei Möglichkeiten, Client-Zertifikate und Schlüssel an Endgeräte zu übergeben:

### Über SCEP (NDES)

SCEP ermöglicht die automatische Bereitstellung von Client-Zertifikaten über einen SCEP-Server und eine Zertifizierungsstelle (CA).

Erfahren Sie, wie Sie es konfigurieren, in dem How-To [Certificate Enrollment and Renewal with SCEP \(NDES\)](#) (see page 505).


### Über Dateien, die von UMS aus bedient werden

Sie brauchen:

- ein Client-Zertifikat im PEM (base64)-Format
- einen privaten Client-Schlüssel (muss passwortgeschützt sein) im PEM-Format (base64)

Alternativ,

- eine PKCS#12-Datei, die sowohl Client-Zertifikat als auch privaten Schlüssel enthält (muss passwortgeschützt sein).

 In beiden Fällen, SCEP und Dateien von UMS, muss das Gerät zuerst eine funktionierende Ethernet- oder WLAN-Verbindung zum SCEP-Server oder UMS haben, damit es die notwendigen Zertifikate holen kann, bevor es sich mit dem Ziel-WLAN verbinden kann.

- 
- [Client-Zertifikate und -Schlüssel bereitstellen](#) (see page 414)
  - [Die Netzwerkschnittstelle konfigurieren](#) (see page 415)

## Client-Zertifikate und -Schlüssel bereitstellen

Um Client-Zertifikate und -Schlüssel über UMS bereitzustellen, führen Sie diese Schritte aus, für das Client-Zertifikat und die privaten Client-Key-Dateien (oder die PKCS#12-Dateien, die beides enthalten):

Klicken Sie im Navigationsbaum der UMS Console mit der rechten Maustaste auf Dateien und wählen Sie Neue Datei aus dem Kontextmenü.

1. Klicken Sie im Navigationsbaum der UMS Console mit der rechten Maustaste auf **Dateien** und wählen Sie **Neue Datei** aus dem Kontextmenü.  
Der Dialog **Neue Datei** wird geöffnet.
2. Wählen Sie unter **Lokale Datei** Ihre Datei aus.
3. Lassen Sie unter **Dateiziel** die **Klassifizierung** als **nicht definiert**.
4. Geben Sie unter **Speicherpfad des Geräts** `/wfs/wpa-tls/` ein.
5. Setzen Sie unter **Zugriffsrechte** die Option **Lesen** und **Schreiben** für den Besitzer und keine für andere.
6. Setzen Sie den **Besitzer** auf **Root**.
7. Klicken Sie auf **OK**, um die Datei hochzuladen.
8. Ziehen Sie das Dateisymbol auf einen Thin Client oder ein Thin Client-Verzeichnis, um die Datei zuzuordnen.

## Die Netzwerkschnittstelle konfigurieren

Hier wird beschrieben, wie Sie die WLAN-Schnittstelle konfigurieren.

**i** In beiden Fällen, SCEP und Dateien von UMS, muss das Gerät zuerst eine funktionierende Ethernet- oder WLAN-Verbindung zum SCEP-Server oder UMS haben, damit es die notwendigen Zertifikate holen kann, bevor es sich mit dem Ziel-WLAN verbinden kann.

### Über SCEP (NDES)

1. Gehen Sie im Setup zu **Netzwerk > LAN-Schnittstellen > WLAN**.
2. Aktivieren Sie **WLAN-Schnittstelle aktivieren**.
3. Gehen Sie zu **Standard-WLAN**.
4. Wählen Sie **WPA-Verschlüsselung aktivieren**.
5. Geben Sie den **Namen** des drahtlosen Netzwerks (SSID) ein.
6. Wählen Sie **WPA Enterprise** oder **WPA2 Enterprise** als **Netzwerkauthentifizierung**.
7. Setzen Sie den **EAP-Typ** auf **TSL** oder **PEAP** und die **Auth Methode** auf **TLS**.

**i** IGEL OS unterstützt sowohl EAP-TLS als auch PEAP-EAP-TLS. Wählen Sie eine, die von Ihrer Infrastruktur unterstützt wird.

8. Lassen Sie **Serverzertifikat prüfen** aktiviert.
9. Geben Sie den Pfad zu einem **CA-Stammzertifikat** ein, wenn Sie eine andere als die von IGEL OS unterstützte CA verwenden.
10. Überprüfen Sie die Verwaltung von Zertifikaten mit SCEP (NDES).
11. Klicken Sie auf **Speichern**.

### Über Zertifikate und Schlüsseldateien

1. Gehen Sie im Setup zu **Netzwerk > LAN-Schnittstellen > WLAN**.
2. Aktivieren Sie **WLAN-Schnittstelle aktivieren**.
3. Gehen Sie zu **Standard-WLAN**.
4. Wählen Sie **WPA-Verschlüsselung aktivieren**.
5. Geben Sie den **Namen** des drahtlosen Netzwerks (SSID) ein.
6. Wählen Sie **WPA Enterprise** oder **WPA2 Enterprise** als **Netzwerkauthentifizierung**.
7. Setzen Sie den **EAP-Typ** auf **TSL** oder **PEAP** und die **Auth Methode** auf **TLS**.

**i** IGEL OS unterstützt sowohl EAP-TLS als auch PEAP-EAP-TLS. Wählen Sie eine, die von Ihrer Infrastruktur unterstützt wird.

8. Lassen Sie **Serverzertifikat prüfen** aktiviert. Geben Sie den Pfad zu einem **CA-Stammzertifikat** ein, wenn Sie eine andere als die von IGEL OS unterstützte CA verwenden.
9. Geben Sie den **CA-Stammzertifikat** im PEM-Format (base64) ein, z.B. `/wfs/wpa-tls/client.crt`.

Lassen Sie dieses Feld leer, wenn Sie eine PKCS#12-Datei verwenden, die sowohl Zertifikat als auch privaten Schlüssel enthält.

10. Geben Sie den Pfad zur **Private Key**-Datei im PEM-Format (base64) ein.  
Wenn Sie eine PKCS#12-Datei verwenden, die sowohl Zertifikat als auch privaten Schlüssel enthält, geben Sie hier den Pfad an.
11. Geben Sie die zu verwendende **Kennung** an, wenn Ihr Schlüssel/Zertifikat mehr als einen Eintrag enthält.
12. Geben Sie das **Passwort** für den privaten Schlüssel ein.
13. Klicken Sie auf **Speichern**.



## IPv6-Einstellungen

Seit IGEL OS 10.01.100 ist es möglich, Netzwerkschnittstellen für IPv6 zu konfigurieren.

### Anwendungsszenario

Da IGEL-Geräte bisher nicht mit der UMS via IPv6 kommunizieren können, ist folgendes Anwendungsszenario häufig:

- Die Geräte beziehen ihre IPv4-Konfiguration und möglicherweise IGEL-spezifische DHCP-Optionen von einem DHCPv4-Server.
- Die meisten Einstellungen werden von der UMS via IPv4 bezogen.
- Nur die Standardeinstellungen werden vom DHCPv6-Server bezogen. Diese sind:
  - IPv6-Adresse
  - Nameserver
  - DNS-Suchliste
- Was DNS betrifft, sollten nur IPv6-Nameserveradressen bereitgestellt werden (durch Router-Ankündigungen, router advertisements, oder DHCPv6-Optionen). Der Resolver sollte in der Lage sein, diese für den Bezug von AAAA-Records, gegebenenfalls auch A-Records, zu verwenden.
- Clients und Server verwenden IPv6, wenn diese IPv6 unterstützen.  
Beispiele:
  - Ein NTP-Server (konfigurierbar in IGEL Setup unter **System > Zeit und Datum**) kann als IPv6-Adresse oder Name hinterlegt sein, wobei der DNS-Server nur über einen AAAA-Record verfügt.
  - Das Gleiche gilt für Browsersitzungen: Wenn der DNS-Server AAAA-Records zur Verfügung stellt, wird IPv6 verwendet.

- 
- [Verfügbare Optionen](#) (see page 418)
  - [Zeitlimit bei automatischer Konfiguration](#) (see page 419)

## Verfügbare Optionen

IPv6-Einstellungen sind in IGEL Setup für die jeweilige Netzwerkschnittstelle unter **Netzwerk > LAN-Schnittstellen** konfigurierbar.

Folgende Werte sind für **IPv6-Konfiguration** möglich:


Wert	Wirkung
<b>Kompatibilitätsmodus</b>	Die gleiche Wirkung wie in früheren Versionen von IGEL Linux: NetworkManager ignoriert das Gerät, doch der Kernel nimmt eine Grundkonfiguration vor. Insbesondere weist der Kernel dem Gerät eine lokale IPv6-Adresse zu.
<b>Deaktiviert</b>	IPv6 ist vollständig deaktiviert.
<b>Automatisch</b>	Das Gerät versucht, je nach Router-Ankündigung (router advertisements), eine Stateless oder Stateful Autoconfiguration durchzuführen.  Je nach Router-Ankündigungen (router advertisements), kann dies DHCPv6 beinhalten (siehe RFC 4861).
<b>DHCPv6</b>	Diese Option wird von NetworkManager unterstützt. Sie kann verwendet werden, wenn ein DHCPv6-Server zur Verfügung steht, aber kein Router-Ankündigungen (router advertisements). Das Routing muss dann auf andere Weise konfiguriert werden. In den meisten Fällen wird <b>Automatisch</b> die bevorzugte Option sein.

## Zeitlimit bei automatischer Konfiguration

Wenn **Automatisch** eingestellt ist, dann steht ein konfigurierbares Zeitlimit für den Dual-Stack-Modus zur Verfügung. Dieses Zeitlimit betrifft die Zeitspanne, die das System wartet, bis nach Abschluss der Konfiguration von IPv4 oder IPv6 die Konfiguration des jeweils anderen Stacks abgeschlossen ist. Wenn die Zeit verstrichen ist, führt das System die Skripte aus, die Netzwerkfunktionalitäten benötigen. Standardmäßig beträgt das Zeitlimit 15 Sekunden.

Das Zeitlimit kann in IGEL Setup über folgende Parameter unter **System > Registry** konfiguriert werden:

Parameter	Device
<code>network.interfaces.ethernet.device0.dual_stack_timeout</code>	Erstes Ethernet-Device
<code>network.interfaces.ethernet.device1.dual_stack_timeout</code>	Zweites Ethernet-Device
<code>network.interfaces.wirelesslan.device0.dual_stack_timeout</code>	WLAN-Device

 Suchen Sie mit der Funktion **Parameter suche...** nach dem String `dual_stack`, um die oben aufgeführten Parameter schnell zu finden.

## Erweitertes Logging mit Syslog, Tcpdump und Netlog

Die Registry von IGEL Linux bietet eine Reihe von erweiterten Logging-Optionen, die Kunden sowie Mitarbeitern von Support und PreSales helfen können, Probleme im System und Netzwerk aufzuspüren.

Anweisungen zum Senden von Protokolldateien an das IGEL-Support-Team über das UMS finden Sie unter [Geräteprotokolldateien an den IGEL Support senden](#) (see page 825).

- [Die Partition debuglog](#) (see page 421)
- [Syslog](#) (see page 423)
- [Tcpdump](#) (see page 424)
- [Netlog](#) (see page 427)


## Die Partition debuglog

Logdateien können schnell sehr groß werden. Darum werden Logdateien auf einer separaten Partition gespeichert. Der Einhängpunkt dieser Partition ist `/debuglog`.

### Die Partition debuglog aktivieren und konfigurieren

So aktivieren und konfigurieren sie die Partition in der Registry:

<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Enable debuglog partition</b>	debug.tools.log_partition.enabled	enabled / <u>disabled</u>
Aktiviert die Partition debuglog.		
<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Size of debuglog partition in MiB</b>	debug.tools.log_partition_size	50 ... 500 / <u>100</u>

 Beim Verkleinern der Partition /debuglog wird ihr Inhalt gelöscht!

### Inhalt der Partition debuglog

Je nachdem, welche Loggingoptionen Sie aktiviert haben (siehe die nachfolgenden Seiten), befinden sich auf der Partition /debuglog folgende Dateien:

- Syslog
  - `messages` (das aktuelle syslog)
  - `messages[1-9].gz` (komprimiertes und rotiertes syslog)
- Ethtool
  - `netlog-ethtool-[device].log`
- Ping
  - `netlog-host-[0-9]-ping.log` (Log von ping)
  - `netlog-host-[0-9]-ping[n].log.gz` (komprimiertes und rotiertes Log von ping)
- Ifconfig
  - `netlog-ifconfig-[device].log`
- Netstat
  - `netlog-netstat.log` (Log von netstat)
  - `netlog-netstat[n].log.gz` (komprimiertes und rotiertes Log von netstat)

- Socket Status
  - `netlog-socket_status.log` (Log zum Socketstatus)
  - `netlog-socket_status[n].log.gz` (komprimiertes und rotiertes Log zum Socketstatus)
- Tcpdump
  - `tcpdump[0-3]_capture_current[n]` (Aufzeichnungen von tcpdump)
  - `tcpdump[0-3]_capture-[n].pcap.{lzo,gz,bzip2,xz}` (komprimierte und rotierte Aufzeichnungen von tcpdump)
- Tcpdump triggered by an error
  - `ERROR_[timestamp]/tcpdump[0-3]_capture-[n].pcap.{lzo,gz,bzip2,xz}` (komprimierte und erhaltene Aufzeichnungen von tcpdump)

<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Enable debuglog partition</b>	<code>debug.tools.log_partition.enabled</code>	enabled / <u>disabled</u>
Aktiviert die Partition /debuglog.		

## Syslog

Es ist möglich, sämtliche syslog-Nachrichten, die nach `/var/log/message` (IGEL Linux 5.10.250 sowie 5.11.x) oder in das `systemd journal` (IGEL Linux 10.01.100) geschrieben werden, zusätzlich an die Partition `/debuglog` zu leiten.

Die Logdateien werden dabei je nach Bedarf rotiert und komprimiert. Dadurch wird der Log erhalten, falls der Thin Client abstürzt, dies gilt ebenfalls für Logs von verschiedenen vorherigen Boots.

In der **Registry** können Sie folgende Einstellungen treffen:

<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Enable syslog log to debuglog partition</b>	debug.tools.syslog0.enabled	true/ <u>false</u>
<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Number of Rotate Files</b>	debug.tools.syslog0.num_rotate_files	<u>2</u> ... 9
Anzahl der Dateien, die beim Rotieren behalten werden.		
<b>IGEL Setup &gt; System &gt; Registry</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.syslog0.rotate_size	<u>2</u> , 4, 8, 16
Rotiere, wenn die Größe der komprimierten Dateien dieser Größe in MiB entspricht.		

## Tcpdump

Tcpdump hilft Ihnen, Netzwerkprobleme zu debuggen, indem es die Netzwerkpakete von bis zu vier unterschiedlichen Netzwerkschnittstellen protokolliert.

**i** Mithilfe von [Netlog](#) (see page 427) können Capture-Dateien in ein Unterverzeichnis kopiert werden. Dieses Verhalten wird von einem Fehler in einem anderen Log ausgelöst, so dass die Captures von vor und nach dem Fehler erhalten bleiben und zur Analyse zur Verfügung stehen.

**i** Mithilfe des Programms Wireshark können Sie die Capture-Dateien auf einem externen System analysieren.

Mehr über tcpdump erfahren Sie auf der offiziellen Webseite [tcpdump.org](http://tcpdump.org)<sup>39</sup>

<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Resolve addresses/ports to names</b>	<code>debug.tools.tcpdump[0-3].address_resolution</code>	enabled / <u>disabled</u>
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Compression Method</b>	<code>debug.tools.tcpdump[0-3].compression</code>	<u>lzop</u> , gzip, bzip2, xz
Die Komprimierungsmethode beeinflusst sowohl die Dateigröße als auch die Systemleistung beim Komprimieren. Der Standard-Lzop-Methode ist relativ leicht auf der CPU.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Interface for tcpdump logging</b>	<code>debug.tools.tcpdump[0-3].interface</code>	user editable string / <u>eth0</u>
Hinweis: Die Namen <code>eth0</code> , <code>eth1</code> , <code>wlan0</code> , usw. werden als symbolische Namen behandelt und werden intern automatisch durch die richtigen PNINs ersetzt. Details zu PNINs finden Sie unter LAN-Schnittstellen.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Number of Rotate Files</b>	<code>debug.tools.tcpdump[0-3].m_rotate_files</code>	<u>3</u> ... 10

<sup>39</sup> <http://www.tcpdump.org>



Anzahl der Dateien, die beim Drehen beibehalten werden sollen.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Only Log Package Headers</b>	debug.tools.tcpdump[0-3].only_headers	enabled / <u>disabled</u>
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Enable promisc tcpdump logging</b>	debug.tools.tcpdump[0-3].promisc	enabled / <u>disabled</u>
Aktivieren Sie den Promiskuitivmodus auf der Netzwerkschnittstelle, um auch Pakete zu erfassen, die nicht für diesen Host bestimmt sind.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.tcpdump[0-3].rotate_size	<u>10</u> , 15, 20, 25, 30, 40
Drehen, wenn die Größe der unkomprimierten Datei diese Größe in MiB erreicht.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Logfile rotate time in s</b>	debug.tools.tcpdump[0-3].rotate_time	<u>0</u> / user editable integer
Zeit in Sekunden, nach der die Logdatei gedreht und komprimiert wird. Bei Einstellung auf 0 erfolgt keine zeitabhängige Drehung.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Additional Parameters for tcpdump</b>	debug.tools.tcpdump[0-3].tcpdump_additional_parameters	user editable string
Mit Vorsicht verwenden.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Enable tcpdump</b>	debug.tools.tcpdump[0-3].tcpdump_enabled	enabled / <u>disabled</u>
<b>IGEL Setup &gt; Registry</b>		

<b>&gt; tcpdump filter expression</b>	debug.tools.tcpdump[0-3] ].tcpdump_filter	user editable string
Tcpdump-Filterausdruck. Für die Ausdruckssyntax siehe die Manpage pcap-filter(7).		

## Netlog

Netlog enthält die folgenden Diagnosetools:

- `ethtool`
- `ifconfig`
- `netstat`
- `ping`
- `ss` (socket status)

Es kann auch `tcpdump` ausführen.

IGEL Setup > Registry		
> <b>Enable netlog logging</b>	debug.tools.netlog.enabled	enabled / <u>disabled</u>
IGEL Setup > Registry		
> <b>period between netlog logs in s</b>	debug.tools.netlog.period	<u>1</u> , 5, 10, 20, 30, 60, 120
Ping-Logging ist davon nicht betroffen und verwendet ein eigenes Timing.		

- [Ethtool](#) (see page 428)
- [Ifconfig](#) (see page 429)
- [Netstat](#) (see page 430)
- [Ping](#) (see page 431)
- [Socket Status \(ss\)](#) (see page 433)

## Ethtool

Ethtool ist unter Linux das Standardwerkzeug, um Diagnoseinformationen über per Kabel angebundene Ethernet-Geräte und deren Gerätetreiber zu erhalten.

<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Disable ethtool logging</b>	debug.tools.netlog.ethtool.disabled	true / <u>false</u>
By default Ethtool logging is included in Netlog logging. However, you can disable it here.		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Log only if ethtool output changes</b>	debug.tools.netlog.ethtool.log_on_changes_only	<u>true</u> / false
Log only if ethtool output changes (on bootup there will always be at least one log entry)		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Number of Rotate Files</b>	debug.tools.netlog.ethtool.num_rotate_files	<u>2</u> ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines)		
<b>IGEL Setup &gt; Registry</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.ethtool.rotate_size	<u>2</u> , 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		

## Ifconfig

### Ifconfig

Neben der Konfiguration von Netzwerkgeräten gibt ifconfig auch Diagnoseinformationen wie RX-Bytes, TX-Bytes und dropped packets an.

<b>IGEL Setup &gt;</b>		
<b>&gt; Disable ifconfig logging</b>	debug.tools.netlog.ifconfig.disabled	true / <a href="#">false</a>
By default Ifconfig logging is included in Netlog logging. However, you can disable it here.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Log only if ifconfig output changes</b>	debug.tools.netlog.ifconfig.log_on_changes_only	<a href="#">no</a> , <a href="#">error_counter</a> , <a href="#">all</a>
<ul style="list-style-type: none"> <li>• <b>no</b>: log on every netlog run</li> <li>• <b>error_counter</b>: log only if an error counter or the address changes</li> <li>• <b>all</b>: log on every change of ifconfig output</li> </ul>		
<b>IGEL Setup &gt;</b>		
<b>&gt; Number of Rotate files</b>	debug.tools.netlog.ifconfig.num_rotate_files	<a href="#">2</a> ... 4
Keep up to this number of rotated files (also compressed), the current log not included (which is limited to 600 lines).		
<b>IGEL Setup &gt;</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.ifconfig.rotate_size	<a href="#">2</a> , 4, 6
Rotate when the size of the uncompressed file reaches this size in MiB.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Trigger tcpdump log</b>	debug.tools.netlog.ifconfig.trigger_tcpdump_save	true / <a href="#">false</a>
Trigger the saving of tcpdump logs if an error counter increases or if the IP address changes.		

## Netstat

Netstat zeigt eine Vielzahl von Netzwerkstatistiken für den lokalen Rechner an.

<b>&gt; Disable netstat logging</b>	debug.tools.netlog.netstat.disabled	true / <u>false</u>
Standardmäßig ist die Protokollierung von <code>netstat -s</code> in der Netlog-Protokollierung enthalten. Sie können es jedoch hier deaktivieren.		
<b>&gt; Number of Rotate files</b>	debug.tools.netlog.netstat.num_rotate_files	2 ... 4
Halten Sie sich an diese Anzahl von rotierten Dateien (auch komprimiert), das aktuelle Protokoll ist nicht enthalten (begrenzt auf 600 Zeilen).		
<b>&gt;Logfile rotate size in MiB</b>	debug.tools.netlog.netstat.rotate_size	2, 4, 6
Rotieren Sie, wenn die Größe der unkomprimierten Datei diese Größe in MiB erreicht.		
<b>&gt;Log only if triggered</b>	debug.tools.netlog.netstat.trigger_log	<u>net_error_changes</u> , net_changes, ifconfig_changes, ethtool_changes, no_trigger
<ul style="list-style-type: none"> <li>• <b>net_error_changes</b>: log if ethtool output changes or ifconfig error counter or address changes</li> <li>• <b>net_changes</b>: log if ethtool or ifconfig output changes</li> <li>• <b>ifconfig_changes</b>: log if ifconfig output changes</li> <li>• <b>ethtool_changes</b>: log if ethtool output changes</li> <li>• <b>no_trigger</b>: log on every netlog run</li> </ul>		

## Ping

<b>IGEL Setup &gt;</b>		
<b>&gt; Enable ping check</b>	debug.tools.netlog.ping_host[0-9].enabled	true / <u>false</u>
<b>IGEL Setup &gt;</b>		
<b>&gt; Log only if ping fails</b>	debug.tools.netlog.ping_host[0-9].log_only_on_error	true / <u>false</u>
Protokollieren Sie nur, wenn einer der konfigurierten Pings[0-9] schlägt fehl.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Number of Rotate Files</b>	debug.tools.netlog.ping_host[0-9].num_rotate_files	<u>2</u> ... 4
Wenn Sie sich an diese Anzahl von rotierten Dateien (auch komprimiert) halten, ist das aktuelle Protokoll nicht enthalten (begrenzt auf 600 Zeilen).		
<b>IGEL Setup &gt;</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.ping_host0.rotate_size	<u>2</u> ... 4
Drehen, wenn die Größe der unkomprimierten Datei diese Größe in MiB erreicht.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Trigger tcpdump save</b>	debug.tools.netlog.ping_host0.trigger_tcpdump_save	<u>2</u> ... 4
Das Speichern von tcpdump-Protokollen wird ausgelöst, wenn ein Fehlerzähler ansteigt oder sich die IP-Adresse ändert.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Ping target</b>	debug.tools.netlog.ping_host0.ping_target	user-editable string
Ziel-IP/Hostname zu Ping (wenn kein Ping angegeben wird, gilt Ping als deaktiviert!)		
<b>IGEL Setup &gt;</b>		
<b>&gt; Time between pings</b>	debug.tools.netlog.ping_host0.ping_time	<u>1</u> , 5, 10, 30, 60, 120
Zeit zwischen den Pings in Sekunden.		

<b>IGEL Setup &gt;</b>		
<b>&gt; Type of ping</b>	debug.tools.netlog.ping_host0.type	icmp, http request, https request
<ul style="list-style-type: none"><li>• <b>icmp:</b> use normal ping command</li><li>• <b>http request:</b> send an http request (fails if no HTTP/*.* * OK answer is received)</li><li>• <b>https request:</b> send an https request (fails if no CONNECTED is returned by openssl)</li></ul>		



Socket Status (ss)

<b>IGEL Setup &gt;</b>		
<b>&gt; Disable socket status Logging</b>	debug.tools.netlog.socket_status.disabled	true / <u>false</u>
Standardmäßig ist die socket_status-Protokollierung in der Netlog-Protokollierung enthalten. Sie können es jedoch hier deaktivieren.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Number of Rotate Files</b>	debug.tools.netlog.socket_status.num_rotate_files	true / <u>false</u>
Halten Sie sich an diese Anzahl von rotierten Dateien (auch komprimiert), ohne das aktuelle Protokoll (begrenzt auf 600 Zeilen).		
<b>IGEL Setup &gt;</b>		
<b>&gt; Logfile rotate size in MiB</b>	debug.tools.netlog.socket_status.rotate_size	true / <u>false</u>
Rotieren, wenn die Größe der unkomprimierten Datei diese Größe in MiB erreicht.		
<b>IGEL Setup &gt;</b>		
<b>&gt; Log only if triggered</b>	debug.tools.netlog.socket_status.trigger_log	<u>ping_errors</u> , no_trigger
<ul style="list-style-type: none"> <li>• <b>ping_errors</b>: log only if ping test fails</li> <li>• <b>no_trigger</b>: log on every netlog run</li> </ul>		

## Eine Telnet-Verbindung von IGEL Linux aus herstellen

### Problem

Sie möchten sich mit einem Telnet-Dienst verbinden, können aber keinen Telnet-Befehl auf dem Gerät finden.

### Lösung

Verwendung von Ericom Powerterm (Erfordert das Ericom Powerteam Firmware Feature):

1. Gehen Sie in Setup unter **Sitzungen > PowerTerm Terminal Emulation > PowerTerm Sitzung**.
2. Erstellen Sie eine neue Sitzung.
3. Bearbeiten Sie die Sitzung.
4. Machen Sie unter **Verbindung**, folgende Einstellungen:
  - a. Wählen Sie **Telnet** als **Sitzungstyp** aus.
  - b. Geben Sie eine IP-Adresse oder einen Namen in **Host Name** ein.
  - c. Wenn Sie einen grafischen Anmeldedialog verwenden möchten, aktivieren Sie **Anmeldedialog aktivieren**.



The screenshot shows the configuration interface for a Telnet session. At the top, the 'Session Type' is set to 'TELNET'. Below this, the 'Parameters' section includes the following fields and options:

- Host Name:** 172.30.91.158
- Port Number:** 23
- Terminal Name:** (empty field)
- Keep Alive Timeout:** 0
- Enable Login Dialog**
- Save last user name**
- Script File:** (empty field)
- Set Window Size**
- Force Binary Mode**

5. Unter **Desktop Integration** einen **Sitzungsnamen** eingeben und die gewünschten **Startmethoden für die Sitzung** aktivieren.
6. Klicken Sie **Anwenden** um Ihre Sitzung zu speichern oder **OK** zum speichern und schließen.
7. Starten Sie die neue Sitzung und geben Sie Ihren Benutzernamen und Passwort ein.

## Dynamische DNS-Aktualisierung via DDNS konfigurieren


### Problem:

Sie möchten die IP-Adresse eines Geräts bei Ihrem DNS Server registrieren.

Sie verwenden kein DHCP.

### Lösung:

Nutzen Sie die in IGEL Linux enthaltene DDNS-Tools, welche im Setup konfiguriert werden können.

 Dies funktioniert nur für BIND9 oder andere Nameserver, die TSIG unterstützen, nicht für Microsoft Active Directory-Server.

Verteilen Sie den gemeinsamen TSIG-Schlüssel Ihres Nameservers mit dem UMS:

1. Erstellen Sie eine **neue Datei**.
2. Setzen Sie den **Geräte Speicherort** auf `/wfs/ddns`.
3. Aktivieren Sie die **Leseberechtigung** für den **Eigentümer** und deaktivieren Sie alle anderen Berechtigungen.
4. Setzen Sie den **Eigentümer** auf **Root**.

### Einrichten der dynamischen DNS-Registrierung:

1. Gehen Sie auf **Netzwerk > LAN Schnittstelle** in Setup.
2. Aktivieren Sie **IP-Adresse manuell festlegen**.
3. Geben Sie eine **IP Adresse** und eine **Netzwerkmaske** ein.
4. Geben Sie einen **Terminalnamen** ein.
5. Aktivieren Sie **DNS aktivieren**.
6. Geben Sie eine **Standarddomäne** ein.
7. Als letztes geben Sie eine **Nameserver IP-Adresse** ein.
8. Aktivieren Sie **Dynamische DNS-Registrierung**
9. Wählen Sie **DNS** als **Methode für dynamische DNS-Registrierung**.
10. Wenn der Nameserver einen TSIG-Schlüssel verlangt: Wählen Sie eine **TSIG-Schlüsseldatei** aus. Andernfalls, lassen Sie das Eingabefeld leer.

11. Klicken Sie auf **Übernehmen** oder **Ok**.

Standardschnittstelle aktivieren (Ethernet)

---

IP vom DHCP-Server beziehen  
 IP-Adresse manuell festlegen

IP-Adresse

Netzwerkmaske

---

Standardgateway  Aktivieren

Terminalname

---

DNS aktivieren

Standarddomäne

Nameserver

Nameserver

---

Manuelles Überschreiben der DHCP-Einstellungen


Dynamische DNS-Registrierung

Methode für dynamische DNS-Registrierung

Privater TSIG Schlüssel für DNS Authentifizierung

## Ändern der SMB-Protokollversion

Je nachdem welchen Windows (Samba)-Server Sie verwenden, benötigen Sie eine bestimmte SMB-Protokollversion.

 Aus Sicherheitsgründen empfiehlt Microsoft, die Unterstützung für SMB Version 1.0 unter Windows zu deaktivieren, so dass Sie auf mindestens Version 2.0 wechseln müssen, um weiterhin auf Systeme mit deaktiviertem SMBV1 zugreifen zu können.

IGEL Linux ab Version 10.04.100 und höher bietet mehrere SMB-Protokollversionen an.


Um die Einstellung der Version zu ändern:

1. Gehen Sie im IGEL Setup unter **System > Registry**.
2. Gehen Sie zum Parameter `network.smbmount.smb_version`.
3. Wählen Sie die passende **SMB Protokoll Version**.  
Mögliche Optionen:
  - 1.0
  - 2.0
  - 2.1
  - 3.0
4. Klicken Sie **Übernehmen** oder **Ok** um Ihre Einstellungen zu speichern.  
Die Windows-Freigaben sind konfigurierbar unter **IGEL Setup > Netzwerk > Netzlaufwerke > Windows Laufwerk**.

## Wie starte ich den WiFi-Manager in IGEL OS, wenn die Taskleiste ausgeblendet ist?

### Problem

Die Taskleiste oder Systemleiste wurde aus irgendeinem Grund deaktiviert (**Benutzeroberfläche > Desktop > Taskleiste / Taskleistenelemente**; auch **Benutzeroberfläche > Bildschirmsperre/-schoner > Taskleiste**). Dadurch ist das Systray-Symbol für den WiFi-Manager nicht mehr zugänglich und der Benutzer kann keine WLAN-Netzwerke verwalten.


 Beachten Sie, dass auch der WLAN-Schalter unzugänglich ist, wenn Sie die Taskleiste oder die Systemleiste deaktivieren, siehe Schalter für die WLAN-Verbindung. Siehe auch "WLAN automatisch einschalten" unter WLAN.

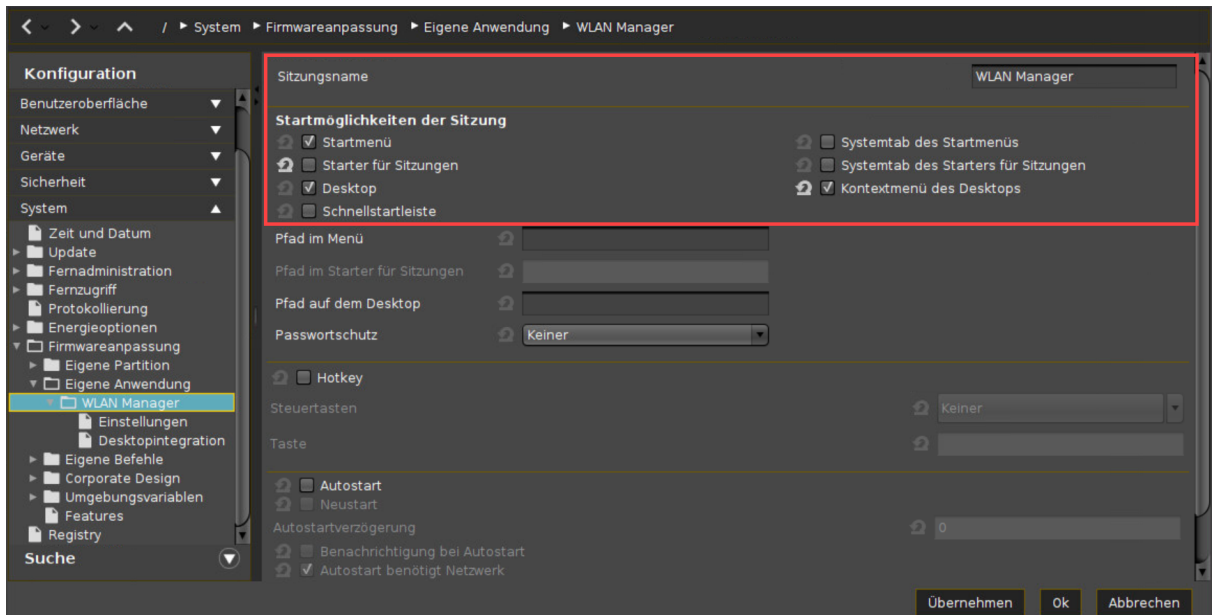
### Umgebung

- IGEL OS 10.06 oder höher

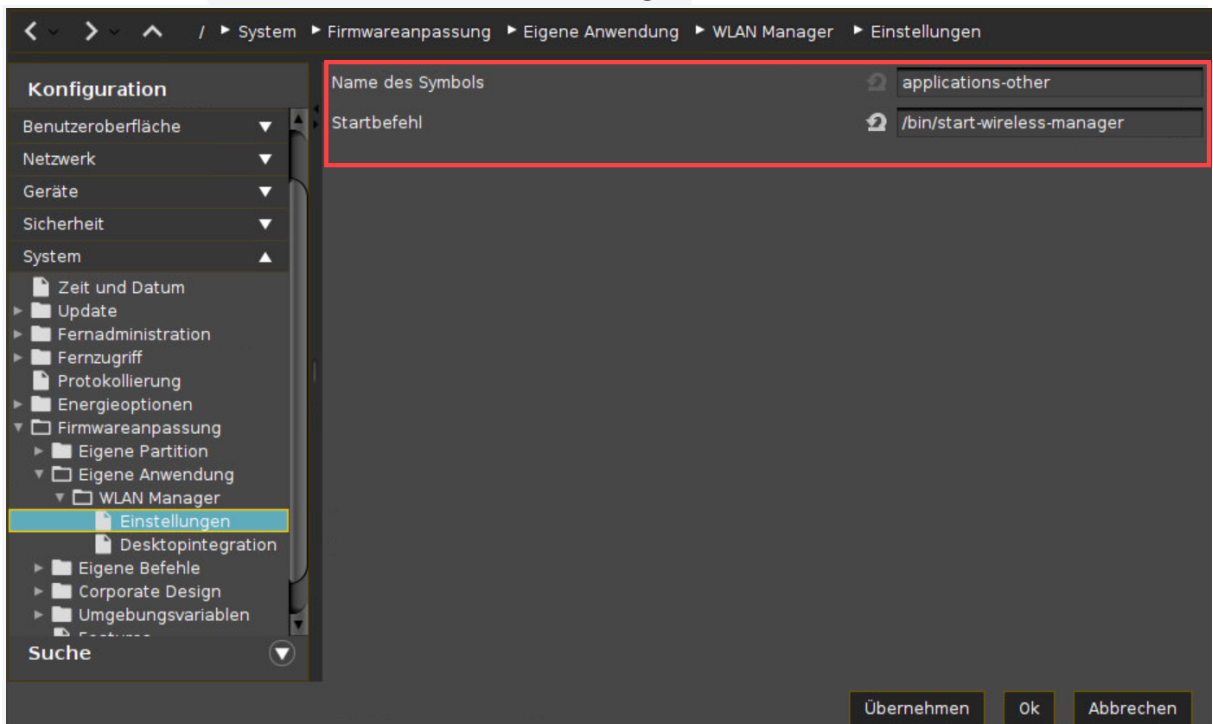
### Lösung

Sie können den WiFi-Manager als benutzerdefinierte Anwendung konfigurieren und festlegen, wie er gestartet werden kann.

1. Gehen Sie zu **Netzwerk > LAN-Schnittstellen > WLAN** und überprüfen Sie, ob die WLAN-Schnittstelle und der WiFi-Manager aktiviert sind.
2. Gehen Sie zu **System > Firmwareanpassung > Eigene Anwendung** und klicken Sie .
3. Geben Sie den **Sitzungsnamen** an und konfigurieren Sie die **Startmöglichkeiten** nach Ihren Bedürfnissen.



4. Geben Sie unter **Einstellungen** den **Namen des Symbols** an und geben Sie den folgenden **Startbefehl** ein: `/bin/start-wireless-manager`



5. Klicken Sie **Übernehmen** oder **OK**.  
 Der WiFi-Manager kann nun mittels der konfigurierten Startmöglichkeiten gestartet werden.

## Sicherheit

- [IGEL OS-Endpoints härten](#) (see page 441)
- [SSH-Zugriff auf Geräten mit Schlüsseln](#) (see page 484)
- [Sicheres Terminal \(Telnet mit TLS/SSL\)](#) (see page 489)
- [Sicheres Spiegeln \(VNC mit TLS/SSL\)](#) (see page 490)
- [Cherry eGK Kanalersetzung](#) (see page 494)
- [Single Sign-on für den Browser Proxy](#) (see page 496)
- [Anzahl der zulässigen Anmeldeversuche begrenzen](#) (see page 499)
- [How to Deploy Device Encryption](#) (see page 500)
- [Sicherheit: Timeout für Sicheres Spiegeln and Sicheres Terminal](#) (see page 501)
- [Entschärfung der Terrapin-Schwachstelle durch Registry-Parameter in IGEL OS](#) (see page 503)



## IGEL OS-Endpoints härten

Dieses Dokument beschreibt Einstellungen, die die Sicherheit von IGEL OS verbessern.

Die Angaben im Dokument gelten für:

- IGEL UD-Geräte
- Mit dem UD Pocket konvertierte Geräte
- Mit dem IGEL OS Creator (OSC) konvertierte Drittherstellergeräte

- 
- [Einführung](#) (see page 442)
  - [Passwörter vergeben](#) (see page 443)
  - [Das System aktuell halten](#) (see page 450)
  - [Zugriff auf bestimmte Komponenten unterbinden](#) (see page 455)
  - [Die Angriffsfläche verringern](#) (see page 460)
  - [UMS und Fernzugriff konfigurieren](#) (see page 472)
  - [WLAN und Bluetooth](#) (see page 480)
  - [IGEL UD Pocket für private Geräte verwenden](#) (see page 483)

## Einführung

Dieses Dokument beschreibt verschiedene Einstellungen, um IGEL OS sicherer zu machen. Umso mehr Sie von diesen Einstellungen vornehmen, desto höher wird die Gerätesicherheit. Jedoch ist es Ihnen überlassen, eine ausgewogene Mitte zwischen Sicherheit und Einschränkung der Benutzer zu finden. Manche Einstellungen können Ihrem Anwendungsfall sogar entgegenstehen. Falls Sie etwa Endgeräte mit Bluetooth verwenden, würde es keinen Sinn ergeben, Bluetooth zu deaktivieren.

Um mehr als ein Gerät auf einmal zu konfigurieren, können Sie die hier beschriebenen Einstellungen in der Universal Management Suite (UMS) in einem Masterprofil hinterlegen und dieses einer beliebigen Anzahl von Geräten zuweisen, wodurch die Sicherheitseinstellungen angewandt werden. Mehr über Masterprofile erfahren Sie unter Masterprofile.

## Passwörter vergeben

Sie können den Zugriff auf verschiedene Systemkomponenten einschränken, indem Sie Passwörter vergeben.

- [Lokale Passwörter festlegen](#) (see page 444)
- [Sitzungen und Zubehör mit Passwörtern schützen](#) (see page 445)
- [Bildschirm sperren](#) (see page 446)
- [Sitzungspasswörter nicht speichern](#) (see page 447)
- [Ein UEFI-Passwort festlegen](#) (see page 448)
- [Zwei-Faktor-Authentisierung \(2FA\) verwenden](#) (see page 449)

## Lokale Passwörter festlegen

### Hintergrund

Passwörter schützen das System vor lokalen Änderungen. Sie beschränken den Zugriff auf das lokale Terminal, IGEL Setup sowie auf die Rescue-Shells in virtuellen Konsolen. Das Administratorpasswort wird außerdem benötigt, um das System auf Werkseinstellungen zurückzusetzen.

Diese Passwörter sind verschlüsselt abgespeichert ("hashed and salted"), womit ihre Rekonstruktion verhindert wird.

In den Standardeinstellungen von IGEL OS sind keine Passwörter festgelegt. Legen Sie mindestens ein Administrator-Passwort fest.

### Schritte

So legen Sie ein Administrator-Passwort fest:

1. Gehen Sie in IGEL Setup zu **Sicherheit > Passwort**.
2. Aktivieren Sie im Bereich **Administrator** die Einstellung **Passwort verwenden**.  
Sie werden aufgefordert, ein Passwort einzugeben und die Eingabe zu wiederholen.  
Optional: Wenn Sie einem normalen Benutzer Zugriff auf IGEL Setup gewähren möchten, aktivieren Sie im Bereich **Benutzer** die Einstellung **Passwort verwenden**.
3. Klicken Sie **Übernehmen** oder **Ok**.

Zum Benutzerkonto für Fernzugriff finden Sie weitere Informationen unter [Sichere SSH-Einstellungen](#) (see page 478).

Weitere Informationen finden Sie im IGEL OS Referenzhandbuch unter [Passwort - den Zugriff auf IGEL OS-Komponenten beschränken](#).

## Sitzungen und Zubehör mit Passwörtern schützen

Sitzungen können für den Zugriff auf Unternehmensressourcen verwendet werden, Zubehör kann verwendet werden, um Änderungen am lokalen System vorzunehmen. Wenn Sie bestimmte Sitzungen oder Zubehör-Elemente nicht vollständig deaktivieren möchten, können Sie den Zugriff durch Vergabe eines Passworts einschränken.

Standardmäßig sind Sitzungen und Zubehör-Elemente durch kein Passwort geschützt.

### Schritte

So aktivieren Sie den Passwortschutz für eine Sitzung oder ein Zubehör-Element:

1. Sitzungen: Gehen Sie in IGEL Setup zu **Sitzungen > [Sitzungstyp] > [Sitzungsname] > Desktopintegration**.  
Zubehör: Gehen Sie in IGEL Setup zu **Zubehör > [Zubehörname]**.
2. Legen Sie mit der Option **Passwortschutz** fest, welches Passwort eingegeben werden muss, um die Sitzung/das Zubehör-Element zu starten.  
Mögliche Werte sind:  
**Administrator**: Das Administrator-Passwort muss eingegeben werden.  
**Benutzer**: Das Benutzer-Passwort muss eingegeben werden.  
**Setupbenutzer**: Das Setupbenutzer-Passwort muss eingegeben werden.
3. Klicken Sie **Übernehmen** oder **Ok**.

## Bildschirm sperren

Den Bildschirm nicht zu sperren, ermöglicht Angreifern, mit den Rechten des aktuell eingeloggtten Benutzers auf das System zuzugreifen. Manuelles oder automatisches Sperren des Bildschirms mit einem Passwort verhindert solch einen Zugriff.

### Bildschirm manuell sperren

Standardmäßig können Benutzer den Bildschirm nicht auf manuelle Weise sperren.

Fahren Sie wie folgt fort, um den Benutzer ein manuelles Sperren des Bildschirms zu ermöglichen:

1. Gehen Sie in IGEL Setup zu **Benutzeroberfläche > Bildschirm Sperre/-schoner**.
2. Aktivieren Sie eine oder beide der folgenden Optionen:
  - Schnellstartleiste:** Dem Benutzer wird in der Schnellstartleiste ein Icon angezeigt, das er klicken kann, um den Bildschirm zu sperren.
  - Hotkey:** Legen Sie einen Hotkey fest, z. B. [STRG+SHIFT+L], mit dem der Benutzer den Bildschirm sperren kann.
3. Klicken Sie **Übernehmen**.

### Bildschirmschoner mit Passwortschutz einrichten

Standardmäßig startet der Bildschirmschoner nach 5 Minuten, jedoch wird der Bildschirm dabei nicht durch ein Passwort geschützt.

Fahren Sie wie folgt fort, um einen Passwortschutz für den Bildschirmschoner festzulegen:

1. Gehen Sie in IGEL Setup zu **Benutzeroberfläche > Bildschirm Sperre/-schoner > Optionen**.
2. Aktivieren Sie die Option **Automatisch starten**.
3. Legen Sie das **Zeitlimit in Minuten** fest. Dabei handelt es sich um die Inaktivitätszeit, die vergehen muss, bis der Bildschirmschoner automatisch startet. (Standard: 5)
4. Wählen Sie im Bereich "Passwort für Bildschirm Sperre" zwischen den Optionen **Benutzerpasswort** und **Eigenes Passwort** sowie vergeben Sie ein Passwort, indem Sie die Schaltfläche **Festlegen** klicken.
5. Aktivieren Sie bei Bedarf die Option **Administratorpasswort zulassen**, um ein Entsperren des Benutzerbildschirms durch den Administrator zu erlauben. (Standard: Aktiviert)
6. Klicken Sie **Übernehmen**.

## Sitzungspasswörter nicht speichern

Sitzungspasswörter sollten aus Sicherheitsgründen nie auf dem Thin Client gespeichert werden.

- ▶ Lassen Sie bei der Konfiguration einer Sitzung im Bereich **Anmeldung** das Feld **Passworten** leer. Der Benutzer wird dann auf interaktive Weise zur Passworteingabe aufgefordert.
- ▶ Nutzen Sie nach Möglichkeit [Zwei-Faktor-Authentifizierung \(2FA\)](#) (see page 449).

## Ein UEFI-Passwort festlegen

In den UEFI-Einstellungen können Sie grundlegende Systemeinstellungen vornehmen, z. B. das Booten von USB deaktivieren. Der Zugriff auf solche Systemeinstellungen sollte durch ein Passwort geschützt sein.

### Anleitung für IGEL UD LX-Geräte


- ▶ Falls UEFI deaktiviert ist, siehe die Anweisungen unter UEFI Secure Boot Enabling Guides.

Standardmäßig ist auf IGEL UD-Geräten kein UEFI-Passwort eingestellt. Um ein Passwort festzulegen, gehen Sie wie folgt vor:

1. Halten Sie die Taste [Entf] ([F2] für UD2) während des Bootvorgangs gedrückt.  
Das UEFI-Menü wird geöffnet
2. Gehen Sie mit den Pfeiltasten und der Eingabetaste zur **SCU**.  
Das **Setup Utility** wird geöffnet.
3. Gehen Sie mit den Pfeiltasten und der Eingabetaste zu **Security**.
4. Verwenden Sie die Pfeiltasten, um **Set Supervisor Password** auszuwählen.
5. Drücken Sie [Enter].
6. Geben Sie das gewünschte UEFI-Passwort ein und drücken Sie die Taste [Enter].
7. Geben Sie das gleiche UEFI-Passwort erneut ein und drücken Sie zweimal [Enter].
8. Drücken Sie [F10], um zu speichern und zu verlassen.
9. Bestätigen Sie die Änderungen unter **Exit Saving Changes?** mit [Enter].  
Das System bootet und die UEFI-Einstellungen sind nun passwortgeschützt.

### Anweisungen für Geräte von Drittanbietern, die mit OSC konvertiert wurden

- ▶ Kontaktieren Sie den Hersteller Ihres BIOS/UEFI.

 Alternativ können Sie auch versuchen, [F12] (im Allgemeinen), [F10] (Intel-Geräte) oder [F9] (Hewlett-Packard-Geräte) zu drücken, um auf die BIOS/UEFI-Einstellungen zuzugreifen. Wenn dies nicht funktioniert, versuchen Sie, während des Bootvorgangs [Entf], [F1] oder [F2] zu drücken.



## Zwei-Faktor-Authentisierung (2FA) verwenden

Zwei-Faktor-Authentisierung (2FA) kombiniert zwei Faktoren, um die Identität eines Benutzers nachzuweisen. Häufig wird ein Hardwaregerät, z. B. eine Smartcard oder ein Smart-Token, mit einem Passwort oder einer PIN kombiniert. Dies erhöht den Schutz, da ein Angreifer sowohl Zugriff auf das Hardwaregerät als auch Kenntnis des Passworts oder der PIN erlangen müsste.

Gehen Sie wie folgt vor

Nutzen Sie nach Möglichkeit Zwei-Faktoren-Authentifizierung mit einer Smartcard oder einem Smart-Token. IGEL OS unterstützt die folgenden Funktionen. Die Links führen zum entsprechenden Eintrag im Handbuch von IGEL OS.

- [Authentifizierung mit Smartcard in IGEL OS \(see page 550\)](#):
  - [Citrix StoreFront \(see page 554\)](#)
  - [RDP-Sitzungen \(see page 556\)](#)
  - [Horizon Sitzungen \(see page 557\)](#)
  - [Web-Browser \(see page 558\)](#)
- [\(Kerberos\) Passthrough-Authentifizierung \(see page 846\)](#)

## Das System aktuell halten

### Begründung

Software Updates beheben neu entdeckte Schwachstellen in IGEL OS und Anwendungen. Damit ist die Aktualisierung eine der wichtigsten Maßnahmen zur Sicherung von IGEL OS-Systemen.

Um Updates zu starten und zu konfigurieren, können Sie IGEL Setup und/oder die UMS-Funktion Universal Firmware Update verwenden.

Die auf dieser Seite beschriebenen Anweisungen verwenden die UMS-Funktion "Universal Firmware Update". Informationen zur Definition einer geplanten Aufgabe finden Sie im Abschnitt "Als Aufgabe" unter Updates zuweisen; zur Konfiguration des Updates auf einem Gerät, siehe Firmwareupdate-Einstellungen für IGEL OS.

### Anleitung

► Um über sicherheitskritische Updates für IGEL OS informiert zu werden und den IGEL Technical Newsletter zu bekommen, abonnieren Sie die IGEL News unter [www.igel.de](http://www.igel.de)<sup>40</sup>.

Der Aktualisierungsvorgang besteht aus den folgenden Schritten:

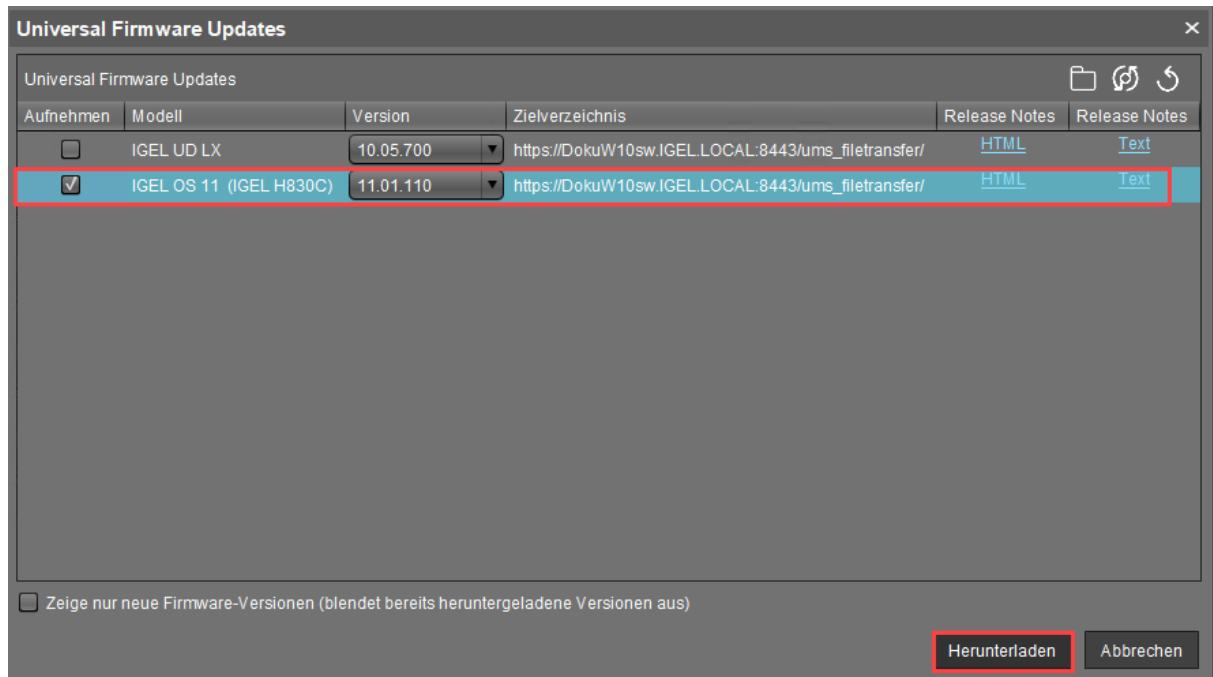
- Update vom IGEL Downloadserver herunterladen
- Update auf einem oder mehreren Geräten testen
- Update auf allen Geräten durchführen

Update vom IGEL Downloadserver herunterladen

1. Gehen Sie in der UMS Konsole auf **Universal Firmware Update**, öffnen Sie das Kontextmenü und wählen Sie **Neue Universal Firmware Update suchen**.
2. Aktivieren Sie die Firmware, die Sie herunterladen möchten und klicken Sie auf **Herunterladen**.

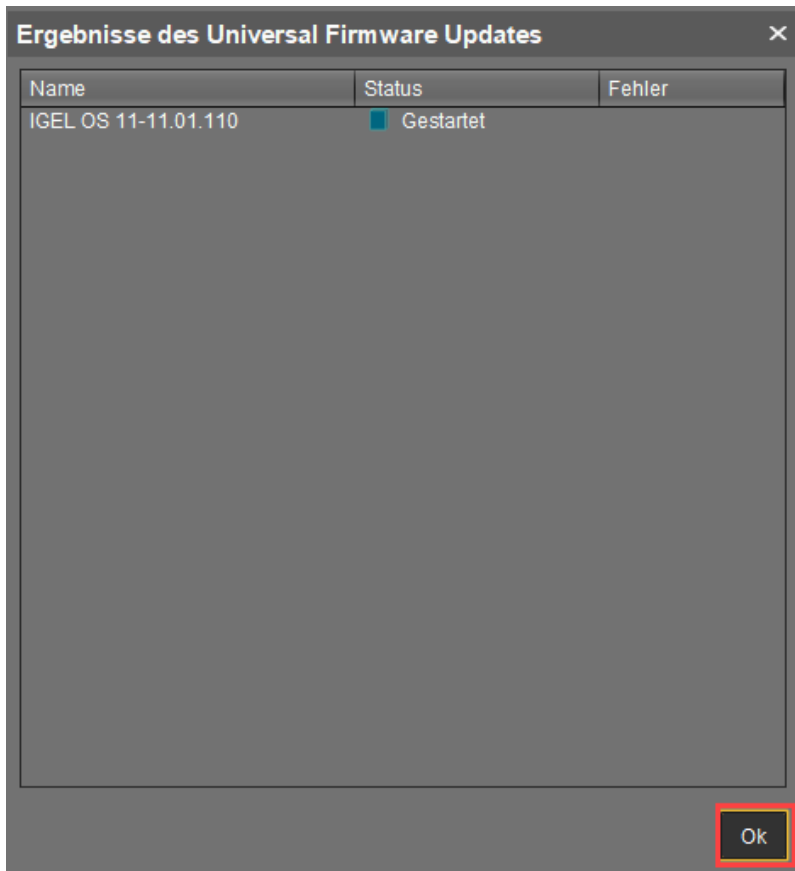
---

<sup>40</sup> <https://www.igel.de/>

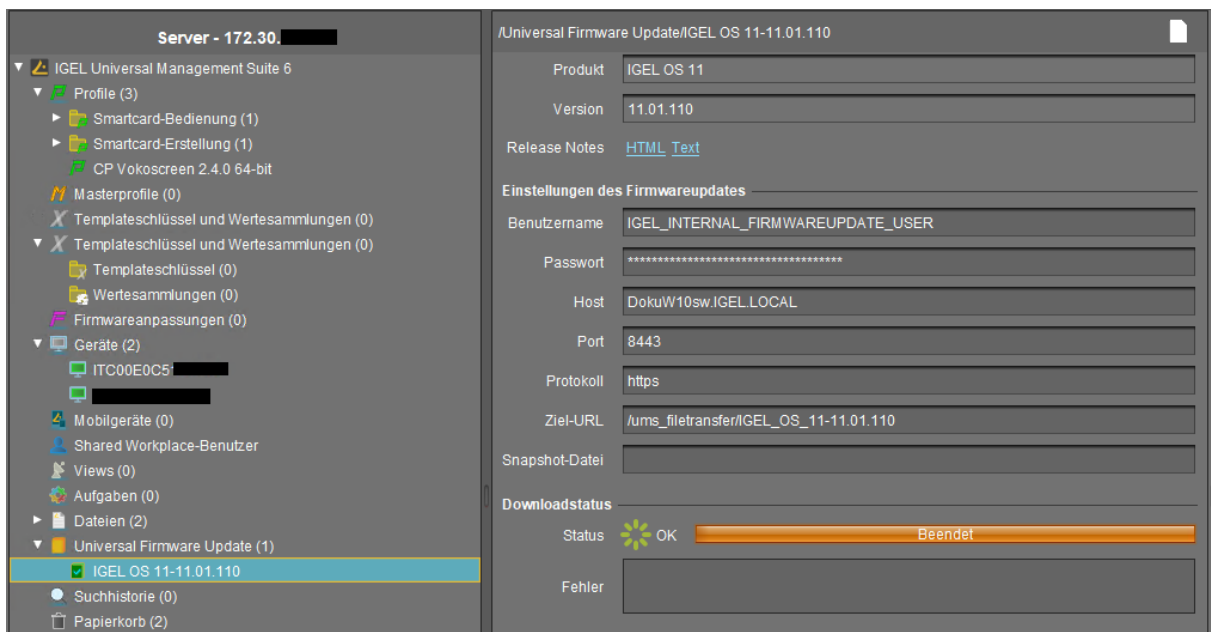


Der aktuelle Status des Firmware-Downloads wird angezeigt.

3. Klicken Sie **Ok**.

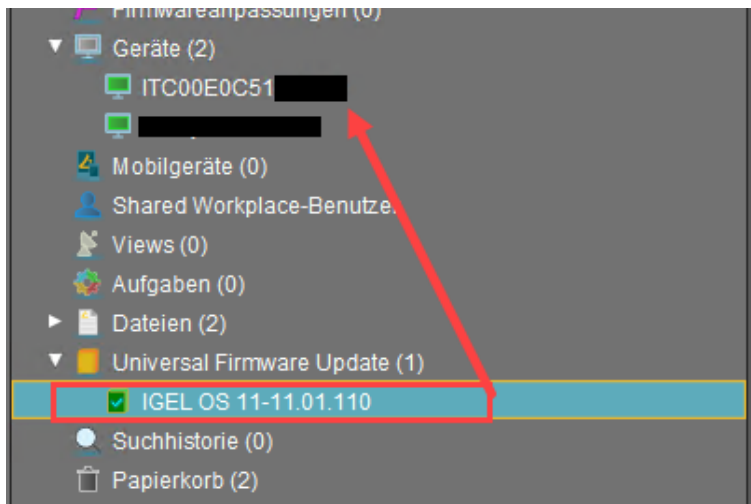


4. Wenn der Download erfolgreich war, wird die Firmware registriert und in der UMS gespeichert.

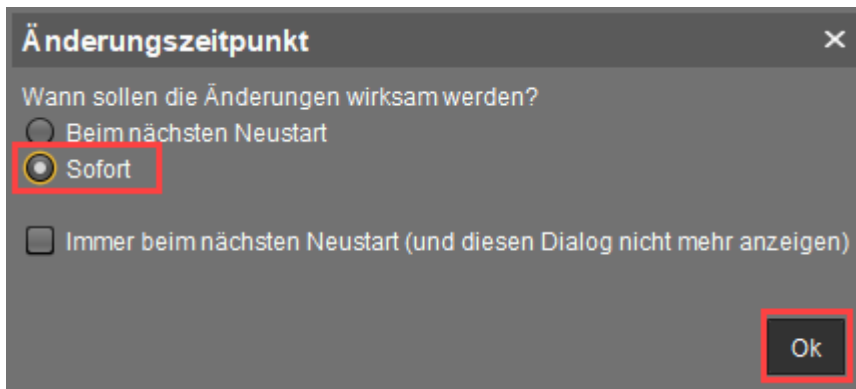


## Update auf einem oder mehreren Geräten testen

1. Gehen Sie in der UMS Konsole auf **Universal Firmware Update**, wählen Sie die gewünschte Firmware aus und ziehen Sie sie per Drag & Drop auf das Testgerät oder auf den Ordner mit den Testgeräten.



2. Wählen Sie **Sofort** im Dialogfenster **Änderungszeitpunkt** und klicken Sie **Ok**.



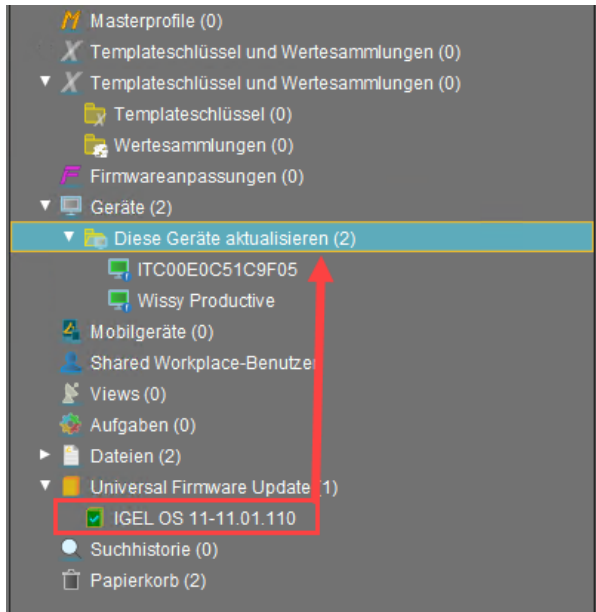
Die Firmware wird auf den Geräten aktualisiert; während des Aktualisierungsvorgangs werden die Geräte neu gestartet.

## Update auf allen Geräten durchführen

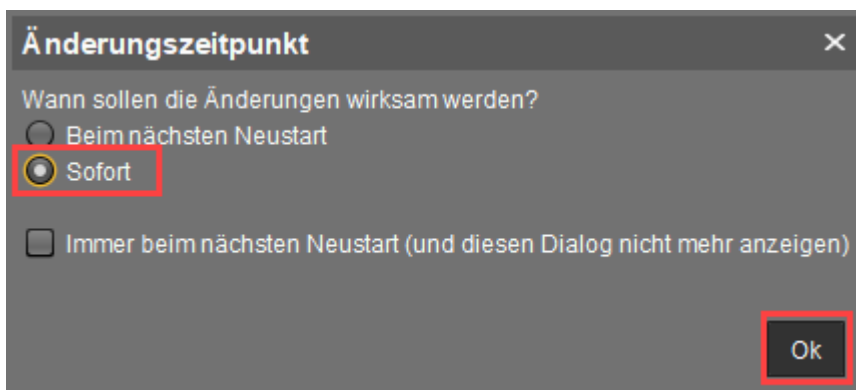
Sie können das Update entweder sofort starten oder es zu einem definierten Zeitpunkt über eine geplante Aufgabe starten.

Um das Update sofort zu starten:

1. Gehen Sie in der UMS Konsole auf **Universal Firmware Update**, wählen Sie die gewünschte Firmware und ziehen Sie sie per Drag & Drop auf den Ordner mit den zu aktualisierenden Geräten.



2. Wählen Sie **Sofort** im Dialogfenster **Änderungszeitpunkt** und klicken Sie **Ok**.



Die Firmware wird auf den Geräten aktualisiert; während des Aktualisierungsvorgangs werden die Geräte neu gestartet.

## Zugriff auf bestimmte Komponenten unterbinden

Sie haben die Möglichkeit, gezielt solche Komponenten zu verbergen, mit deren Hilfe der Benutzer Änderungen am System vornehmen könnte.

- [Zugriff auf lokales Terminal deaktivieren \(see page 456\)](#)
- [Zugriff auf virtuelle Konsolen deaktivieren \(see page 457\)](#)
- [Appliance-Modus verwenden \(see page 458\)](#)
- [Zubehör-Anwendungen ausblenden \(see page 459\)](#)


## Zugriff auf lokales Terminal deaktivieren

Mithilfe eines **lokalen Terminals** können Benutzer Befehle ausführen und dadurch Änderungen am System vornehmen. Standardmäßig sind Terminal-Sitzungen deaktiviert, d.h. es sind keine Terminal-Sitzungen konfiguriert. Um die Sicherheit zu erhöhen, sollten Sie eine der folgenden Maßnahmen ergreifen:

- Das lokale Terminal deaktiviert lassen
- Falls die Terminal-Sitzung konfiguriert ist, aber nicht gebraucht wird, deaktivieren Sie sie.
- Falls die Terminal-Sitzung notwendig ist, schützen Sie sie durch ein Passwort.

### Schritte

So entfernen Sie eine vorhandene Sitzung:

1. Gehen Sie in IGEL Setup zu **Zubehör > Terminals**.
2. Wählen Sie die Sitzung aus, die Sie entfernen möchten.
3. Klicken Sie , um die ausgewählte Sitzung zu entfernen.
4. Bestätigen Sie, dass Sie die Sitzung entfernen möchten.
5. Klicken Sie **Übernehmen**.

Als Alternative können Sie lokale Terminals durch ein Passwort schützen.

So schützen Sie das lokale Terminal durch ein Passwort:

1. Wählen Sie das lokale Terminal unter **Zubehör > Terminals** aus.
2. Folgen Sie die Anweisungen unter [Sitzungen und Zubehör mit Passwörtern schützen](#) (see page 445).



## Zugriff auf virtuelle Konsolen deaktivieren

Die virtuellen Konsolen `tty11` und `tty12` geben dem Benutzer Zugriff auf eine Shell. Eine Deaktivierung beider Konsolen erschwert das Ausführen von Befehlen oder die Vornahme von Änderungen am System.

Standardmäßig kann der Benutzer mithilfe der Tastenkombinationen `[STRG]+[Alt]+[F11]` und `[STRG]+[Alt]+[F12]` auf `tty11` bzw. `tty12` zugreifen.

So deaktivieren Sie den Zugriff auf die virtuellen Konsolen:

1. Gehen Sie in IGEL Setup zu **Benutzeroberfläche > Bildschirm > Zugriffskontrolle**.
2. Aktivieren Sie **Konsolenzugriff abschalten**.
3. Klicken Sie **Übernehmen**.

## Appliance-Modus verwenden

Standardmäßig werden Sitzungen unter IGEL OS nicht im Vollbildmodus ausgeführt, wodurch der Benutzer Zugriff auf das Startmenü sowie den gesamten Desktop hat. Im Appliance-Modus wird hingegen eine einzelne Sitzung im Vollbildmodus ausgeführt. Dadurch ist kein Zugriff auf andere Anwendungen auf dem Gerät möglich, was die Angriffsfläche verringert.


Der Appliance-Modus ist verfügbar für die folgenden Sitzungen:

- VMware Horizon
- Browser
- Citrix Self-Service
- RHEV/Spice
- Imprivata
- RDP MultiPoint Server
- XDMCP für dieses Display

So aktivieren Sie den Appliance-Modus:

1. Gehen Sie in IGEL Setup zu **Sitzungen > Appliance-Modus**.
2. Wählen Sie aus dem Dropdownmenü **Appliance-Modus** die gewünschte Sitzungsart und konfigurieren Sie die Sitzung.

Weitere Informationen zum Appliance-Modus finden Sie im IGEL OS Handbuch.

 Die meisten Sitzungsarten, die für den Appliance-Modus zur Verfügung stehen, können mit [Zwei-Faktor-Authentisierung](#) (see page 449) kombiniert werden, um die Sicherheit zusätzlich zu erhöhen.

## Zubehör-Anwendungen ausblenden

Mithilfe von Sitzungen vom Typ **Zubehör** können Änderungen am System vorgenommen werden. Den Zugriff auf **Zubehör** zu deaktivieren, kann das System sicherer machen.

So entfernen Sie einzelne Zubehör-Anwendungen (sowohl aus dem Startmenü als aus dem Starter für Sitzungen):

1. Gehen Sie in IGEL Setup zu **Zubehör > [Zubehörname]**.
2. Deaktivieren Sie alle Optionen im Bereich **Startmöglichkeiten der Sitzung**.
3. Klicken Sie **Übernehmen**.

So können Sie für Zubehör-Elemente den Passwortschutz aktivieren

- ▶ Folgen Sie die Schritten unter [Sitzungen und Zubehör mit Passwörtern schützen](#) (see page 445).

So blenden Sie das gesamte Symbol **System** im Startmenü aus:

1. Gehen Sie in IGEL Setup zu **Benutzeroberfläche > Desktop > Startmenü**.
2. Deaktivieren Sie **Systemtab**.
3. Klicken Sie **Übernehmen**.

So blenden Sie das gesamte Symbol **System** im Starter für Sitzungen aus:

1. Gehen Sie in IGEL Setup zu **Zubehör > Starter für Sitzungen > Konfiguration des Starters für Sitzungen**.
2. Aktivieren Sie **Systemseite ausblenden**.
3. Klicken Sie **Übernehmen**.


## Die Angriffsfläche verringern

Das Entfernen von nicht verwendeten Anwendungen sowie das Abschalten nicht benötigter Netzwerkdienste verringert die Angriffsfläche.

- [Lokalen Webbrowser entfernen](#) (see page 461)
- [Browser konfigurieren \(Kiosk-Modus\)](#) (see page 462)
- [Java im Browser deaktivieren](#) (see page 464)
- [PC/SC-Dämon deaktivieren](#) (see page 465)
- [TCP-Verbindungen für X-Server deaktivieren](#) (see page 466)
- [Nicht benötigte Features deaktivieren](#) (see page 467)
- [Hotplugspeichergeräte deaktivieren](#) (see page 468)
- [USB-Zugriffskontrolle aktivieren](#) (see page 469)
- [USB-Boot deaktivieren](#) (see page 470)
- [Leveraging AppArmor](#) (see page 471)

## Lokalen Webbrowser entfernen

Der lokal installierte Webbrowser kann Sicherheitslücken haben, die eine Eintrittspforte für Malware aus dem Internet sein können. Darum sollte der Browser, wenn er nicht benötigt wird, entfernt werden.

 Entfernen Sie den Browser nicht, wenn Sie Citrix StoreFront-Sitzungen verwenden.

Standardmäßig ist auf IGEL OS der lokale Browser (Firefox und Chromium) vorinstalliert. Dies ist unabhängig davon, ob eine Browsersitzung konfiguriert ist.

So entfernen Sie den Browser:

1. Gehen Sie in IGEL Setup zu **System > Firmwareanpassung > Features**.
2. Deaktivieren Sie das Feature **Lokaler Internetbrowser (Firefox)** und **Lokaler Browser (Chromium)**.
3. Klicken Sie **Übernehmen**.
4. Starten Sie das Gerät neu.

## Browser konfigurieren (Kiosk-Modus)

Wenn Sie einen lokalen Webbrowser anbieten möchten, können verschiedene Einstellungen die Sicherheit erhöhen.

Diese Einstellungen entsprechen der Konfiguration eines Kiosk-Modus. Das heißt, bis auf den Browser wird IGEL OS für den Benutzer ausgeblendet.

Standardmäßig sind im Webbrowser alle Funktionen und Menüs verfügbar. So konfigurieren Sie einen Kiosk-Modus:

### Firefox

1. Gehen Sie in IGEL Setup zu **Sitzungen > Firefox Browser > Firefox Browser Global > Sicherheit** und aktivieren Sie:
  - **Alle Webseiten auf Echtheit prüfen**
  - **Schutz gegen Malware**
  - **Lokales Dateisystem verbergen**
2. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global > Inhalt** und aktivieren Sie **Popups blockieren**, falls erforderlich.
3. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global > Datenschutz** und aktivieren Sie die folgenden Optionen:
  - **Private Daten löschen, sobald Browser beendet wurde** und alle Optionen im Bereich **Welche privaten Daten sollen gelöscht werden?**
  - **Privaten Browsermodus erlauben**
  - **Browser standardmäßig im privaten Modus starten**
  - **Nicht-Verfolgen-Funktion einschalten** und **Tracking-Schutz aktivieren**, falls notwendig
4. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global > Neustart** und aktivieren Sie **Neustart**.
5. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global > Fenstereinstellungen** und aktivieren Sie die folgenden Optionen:
  - **Start im Vollbildmodus**
  - **Konfigurationsseite des Browsers verbergen**
6. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global > Menüs & Symbolleisten** und aktivieren Sie **Firefoxschaltfläche Menü/Menüleiste verbergen**.
7. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browser Global > Kontextmenü** und aktivieren Sie **Kontextmenü ausblenden**.
8. Gehen Sie zu **Sitzungen > Firefox Browser > Firefox Browsersitzungen > [Sitzungsname] > Einstellungen** und aktivieren Sie **Autostart**.
9. Klicken Sie **Übernehmen**.
10. Starten Sie das Gerät neu.

Weitere Informationen finden Sie auch unter [Den Firefox-Browser im Kiosk-Modus verwenden \(see page 358\)](#).

### Chromium

1. Gehen Sie in IGEL Setup zu **Sitzungen > Chromium Browser > Chromium Browser Global > Sicherheit** und aktivieren Sie **Safe Browsing** und deaktivieren Sie **Dateizugriff**.

2. Gehen Sie zu **Sitzungen > Chromium Browser > Chromium Browser Global** und aktivieren Sie **Automatischer Neustart des Browsers bei Beenden**.
3. Gehen Sie zu **Sitzungen > Chromium Browser > Chromium Browser Global > Inhalt** und aktivieren Sie **Popups und Weiterleitungen blockieren**, falls erforderlich.
4. Gehen Sie zu **Sitzungen > Chromium Browser > Chromium Browser Global > Datenschutz** und aktivieren Sie die folgenden Optionen:
  - **Private Daten löschen, sobald Browser beendet wurde** und alle Optionen im Bereich **Welche privaten Daten sollen gelöscht werden?**
  - "Erzwingen" für die Einstellung **Inkognito-Modus erlauben**
  - **Nicht-Verfolgen-Funktion einschalten**, falls notwendig
5. Unter **Sitzungen > Chromium Browser > Chromium Browser Global > Fenster** aktivieren Sie **Kioskmodus aktivieren**.
6. Unter **Sitzungen > Chromium Browser > Chromium Sitzungen > [Sitzungsname]** aktivieren Sie **Autostart**.
7. Klicken Sie **Übernehmen**.
8. Starten Sie das Gerät neu.

## Java im Browser deaktivieren


Java Applets und Java Web Start können eine potenzielle Sicherheitsbedrohung darstellen und gelten inzwischen als veraltet. Ab Version 10.06.100 sind sie nicht mehr in IGEL OS enthalten. Die Registry Keys unter **System > Registry > java > deployment** sind obsolet.



## PC/SC-Dämon deaktivieren

Wenn Sie keine Smartcardleser verwenden, können Sie den PC/SC-Dämon deaktivieren. Das Deaktivieren von Diensten verkleinert die Angriffsfläche.

Standardmäßig ist PC/SC-Dämon aktiviert. So deaktivieren Sie ihn:

 Deaktivieren Sie den PC/SC-Dämon nur dann, wenn Sie sicher sind, dass er von keinem Smartcardleser benötigt wird.

1. Gehen Sie in IGEL Setup zu **Sicherheit > Smartcard > Dienste**.
2. Deaktivieren Sie **PC/SC-Dämon aktivieren**.
3. Klicken Sie **Übernehmen**.

## TCP-Verbindungen für X-Server deaktivieren

Der X-Server in IGEL OS hat Netzwerkfunktionalitäten, die Dritten erlauben könnten, Ihren Bildschirm zu sehen und Ihre Tastatureingaben mitzulesen. Deaktivieren Sie die Netzwerkfunktionalität, um Ihre Daten besser zu schützen.

Standardmäßig ist die Netzwerkfunktionalität von X-Server aktiviert. So deaktivieren Sie sie:

1. Gehen Sie in IGEL Setup zu **Benutzeroberfläche > Bildschirm > Zugriffskontrolle**.
2. Aktivieren Sie **Zugriffskontrolle**.
3. Aktivieren Sie **TCP-Verbindungen deaktivieren**.
4. Klicken Sie **Übernehmen**.

## Nicht benötigte Features deaktivieren

Eine Reduzierung der Anzahl von Software, die auf dem System ausgeführt wird, kann die Angriffsfläche verringern. Darum besteht eine allgemeine Sicherheitsmaßnahme unter IGEL OS 11 darin, sämtliche nicht benötigten Features zu deaktivieren.

So können Sie Features deaktivieren:


1. Gehen Sie in IGEL Setup zu **System > Firmwareanpassung > Features**.
2. Deaktivieren Sie alle nicht benötigten Features.
3. Falls an Ihr Gerät keine lokalen Drucker angeschlossen sind, die Sie mit anderen teilen möchten, aktivieren Sie folgende Features:


**Drucken (Internet printing protocol CUPS)**

**Drucken (Line Printer LPD)**


**Drucken (TCP/IP)**

**Drucken (ThinPrint)**

 Falls Sie eine eigene Partition verwenden: Deaktivieren Sie das Feature **Eigene Partition** nur dann, wenn Sie über eine Sicherheitskopie der Software und Daten der Partition verfügen. Wenn Sie das Feature deaktivieren, wird bei Neustart des Systems der gesamte Inhalt der eigenen Partition gelöscht.

 Deaktivieren Sie die Features **Fluendo Gstreamer Codec Plugins** sowie **Hardware Video Acceleration** nur dann, wenn Sie keine Sitzungen verwenden, die die Features benötigen.

4. Klicken Sie **Übernehmen**.
5. Starten Sie das Gerät neu.

 **Alternative Methode zur Reduzierung des Feature-Umfangs ab IGEL OS 11.04**  
Wenn Sie auf IGEL OS 11.04 oder höher aktualisieren, können Sie als Alternative die unter [Error: "Not enough space on local drive" when Updating to IGEL OS 11.04 or Higher \(see page 212\)](#) beschriebene Methode verwenden. Im Vergleich zur Deaktivierung von Features über das IGEL Setup hat diese Methode den Vorteil, dass Sie die deaktivierten Features nicht erneut deaktivieren müssen, falls Sie das Endgerät auf die Werkseinstellungen zurücksetzen (siehe Reset to Factory Defaults).

## Hotplugspeichergeräte deaktivieren

USB-Speichergeräte können für den Datendiebstahl oder die Ausführung von nicht autorisierter Software oder von Malware verwendet werden.

Storage-Hotplugging ist standardmäßig deaktiviert. Sollten Sie aus es irgendeinem Grund aktiviert haben, können Sie es folgendermaßen wieder deaktivieren:


1. Gehen Sie in IGEL Setup zu **Geräte > Speichergeräte > Hotplugspeichergeräte**.
2. Deaktivieren Sie **Dynamische Laufwerkszuordnung aktivieren**.
3. Geben Sie für **Zahl der Hotplug-Speichergeräte** den Wert **0** ein.
4. Klicken Sie **Übernehmen**.

## USB-Zugriffskontrolle aktivieren

USB-Speichergeräte wie USB-Sticks, WLAN-Controller oder Drucker können für den Datendiebstahl oder zur Ausführung von nicht autorisierter Software oder Malware verwendet werden. Zur Erhöhung der Sicherheit sollten so viele USB-Geräteklassen wie möglich deaktiviert werden.

Standardmäßig ist die USB-Zugriffskontrolle nicht aktiviert. So aktivieren Sie sie:

1. Gehen Sie in IGEL Setup zu **Geräte > USB-Zugriffskontrolle**.
2. Aktivieren Sie das Kontrollkästchen **Aktiviert**.

 Das Aktivieren der **USB-Zugriffskontrolle** und das Setzen der **Vorgaberegeln** auf **Verbieten** blockiert die Verwendung von USB-Geräten lokal und in der Sitzung und kann somit die Geräte deaktivieren, die die Benutzer benötigen. Aktivieren Sie daher die USB-Zugriffskontrolle nur, wenn Ihre Sicherheitsrichtlinie dies erfordert. Setzen Sie in diesem Fall die **Vorgaberegeln** auf **Verbieten** und konfigurieren Sie die **Erlauben**-Regeln für die erforderlichen USB-Geräte und USB-Geräteklassen.

Es wird empfohlen, die Einstellungen für die **USB-Zugriffskontrolle** als letzten Schritt in der Gerätekonfiguration vorzunehmen. Bevor Sie die USB-Zugriffskontrolle aktivieren, überprüfen Sie, ob alle anderen Einstellungen für Drucker, Unified Communication, USB Redirection und Mapping-Einstellungen für USB-Geräte wie erwartet funktionieren.

Beachten Sie, dass die USB-Zugriffskontrolle völlig getrennt von der USB-Umleitung für Remotesitzungen ist, siehe [When to Use USB Redirection \(see page 792\)](#).

Beachten Sie auch, dass das Feature einen USB-Anschluss nicht physisch deaktiviert, d. h. die Spannungsversorgung wird weiterhin funktionieren.

3. Setzen Sie **Vorgaberegeln** auf **Verbieten**.  
Durch die vordefinierte Regel "Human Interface Devices (HID)" sind jetzt bis auf z. B. Mäuse und Keyboards keine USB-Geräte erlaubt.
4. Konfigurieren Sie weitere Regeln gemäß Ihren Anforderungen. Anweisungen dazu finden Sie unter [USB-Zugriffskontrolle konfigurieren \(see page 793\)](#).
5. Klicken Sie **Übernehmen**.
6. Starten Sie das Gerät neu.

## USB-Boot deaktivieren


### Begründung

Die Deaktivierung des USB-Boot verhindert das Booten eines anderen Betriebssystems, mit dem IGEL OS auf dem Massenspeicher manipuliert oder (sogar versehentlich) überschrieben werden kann.

### Anleitung für IGEL Geräte


In Modellen der Geräteserie IGEL UD LX ist Booten von USB in den Werkseinstellungen deaktiviert. Sollten Sie es aus irgendeinem Grund aktiviert haben, dann können Sie es folgendermaßen wieder deaktivieren:

1. Halten Sie die Taste [Entf] ([F2] für UD2) gedrückt, während das System hochfährt.  
Das UEFI-Menü wird geöffnet.
2. Verwenden Sie die Pfeiltasten und die Eingabetaste, um zur **SCU** zu gelangen.
3. Optional: Geben Sie das UEFI-Passwort ein (falls vorhanden).  
Das **Setup Utility** wird geöffnet.
4. Gehen Sie zu **Boot**.
5. Stellen Sie den **USB Boot** auf **Disabled**.
6. Drücken Sie [F10].
7. Bestätigen Sie die Änderungen unter **Exit Saving Changes?**  
Das Gerät startet.

 Setzen Sie zusätzlich ein [UEFI-Passwort](#) (see page 448), damit die Boot-Einstellungen nicht zurückgesetzt werden können.

### Anweisungen für Geräte von Drittanbietern, die mit OSC konvertiert wurden

- Beachten Sie die Anweisungen Ihres BIOS/UEFI-Anbieters.

 Alternativ können Sie auch versuchen, [F12] (im Allgemeinen), [F10] (Intel-Geräte) oder [F9] (Hewlett-Packard-Geräte) zu drücken, um auf die BIOS/UEFI-Einstellungen zuzugreifen. Wenn dies nicht funktioniert, versuchen Sie, während des Bootvorgangs [Entf], [F1] oder [F2] zu drücken.

## Leveraging AppArmor

AppArmor steuert, welche Berechtigungen einer Anwendung, die auf dem System läuft, gewährt werden sollen. Auf diese Weise können auch noch unbekannte Schwachstellen beseitigt werden.

Die folgenden Anwendungen werden von AppArmor überwacht:

- Firefox browser
- Cups print server
- Evince pdf Viewer

Die folgenden Systemprogramme werden von AppArmor überwacht:

- tcpdump
- haveged
- dhclient

Standardmäßig ist AppArmor aktiviert. Ihr Registrierungsschlüssel ist `system.security.apparmor`

## UMS und Fernzugriff konfigurieren

Die Fernadministration mit der UMS sowie Fernzugriff sind mächtige Features von IGEL OS. Verwenden Sie sichere Einstellungen und deaktivieren Sie nicht benötigte Funktionen.

- [Endpoints an UMS-Instanz binden](#) (see page 473)
- [Spiegeln deaktivieren](#) (see page 474)
- [Sichere VNC-Einstellungen](#) (see page 475)
- [SSH-Server deaktivieren](#) (see page 476)
- [X11-Weiterleitung deaktivieren](#) (see page 477)
- [Sichere SSH-Einstellungen](#) (see page 478)
- [Sicheres Terminal deaktivieren](#) (see page 479)




## Endpoints an UMS-Instanz binden

Endpoints, auf denen Fernzugriff aktiviert ist, und noch nicht bei einer UMS-Instanz registriert sind, können von der UMS eines Angreifers übernommen werden. Stellen Sie sicher, alle IGEL Endpoints, die sich in Ihrem Netzwerk befinden, zu registrieren.

Unter IGEL OS ist der Fernzugriff standardmäßig aktiviert. Durch Autoregistrierung stellen Sie sicher, dass alle Endpoints in Ihrem Unternehmensnetzwerk registriert werden\_

1. Erzeugen Sie für Host, auf dem die UMS läuft, einen DNS-Eintrag mit dem Namen `igelrmsrver`
2. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > TC Netzwerk Einstellungen**.
3. Aktivieren Sie das Kontrollkästchen **Automatisches Registrieren aktivieren (ohne MAC-Adressenimport)**.  
Jetzt werden alle IGEL Thin Clients sowie mithilfe des UDC3 konvertierten Geräte beim Booten automatisch bei der UMS-Instanz registriert.
4. Klicken Sie Übernehmen.

Sie können außerdem mithilfe von Vorgabeverzeichnisse neu registrierte Geräte in ein Quarantäneverzeichnis verschieben. Dem Verzeichnis können Sie ein Masterprofil zuweisen und dadurch sichere Einstellungen erzwingen, z. B. ein lokales Administrator-Passwort.

 Sie können Fernzugriff auch deaktivieren. Die Einstellung dafür finden Sie im auf dem Thin Client in IGEL Setup unter **System > Fernzugriff**. Allerdings stehen Ihnen dadurch wesentliche Features von IGEL OS nicht zur Verfügung. Dieses Vorgehen mag dennoch für bestimmte Anwendungsfälle sinnvoll sein.

## Spiegeln deaktivieren

Das Spiegeln wird von einem VNC-Server ermöglicht, der als Netzwerkdienst unter IGEL OS läuft. Eine Reduzierung der Anzahl von Netzwerkdiensten verringert die Angriffsfläche des Systems.

Standardmäßig ist Spiegeln unter IGEL OS nicht aktiviert. Sollten Spiegeln aus irgendeinem Grund aktiviert sein, dann können Sie es folgendermaßen deaktivieren:


1. Gehen Sie in IGEL Setup zu **System > Fernzugriff > Spiegeln**.
2. Aktivieren Sie **Spiegeln des Desktops mit VNC erlauben**.
3. Klicken Sie **Übernehmen**.

## Sichere VNC-Einstellungen

Das Spiegeln kann mithilfe folgender VNC-Einstellungen sicherer gemacht werden.

Standardmäßig wird für das Spiegeln keine verschlüsselte Netzwerkverbindung und auch kein Passwort verwendet. So aktivieren Sie diese sicherheitsrelevanten Features:

1. Gehen Sie in IGEL Setup zu **System > Fernzugriff > Spiegeln**.
2. Nehmen Sie möglichst alle der folgenden Einstellungen vor:
  - Aktivieren Sie **Sichere Verbindung**.
  - Aktivieren Sie **Passwort verwenden** und legen Sie ein starkes Passwort fest.
  - Aktivieren Sie **Benutzer um Erlaubnis fragen**.
  - Aktivieren Sie **Benutzer darf Fernspiegelung unterbrechen**.
  - Deaktivieren Sie **Eingaben vom entfernten Rechner aus zulassen**.
3. Klicken Sie **Übernehmen**.

 Die Einstellung "Sichere Verbindung" kann global aktiviert werden in der UMS unter **UMS Administration > Globale Konfiguration > Fernzugriff**. Dort können sich auch aktivieren, dass protokolliert wird, wenn Benutzer eine Spiegelung über eine gesicherte Verbindung durchführen.

## SSH-Server deaktivieren


Der SSH-Server unter IGEL OS ist ein Netzwerkdienst. Eine Reduzierung der Anzahl von Netzwerkdiensten verringert die Angriffsfläche des Systems. Dies trifft besonders auf SSH zu, insofern der Dienst dafür konzipiert wurde, aus der Ferne Befehle auf dem System auszuführen.

Standardmäßig ist der SSH-Server aktiviert. So deaktivieren Sie ihn:

- Gehen Sie in IGEL Setup zu **System > Fernzugriff > SSH-Zugriff**.
- Deaktivieren Sie das Kontrollkästchen **Aktivieren**.
- Klicken Sie **Übernehmen**.

## X11-Weiterleitung deaktivieren

Wenn die X11-Weiterleitung deaktiviert ist, können Grafikanwendungen nicht per SSH ausgeführt werden. Standardmäßig ist die X11-Weiterleitung deaktiviert.

 Wenn die X11-Weiterleitung deaktiviert ist, ist es nicht möglich, das IGEL Setup von einer SSH-Sitzung aus zu starten.

Um sicherzustellen, dass die X11-Weiterleitung deaktiviert ist:

1. Gehen Sie im IGEL Setup unter **System > Fernzugriff > SSH-Zugriff** und stellen Sie sicher, dass die Option **X11-Weiterleitung zulassen** deaktiviert ist.
2. Klicken Sie **Übernehmen** oder **Ok**.

## Sichere SSH-Einstellungen

Wenn Sie SSH-Verbindungen zu IGEL OS erlauben möchten, dann können Sie diese mithilfe folgender Einstellungen sicherer machen.


1. Gehen Sie in IGEL Setup zu **System > Fernzugriff > SSH-Zugriff**.
2. Nehmen Sie so viele der folgenden Einstellungen wie möglich vor:
  - Deaktivieren Sie **Leere Passwörter zulassen**.
  - Deaktivieren Sie **Administratoranmeldung zulassen**.
  - Deaktivieren Sie den Benutzerzugriff für den Benutzer `user`. Dieser Benutzer ist in der Lage, Kommandos mit normalen Benutzerrechten auszuführen.
  - Erlauben Sie stattdessen Benutzerzugriff für den Benutzer `ruser`. Die Befehle, die dieser Benutzer ausführen darf, können in der Liste **Zugriff auf Anwendungen für Fernbenutzer 'ruser'** festgelegt werden. Standardmäßig kann `ruser` eine lokale Shell sowie IGEL Setup ausführen.
  - Klicken Sie **Übernehmen**.
  - Gehen Sie zu **Sicherheit > Passwort** und aktivieren Sie im Abschnitt **Benutzerkonto für Fernzugriff** die Einstellung **Passwort verwenden**. Legen Sie ein Passwort fest.
  - Klicken Sie **Übernehmen**.

## Sicheres Terminal deaktivieren

Sicheres Terminal ist ein Netzwerkdienst unter IGEL OS, der eine TLS/SSL-verschlüsselte Telnetsitzung anbietet. Eine Reduzierung der Anzahl von Netzwerkdiensten verringert die Angriffsfläche des Systems. Dies trifft besonders auf Sicheres Terminal zu, insofern der Dienst dafür konzipiert wurde, aus der Ferne Befehle auf dem System auszuführen.

Sicheres Terminal ist standardmäßig nicht aktiviert. Sie können den Dienst jederzeit folgendermaßen deaktivieren:

1. Gehen Sie in IGEL Setup zu **System > Fernzugriff > Sicheres Terminal**.
2. Deaktivieren Sie **Sicheres Terminal**.
3. Klicken Sie **Übernehmen**.

 Sicheres Terminal kann global in der UMS aktiviert werden unter **UMS Administration > Globale Konfiguration > Fernzugriff**. Dort kann auch eingestellt werden, ob Zugriffe via Sicheres Terminal protokolliert werden sollen.

## WLAN und Bluetooth

Von Angreifern eingerichtete oder unverschlüsselte WLAN-Access-Points können genauso wie Bluetoothgeräte ein Risiko für Ihre Datensicherheit darstellen. Falls Ihr Gerät WLAN und/oder Bluetooth verwendet, stellen Sie sicher, diese sicher zu konfigurieren oder vollständig zu deaktivieren.

- [Sichere WLAN-Einstellungen](#) (see page 481)
- [Bluetooth deaktivieren](#) (see page 482)




## Sichere WLAN-Einstellungen

So aktivieren Sie eine starke Verschlüsselung für WLAN und konfigurieren, dass nur mit einem von Ihnen festgelegten WLAN-Zugangspunkt eine Verbindung aufgebaut werden kann. Außerdem können Sie eine Whitelist mit weiteren erlaubten Zugangspunkten festlegen.

Standardmäßig ist WLAN nicht aktiviert. So aktivieren Sie WLAN und konfigurieren einen oder mehrere erlaubte Zugangspunkte:

1. Gehen Sie in IGEL Setup zu **Netzwerk > LAN-Schnittstellen > WLAN**.
2. Aktivieren Sie die Einstellung **WLAN-Netzwerkschnittstelle aktivieren**.
3. Stellen Sie sicher, dass die Einstellung **WiFi-Manager aktivieren** deaktiviert ist.

 Wenn der WiFi-Manager aktiviert ist, kann der Benutzer den WLAN-Zugangspunkt frei auswählen.

4. Klicken Sie **Übernehmen**.
5. Gehen Sie zu **Netzwerk > LAN-Schnittstellen > WLAN > Standard-WLAN**.
6. Aktivieren Sie die Einstellung **WPA-Verschlüsselung aktivieren**.
7. Geben Sie den **WLAN-Namen (SSID)** ein.
8. Nehmen Sie die Einstellungen für Authentifizierung und Verschlüsselung vor; siehe Standard-WLAN im IGEL OS Handbuch.
9. Klicken Sie **Übernehmen**.

Bei Bedarf können Sie unter **Netzwerk > LAN-Schnittstellen > WLAN > Weitere WLANs** zusätzliche erlaubte WLAN-Zugangspunkte konfigurieren.

## Bluetooth deaktivieren

Wenn Ihr Gerät über eine Bluetoothschnittstelle verfügt, dann könnte diese für einen Datenzugriff verwendet werden. Bluetooth zu deaktivieren verringert die Gefahr eines Datendiebstahls.

Standardmäßig ist Bluetooth deaktiviert. Sie können Bluetooth jederzeit folgendermaßen deaktivieren:

1. Gehen Sie in IGEL Setup zu **Geräte > Bluetooth**.
2. Deaktivieren Sie die Einstellung **Bluetooth aktivieren**.
3. Klicken Sie **Übernehmen**.

## IGEL UD Pocket für private Geräte verwenden

Im folgenden Dokument wird erläutert, wie Sie die Unternehmenssicherheit in einem BYOD-Modell (Bring Your Own Device) durch den Einsatz von IGEL UD Pocket gewährleisten können.

---

Benutzern den Zugriff auf Unternehmensressourcen mit privaten Geräten und privater Software zu erlauben, ist ein Sicherheitsrisiko. Diese Systeme können über unsichere Konfigurationen verfügen oder von Malware infiziert sein. Außerdem sollten Unternehmensdaten nicht auf privaten Geräten gespeichert werden.

► Verwenden Sie als Sicherheitsmaßnahme IGEL UD Pocket. Dadurch wird die Verwendung von sicherer und vertrauenswürdiger Software sichergestellt. Da UD Pocket nicht auf den Massenspeicher des Geräts zugreift, sind die privaten Daten des Benutzer und die Unternehmensdaten getrennt.

Informationen zum IGEL UD Pocket und wie Sie den während des Bootvorgangs auswählen können, finden Sie im IGEL UD Pocket Handbuch.

## SSH-Zugriff auf Geräten mit Schlüsseln

IGEL OS verfügt über einen integrierten OpenSSH-Server, der über das IGEL Setup aktiviert und konfiguriert werden kann. Via SSH kann eine sichere Verbindung zum Gerät aufgebaut werden, um Befehle sowie Dateiübertragungen auszuführen. Während eine Authentifizierung mit Benutzername und Passwort möglich ist, kann die Verwendung eines Public-Private-Schlüsselpaares die Sicherheit erhöhen und die Nutzung von SSH vereinfachen. In diesem Dokument wird beschrieben, wie Sie die benötigten Schlüssel erzeugen sowie an Geräte übertragen.

- [SSH-Schlüsselpaar erzeugen \(see page 485\)](#)
- [Öffentlichen Schlüssel mit der UMS übertragen \(see page 487\)](#)
- [SSH-Zugriff auf dem Gerät aktivieren \(see page 488\)](#)

## SSH-Schlüsselpaar erzeugen

### Voraussetzungen

- Unix-/Linux-Betriebssystem
- Installierter OpenSSH-Client

### Allgemeines

In den folgenden Schritten werden zwei Schlüssel erzeugt:

- Der öffentliche Schlüssel (Public Key): Dieser Schlüssel wird an alle Geräte übertragen, auf die der Administrator zugreifen möchte. Dieser Schlüssel kann öffentlich verfügbar gemacht werden.
- Privater Schlüssel (Private Key): Dieser Schlüssel bleibt auf dem Computer des Administrators und muss geheim gehalten werden.

⚠ Für die Vertraulichkeit von verschlüsselten Verbindungen mit Geräten ist es essentiell, den privaten Schlüssel geheim zu halten.

### Das Schlüsselpaar erzeugen

1. Öffnen Sie ein Terminal als Benutzer, der eine SSH-Verbindung zu Geräten aufbauen möchte.
2. Führen Sie folgenden Befehl aus:  
`ssh-keygen`
3. Wenn Sie aufgefordert werden, einen Speicherort für das Schlüsselpaar einzugeben, haben Sie folgende Möglichkeiten:
  - Drücken Sie ENTER, dadurch wird der Standarddateiname `~/.ssh/id_rsa` verwendet.

⚠ Bei Verwendung des Standarddateinamens können vorhandene SSH-Schlüsselpaare überschrieben werden!

- 
- 
- 
4. Wenn Sie aufgefordert werden, eine Passphrase einzugeben, haben Sie folgende Möglichkeiten:
  - Geben Sie den absoluten Pfad zu einer Datei Ihrer Wahl ein.
  - Geben Sie eine Passphrase ein (zweimal).

ℹ Eine Passphrase kann den privaten Schlüssel vor unbefugtem Zugriff Dritter schützen, sollte der Schlüssel gestohlen werden. Andererseits muss die Passphrase bei jedem Verbindungsaufbau erneut eingegeben werden, was umständlich sein kann.

- Drücken Sie ENTER, um keine Passphrase zu verwenden.

⚠ Der Verzicht auf eine Passphrase kann komfortabel sein, aber auch das Sicherheitsrisiko erhöhen.

Es wurden zwei Dateien erstellt (Standarddateinamen):


- `id_rsa` - Datei mit dem privaten Schlüssel
- `id_rsa.pub` - Datei mit dem öffentlichen Schlüssel

## Öffentlichen Schlüssel mit der UMS übertragen

1. Starten Sie die UMS.
2. Klicken Sie mit der rechten Maustaste im Navigationsbaum auf das Verzeichnis **Dateien**.
3. Wählen Sie im Kontextmenü **Neue Datei**.
4. Wählen Sie bei **Lokale Datei** die Datei mit dem öffentlichen Schlüssel (Dateiendung \*.pub).

 Achten Sie darauf, nicht versehentlich den privaten Schlüssel hochzuladen.

5. Setzen Sie **Klassifizierung** auf **Nicht definiert**.
6. Geben Sie bei **Speicherpfad des Thin Clients** `/wfs/user/.ssh/authorized_keys` ein.
7. Lassen Sie **Zugriffsrechte** auf **Lesen, Schreiben, Ausführen**.
8. Weisen sie die Datei den gewünschten Thin Clients, Profilen oder Verzeichnissen zu.

 Wenn Sie mehrere Schlüssel für SSH-Verbindungen mit Thin Clients zulassen möchten, können Sie eine Datei mit dem Namen `authorized_keys` erstellen und in dieser die öffentlichen Schlüssel auflisten. Verwenden Sie dazu einen Texteditor.

## SSH-Zugriff auf dem Gerät aktivieren

1. Gehen Sie in IGEL Setup oder einem Profil zu **System > Fernzugriff > SSH-Zugriff**.
2. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
3. Optional: Falls `user` ein leeres Passwort hat, können Sie **Leeres Passwort zulassen** aktivieren.
4. Setzen Sie im Bereich **Benutzerzugriff** bei dem Eintrag `user` den Wert von **Abweisen** auf **Nein**.

 Die Einstellung gibt Remotebenutzern den gleichen Zugriff auf das System wie lokalen Benutzer.

Sie können sich jetzt vom Computer des Administrators mit dem Gerät verbinden. Geben Sie dazu in einem Terminal folgenden Befehl ein:

```
ssh user@[client name or IP address]
```

Wenn Sie für den privaten Schlüssel eine Passphrase festgelegt haben, werden Sie aufgefordert, diese einzugeben.



## Sicheres Terminal (Telnet mit TLS/SSL)

IGEL Linux Version 5.11.100 oder neuer und IGEL Linux Version 10.01.100 oder neuer ermöglichen den Zugriff auf das Terminal über die UMS mit Transportverschlüsselung. In Analogie zu [Sicheres Spiegeln \(VNC mit TLS/SSL\)](#) (see [page 490](#)) wird der Netzwerkverkehr mit TLS/SSL verschlüsselt. Sichere Terminalverbindungen können nur von dem UMS initiiert werden, dessen Zertifikat auf dem Gerät gespeichert ist.


Details zur Einrichtung eines sicheren Terminals finden Sie im UMS-Handbuch unter Sicheres Terminal (Secure Shell).

Secure Terminal ist der beste Weg, um einen Fernzugriff von der UMS (unter Linux oder Windows installiert) auf Linux-Geräte zu erstellen, ohne eine zusätzliche Terminal-Software zu installieren. Da die UMS die Software beinhaltet.


## Sicheres Spiegeln (VNC mit TLS/SSL)

Die **Sicheres Spiegeln**-Funktion verbessert die Sicherheit bei der maintaining eines Geräts über VNC an mehreren Standorten:

- **Verschlüsselung:** Die Verbindung zwischen dem gespiegelten Computer und dem gespiegelten Gerät ist verschlüsselt.  
Dies ist unabhängig vom verwendeten VNC-Viewer.
- **Vollständigkeit:** Nur Geräte in der UMS Datenbank können gespiegelt werden.
- **Berechtigung:** Nur autorisierte Personen (UMS-Administratoren mit ausreichenden Berechtigungen) können Geräte spiegeln.  
Direktes Spiegeln ohne Anmeldung auf der UMS ist nicht möglich.
- **Begrenzung:** Nur das in der UMS konfigurierte VNC-Viewer Programm (interner oder externer VNC-Viewer) kann zum spiegeln verwendet werden.  
Eine direkte Spiegelung eines Gerätes durch ein anderes Gerät ist ebenfalls nicht zulässig.

 Darüber hinaus bietet die IGEL Management Interface (IMI) in Version 2 oder neuer eine API für Sicheres Spiegeln.

- **Aufzeichnung:** Verbindungen, die über eine sichere Spiegelung hergestellt werden, werden im UMS-Serverprotokoll aufgezeichnet.  
Zusätzlich zu den Verbindungsdaten können auch die zugehörigen Benutzerdaten (Spiegelung-UMS-Administrator, optional) im Protokoll erfasst werden.

 Dies ist natürlich nur für Geräte relevant, die die Anforderungen an eine sichere Spiegelung erfüllen und die entsprechende Option aktiviert haben. Andere Geräte können in gewohnter Weise "frei" abgespiegelt und bei Bedarf durch die Anforderung eines Passworts gesichert werden. Wenn Sie nur eine sichere Spiegelung zulassen möchten, können Sie dies in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Fernzugriff** festlegen.

- 
- [Grundprinzipien und Anforderungen](#) (see page 491)
  - [Geräte sicher spiegeln](#) (see page 492)
  - [VNC Logging](#) (see page 493)

## Grundprinzipien und Anforderungen

Die Option **Sicheres Spiegeln** kann aktiviert werden, wenn die folgenden Voraussetzungen erfüllt sind:

- IGEL Linux ab Version 5.03.190 und 10.01.100 oder IGEL Windows Embedded Standard 7 ab Version 3.09.100
- IGEL Universal Management Suite ab Version 4.07.100 aufwärts
- Das Gerät ist am UMS Server registriert
- Die Geräte können mit der UMS Konsole und dem UMS Server kommunizieren (siehe unten)

### Technische Grundprinzipien

Im Gegensatz zum "normalen" Spiegeln wird die Verbindung zwischen dem VNC-Viewer und dem VNC-Server (auf dem Gerät) nicht direkt beim sicheren Spiegeln hergestellt. Stattdessen läuft es über zwei Proxies – einen für die UMS Konsole und einen für den VNC-Server auf dem Gerät. Diese Proxies kommunizieren über einen TLS/SSL-verschlüsselten Kanal, während die lokale Kommunikation, z. B. zwischen der VNC-Viewer-Anwendung und dem UMS Proxy, auf herkömmliche Weise unverschlüsselt erfolgt. Dadurch kann auch mit externen VNC-Programmen, die keine TLS/SSL-Verbindungen unterstützen, eine sichere Verbindung aufgebaut werden.

Die beiden Proxies (UMS Konsole und Gerät) kommunizieren mit TLS/SSL-Verschlüsselung über denselben Port wie die "normale" VNC-Verbindung: 5900. Daher müssen keine speziellen Regeln für Firewalls konfiguriert werden, um eine sichere Spiegelung zu gewährleisten.

Wenn sicheres Spiegeln auf dem Gerät unter **Setup > System > Fernzugriff > Spiegeln > Sichere Verbindung** aktiviert ist, erzeugt das Gerät ein Zertifikat nach dem Standard X.509 und überträgt es beim nächsten Systemstart an den UMS Server. Der UMS Server überprüft nachfolgende Anfragen nach einer sicheren VNC-Verbindung anhand des Zertifikats. Das Zertifikat im PEM-Format finden Sie auf dem Gerät im Verzeichnis `/wfs/client-certs/tc_ca.crt`. Die Gültigkeit des Zertifikats kann auf dem (Linux-)Client mit dem folgenden Befehl überprüft werden: `x11vnc -sslCertInfo /wfs/client-certs/tc_ca.crt`.

Wenn ein UMS-Administrator für das Gerät die Funktion **Spiegeln** in der UMS Konsole aufruft, erhält die Konsole eine signierte Anforderung vom UMS Server, die dann an das zu spiegelnde Gerät weitergeleitet wird. Dieser wiederum leitet die Anforderung an den UMS Server weiter, der die Gültigkeit der Anforderung anhand des Originalzertifikats überprüft. Wenn die Überprüfung erfolgreich war, berichtet die Konsole, dass der Kanal für die Verbindung zwischen den Proxies hergestellt werden kann. Der UMS Proxy auf der Konsole verbindet sich mit dem Server-Proxy auf dem Gerät und der Server-Proxy wiederum stellt die Verbindung auf dem Gerät zu seinem VNC-Server her.

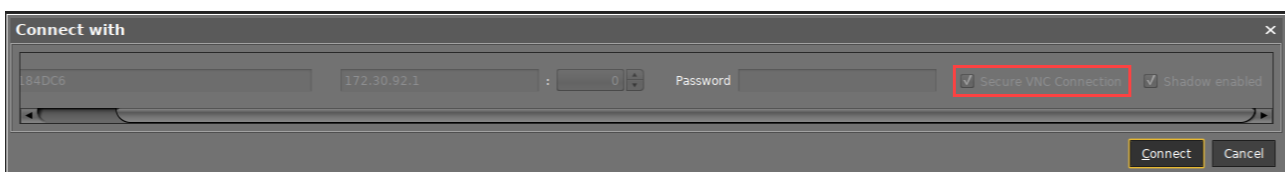
Erst wenn diese Verbindungen hergestellt sind, ruft die Konsole den VNC-Viewer auf, der sich dann mit dem Proxy der Konsole verbindet. Das VNC-Gerät und der VNC-Server sind nun über die beiden Proxies verbunden, welche die Daten mit TLS/SSL-Verschlüsselung übertragen.

Für alle Geräte, die diese Funktion unterstützen, kann sicheres Spiegeln unabhängig von der Gerätekonfiguration erzwungen werden: **UMS Administration > Globale Konfiguration > Fernzugriff > Sicheres VNC global aktivieren**.

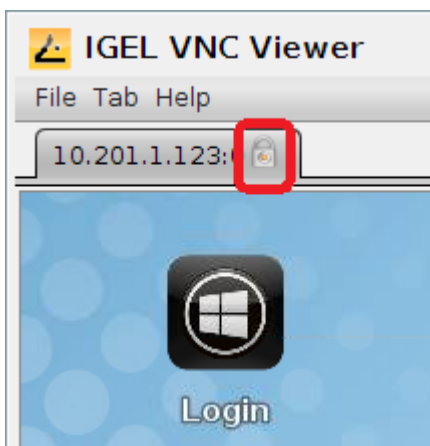
## Geräte sicher spiegeln

Um ein Gerät sicher (mit Verschlüsselung) zu schützen, muss sich der Administrator über die UMS-Konsole am Server anmelden. Dabei ist es unerheblich, ob ein rein lokales UMS-Administratorkonto verwendet wird oder der Benutzer z.B. über ein Active Directory übernommen wurde. Wie immer muss der UMS-Administrator jedoch die Berechtigung haben, das Objekt zu spiegeln, siehe Objektbezogene Zugriffsrechte.

Das zu spiegelnde Gerät wird im Strukturbaum aufgerufen und kann wie gewohnt über **Spiegeln** im Kontextmenü ausgeführt werden. Das Verbindungsfenster unterscheidet sich jedoch vom Dialog für die normale VNC-Spiegelung. Die IP und der Port des zu spiegelnden Geräts können nicht geändert werden, und es wird kein Passwort für die Verbindung angefordert - dies ist nach vorheriger Anmeldung an der Konsole überflüssig.



Wenn eine VNC-Verbindung hergestellt wurde, zeigt das Symbol im Reiter eine sichere Spiegelung an:

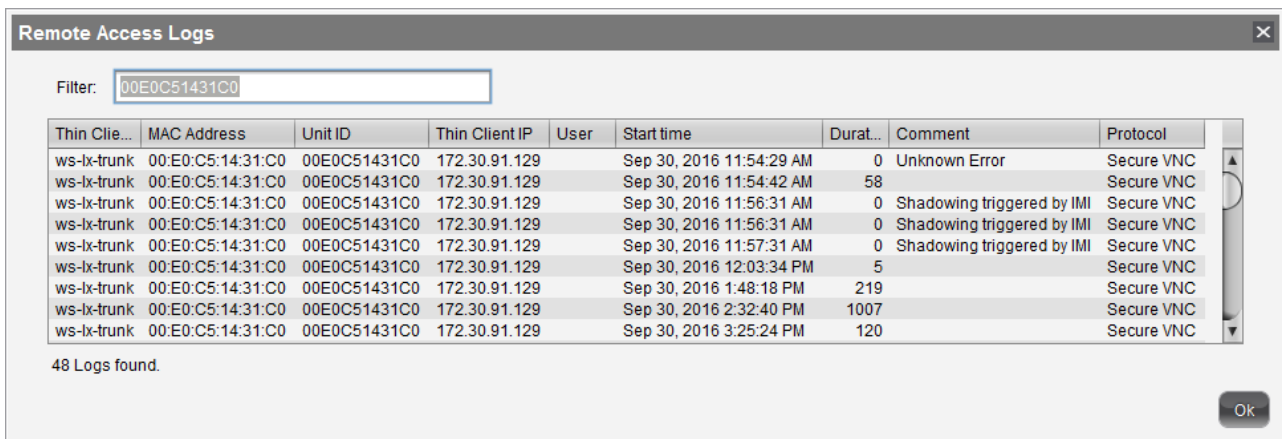


## VNC Logging

Verbindungen über sicheres Spiegeln werden immer in der UMS aufgezeichnet. Über **UMS Administration > Globale Konfiguration > Fernzugriff > Sicheres VNC** können Sie konfigurieren, ob der Benutzername im Protokoll erfasst werden soll:

- **Benutzer für sicheres VNC protokollieren**
  - Der Benutzername ist im Protokoll enthalten.
  - Der Benutzername ist nicht im Protokoll enthalten. (Standard)

Das VNC-Protokoll kann über das Kontextmenü eines Geräts oder Verzeichnisses aufgerufen werden (für mehrere Geräte, **Logging > Logging: Sichere Zugriffe**). Der Name, MAC-Adresse und IP-Adresse des gespiegelten Gerätes, die Zeit und Dauer des Vorgangs und, wenn entsprechend konfiguriert, der Benutzername des spiegelnden UMS-Administrators werden protokolliert.



Thin Client	MAC Address	Unit ID	Thin Client IP	User	Start time	Durat...	Comment	Protocol
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:54:29 AM	0	Unknown Error	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:54:42 AM	58		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:56:31 AM	0	Shadowing triggered by IMI	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:56:31 AM	0	Shadowing triggered by IMI	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 11:57:31 AM	0	Shadowing triggered by IMI	Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 12:03:34 PM	5		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 1:48:18 PM	219		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 2:32:40 PM	1007		Secure VNC
ws-lx-trunk	00:E0:C5:14:31:C0	00E0C51431C0	172.30.91.129		Sep 30, 2016 3:25:24 PM	120		Secure VNC

48 Logs found.

► Um die Liste zu sortieren (z. B. nach Benutzernamen), klicken Sie auf die entsprechende Spaltenüberschrift oder filtern Sie den angezeigten Inhalt, indem Sie Einträge im Feld **Filter** vornehmen.

## Cherry eGK Kanalersetzung

Ab Firmware-Version 10.05.100, steht die Cherry eGK Kanalersetzung nicht mehr zur Verfügung. In der Igel Universal Desktop Firmware, Linux V5, ist der VirtualChannel für Cherry eGK Geräten noch parallel zu Cherry USB2LAN Proxy enthalten.

Wenn Sie das G87-1504/ST-1503 wie bisher weiter verwenden möchten, müssen Sie ab Firmware-Version 10.05.100 den Proxy aktivieren. Alle Einstellung werden automatisch übernommen und laufen über den Anschluss im Netzwerk.

### Nutzung des G87-1504/ST-1503 mit der Firmware-Version 10.05.100 und höher:

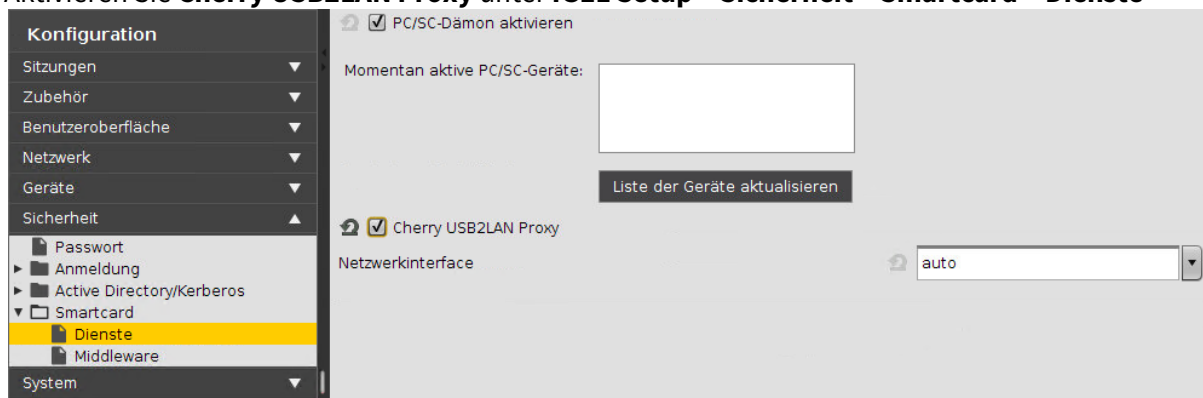
- Aktivieren Sie den Proxy - Dies kann auch aus dem Backend heraus erfolgen.



- Cherry USB2LAN Proxy (Unter Smartcard) (siehe Screenshot)
- IGEL Gerät, gültig für Cherry-Geräte G87-1505, G87-1504/ST-1503 zu USB

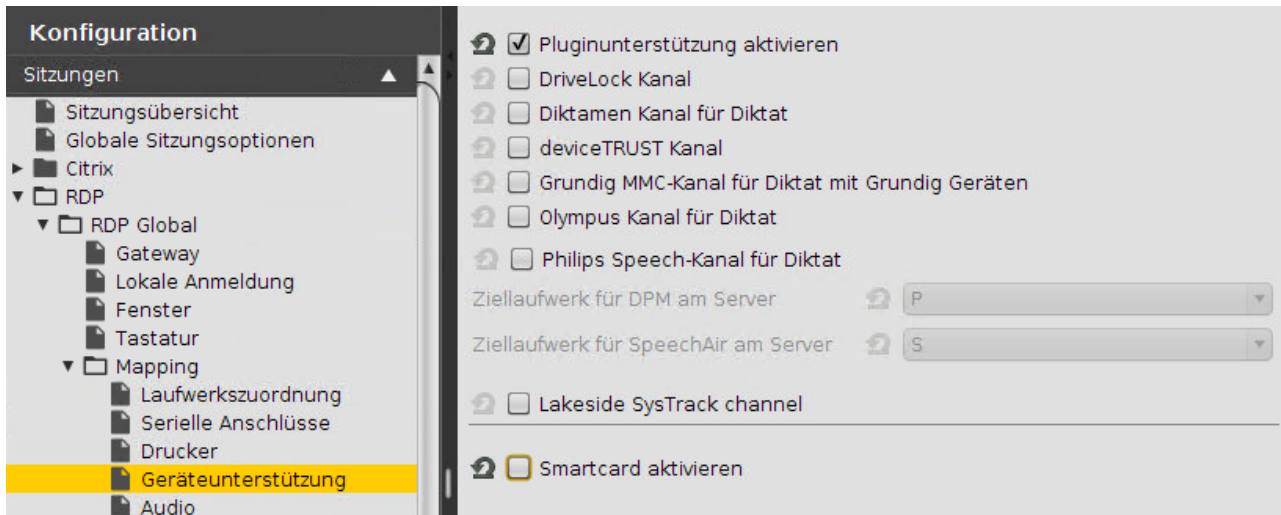
### Für IGEL Lx v5 und OS10:

- Aktivieren Sie **Cherry USB2LAN Proxy** unter **IGEL Setup > Sicherheit > Smartcard > Dienste**



### Für IGEL Lx v5:

- Deaktivieren Sie **Cherry Cannel 0** und **Cherry Cannel 1** unter **IGEL Setup > Sitzungen > RDP > RDP Global > Mapping > Geräteunterstützung**
- Aktivieren Sie die Smartcard nicht



Installieren Sie die Cherry eGK KVK Software auf dem Server. Siehe [https://www.cherry.de/files/software/Cherry-eGK-KVK\\_Software\\_33.zip](https://www.cherry.de/files/software/Cherry-eGK-KVK_Software_33.zip)

Installieren Sie die Cherry Linux Software auf dem Gerät.

- In der CT-API Konfiguration kann das G87-1504/ST-1503 als Netzwerkgerät konfiguriert werden.
- Link zur Doku Client Serverintegration: [https://www.cherry.de/files/manual/64410063-01\\_USBLANProxyClientServerUndCitrix.pdf](https://www.cherry.de/files/manual/64410063-01_USBLANProxyClientServerUndCitrix.pdf)
- Link zur Dokumentation der Softwarearchitektur: [https://www.cherry.de/files/manual/Cherry-eGK-KVK\\_Software-Architektur\\_Windows-20130927-v04.pdf](https://www.cherry.de/files/manual/Cherry-eGK-KVK_Software-Architektur_Windows-20130927-v04.pdf)

- i** Der VirtualChannel wurde aufgrund folgender Schwierigkeiten und der zukünftigen Nutzung der Telematikinfrastruktur ersetzt (siehe auch gematik Anforderung Ian)
- Unabhängig von der Citrix Version (keine Kompatibilitätsprüfung mehr notwendig)
  - Unabhängig von der Server Version (2008, 2012 ...), wenn die Verbindung über RDP läuft.

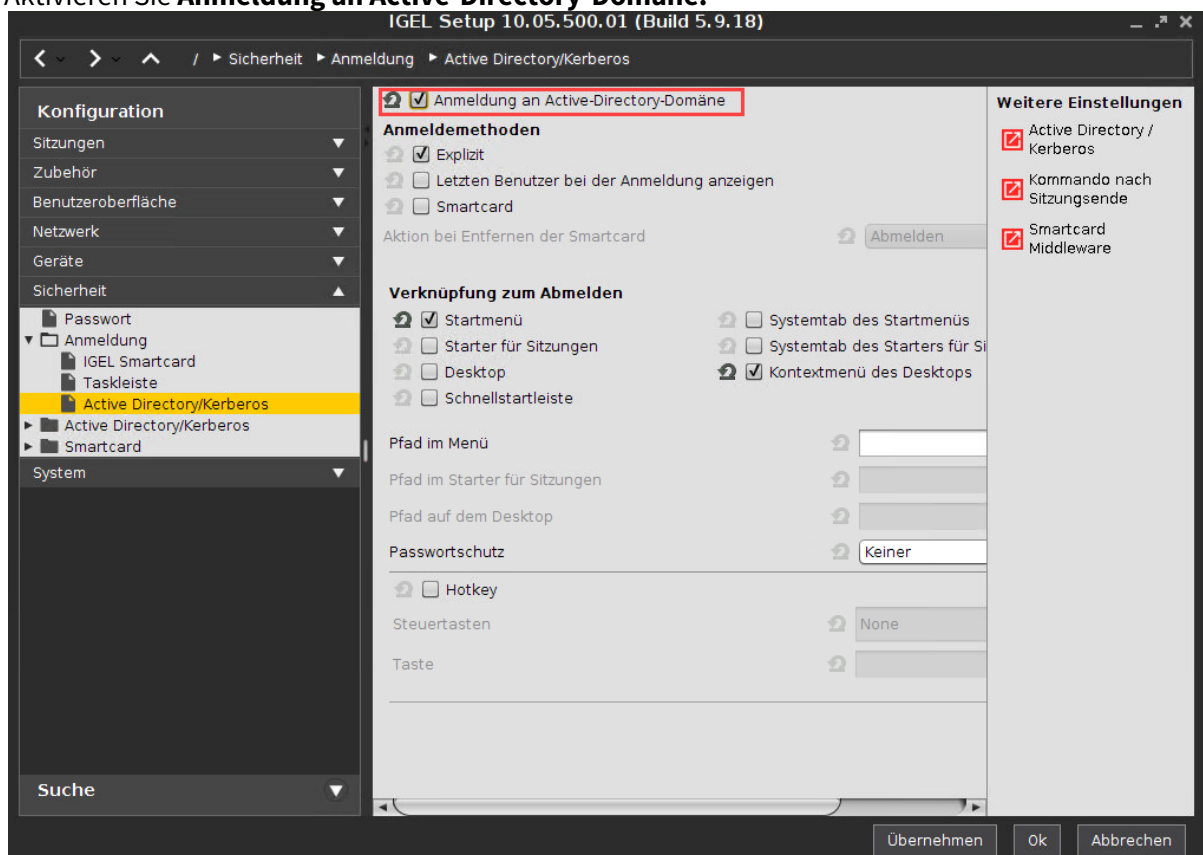
## Single Sign-on für den Browser Proxy

Die Verwendung eines Proxys zur Abwicklung des Internetverkehrs eines Browsers bietet zusätzliche Sicherheit und Kontrolle. Wenn der Proxy jedoch Passwort-authentifiziert ist, muss der Benutzer seine Anmeldeinformationen eingeben, was zusätzliche Unannehmlichkeiten mit sich bringt.

Ab IGEL Linux Version 5.08 oder neuer und IGEL Linux Version 10.01.100 oder neuer können Sie diese Unannehmlichkeiten durch die Passthrough-Funktion vermeiden.

### Single Sign-on für den Browser-Proxy aktivieren:

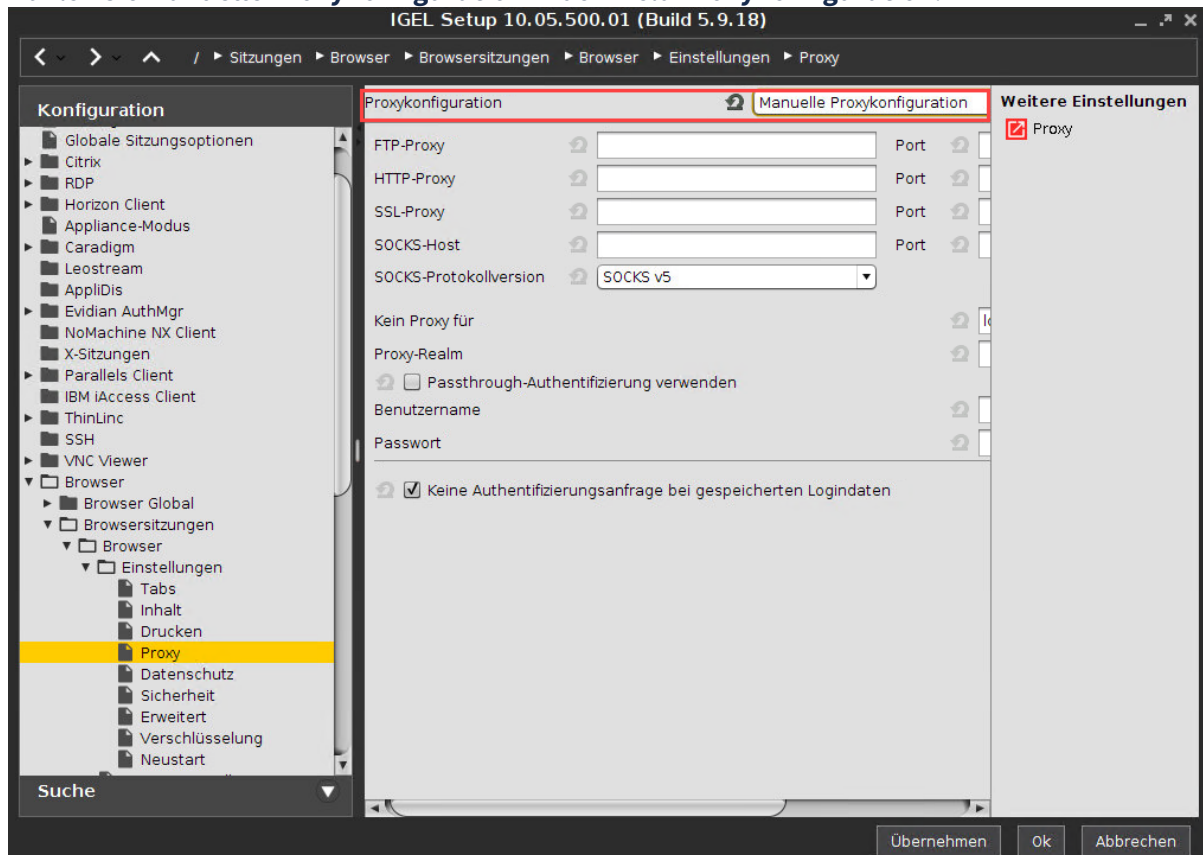
1. Öffnen Sie Setup und gehen Sie zu **Sicherheit > Anmeldung > Active Directory/Kerberos**.
2. Aktivieren Sie **Anmeldung an Active-Directory-Domäne**.



3. Gehen Sie auf **Sitzungen > Browser > Browsersitzungen > [Name der Browsersitzung] > Einstellungen > Proxy**.



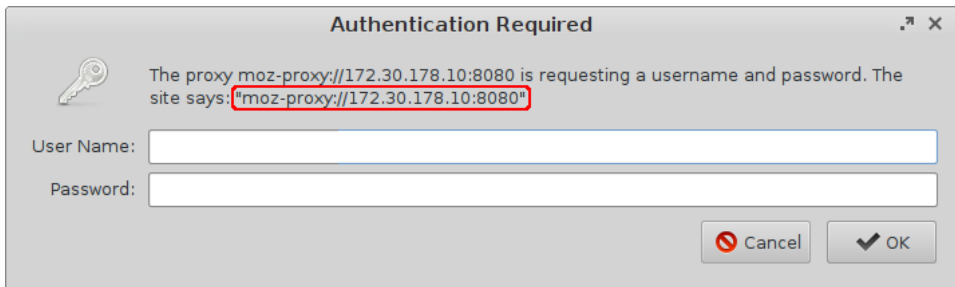
#### 4. Wählen Sie **Manuelle Proxykonfiguration** in dem Feld **Proxykonfiguration**.



#### 5. Für einen HTTP Proxy, wählen Sie folgende Einstellungen:

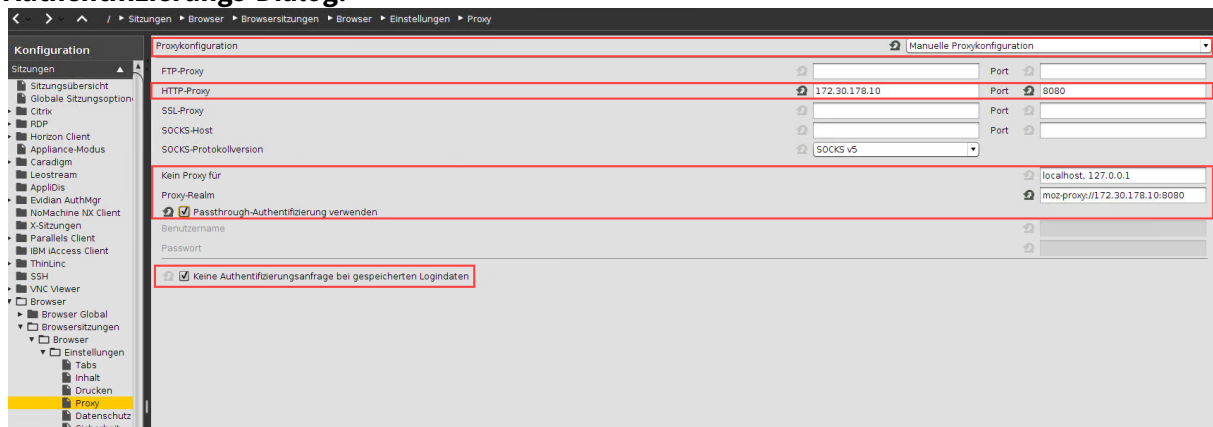
- **HTTP-Proxy:** Verwenden Sie die IP-Adresse oder den Hostname des Proxy.
- **Port:** Port des Proxy für HTTP
- **Kein Proxy für:** IP-Adressen oder Host-Namen, auf die direkt zugegriffen werden kann.
- **Proxy-Realm:** Bereich, in dem sich der Browser für den Proxy authentifiziert. Diese Informationen sind zusammen mit dem Benutzernamen und Passwort für die Authentifizierung erforderlich.

**i** Das **Proxy-Realm** Feld ist intern mit dem Wert `moz-proxy:// [HTTP Proxy]: [Port]` vorausgefüllt. Wenn das Feld leer ist, wird der Wert bei der Authentifizierung des Browsers verwendet. Wenn der Proxy einen weiteren unbekanntenen Wert für den Proxy-Realm erwartet, können Sie folgendes bestimmen: Lassen Sie die Felder **Benutzername** und **Passwort** leer und starten Sie den Browser. Das Dialog-Fenster, das erscheint, wird den richtigen Wert für das **Proxy-Realm** Feld enthalten.



Im obigen Beispiel, ist der Wert für das **Proxy-Realm** Feld folgender: moz-proxy://172.30.178.10:8080

- **Passthrough-Authentifizierung verwenden:** Muss aktiviert sein, um den Single Sign-on für den Browser-Proxy zu erlauben.
- **Keine Authentifizierungsanfrage bei gespeicherten Logindaten:** Muss aktiviert sein, um eine nahtlose Single Sign-on für den Browser-Proxy zu ermöglichen; unterdrückt den **erforderlichen Authentifizierungs-Dialog.**



Wenn sich der Nutzer beim nächsten Mal am Gerät anmeldet, ist der Browser-Proxy betriebsbereit.

## Anzahl der zulässigen Anmeldeversuche begrenzen

### Symptom

Benutzer können versuchen, sich so oft und so schnell wie möglich am Bildschirm anzumelden, um die Sperre aufzuheben und lokale Anmeldeaufforderungen zu stellen (z.B. für Kerberos, Shared Workplace, IGEL Smartcard).

### Problem

Dies macht das System und die Remote-Sitzungen anfällig für Brute-Force-Login-Angriffe.


### Lösung

Ab IGEL OS 10.03.100 ist die Anzahl der Anmeldeversuche innerhalb von 30 Sekunden auf 5 begrenzt.

Dieser Wert kann im System Registry geändert werden:

1. Gehen Sie im Setup unter **System > Registry**.
2. Geben Sie in der Parametersuche `auth.login.lockout_threshold` ein um die maximale Anzahl an Login- oder Entsperrversuchen innerhalb des angegebenen Intervalls einzustellen.
3. Geben Sie in der Parametersuche `auth.login.lockout_duration` ein um die Zeitspanne für das Zählen von Login- und Entsperrversuchen in Sekunden anzugeben.
4. Klicken Sie **Übernehmen** oder **Ok**.

## How to Deploy Device Encryption

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Sicherheit: Timeout für Sicheres Spiegeln and Sicheres Terminal

### Überblick

Um eine Denial-of-Service-Attacke durch Blockieren des Ports 30022 zu vermeiden, der für Sicheres Spiegeln (Secure VNC) und Sicheres Terminal verwendet wird, kann ein Timeout konfiguriert werden. Dieser Timeout begrenzt den Aufbau von Verbindungen zu Port 30022. Die Dauer beträgt standardmäßig 180 Sekunden und kann über eine Umgebungsvariable geändert werden.

### Timeout konfigurieren

1. Öffnen Sie den UMS Konfigurationsdialog oder das lokale Setup und gehen Sie zu **System > Firmwareanpassung > Umgebungsvariablen > Vordefiniert**.
2. Geben Sie die folgenden Daten ein und klicken Sie **Ok**:
  - **Name der Variablen:** IGEL\_TLS\_TUNNEL\_TIMEOUT
  - **Wert:** Timeout in Sekunden. Der Wertebereich ist 0 bis 180. Wenn der Wert auf 0 gesetzt wird, gibt es keinen Timeout.

Name der Variablen	Wert
IGEL_TLS_TUNNEL_TIMEOUT	30

Übernehmen Ok Abbrechen

Einige Dienste werden auf dem Gerät neu gestartet. Danach wird die neue Umgebungsvariable gesetzt und der Timeout ist gesetzt.

## Entschärfung der Terrapin-Schwachstelle durch Registry-Parameter in IGEL OS

Um ISN 2023-39: SSH Terrapin Vulnerability zu entschärfen, können Sie einen Registrierungsparameter aktivieren, der schwache MACs und Chipper deaktiviert, um Terrapin-Angriffe zu verhindern. Weitere Informationen zu Terrapin-Angriffen und der damit verbundenen CVE-2023-48795 finden Sie unter <https://terrapin-attack.com/> und <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-48795>.

**i** Wenn Sie OpenSSH 9.6p1 sowohl auf dem Client als auch auf dem Server verwenden, ist die Verwendung dieses Registrierungsparameters nicht erforderlich. IGEL OS-Versionen 11.09.210 oder höher verwenden die neueste Version von OpenSSH 9.6p1. Wenn Sie diese Version oder eine neuere auf der Gegenstelle verwenden, wird automatisch die neue "strenge KEX"-Protokollerweiterung verwendet.

So aktivieren Sie die Terrapin-Abschwächung über den Registrierungsparameter:

1. Gehen Sie im IGEL Setup zu **System > Registry > network > ssh\_server > enable\_terrapi\_n\_mitigation**.
2. Aktivieren Sie den Parameter.
3. Klicken Sie auf **Übernehmen** oder **OK**, um die Änderung zu speichern.

Die folgenden für Terrapin-Angriffe anfälligen Optionen sind deaktiviert:

- die ChaCha20-Poly1305-Chiffre
- alle -cbc ciphers
- alle -ctr ciphers
- alle -etm@openssh.com macs

**i** Wenn Sie SSH vollständig deaktivieren möchten, folgen Sie den Anweisungen unter [SSH-Server deaktivieren](#) (see page 476).

## Zertifikate


- [Einspielung und Erneuerung von Zertifikaten mit SCEP \(NDES\) \(see page 505\)](#)
- [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen \(see page 523\)](#)
- [Welche CA-Zertifikate sind in IGEL OS enthalten? \(see page 527\)](#)



## Einspielung und Erneuerung von Zertifikaten mit SCEP (NDES)

SCEP ist ein Protokoll für das Zertifikatsmanagement und unterstützt die sichere Herausgabe von Zertifikaten an Netzwerkgeräte.

### Voraussetzungen

 Die Anwendung des Microsoft-Patches [KB5014754](https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16)<sup>41</sup> auf Ihren NDES-Server kann dazu führen, dass Zertifikatsanforderungen von Clients, die SCEP-Clients zur Authentifizierung verwenden, nicht mehr funktionieren. Dies gilt auch für IGEL OS Geräte. Derzeit gibt es keinen offiziellen Workaround oder Patch von Microsoft.

- SCEP-Server  
Folgende Versionen von Windows Server werden unterstützt:
  - Windows 2008 Server mit der Serverrolle "Registrierungsdienst für Netzwerkgeräte" (NDES)
  - Windows 2012 Server
  - Windows 2016 ServerFür Informationen über NDES siehe <http://aka.ms/ndes>.
- Eine Verbindung zwischen dem SCEP-Server und der Zertifizierungsstelle.

In diesem Dokument wird die Einspielung von Zertifikaten mithilfe von SCEP beschrieben.

- [Technische Grundlagen](#) (see page 506)
- [Details der Client-Registrierung](#) (see page 508)
- [Konfiguration des SCEP-Clients](#) (see page 510)
- [Dateien](#) (see page 520)
- [Fehlerbehebung](#) (see page 521)

---

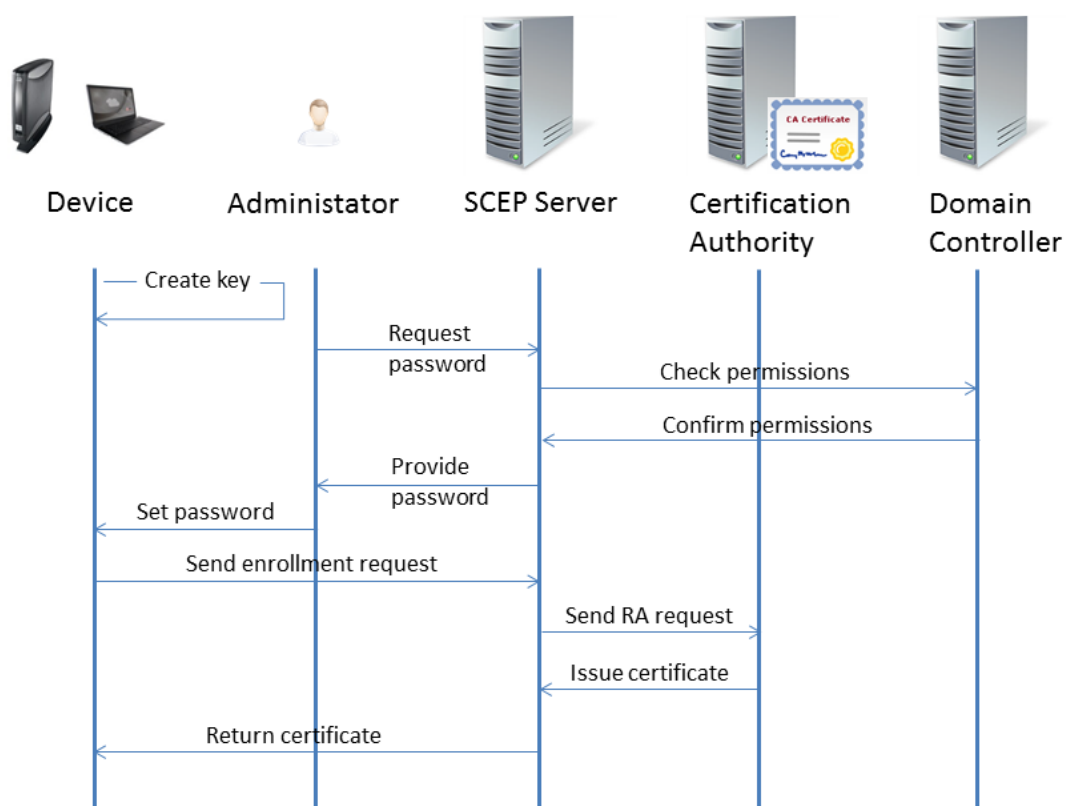
<sup>41</sup> <https://support.microsoft.com/en-us/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16>

## Technische Grundlagen

Das Simple Certificate Enrollment Protocol (SCEP) definiert eine Vorgehensweise zum automatischen Einspielen von Zertifikaten für die Authentifizierung von Netzwerkgeräten oder VPNs. Der Client verwendet HTTP zum Empfangen von Wurzelzertifikaten, dem Senden von Zertifikatsanfragen sowie dem Empfangen von Client-Zertifikaten vom Server.

Eine detaillierte Beschreibung finden Sie in folgendem Artikel von Microsoft TechNet: <https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx>


In nachfolgender Darstellung ist ein typischer Registrierungsstelle dargestellt.



1. Das Gerät erzeugt ein RSA-Public-Private-Schlüsselpaar.
2. Der Administrator fordert beim SCEP-Dienst ein Challenge-Passwort an.

**i** Das Challenge-Passwort wird nur bei der erstmaligen Registrierung benötigt. Bei Zertifikatserneuerungen wird das aktuelle Zertifikat zur Authentifizierung verwendet.


3. Der SCEP-Server fragt beim Domänencontroller an, ob der Administrator über die für die konfigurierten Zertifikatsvorlagen erforderlichen Rechte verfügt.
4. Der Domänencontroller bestätigt, dass der Administrator über die erforderlichen Rechte verfügt.
5. Der SCEP-Server erzeugt ein Challenge-Passwort und überträgt es zum Administrator.

 Normalerweise verfällt das Challenge-Passwort nach einer bestimmten Zeit. Beim in Windows 2008 enthaltenen NDES beträgt diese Zeit standardmäßig 60 Minuten.

6. Das Challenge-Passwort, der CA-Identifizierer sowie der Fingerprint des CA-Zertifikats werden vom Administrator dem Client bereitgestellt.
7. Das Gerät sendet die Registrierungsanfrage an den SCEP-Server, wobei es zur Authentifizierung das Challenge-Passwort verwendet. Dieser Vorgang wird vom Administrator ausgelöst.
8. Der SCEP-Server signiert das Registrierungszertifikat mit dem Enrollment-Agent-Zertifikat und sendet es an die Certificate Authority (CA).
9. Die CA stellt das angeforderte Zertifikat aus und sendet es an den SCEP-Server.
10. Der SCEP-Server sendet das Zertifikat an das Gerät.

## Details der Client-Registrierung

In diesem Abschnitt werden die Details der eigentlichen Zertifikatsregistrierung beschrieben. Der hier beschriebene Prozess entspricht den Schritten 7 bis 10 im [Gesamtprozess](#) (see page 506).

 Die Registrierungsanfrage und die Antwort der CA enthalten den req

1. Der Client erfragt vom SCEP-Server das öffentliche Zertifikat der CA.
2. Der SCEP-Server sendet das öffentliche Zertifikat der CA an den Client.
3. Der Client prüft das öffentliche Zertifikat der CA gegen den relevanten Fingerprint. Der Fingerprint ist vom Administrator mithilfe von einem UMS-Profil bereitgestellt worden; siehe [Die Zertifizierungsstelle festlegen](#) (see page 515).
4. Der Client sendet eine Registrierungsanfrage an den SCEP-Server. Der Registrierungsanfrage ist eine HTTP-Anfrage vom Typ GET und enthält folgende Daten:

Signed data PKCS7	Enveloped data PKCS7	Certificate Signing Request (PKCS 10)
Version		
Hashing algorithm		
Signed (unencrypted) data:	Version	
Recipient and related encrypted data encryption key; the recipient is the CA.		
Encrypted data: (encrypted with a randomly generated key that is encrypted with the recipient's public key)	Version	
Requested subject name		
Public key of client		
Challenge password		
Requested extensions		
Signature algorithm		
Digital signature		
Client certificate		
Digital signature		

5. Wenn die Anfrage erfolgreich war, beinhaltet die HTTP-Antwort des SCEP-Servers folgende Daten:

Signed data PKCS7	Enveloped data PKCS7	Degenerate Certificates (only PKCS7)
Version		
Hashing algorithm		
Signed (unencrypted) data:	Version	
List of recipients		
Encrypted data:	Version	
Issued X.509 certificate		
CA certificate		
Digital signature		

## Konfiguration des SCEP-Clients

Die Konfiguration des SCEP-Clients auf dem Gerät mit IGEL OS erfolgt wie folgt:

- [Profile in der UMS erstellen \(see page 511\)](#)
- [Den SCEP-Client aktivieren \(see page 512\)](#)
- [Daten für die Zertifikatsignierungsanforderung \(CSR\) eingeben \(see page 513\)](#)
- [Die Zertifizierungsstelle festlegen \(see page 515\)](#)
- [Daten des SCEP-Servers festlegen \(see page 517\)](#)
- [Geräten das Profil zuweisen \(see page 518\)](#)

## Profile in der UMS erstellen

1. Klicken Sie im Strukturbaum der UMS mit der rechten Maustaste auf das Verzeichnis **Profile**.
2. Wählen Sie im Kontextmenü **Neues Profil**.
3. Geben Sie einen **Profilname** ein.
4. Wählen Sie bei **Basiert auf** die Firmwareversion, die auf den Geräten, um die es geht, installiert ist.
5. Klicken Sie **Ok**.  
Der Konfigurationsdialog öffnet sich. Der Konfigurationsdialog entspricht dem IGEL Setup auf den Geräten, denen das Profil zugewiesen wird.

## Den SCEP-Client aktivieren

1. Gehen Sie zu **Netzwerk > SCEP-Client (NDES)**.
2. Aktivieren Sie **Zertifikate mit SCEP (NDES) verwalten**.



## Daten für die Zertifikatsignierungsanforderung (CSR) eingeben

- Gehen Sie zu **Netzwerk > SCEP-Client (NDES) > Zertifikate** und geben Sie die folgenden Daten ein:

**Typ des CommonName/SubjectAltName:** Das Merkmal zur Bindung des Zertifikats an das Gerät.

- IP-Adresse: Die IP-Adresse des Geräts.
- DNS-Name: Der DNS-Name des Geräts.
- IP-Adresse (auto): Die IP-Adresse des Geräts (wird automatisch eingefügt).
- DNS-Name (auto): Der DNS-Name des Geräts (wird automatisch eingefügt).
- E-Mail-Adresse: Eine E-Mail-Adresse.
- DNS-Name als UPN (auto)

**i** Für ein Clientzertifikat des Geräts bietet sich der Typ **DNS-Name (auto)** an, falls der Client seinen Netzwerknamen automatisch bezieht.

Der folgende Parameter ist verfügbar, wenn **Typ des CommonName/SubjectAltName** auf **IP-Adresse**, **DNS-Name** oder **E-Mail-Adresse** eingestellt ist:

**CommonName/SubjectAltName:** Geben Sie eine zum **Typ des CommonName/SubjectAltName** passende Bezeichnung ein. Bei manchen Typen erfolgt das automatisch, dann ist keine Eingabe möglich.

Der folgende Parameter ist verfügbar, wenn **Typ des CommonName/SubjectAltName** auf **IP-Adresse (auto)**, **DNS-Name (auto)** oder **DNS-Name als UPN (auto)** eingestellt ist:

**Suffix von CommonName/SubjectAltName:** Gibt ein Suffix an, das an **CommonName/SubjectAltName** angehängt wird.

Mögliche Optionen:

- "<leer>": Kein Suffix wird hinzugefügt.
- ".<DNS-Domäne (auto)>": Der durch einen Punkt getrennte aktuelle DNS-Domänenname des Systems wird hinzugefügt. Beispiel: `.igel.local`
- Freie Texteingabe: Das manuell eingegebene Suffix wird hinzugefügt. Beachten Sie, dass das Prozentzeichen "%" als Einleitung einer Escape-Sequenz verwendet wird und die folgenden Ersetzungen dementsprechend automatisch erfolgen:
  - % D wird durch den DNS-Domänennamen des Systems ersetzt, der zum Zeitpunkt der Erstellung der Zertifikatsignierungsanforderung (CSR) verwendet wird. Beispiel: @% D wird durch @ igel.de ersetzt, falls der aktuelle DNS-Domänenname des Systems igel.de ist.
  - %% wird durch % ersetzt. Beispiel: A %% B wird durch A % B ersetzt.
  - Andere Zeichenkombinationen mit % werden derzeit verworfen. Beispiel: A % BC wird durch A C ersetzt.

**i** Wenn Sie das Suffix manuell eingeben müssen, achten Sie darauf, dass Sie das Trennzeichen eingeben.

**Organisationseinheit:** Wird von der Zertifizierungsstelle vorgegeben.

**Organisation:** Frei definierbare Bezeichnung der Organisation, welcher der Client angehört.

**Ort:** Örtliche Zuordnung des Geräts. Beispiel: "Augsburg".

**Bundesland:** Örtliche Zuordnung des Geräts. Beispiel: "Bayern".

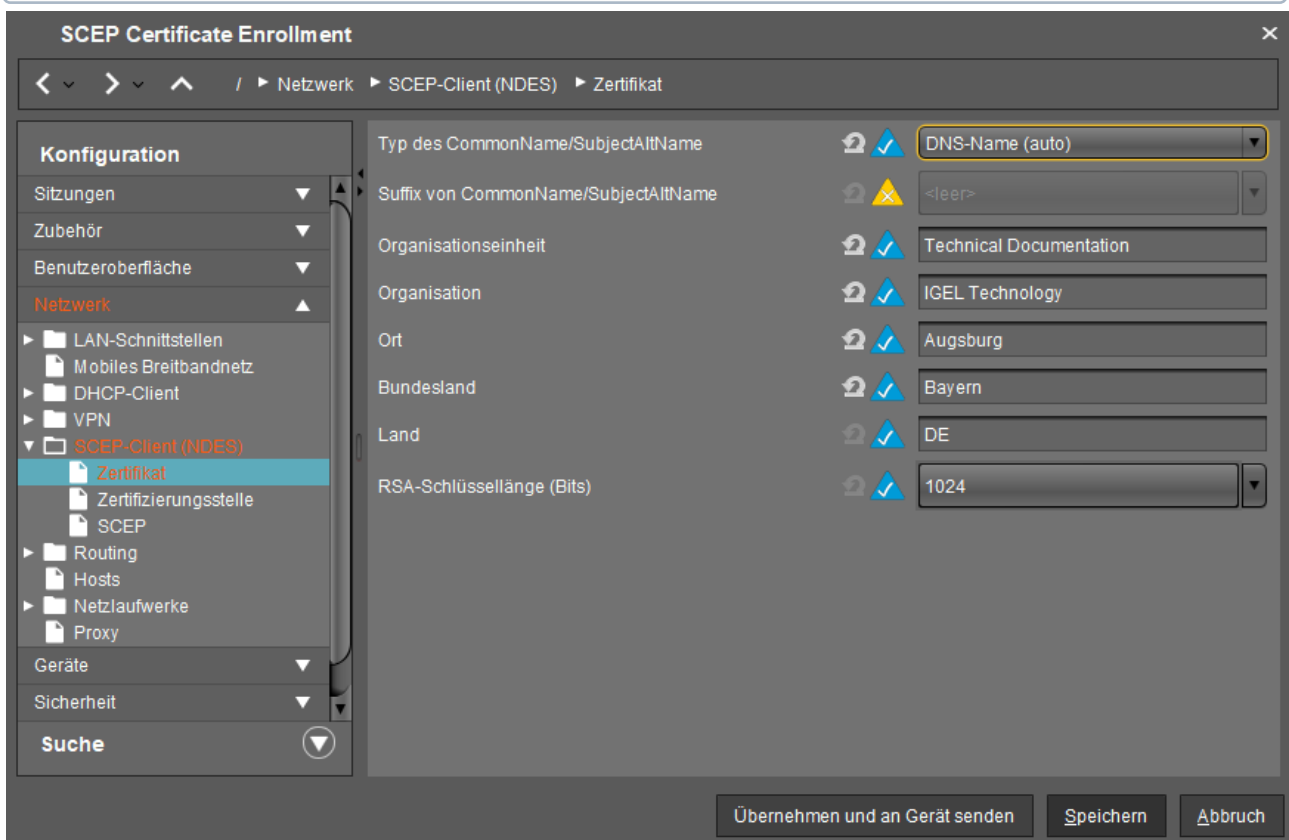
**Land:** Zweistelliger ISO 3166-1 Ländercode. Beispiel: "DE".

**RSA-Schlüssellänge (Bits):** Wählen Sie eine (von der Zertifizierungsstelle verwendbare) Schlüssellänge für das auszustellende Zertifikat.

Mögliche Werte:

- "1024"
- "2048"
- "4096"

**i** Die hier angegebene RSA-Schlüssellänge darf nicht niedriger sein als die auf dem Server konfigurierte Mindestschlüssellänge.



**SCEP Certificate Enrollment**

Netzwerk > SCEP-Client (NDES) > Zertifikat

**Konfiguration**

- Sitzungen
- Zubehör
- Benutzeroberfläche
- Netzwerk**
  - LAN-Schnittstellen
  - Mobiles Breitbandnetz
  - DHCP-Client
  - VPN
  - SCEP-Client (NDES)**
    - Zertifikat**
    - Zertifizierungsstelle
    - SCEP
  - Routing
  - Hosts
  - Netzlaufwerke
  - Proxy
- Geräte
- Sicherheit
- Suche

Typ des CommonName/SubjectAltName: DNS-Name (auto)

Suffix von CommonName/SubjectAltName: <empty>

Organisationseinheit: Technical Documentation

Organisation: IGEL Technology

Ort: Augsburg

Bundesland: Bayern

Land: DE


RSA-Schlüssellänge (Bits): 1024

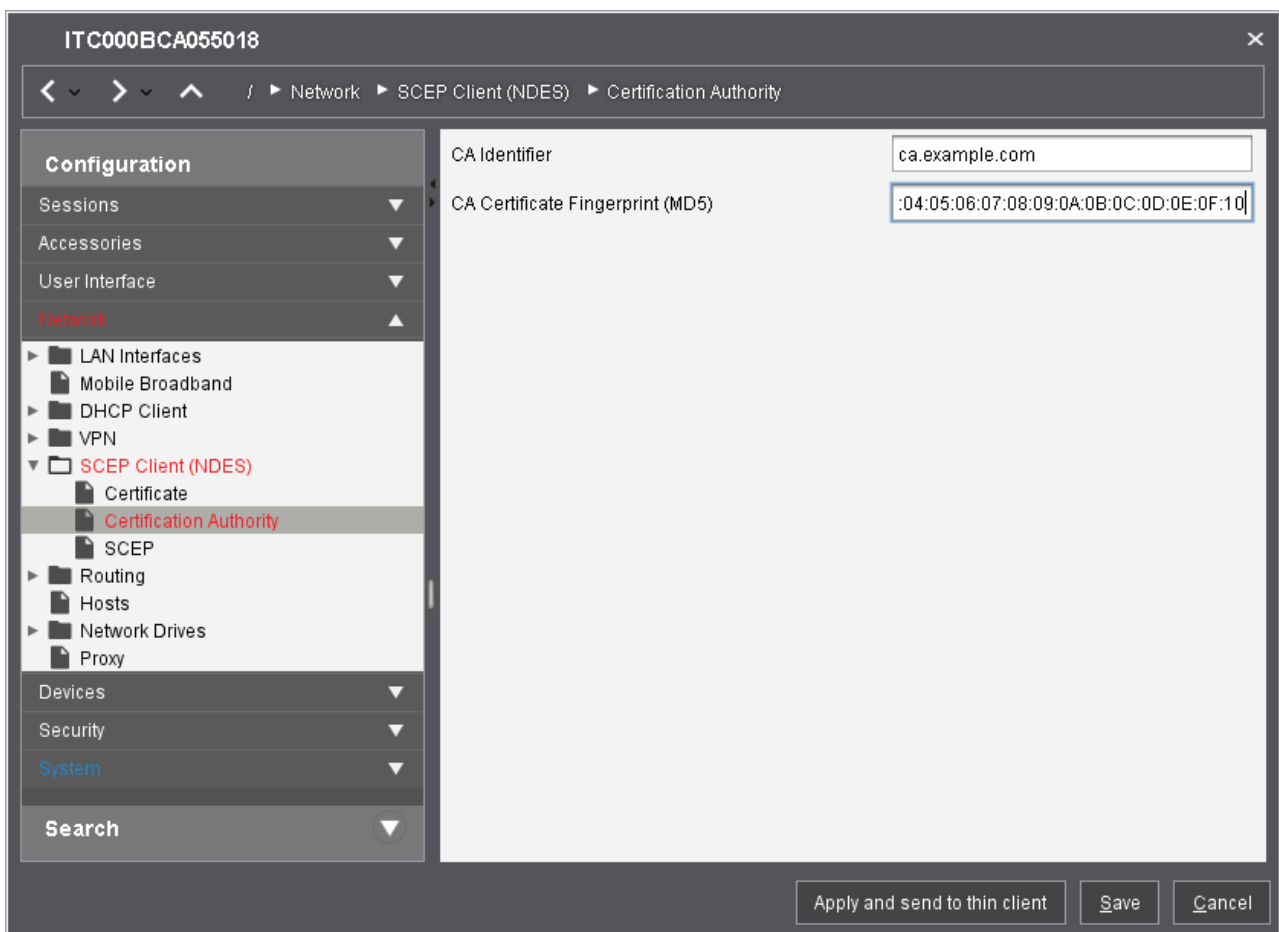
Übernehmen und an Gerät senden | Speichern | Abbruch

## Die Zertifizierungsstelle festlegen

1. Gehen Sie zu **Netzwerk > SCEP-Client (NDES) > Zertifizierungsstelle**.
2. Geben Sie die Daten der Zertifizierungsstelle ein:
  - **Kenntung der Zertifizierungsstelle:** FQDN (Fully Qualified Domain Name) der Zertifizierungsstelle
  - **CA Certificate Fingerprint (MD5):** Fingerprint des CA-Zertifikats in der Form

01:02:03:04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10


 Der NDES-Server stellt den Fingerprint unter folgender URL bereit: `https://<NDES Servername>/certsrv/mscep_admin`




Wenn der Fingerprint des CA-Zertifikats angegeben wird, überprüft der Client mit dessen Hilfe die Integrität des vom SCEP-Server erhaltenen CA-Zertifikats.


## Daten des SCEP-Servers festlegen

1. Gehen Sie zu **Netzwerk > SCEP-Client (NDES) > SCEP**.
2. Geben Sie die folgenden Daten ein:
  - **SCEP-Server-URL**: URL, über die der SCEP-Client mit dem SCEP-Server kommuniziert.

 HTTPS wird nicht unterstützt; trotzdem findet die Übertragung von sicherheitskritischen Daten zwischen dem SCEP-Client und anderen Komponenten verschlüsselt statt.

- **Proxyserver für SCEP-Anfragen** (optional): IP-Adresse oder Hostname des Proxy-Servers, der für die Kommunikation zwischen dem Gerät und dem SCEP-Server verwendet wird. Wird anstelle eines Proxys eine Web Application Firewall verwendet, muss hier deren IP-Adresse oder Hostname des Proxy-Servers eingetragen werden.
- **Anfragepasswort**: Passwort, das der SCEP-Client dem SCEP-Server in seiner Anfrage (CSR) mitteilen muss.


 Auf einem Microsoft NDES-Server können Sie das Passwort standardmäßig unter `https:///certsrv/mscep_admin` abrufen.

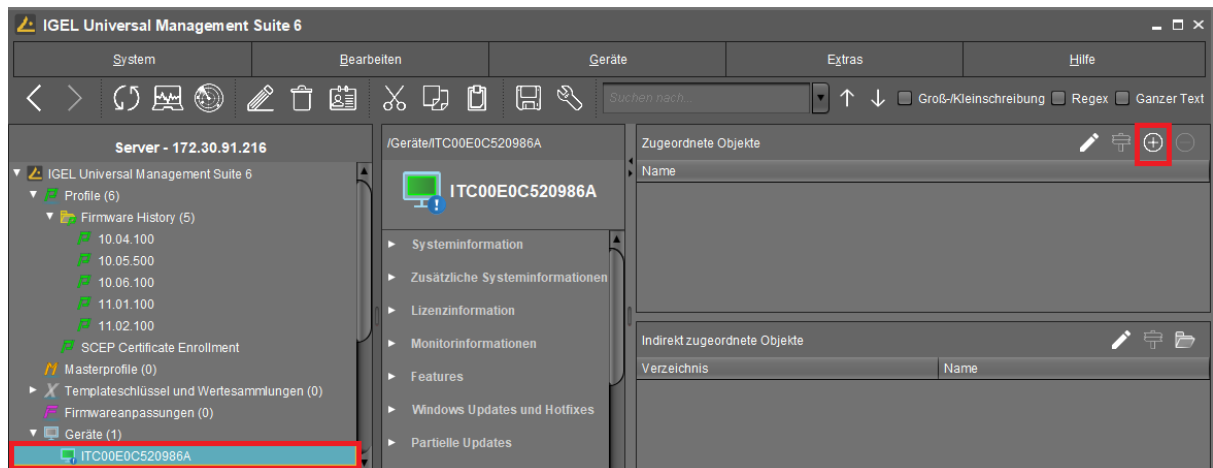
 Standardmäßig ist das Passwort auf einem Microsoft NDES-Server eine Stunde lang gültig und kann nur einmal verwendet werden. Um das Passwort auf mehreren Geräten verwenden zu können, müssen zusätzliche Einstellungen auf dem NDES-Server vorgenommen werden, siehe "Password and Password Cache" auf <https://social.technet.microsoft.com><sup>42</sup>.

- **Zeitraum für Zertifikatserneuerung (Tage)**: Zeitintervall vor Ablauf des Zertifikats, nach dem der Zertifikatsverlängerungsvorgang gestartet wird. (Standard: 30)
  - **Prüfintervall für Zertifikatsablauf (Tage)**: Gibt an, wie oft das Zertifikat gegen sein Ablaufdatum geprüft wird. (Standard: 1)
3. Speichern Sie die Einstellungen.

<sup>42</sup> <https://social.technet.microsoft.com/wiki/contents/articles/9063.active-directory-certificate-services-ad-cs-network-device-enrollment-service-ndes.aspx>

## Geräten das Profil zuweisen

1. Selektieren Sie im Strukturbaum unter **Geräte** alle Geräte, denen Sie das Profil zuweisen wollen.
2. Klicken Sie im Bereich **Zugeordnete Objekte** auf .



3. Selektieren Sie im Dialog **Zuweisbare Objekte auswählen** das relevante Profil und weisen Sie es durch Klick auf  zu.



4. Klicken Sie **Ok**.
5. Aktivieren Sie im Dialog **Änderungszeitpunkt** die Option **Sofort**.
6. Klicken Sie **Ok**.  
Auf dem Gerät werden die unter [Details der Client-Registrierung](#) (see page 508) beschriebenen Aktionen ausgeführt.

## Dateien

Alle wichtigen Dateien befinden sich im Verzeichnis `/wfs/scep_certificates/cert0`. Die folgenden fixen Dateinamen werden verwendet.


<code>cacert.pem</code>	CA-Zertifikat
<code>racert_enc.pem</code>	RA-Zertifikat, mit dem verschlüsselt wird used for encryption (optional)
<code>racert_sig.pem</code>	RA-Zertifikat, mit dem signiert wird (optional)
<code>client.csr</code>	Zertifikatsanforderung
<code>client.cert</code>	Client-Zertifikat
<code>client.key</code>	Privater Schlüssel des Client-Zertifikats



## Fehlerbehebung

- [Diagnostics \(see page 522\)](#)

## Diagnostics

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## Vertrauenswürdige Stammzertifikate in IGEL OS einspielen

IGEL OS wird mit einer Vielzahl von vertrauenswürdigen Stammzertifikaten bestimmter Zertifizierungsstellen (CAs) ausgeliefert. Eine vollständige Liste der vorinstallierten Root-Zertifikate finden Sie unter [Welche CA-Zertifikate sind in IGEL OS enthalten?](#) (see page 527)

Zertifikate, die mit diesen Stammzertifikaten signiert wurden, können zur Serverauthentifizierung und Verschlüsselung von ICA-, RDP-, Horizon- und Browser-Sitzungen verwendet werden. Mit ihnen kann auch der Ursprung von Java-Anwendungen verifiziert werden.

Trotzdem kann es vorkommen, dass das von Ihnen benötigte Stammzertifikat fehlt. In diesem Artikel erfahren Sie, wie Sie fehlende Stammzertifikate einspielen.

### Voraussetzungen

Das Zertifikat muss im Base64-Format mit der Erweiterung `.pem`, `.crt` oder `.cer` vorliegen.

Um das Format zu überprüfen, öffnen Sie das Zertifikat in einem Texteditor. Es soll eine folgende Form haben:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIQa64Bw7UV06dG
MRQwEgYKCZIm1ZPyLGQBGRYEdGVzdDEI
...
31NjPszgHJs9LmHM9mmy5q29z8B0GZUJl
JUzn3svfZTUzSxw+DXH9MdQPZvDcEMyxi
-----END CERTIFICATE-----
```

### Lösung

#### Zertifikate über die UMS bereitstellen

Wir empfehlen Ihnen, die IGEL Universal Management Suite (UMS) für die Bereitstellung von Zertifikaten zu verwenden, besonders wenn Sie dies für mehrere Endgeräte tun müssen.

Sie können Zertifikate in der UMS Konsole über **Dateien > Neue Datei** laden: Wählen Sie einfach Ihre Zertifikatsdatei unter **Lokale Datei** aus, wählen Sie die passende Klassifizierung des Zertifikats aus und weisen Sie die Zertifikatsdatei den gewünschten Geräten zu; siehe Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen.

Wir empfehlen Ihnen folgende Dateiübertragungstypen für die Verteilung von Zertifikaten über die UMS:

Typ	Verwendungszweck
Nicht definiert	Allzweckkategorie; Sie müssen Zugriffsrechte und den Besitzer manuell angeben.

Typ	Verwendungszweck
Webbrowserzertifikat	Serverauthentifizierung/Verschlüsselung von HTTPS-Websites in Browser
SSL-Zertifikat	Serverauthentifizierung/Verschlüsselung von ICA-, RDP- oder Horizon-Sitzungen Authentifizierung über Active Directory (AD)
Java Zertifikat	Authentifizierung/Verschlüsselung von Java-Anwendungen
IBM iAccess Zertifikat	Serverauthentifizierung und Verschlüsselung von IBM iAccess Sitzungen
Allgemeines Zertifikat (allzweck)	Mehrere Anwendungen, die ein Zertifikat brauchen, z. B. wenn Sie eine ICA-Sitzung im Browser oder eine sichere Java-Sitzung auf einer geschützten Website starten möchten.

Diese Dateiübertragungstypen verlangen keinen nachfolgenden Systemneustart.

### Zertifikate manuell bereitstellen

Wenn Sie Zertifikate manuell installieren möchten, lesen Sie [Zertifikate manuell in IGEL OS installieren \(see page 525\)](#).

## Zertifikate manuell in IGEL OS installieren

Ein gewünschtes Zertifikat ist in IGEL OS nicht vorinstalliert und Sie möchten IGEL Universal Management Suite (UMS) für die Zertifikatsbereitstellung aus irgendeinem Grund nicht verwenden, siehe [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen \(see page 523\)](#). In diesem Fall können Sie die Zertifikate manuell installieren. Für den manuellen Import von Zertifikaten kann ein USB-Stick verwendet werden.

### SSL Zertifikate (ICA, RDP, Horizon) importieren

Wenn ein CA-Zertifikat für RDP, ICA oder VMware Horizon fehlt, können Sie es von einem USB-Speichergerät auf das Endgerät kopieren:

1. Verbinden Sie Ihr USB-Speichergerät mit dem Endgerät.
2. Starten Sie eine **Terminalsitzung** oder drücken Sie [STRG]+[ALT]+[F11], um sich als **ROOT** auf der Linux-Konsole des Endgeräts anzumelden.
3. Erstellen Sie ein Verzeichnis für Zertifikate:  


```
mkdir /wfs/ca-certs
```
4. Wechseln Sie in das Verzeichnis:  

```
cd /wfs/ca-certs
```
5. Ermitteln Sie den Namen Ihres USB-Speichermediums:  

```
ls /userhome/media
```
6. Kopieren Sie das Zertifikat auf das Endgerät:  

```
cp /userhome/media/// /wfs/ca-certs
```
7. Überprüfen Sie, ob das Zertifikat übertragen wurde:  

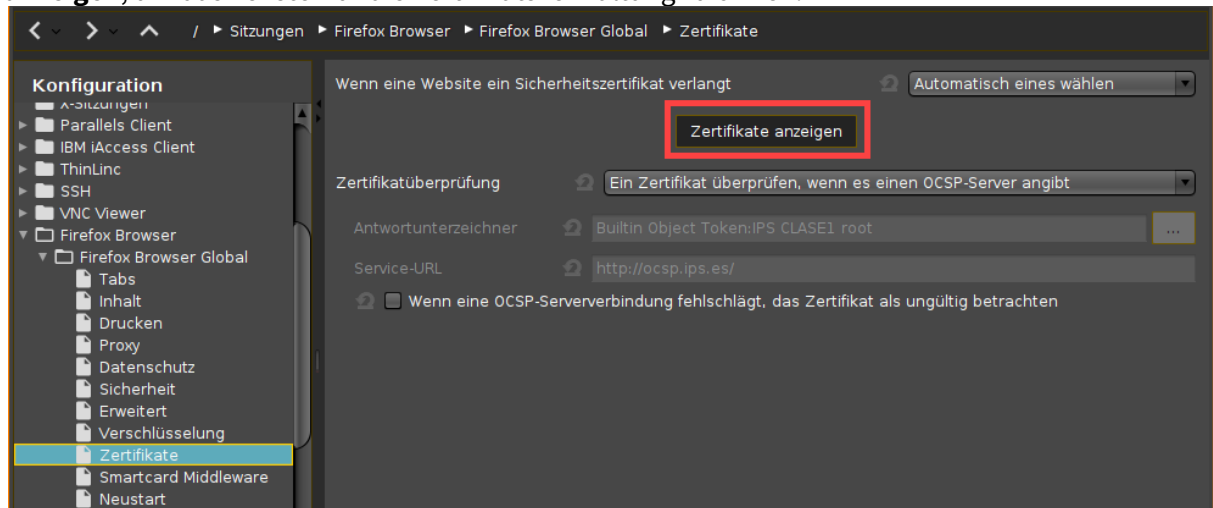
```
ls -al /wfs/ca-certs
```
8. Beenden Sie die Terminalsitzung oder drücken Sie [STRG]+[ALT]+[F1], um die Konsole zu verlassen.

 Die von Ihnen gespeicherten Zertifikate sind beim nächsten Neustart des Endgeräts verfügbar.

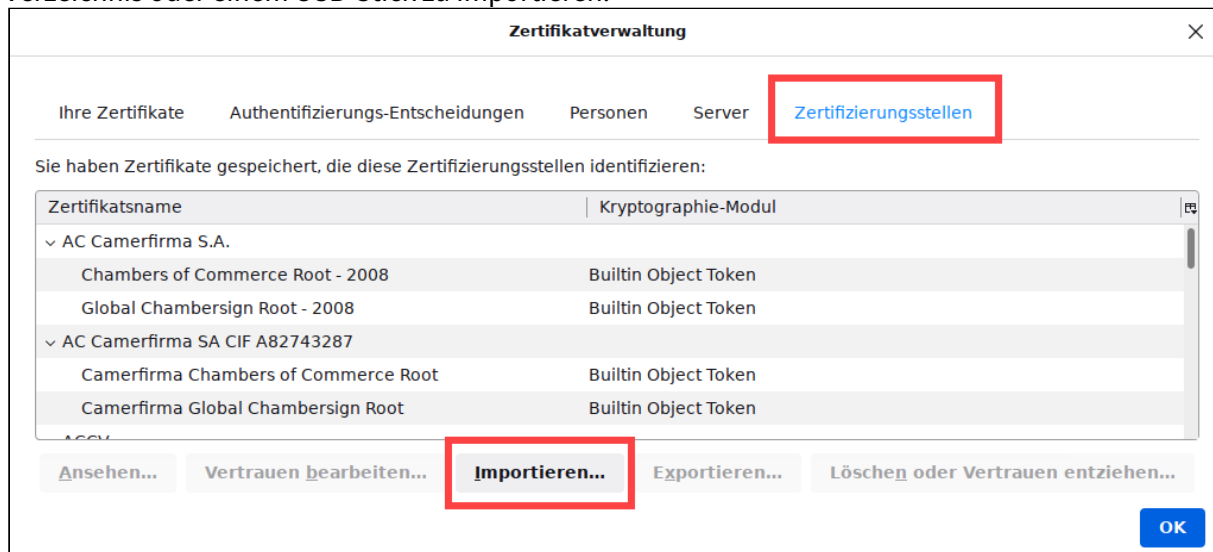
### Zertifikate für Webbrowser installieren

Verwenden Sie den **Firefox Certificate Manager**, um Webbrowser-Zertifikate manuell zu installieren:

1. Öffnen Sie das IGEL Setup.
2. Klicken Sie auf **Sitzungen > Firefox Browser > Firefox Browser Global > Zertifikate > Zertifikate anzeigen**, um das Fenster für die Zertifikatsverwaltung zu öffnen.



3. Klicken Sie unter **Zertifizierungsstellen** auf **Importieren...**, um ein neues Zertifikat aus einem Verzeichnis oder einem USB-Stick zu importieren.



 Manuell installierte Zertifikate werden ohne weitere Konfiguration dauerhaft gespeichert.

## Welche CA-Zertifikate sind in IGEL OS enthalten?

Die folgenden CA-Zertifikate sind in IGEL OS 11.08.330 enthalten:

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
ACCVRAIZ1	Dec 31 09:37:37 2030 GMT	ACCVRAIZ1.crt
AC RAIZ FNMT-RCM	Jan 1 00:00:00 2030 GMT	AC_RAIZ_FNMT-RCM.crt
AC RAIZ FNMT-RCM SERVIDORES SEGUROS	Dec 20 09:37:33 2043 GMT	AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt
ANF Secure Server Root CA	Aug 30 10:00:38 2039 GMT	ANF_Secure_Server_Root_CA.crt
Actalis Authentication Root CA	Sep 22 11:22:02 2030 GMT	Actalis_Authentication_Root_CA.crt
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT	AffirmTrust_Commercial.crt
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT	AffirmTrust_Networking.crt
AffirmTrust Premium	Dec 31 14:10:36 2040 GMT	AffirmTrust_Premium.crt
AffirmTrust Premium ECC	Dec 31 14:20:24 2040 GMT	AffirmTrust_Premium_ECC.crt
Amazon Root CA 1	Jan 17 00:00:00 2038 GMT	Amazon_Root_CA_1.crt
Amazon Root CA 2	May 26 00:00:00 2040 GMT	Amazon_Root_CA_2.crt
Amazon Root CA 3	May 26 00:00:00 2040 GMT	Amazon_Root_CA_3.crt
Amazon Root CA 4	May 26 00:00:00 2040 GMT	Amazon_Root_CA_4.crt

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
Atos TrustedRoot 2011	Dec 31 23:59:59 2030 GMT	Atos_TrustedRoot_2011.crt
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT	Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt
Autoridad de Certificacion Firmaprofesional CIF A62634068	May 5 15:22:07 2036 GMT	Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068_2.crt
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT	Baltimore_CyberTrust_Root.crt
Bypass Class 2 Root CA	Oct 26 08:38:03 2040 GMT	Bypass_Class_2_Root_CA.crt
Bypass Class 3 Root CA	Oct 26 08:28:58 2040 GMT	Bypass_Class_3_Root_CA.crt
CA Disig Root R2	Jul 19 09:15:30 2042 GMT	CA_Disig_Root_R2.crt
CFCA EV ROOT	Dec 31 03:07:01 2029 GMT	CFCA_EV_ROOT.crt
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT	COMODO_Certification_Authority.crt
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT	COMODO_ECC_Certification_Authority.crt
COMODO RSA Certification Authority	Jan 18 23:59:59 2038 GMT	COMODO_RSA_Certification_Authority.crt
Certainly Root E1	Apr 1 00:00:00 2046 GMT	Certainly_Root_E1.crt
Certainly Root R1	Apr 1 00:00:00 2046 GMT	Certainly_Root_R1.crt



Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
Certigna	Jun 29 15:13:05 2027 GMT	Certigna.crt
Certigna Root CA	Oct 1 08:32:27 2033 GMT	Certigna_Root_CA.crt
Certum EC-384 CA	Mar 26 07:24:54 2043 GMT	Certum_EC-384_CA.crt
Certum Trusted Network CA	Dec 31 12:07:37 2029 GMT	Certum_Trusted_Network_CA.crt
Certum Trusted Network CA 2	Oct 6 08:39:56 2046 GMT	Certum_Trusted_Network_CA_2.crt
Certum Trusted Root CA	Mar 16 12:10:13 2043 GMT	Certum_Trusted_Root_CA.crt
AAA Certificate Services	Dec 31 23:59:59 2028 GMT	Comodo_AAA_Services_root.crt
D-TRUST BR Root CA 1 2020	Feb 11 09:44:59 2035 GMT	D-TRUST_BR_Root_CA_1_2020.crt
D-TRUST EV Root CA 1 2020	Feb 11 09:59:59 2035 GMT	D-TRUST_EV_Root_CA_1_2020.crt
D-TRUST Root Class 3 CA 2 2009	Nov 5 08:35:58 2029 GMT	D-TRUST_Root_Class_3_CA_2_2009.crt
D-TRUST Root Class 3 CA 2 EV 2009	Nov 5 08:50:46 2029 GMT	D-TRUST_Root_Class_3_CA_2_EV_2009.crt
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	DigiCertGlobalRootCA.pem)

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT	DigiCert_Assured_ID_Root_CA.crt
DigiCert Assured ID Root G2	Jan 15 12:00:00 2038 GMT	DigiCert_Assured_ID_Root_G2.crt
DigiCert Assured ID Root G3	Jan 15 12:00:00 2038 GMT	DigiCert_Assured_ID_Root_G3.crt
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT	DigiCert_Global_Root_CA.crt
DigiCert Global Root G2	Jan 15 12:00:00 2038 GMT	DigiCert_Global_Root_G2.crt
DigiCert Global Root G3	Jan 15 12:00:00 2038 GMT	DigiCert_Global_Root_G3.crt
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT	DigiCert_High_Assurance_EV_Root_CA.crt
DigiCert TLS ECC P384 Root G5	Jan 14 23:59:59 2046 GMT	DigiCert_TLS_ECC_P384_Root_G5.crt
DigiCert TLS RSA4096 Root G5	Jan 14 23:59:59 2046 GMT	DigiCert_TLS_RSA4096_Root_G5.crt
DigiCert Trusted Root G4	Jan 15 12:00:00 2038 GMT	DigiCert_Trusted_Root_G4.crt
E-Tugra Global Root CA ECC v3	Mar 12 09:46:58 2045 GMT	E-Tugra_Global_Root_CA_ECC_v3.crt

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
E-Tugra Global Root CA RSA v3	Mar 12 09:07:17 2045 GMT	E-Tugra_Global_Root_CA_RSA_v3.crt
Entrust.net <sup>43</sup> Certification Authority (2048)	Jul 24 14:15:12 2029 GMT	Entrust.net_Premium_2048_Secure_Server_CA.crt
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT	Entrust_Root_Certification_Authority.crt
Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	Entrust_Root_Certification_Authority_-_EC1.crt
Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	Entrust_Root_Certification_Authority_-_G2.crt
Entrust Root Certification Authority - G4	Dec 27 11:41:16 2037 GMT	Entrust_Root_Certification_Authority_-_G4.crt
GDCA TrustAUTH R5 ROOT	Dec 31 15:59:59 2040 GMT	GDCA_TrustAUTH_R5_ROOT.crt
GLOBALTRUST 2020	Jun 10 00:00:00 2040 GMT	GLOBALTRUST_2020.crt
GTS Root R1	Jun 22 00:00:00 2036 GMT	GTS_Root_R1.crt
GTS Root R2	Jun 22 00:00:00 2036 GMT	GTS_Root_R2.crt
GTS Root R3	Jun 22 00:00:00 2036 GMT	GTS_Root_R3.crt
GTS Root R4	Jun 22 00:00:00 2036 GMT	GTS_Root_R4.crt
GlobalSign	Jan 19 03:14:07 2038 GMT	GlobalSign_ECC_Root_CA_-_R4.crt

---

<sup>43</sup> <http://Entrust.net>

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
GlobalSign	Jan 19 03:14:07 2038 GMT	GlobalSign_ECC_Root_CA_-_R5.crt
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT	GlobalSign_Root_CA.crt
GlobalSign	Mar 18 10:00:00 2029 GMT	GlobalSign_Root_CA_-_R3.crt
GlobalSign	Dec 10 00:00:00 2034 GMT	GlobalSign_Root_CA_-_R6.crt
GlobalSign Root E46	Mar 20 00:00:00 2046 GMT	GlobalSign_Root_E46.crt
GlobalSign Root R46	Mar 20 00:00:00 2046 GMT	GlobalSign_Root_R46.crt
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT	Go_Daddy_Class_2_CA.crt
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	Go_Daddy_Root_Certificate_Authority_-_G2.crt
HARICA TLS ECC Root CA 2021	Feb 13 11:01:09 2045 GMT	HARICA_TLS_ECC_Root_CA_2021.crt
HARICA TLS RSA Root CA 2021	Feb 13 10:55:37 2045 GMT	HARICA_TLS_RSA_Root_CA_2021.crt
Hellenic Academic and Research Institutions ECC RootCA 2015	Jun 30 10:37:12 2040 GMT	Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt
Hellenic Academic and Research Institutions RootCA 2015	Jun 30 10:11:21 2040 GMT	Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt
HiPKI Root CA - G1	Dec 31 15:59:59 2037 GMT	HiPKI_Root_CA_-_G1.crt

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT	Hongkong_Post_Root_CA_1.crt
Hongkong Post Root CA 3	Jun 3 02:29:46 2042 GMT	Hongkong_Post_Root_CA_3.crt
ISRG Root X1	Jun 4 11:04:38 2035 GMT	ISRG_Root_X1.crt
ISRG Root X2	Sep 17 16:00:00 2040 GMT	ISRG_Root_X2.crt
IdenTrust Commercial Root CA 1	Jan 16 18:12:23 2034 GMT	IdenTrust_Commercial_Root_CA_1.crt
IdenTrust Public Sector Root CA 1	Jan 16 17:53:32 2034 GMT	IdenTrust_Public_Sector_Root_CA_1.crt
Imprivata Embedded Code Signing CA	Sep 7 16:20:00 2033 GMT	Imprivata.crt
<a href="http://izenpe.com">izenpe.com</a> <sup>44</sup>	Dec 13 08:27:25 2037 GMT	<a href="http://izenpe.com">Izenpe.com</a> <sup>45</sup> .crt
Microsec e-Szigno Root CA 2009	Dec 30 11:30:18 2029 GMT	Microsec_e-Szigno_Root_CA_2009.crt
Microsoft ECC Root Certificate Authority 2017	Jul 18 23:16:04 2042 GMT	Microsoft_ECC_Root_Certificate_Authority_2017.crt
Microsoft RSA Root Certificate Authority 2017	Jul 18 23:00:23 2042 GMT	Microsoft_RSA_Root_Certificate_Authority_2017.crt
NAVER Global Root Certification Authority	Aug 18 23:59:59 2037 GMT	NAVER_Global_Root_Certification_Authority.crt

---

<sup>44</sup> <http://izenpe.com>

<sup>45</sup> <http://izenpe.com>

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
NetLock Arany (Class Gold) Főtanúsítvány	Dec 6 15:08:21 2028 GMT	NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt
OISTE WiSeKey Global Root GB CA	Dec 1 15:10:31 2039 GMT	OISTE_WiSeKey_Global_Root_GB_CA.crt
OISTE WiSeKey Global Root GC CA	May 9 09:58:33 2042 GMT	OISTE_WiSeKey_Global_Root_GC_CA.crt
QuoVadis Root CA 1 G3	Jan 12 17:27:44 2042 GMT	QuoVadis_Root_CA_1_G3.crt
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT	QuoVadis_Root_CA_2.crt
QuoVadis Root CA 2 G3	Jan 12 18:59:32 2042 GMT	QuoVadis_Root_CA_2_G3.crt
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT	QuoVadis_Root_CA_3.crt
QuoVadis Root CA 3 G3	Jan 12 20:26:32 2042 GMT	QuoVadis_Root_CA_3_G3.crt
<a href="http://SSL.com">SSL.com</a> <sup>46</sup> EV Root Certification Authority ECC	Feb 12 18:15:23 2041 GMT	SSL.com_EV_Root_Certification_Authority_ECC.crt
<a href="http://SSL.com">SSL.com</a> <sup>47</sup> EV Root Certification Authority RSA R2	May 30 18:14:37 2042 GMT	SSL.com_EV_Root_Certification_Authority_RSA_R2.crt
<a href="http://SSL.com">SSL.com</a> <sup>48</sup> Root Certification Authority ECC	Feb 12 18:14:03 2041 GMT	SSL.com_Root_Certification_Authority_ECC.crt

---

<sup>46</sup> <http://SSL.com>

<sup>47</sup> <http://SSL.com>

<sup>48</sup> <http://SSL.com>

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
SSL.com <sup>49</sup> Root Certification Authority RSA	Feb 12 17:39:39 2041 GMT	SSL.com_Root_Certification_Authority_RSA.crt
SZAFIR ROOT CA2	Oct 19 07:43:30 2035 GMT	SZAFIR_ROOT_CA2.crt
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT	SecureSign_RootCA11.crt
SecureTrust CA	Dec 31 19:40:55 2029 GMT	SecureTrust_CA.crt
Secure Global CA	Dec 31 19:52:06 2029 GMT	Secure_Global_CA.crt
Security Communication ECC RootCA1	Jan 18 05:15:28 2038 GMT	Security_Communication_ECC_RootCA1.crt
Security Communication RootCA2	May 29 05:00:39 2029 GMT	Security_Communication_RootCA2.crt
Security Communication RootCA3	Jan 18 06:17:16 2038 GMT	Security_Communication_RootCA3.crt
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT	Security_Communication_Root_CA.crt
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT	Starfield_Class_2_CA.crt
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	Starfield_Root_Certificate_Authority_-_G2.crt
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	Starfield_Services_Root_Certificate_Authority_-_G2.crt
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT	SwissSign_Gold_CA_-_G2.crt

---

<sup>49</sup> <http://SSL.com>

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT	SwissSign_Silver_CA_-_G2.crt
T-TeleSec GlobalRoot Class 2	Oct 1 23:59:59 2033 GMT	T-TeleSec_GlobalRoot_Class_2.crt
T-TeleSec GlobalRoot Class 3	Oct 1 23:59:59 2033 GMT	T-TeleSec_GlobalRoot_Class_3.crt
TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1	Oct 25 08:25:55 2043 GMT	TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt
TWCA Global Root CA	Dec 31 15:59:59 2030 GMT	TWCA_Global_Root_CA.crt
TWCA Root Certification Authority	Dec 31 15:59:59 2030 GMT	TWCA_Root_Certification_Authority.crt
TeliaSonera Root CA v1	Oct 18 12:00:50 2032 GMT	TeliaSonera_Root_CA_v1.crt
Telia Root CA v2	Nov 29 11:55:54 2043 GMT	Telia_Root_CA_v2.crt
TrustCor ECA-1	Dec 31 17:28:07 2029 GMT	TrustCor_ECA-1.crt
TrustCor RootCert CA-1	Dec 31 17:23:16 2029 GMT	TrustCor_RootCert_CA-1.crt
TrustCor RootCert CA-2	Dec 31 17:26:39 2034 GMT	TrustCor_RootCert_CA-2.crt
Trustwave Global Certification Authority	Aug 23 19:34:12 2042 GMT	Trustwave_Global_Certification_Authority.crt



Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
Trustwave Global ECC P256 Certification Authority	Aug 23 19:35:10 2042 GMT	Trustwave_Global_ECC_P256_Certification_Authority.crt
Trustwave Global ECC P384 Certification Authority	Aug 23 19:36:43 2042 GMT	Trustwave_Global_ECC_P384_Certification_Authority.crt
TunTrust Root CA	Apr 26 08:57:56 2044 GMT	TunTrust_Root_CA.crt
UCA Extended Validation Root	Dec 31 00:00:00 2038 GMT	UCA_Extended_Validation_Root.crt
UCA Global G2 Root	Dec 31 00:00:00 2040 GMT	UCA_Global_G2_Root.crt
USERTrust ECC Certification Authority	Jan 18 23:59:59 2038 GMT	USERTrust_ECC_Certification_Authority.crt
USERTrust RSA Certification Authority	Jan 18 23:59:59 2038 GMT	USERTrust_RSA_Certification_Authority.crt
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT	XRamp_Global_CA_Root.crt
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT	certSIGN_ROOT_CA.crt
certSIGN ROOT CA G2	Feb 6 09:27:35 2042 GMT	certSIGN_Root_CA_G2.crt
e-Szigno Root CA 2017	Aug 22 12:07:06 2042 GMT	e-Szigno_Root_CA_2017.crt
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT	ePKI_Root_Certification_Authority.crt
emSign ECC Root CA - C3	Feb 18 18:30:00 2043 GMT	emSign_ECC_Root_CA_-_C3.crt

Name des Zertifikats	Ablaufdatum	Datei in /etc/ssl/certs
emSign ECC Root CA - G3	Feb 18 18:30:00 2043 GMT	emSign_ECC_Root_CA_-_G3.crt
emSign Root CA - C1	Feb 18 18:30:00 2043 GMT	emSign_Root_CA_-_C1.crt
emSign Root CA - G1	Feb 18 18:30:00 2043 GMT	emSign_Root_CA_-_G1.crt
vTrus ECC Root CA	Jul 31 07:26:44 2043 GMT	vTrus_ECC_Root_CA.crt
vTrus Root CA	Jul 31 07:24:05 2043 GMT	vTrus_Root_CA.crt

## Smartcard

- [Authentifizierung mit IGEL Smartcard \(see page 540\)](#)
- [Authentifizierung mit Smartcard in IGEL OS \(see page 550\)](#)

## Authentifizierung mit IGEL Smartcard

Smartcards machen die Benutzererfahrung komfortabler, indem sie ein einziges Gerät bereitstellen, das mehrere Authentifizierungsprodukte im gesamten Unternehmen unterstützt. Der Benutzer muss sich nur eine einzige PIN merken, die die Smartcard entsperrt, um auf das Netzwerk zuzugreifen.

### Voraussetzungen

Vor der Verwendung der IGEL Smartcard, müssen die relevanten Profile und Sitzungsinformationen auf die Smartcard geschrieben werden.

Wir beschreiben einen optimalen Weg, wie man vorgehen sollte. Die Namen der Verzeichnisse und Profile sind nur Beispiele und können individuell geändert werden.

Es ist sinnvoll, einen der folgenden Verzeichnisse und Profile auf der Universal Management Suite (UMS) zu verwenden:

Verzeichnis	Profile	Verwendungszweck
Smartcard-Erstellung		Ordner für Geräte, welcher für die Smartcard-Erstellung verwendet wird.
	Smartcard-Schlüssel	Dieses Profil wendet den definierten Firmenschlüssel auf den Geräten an. Dieser Schlüssel wird beim Erstellen der IGEL Smartcard geschrieben.
Smartcard-Bedienung		Ordner für Geräte, deren Authentifizierungsprozess nur über die IGEL Smartcard funktioniert.
	Smartcard-Anmeldung	Dieses Profil wendet den definierten Firmenschlüssel auf den Geräten an und aktiviert die Anmeldung mit IGEL Smartcard.

▶ Erstellen Sie zwei Verzeichnisse unter **Profile** in der Universal Management Suite (UMS), z. B. "Smartcard-Bedienung" und "Smartcard-Erstellung".

▶ Erstellen Sie das Profil "Smartcard-Anmeldung" für "Smartcard-Bedienung".

▶ Erstellen Sie das Profil "Smartcard-Schlüssel" für "Smartcard-Erstellung".

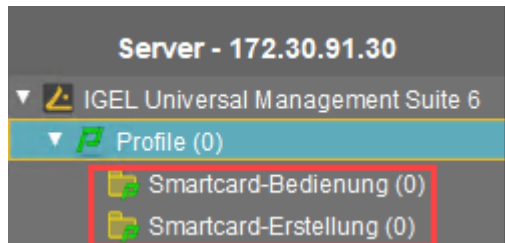
- 
- [IGEL Smartcard-Verzeichnisse erstellen](#) (see page 542)
  - [Ordner "Smartcard-Bedienung"](#) (see page 543)
  - [Ordner "Smartcard-Erstellung"](#) (see page 544)

- [IGEL Smartcard beschreiben \(see page 545\)](#)
- [Smartcardleser, die von IGEL Smartcards unterstützt werden \(see page 549\)](#)

## IGEL Smartcard-Verzeichnisse erstellen

Fügen Sie als Erstes zwei neue Profilordner hinzu, in denen Sie dann Profile erstellen und sie den Geräten zuordnen:

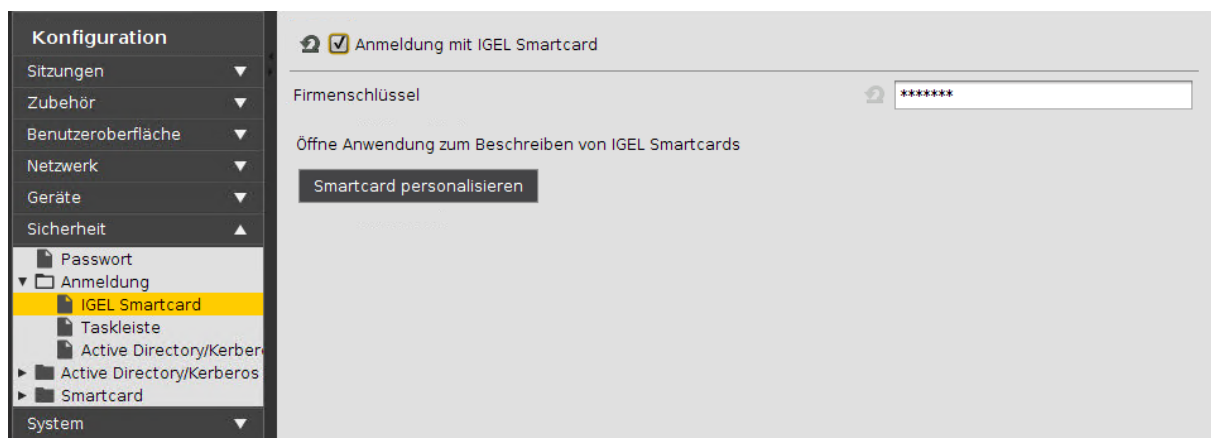
- "Smartcard-Bedienung";
- "Smartcard-Erstellung".



## Ordner "Smartcard-Bedienung"

In diesem Ordner erstellen Sie das neue Profil "Smartcard-Anmeldung":

1. Klicken Sie mit Rechtsklick auf den Ordner "Smartcard-Bedienung".
2. Wählen Sie **Neues Profil**.
3. Geben Sie einen **Profilnamen**, z. B. "Smartcard-Anmeldung" ein.
4. Klicken Sie **Sicherheit > Anmeldung > IGEL Smartcard**.
5. Aktivieren Sie **Anmeldung mit IGEL Smartcard**.
6. Geben Sie Ihren **Firmenschlüssel** ein.



- i** Dieses Profil wird später auf alle Geräte angewendet, bei denen der Authentifizierungsprozess nur mit Smartcard funktionieren soll.  
Auf diese Weise erhalten die Geräte:
- den Firmenschlüssel und
  - die Information, dass die Authentifizierung ausschließlich mit der Smartcard möglich ist.

- i** Der Firmenschlüssel ist ein privater Schlüssel der zwischen den Geräten und den Smartcards geteilt wird. Er sollte wie ein gutes Passwort gewählt werden. Wenn die Smartcard nicht den gleichen Schlüssel wie das Gerät enthält, wird die Authentifizierung nicht möglich sein, da Sie später genau den gleichen Schlüssel auf die Smartcard schreiben müssen.

## Ordner "Smartcard-Erstellung"

In diesem Ordner erstellen Sie ein neues Profil "Smartcard-Schlüssel":

1. Rechtsklicken Sie auf den Ordner "Smartcard-Erstellung".
2. Wählen Sie **Neues Profil**.
3. Geben Sie einen Profilnamen ein, z. B. "Smartcard-Schlüssel".
4. Klicken Sie **Sicherheit > Anmeldung > IGEL Smartcard**.
5. Geben Sie den gleichen **Firmenschlüssel** wie im Profil "Smartcard-Anmeldung" ein.

Ein weiterer zusätzlicher Ordner ist nützlich:

► Erstellen Sie das Unterverzeichnis "Einstellungen abrufen von" unter "Smartcard-Erstellung". In diesem Verzeichnis erstellen Sie das Profil mit der Sitzungsinformation, die Sie auf die Smartcard schreiben wollen.



**i** Sie benötigen dieses zusätzliche Verzeichnis, da die Zuordnung von aktiven Profilen aus der UMS zur IGEL Smartcard Probleme verursachen kann (Firmware-Version < 5.06.100). Später werden Sie das Verzeichnis lokal auf Ihr Gerät kopieren.



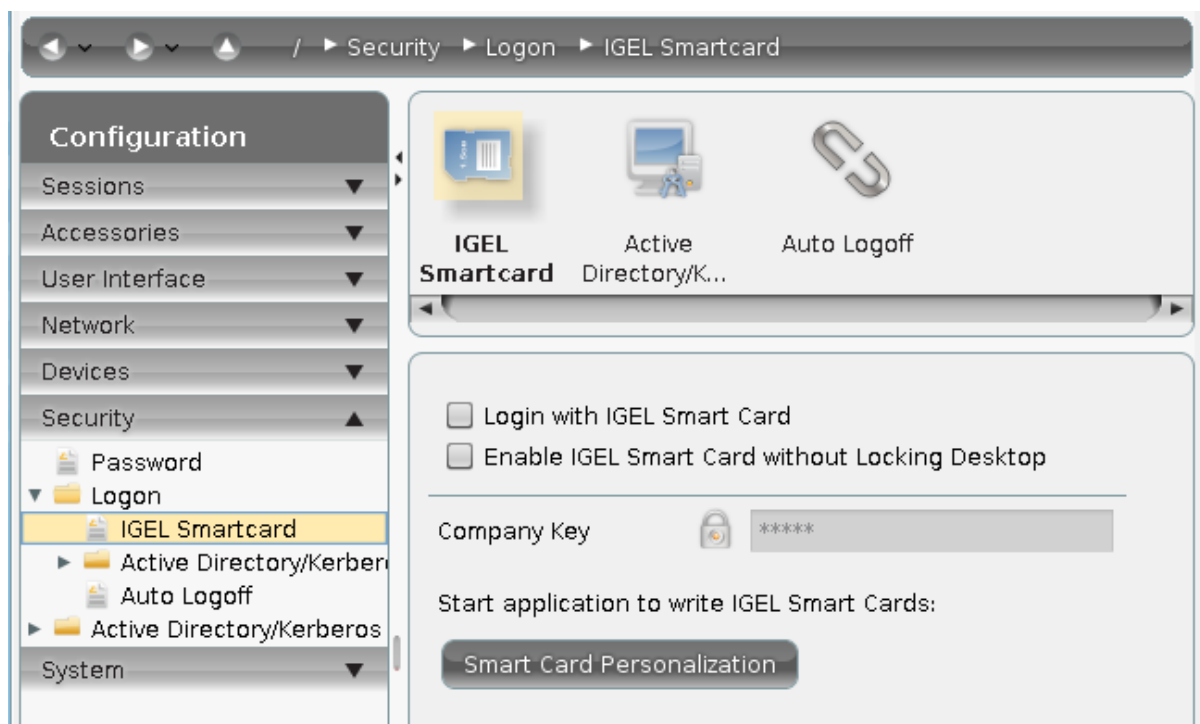
## IGEL Smartcard beschreiben

### Das Profil "Smartcard-Erstellung" zum Gerät zuordnen

- Bereiten Sie ein Gerät vor, das über einen Smartcardleser/-schreiber verfügt.
- Integrieren Sie das Gerät in der UMS und schieben Sie es in das Verzeichnis "Smartcard-Erstellung".  
Nun erhält das Gerät automatisch den Firmenschlüssel aus dem Profil. Er wird beim Beschreiben der Smartcard verwendet.

### Sicherstellen, dass die Profilzuordnung erfolgreich war

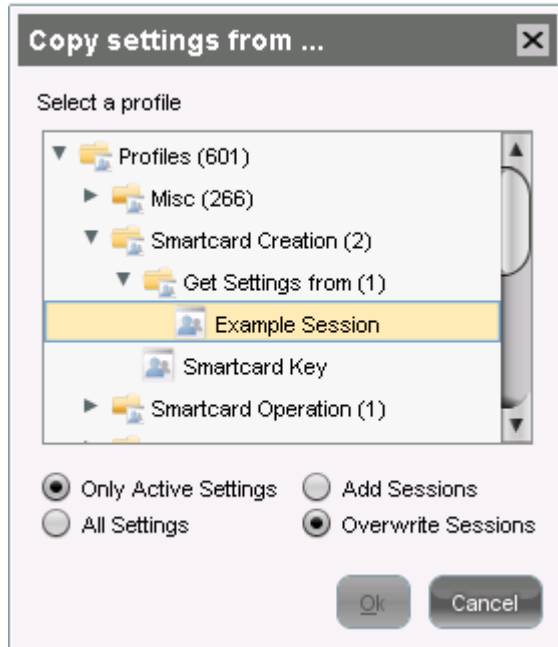
1. Öffnen Sie das lokale Setup Ihres Gerätes.
2. Klicken Sie **Sicherheit > Anmeldung > IGEL Smartcard**.  
Sie sollten nun ein deaktiviertes Feld **Firmenschlüssel** mit einem Schlosssymbol sehen.



### Profile auf die Smartcard beschreiben

1. Öffnen Sie das Verzeichnis "Smartcard-Erstellung" in der UMS.
2. Klicken Sie mit Rechtsklick auf Ihr Gerät.
3. Wählen Sie **Einstellungen von Geräten exportieren**, um die Profileinstellungen auf das Gerät zu kopieren. Der Dialog **Geräte - Einstellungen exportieren** öffnet sich.

4. Wählen Sie Ihr Profil aus dem Verzeichnis "Smartcard-Erstellung" > "Einstellungen abrufen von".
5. Aktivieren Sie **Sitzung überschreiben**.

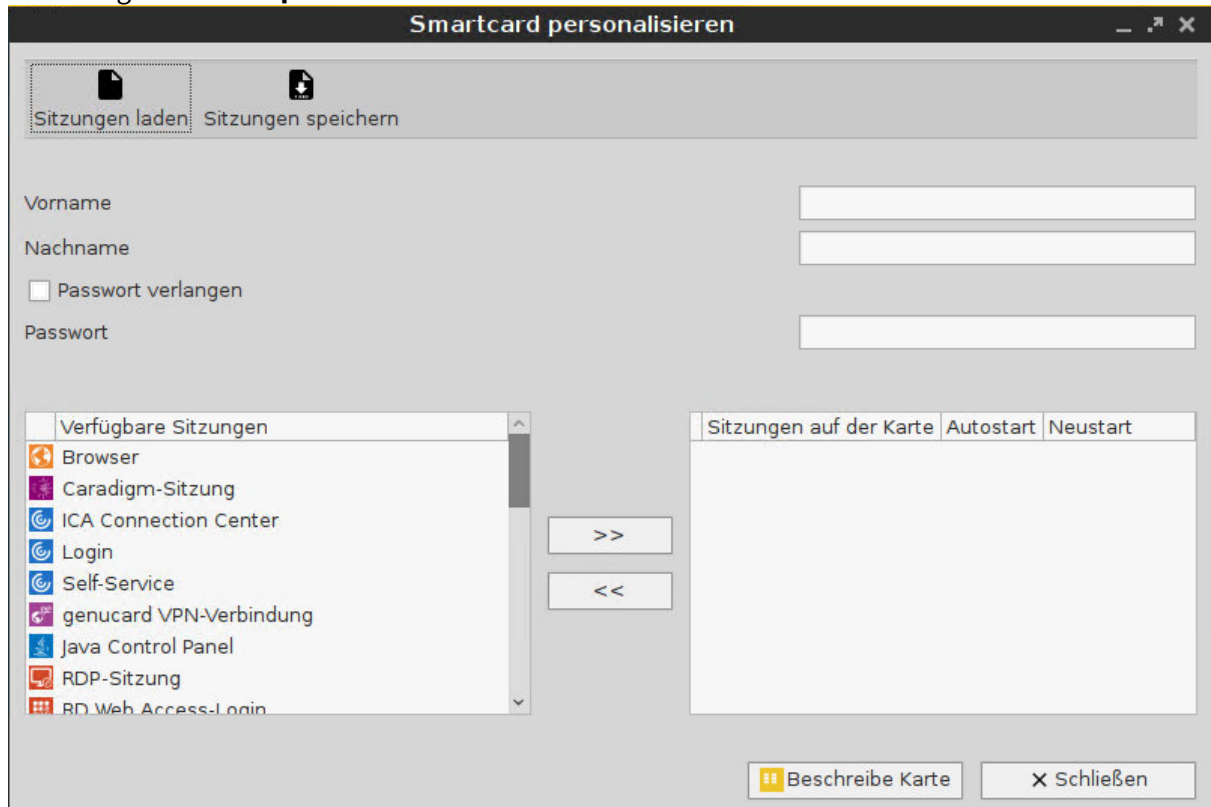


6. Klicken Sie **Ok**, um das Profil mit den Einstellungen und den Firmenschlüssel auf das Gerät zu kopieren.


### Smartcard beschreiben

1. Öffnen Sie das lokale Setup Ihres Gerätes.
2. Klicken Sie **Setup > Anmeldung > IGEL Smartcard**.


- Klicken Sie **Smartcard personalisieren**.  
Der Dialog **Smartcard personalisieren** öffnet sich.



- Geben Sie den **Vornamen** und **Nachnamen** des Smartcard-Inhabers ein, die bei der Anmeldeaufforderung erscheinen sollen.
- Aktivieren Sie **Passwort verlangen** und geben Sie ein **Passwort** ein, falls ein Passwort bei der Smartcard-Anmeldung verlangt werden soll.
- Wählen Sie die lokalen Sitzungen, die Sie auf die Smartcard beschreiben möchten.

 Benutzen Sie die Pfeiltasten, um eine Sitzung der Smartcard-Sitzungsliste hinzuzufügen.

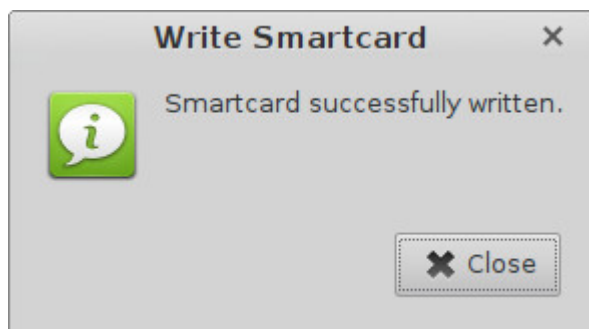
- Aktivieren Sie **Autostart** für eine Sitzung in der Smartcard-Sitzungsliste, wenn diese automatisch während der Anmeldung starten soll. Aktivieren Sie ggf. **Neustart**.

 Die Konfiguration der Sitzungen kann zu einem späteren Zeitpunkt gespeichert und neu geladen werden.

- Klicken Sie **Beschreibe Karte**, um den Beschreibungsprozess mit den festgelegten Einstellungen zu starten.
- Akzeptieren Sie die Sicherheitsfrage mit **Ja**.



Die Meldung "Karte erfolgreich beschrieben" erscheint.



#### Die neue IGEL Smartcard testen

1. Gehen Sie in die UMS.
2. Registrieren Sie das neue Gerät in der UMS und schieben Sie es in das Verzeichnis "Smartcard-Bereitstellung".  
Das Gerät erhält den Firmenschlüssel und die Profilinformationen, dass die Authentifizierung nur mit der IGEL Smartcard möglich ist.
3. Starten Sie das Gerät neu.  
Der Dialog **Smartcard einlegen...** öffnet sich.
4. Legen Sie die IGEL Smartcard in Ihr Gerät ein und überprüfen Sie die ausgewählte Konfiguration.

## Smartcardleser, die von IGEL Smartcards unterstützt werden

Hier ist die Liste der Smartcardleser von Drittherstellern, die IGEL Smartcards unterstützen:

- OMNIKEY CardMan 3111
- OMNIKEY CardMan 3x21
- OMNIKEY CardMan 3621
- OMNIKEY CardMan 6121
- OMNIKEY CardMan 3821
- USB CCID Smart Card Reader
- USB CCID Smart Card Reader Keyboard
- Fujitsu Siemens Computers SmartCard-Reader USB 2A
- Fujitsu Siemens Computers SmartCard-Reader Keyboard USB 2A
- Fujitsu Siemens Computers SmartCard-Reader USB 2C
- Cherry SmartBoard XX44
- OMNIKEY CardMan 5121
- OMNIKEY CardMan 5x21
- HID Global OMNIKEY 3x21 Smart Card Reader
- Cherry KC 1000 SC
- Cherry KC 1000 SC/DI
- Cherry KC 1000 SC Z
- Cherry KC 1000 SC/DI Z
- Cherry SmartTerminal XX44 v2
- Cherry SmartTerminal XX44
- OMNIKEY CardMan
- CCID SC Reader
- Cherry SC Reader.

## Authentifizierung mit Smartcard in IGEL OS

Der folgende Artikel gibt einen Überblick darüber, wie Sie in IGEL OS die Authentifizierung mit Smartcard für verschiedene Sitzungen wie RDP, VMware Horizon usw. konfigurieren können, sowie erklärt, wie Sie die Active Directory Anmeldung mit Smartcard und die lokale Anmeldung mit Smartcardzertifikat einrichten können.

Wenn Sie IGEL Smartcards verwenden, siehe auch [Authentifizierung mit IGEL Smartcard](#) (see page 540).

## Authentifizierung mit Zertifikaten

Die in diesem How-To behandelten Smartcards können digitale Zertifikate (X.509) und die dazugehörigen privaten Schlüssel speichern. Der private Schlüssel kann nicht von der Smartcard ausgelesen werden, aber von der Smartcard zum Signieren und Entschlüsseln von Daten verwendet werden.

Dadurch wird eine Zwei-Faktoren-Authentifizierung möglich: Der Benutzer authentifiziert sich nicht nur durch den Besitz der Smartcard, sondern zusätzlich mit einer PIN.

Wenn Sie Active Directory (AD) verwenden möchten, muss die von der Key Distribution Center (Domain Controller) verwendete Zertifikatskette auf dem Gerät verfügbar sein. Um Zertifikatsdateien bereitzustellen, registrieren Sie sie in der UMS (Klassifizierung auf "SSL-Zertifikat" setzen) und weisen den Geräten zu, siehe Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen.

## Smartcardleser

Auf Smartcards wird mit einem Smartcardleser zugegriffen, der kontaktlos oder kontaktbehaftet sein kann. Von IGEL OS unterstützte Smartcardleser können Sie in der [IGEL Third Party Database](#)<sup>50</sup> nachschlagen.

## PC/SC Resource Manager

Der PC/SC Resource Manager ist eine Programmierschnittstelle (API), die unter Microsoft Windows und Linux-basierten Betriebssystemen vorhanden ist. Sie standardisiert den Zugriff von Anwendungen auf Smartcards und Lesegeräte.

Der PC/SC Resource Manager ist in IGEL OS standardmäßig aktiviert. Er kann in IGEL Setup unter **Sicherheit > Smartcard > Dienste** über die Einstellung **PC/SC Dämon aktivieren** aktiviert und deaktiviert werden.

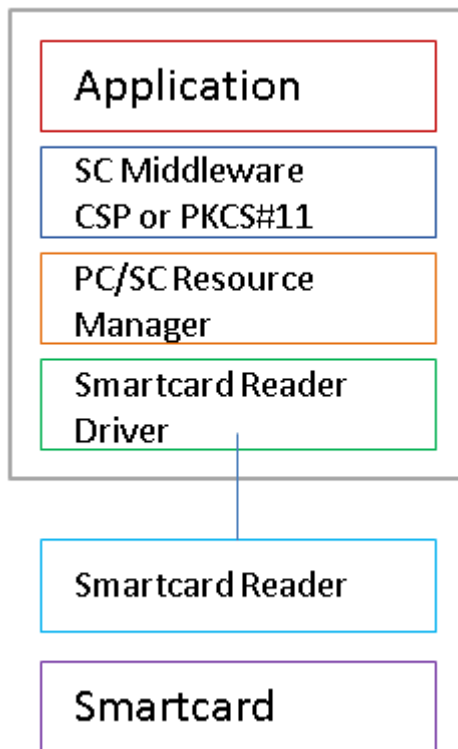
## Smartcard-Middleware

Smartcard-Middleware stellt eine allgemeine Schnittstelle für verschiedene Arten von Smartcard-Hardware bereit.

Es gibt verschiedene Arten von Middleware:

	Windows	Linux
<i>CSP, Cryptographic Service Provider</i>	✓	
<i>PKCS#11, Public-Key Cryptographic Standards</i>	✓	✓

<sup>50</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>



Für manche Authentifizierungsmethoden von Smartcards muss auf dem Endgerät eine zusätzliche Middleware installiert werden. Die folgenden Softwaremodule sind verfügbar:

- Gemalto SafeNet
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T.SafeSign
- SecMaker Net iD Enterprise (früher als "SecMaker Net iD" bezeichnet)
- SecMaker Net iD Client (die nächste Generation von SecMaker Net iD Enterprise, siehe <http://docs.secmaker.com/net-id-client/latest/index.html>)
- Coolkey
- OpenSC
- 90meter

**i** **Lizenziertes Feature**

Für dieses Feature ist eine Add-on-Lizenz erforderlich; siehe Add-on-Lizenzen. Bitte kontaktieren Sie Ihren IGEL Vertriebspartner.

Wie Sie benutzerdefinierte PKCS#11-Bibliothek benutzen können, erfahren Sie unter [Benutzerdefinierte PKCS#11-Bibliothek verwenden](#) (see page 623).

- [Active Directory Anmeldung mit Smartcard \(see page 553\)](#)
- [Citrix StoreFront \(see page 554\)](#)
- [RDP-Sitzungen \(see page 556\)](#)
- [Horizon Sitzungen \(see page 557\)](#)
- [Smartcard-Authentifizierung im Browser \(see page 558\)](#)
- [Local Login with Smartcard Certificate \(see page 559\)](#)



## Active Directory Anmeldung mit Smartcard

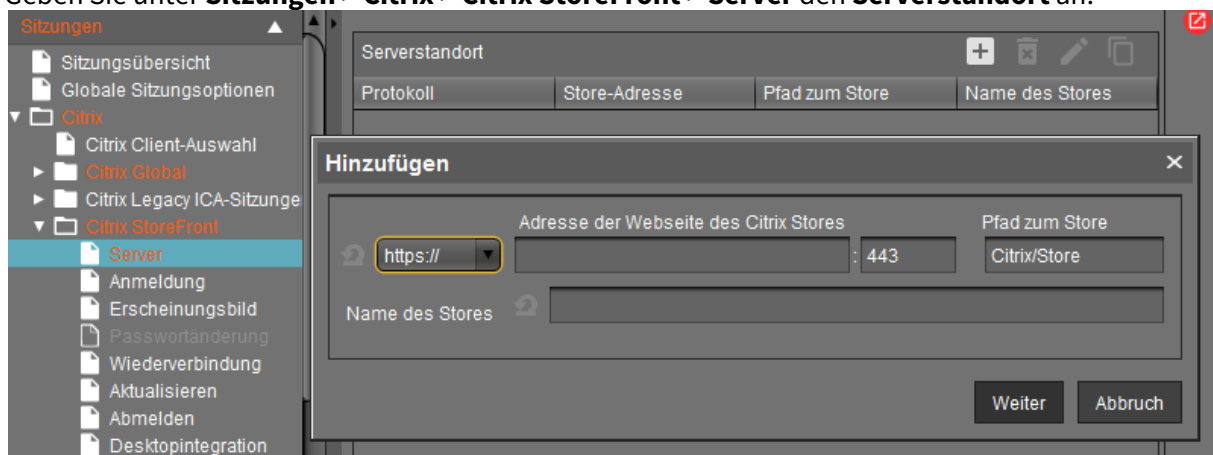
Siehe das How-To [Passthrough-Authentifizierung](#) (see page 838).

## Citrix StoreFront

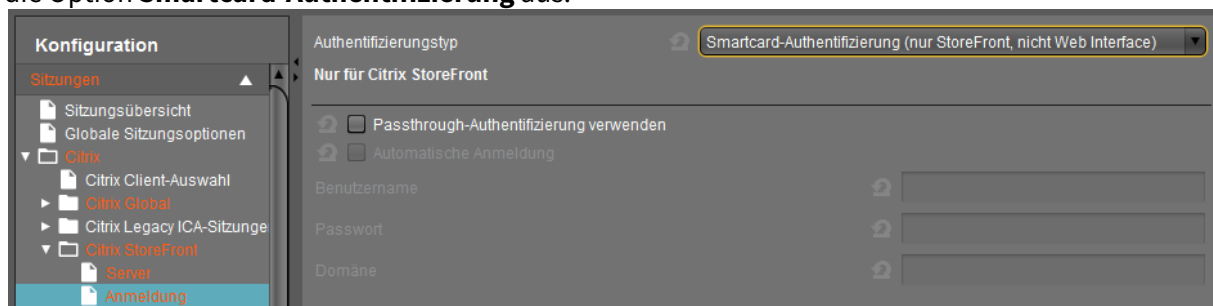
Der folgende Artikel beschreibt, wie Sie in IGEL OS die Authentifizierung mit Smartcard für Citrix StoreFront konfigurieren können.

Beachten Sie, dass das Root-Zertifikat des vom StoreFront-Server verwendeten Webserver-Zertifikats als vertrauenswürdiges Root-Zertifikat auf dem Gerät bekannt sein muss – siehe [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen](#) (see page 523), Zertifikatstyp **SSL-Zertifikat**.

1. Geben Sie unter **Sitzungen > Citrix > Citrix StoreFront > Server** den **Serverstandort** an.



2. Wählen Sie unter **Sitzungen > Citrix > Citrix StoreFront > Anmeldung > Authentifizierungstyp** die Option **Smartcard-Authentifizierung** aus.



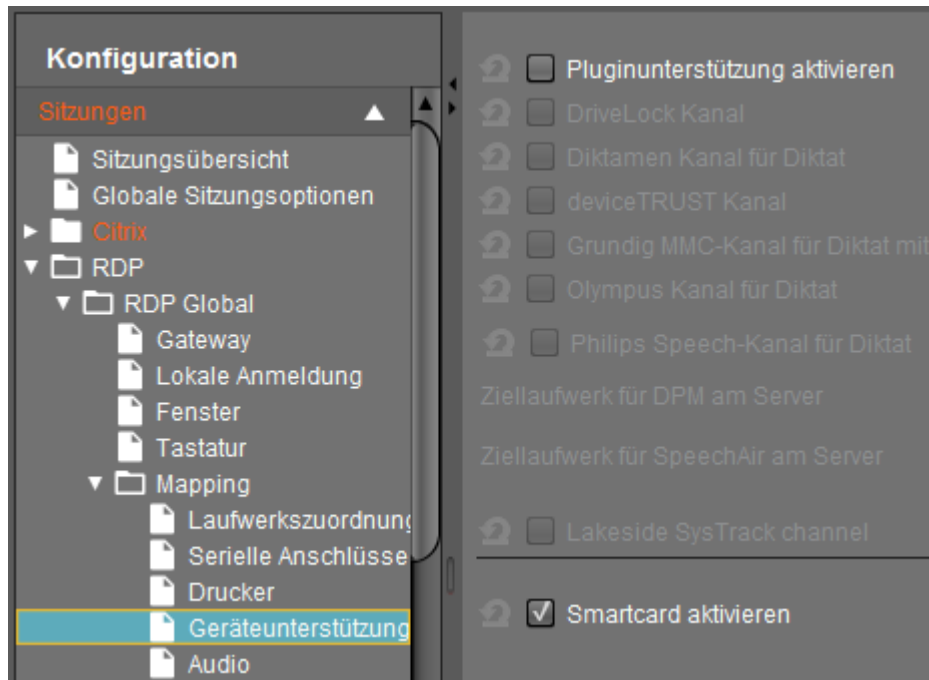
**i** In Kombination mit der **Active Directory-Anmeldung** aktiviert **Passthrough-Authentifizierung verwenden** Single Sign-on mit Smartcard.

3. Wählen Sie das passende PKCS#11-Modul für die Smartcard unter **Sicherheit > Smartcard > Middleware** aus oder geben Sie dort Ihre eigene PKCS#11-Bibliothek an, siehe Middleware für Smartcards in IGEL OS.

## RDP-Sitzungen

In diesem Szenario muss die Smartcard-Middleware serverseitig installiert werden.


1. Aktivieren Sie **PC/SC-Dämon aktivieren** unter **Sicherheit > Smartcard > Dienste**.
2. Aktivieren Sie **Smartcard aktivieren** unter **Sitzungen > RDP > RDP Global > Mapping > Geräteunterstützung**.



## Horizon Sitzungen

In diesem Szenario muss die Smartcard-Middleware sowohl auf den virtuellen Desktops als auch geräteseitig konfiguriert werden.

Der View Connection Server muss auf dem Gerät konfiguriert werden.

 Der View Connection Server muss so konfiguriert sein, dass er Verbindungen über SSL/TLS gesicherte https-URLs akzeptiert. Das Root-Zertifikat des für diesen Dienst verwendeten Zertifikats muss als vertrauenswürdige Root-Zertifikat auf dem Gerät bekannt sein – siehe [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen](#) (see page 523).

1. Wählen Sie das entsprechende PKCS#11-Modul für die Smartcard unter **Sitzungen > Horizon Client > Horizon Client Global > Smartcard**, siehe Smartcard Middleware-Einstellungen für VMware Horizon Sitzungen in IGEL OS.

Für Informationen zur benutzerdefinierten PKCS#11-Bibliothek siehe [Benutzerdefinierte PKCS#11-Bibliothek verwenden](#) (see page 623).

2. Konfigurieren Sie die **Server URL** unter **Sitzungen > Horizon Client > Horizon Client-Sitzungen > [Sitzungsname] > Verbindungseinstellungen**.

 Beginnen Sie die URL mit `https://`

## Smartcard-Authentifizierung im Browser

Die Authentifizierung mit einer Smartcard ist auf Websites möglich, z. B. bei Citrix Web Interface oder StoreFront.

Bei einer Verbindung über eine SSL/TLS-gesicherte https-URL muss das Root-Zertifikat des Webserver-Zertifikats als **Trusted Root-Zertifikat** auf dem Endgerät bekannt sein; siehe [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen](#) (see page 523), Zertifikatstypen **Webbrowserzertifikat** und (!) **SSL-Zertifikat**.

► Wählen Sie das entsprechende PKCS#11-Modul (Sicherheitsgerät) für die Smartcard unter **Sitzungen > Firefox Browser > Firefox Browser Global > Smartcard Middleware** oder/und unter **Sitzungen > Chromium Browser > Chromium Browser Global > Smartcard Middleware**.


- Gemalto SafeNet
- cryptovision sc/interface
- Gemalto IDPrime
- Athena IDProtect
- A.E.T. SafeSign
- SecMaker Net iD Enterprise (früher als "SecMaker Net iD" bezeichnet)
- SecMaker Net iD Client (die nächste Generation von SecMaker Net iD Enterprise, siehe <http://docs.secmaker.com/net-id-client/latest/index.html>)
- Coolkey
- OpenSC
- 90meter

### **Lizenziertes Feature**


Für dieses Feature ist eine Add-on-Lizenz erforderlich; siehe Add-on-Lizenzen. Bitte kontaktieren Sie Ihren IGEL Vertriebspartner.

Für Informationen zur benutzerdefinierten PKCS#11-Bibliothek siehe [Benutzerdefinierte PKCS#11-Bibliothek verwenden](#) (see page 623).

## Local Login with Smartcard Certificate


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Standalone Authentication Method

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## Combination with the "AD/Kerberos with Smartcard" Method

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Desktop und Bildschirm

- [Troubleshooting: Display Configurations Change with Downgrade](#) (see page 563)
- [Shared Workplace \(SWP\)-Konfiguration anzeigen](#) (see page 564)
- [Bildschirm umschalten](#) (see page 565)
- [Multimonitor](#) (see page 570)
- [Bildschirmtastatur automatisch einblenden und ausblenden](#) (see page 582)
- [Sitzungssteuerleiste in einer Vollbildsitzung](#) (see page 583)
- **Screen Issues When Redocking Notebook**
- [Externe NVIDIA-Grafikkarte verwenden](#) (see page 585)
- [Bluelight Filter for Nighttime Display](#) (see page 586)
- [Screen Flickers on Intel Devices, Error Log Shows " \[drm\] \\*ERROR\\* CPU pipe C FIFO underrun "](#) (see page 587)

## Troubleshooting: Display Configurations Change with Downgrade

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

## Shared Workplace (SWP)-Konfiguration anzeigen

Ab IGEL Universal Desktop Linux Version 4.14.100 und Version 5.06.100 ermöglicht Shared Workplace benutzerspezifische Bildschirmauflösungen und Konfigurationen.

- i** Für benutzerspezifische Einstellungen gibt es technische Einschränkungen: Für VIA-Grafiktreiber/Hardware wird die maximale Desktopgröße im Abschnitt `Screen` der X-Konfigurationsdatei festgelegt. Der Name und Speicherort der X-Konfigurationsdatei hängt von der Firmware ab:
- IGEL Linux version 10: `/config/Xserver/xorg.conf-0`
  - IGEL Linux version 5: `/config/Xserver/xorg.conf-0` oder `/etc/X11/xorg.conf` (dies ist ein symbolischer Link, der auf Folgendes zeigt `/config/Xserver/xorg.conf-0`)

Im Abschnitt `Screen` der oben genannten Konfigurationsdatei finden Sie eine Zeile wie `Virtual 1920 1200`. Die hier definierte Größe kann nicht dynamisch geändert werden; sie ist eine harte Grenze für die Gesamtgröße des Desktops.

Es wird empfohlen, die anfängliche Desktopkonfiguration auf die maximale Anzahl von Bildschirmen und die Auflösungen auf `Autodetect` zu setzen. Auf diese Weise werden die benutzerspezifischen Auflösungen nicht eingeschränkt.

## Fehlersuche

Wenn die gesamte Framebuffergröße der benutzerspezifischen Auflösungen die Grenzen der Einstellung `Virtual [width] [height]` aus `/config/Xserver/xorg.conf-0` (oder `/etc/X11/xorg.conf`) überschreitet, können die benutzerspezifischen Auflösungen nicht aktiviert werden und die Bildschirmkonfigurationen werden nicht dynamisch geändert.

Es gibt keinen Warnhinweis oder etwas anderes um den Benutzer auf diese Einschränkung hinzuweisen. Aber Sie können verwandte Logmeldungen über `journalctl` oder in `/var/log/messages` finden:

```
XANDR: ERROR: CANNOT APPLY CHANGES ->
```

```
XANDR: ERROR: -> Selected modes ([width]x[height]) would exceed the maximum framebuffer size ([width]x[height])
```

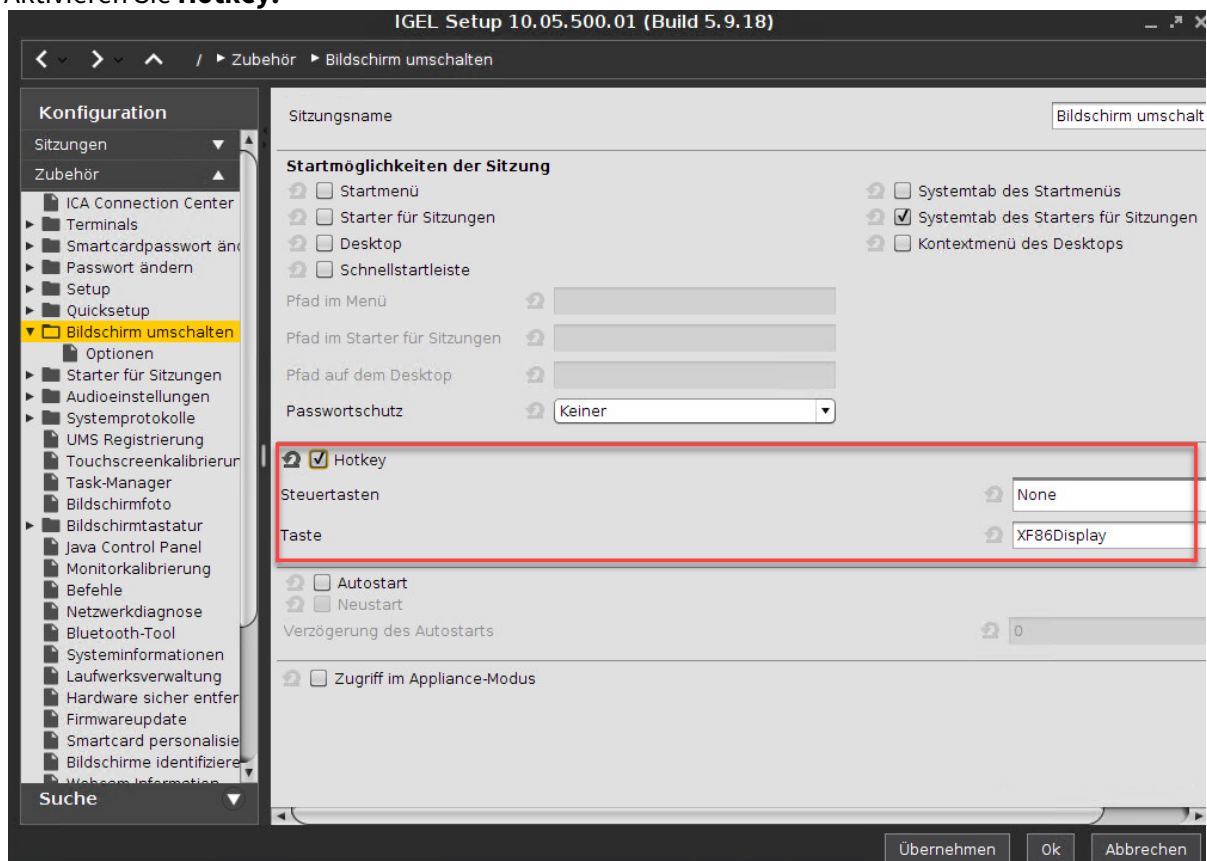
## Bildschirm umschalten

Wenn Sie ein Notebook mit IGEL UDC2, UDC3 oder UD Pocket verwenden, möchten Sie möglicherweise einen zusätzlichen Monitor anschließen. Wenn Sie das Gerät (UD Serie) nutzen, sollten Sie möglicherweise zwei Monitore verwenden. Jeder denkbare Display-Modus, wie Klon-Modus/Spiegelung oder erweiterter Modus, ist möglich. Außerdem können Sie schnell zwischen den Display-Modi wechseln.

### Konfigurieren eines Starter für den Bildschirm umschalten

Es gibt viele Arten das Umschalten des Bildschirms zu starten. Die folgende Beispiel zeigt, wie man eine für ein Notebook typische Tastenkombination definiert.

1. Öffnen sie Setup und gehen Sie zu **Zubehör > Bildschirm umschalten**.
2. Aktivieren Sie **Hotkey**.



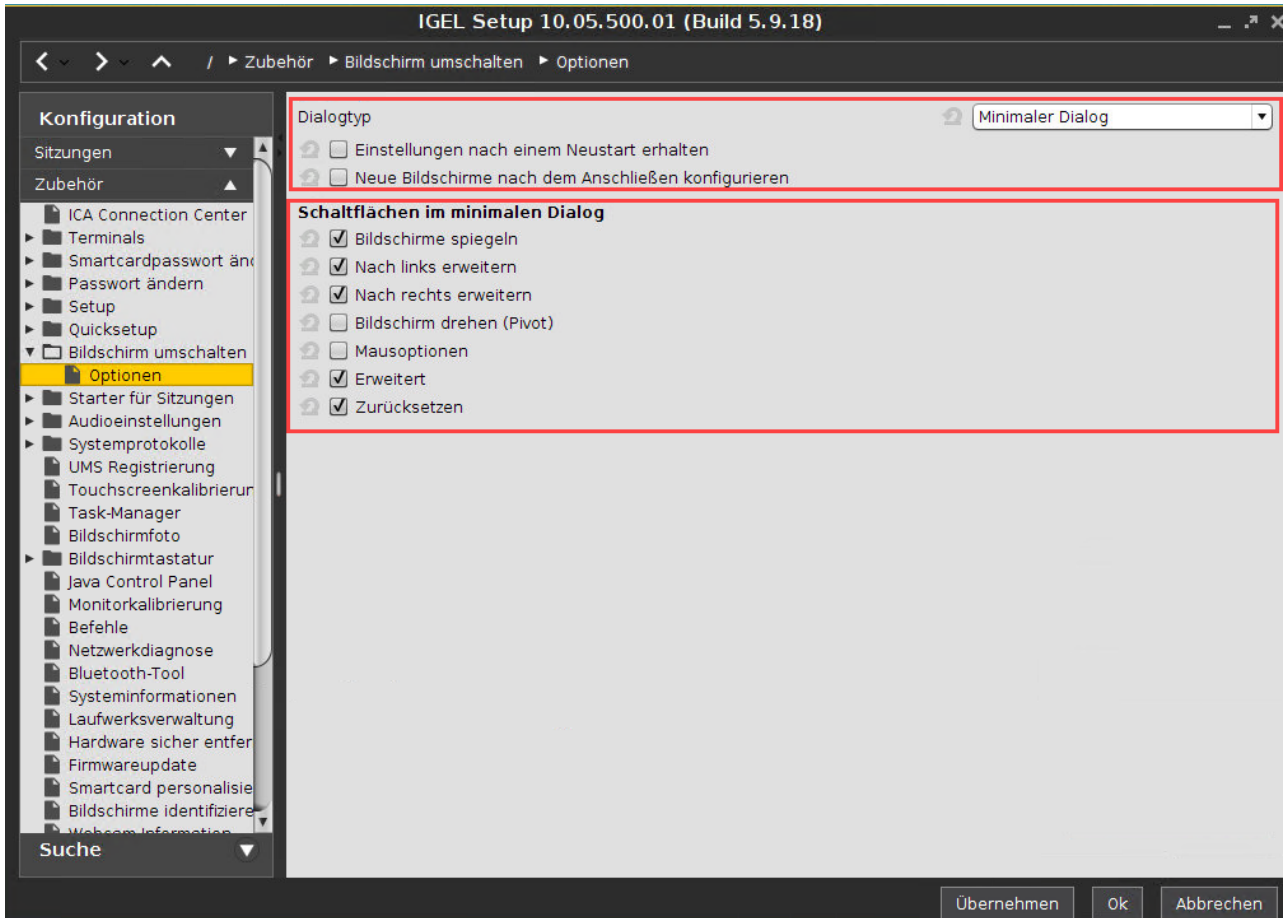
Standardmäßig wird dieser Hotkey, [Fn]+[F7] ( XF86Display ) zum starten des Display-Wechsel genutzt. Sie können den Hotkey ändern indem sie in **Modifikatoren** oder **Tastenkombinationen** auswählen oder eingeben.

**i** Zum eingeben eines Schlüssel, der kein sichtbares Zeichen hat, z. B. der [Tab] Schlüssel, öffnen sie ein Bedienpult, melden Sie sich als `user` an und geben Sie `xev -event keyboard` ein. Drücken Sie die Taste, die für den Hotkey verwendet werden soll. Der Text in Klammern, der mit `keysym` beginnt, erhält das Schlüsselsymbol für das Feld **Key**. Beispiel: `Tab in (keysym 0xff09, Tab)`

3. Drücken Sie **Anwenden** oder **OK**.

## Bildschirm umschalten konfigurieren

1. Öffnen Sie Setup und gehen Sie zu **Zubehör > Bildschirm umschalten > Optionen**.
2. Beachten Sie die folgenden Einstellungen:
  - **Dialogtyp:** In den meisten Fällen, kann man es bei **Minimaler Dialog** belassen. Der Nutzer kann jederzeit zum erweiterten Dialog wechseln, vorausgesetzt, dass der Bereich **Erweitert** in den Schaltflächen des **Minimalen Dialogs** aktiviert ist
  - **Einstellungen nach dem Neustart erhalten:** Aktivieren Sie dies, wenn die Einstellungen des Displaywechsels nach dem Neustart unverändert bleiben sollen.
  - **Neue Bildschirme nach dem Anschließen konfigurieren:** Aktivieren Sie dies, wenn sie möchten, dass der Bildschirm wechselt sobald eine neuer Monitor verbunden ist.
  - Um den Minimal Dialog zu verfeinern, ändern Sie die Einstellungen in der **Schaltflächen in minimalen Dialog**.



## Bildschirm Umschaltung benutzen

Der minimale Dialog wird ähnlich aussehen; Details hängen von Ihrem spezifischen Setup ab:

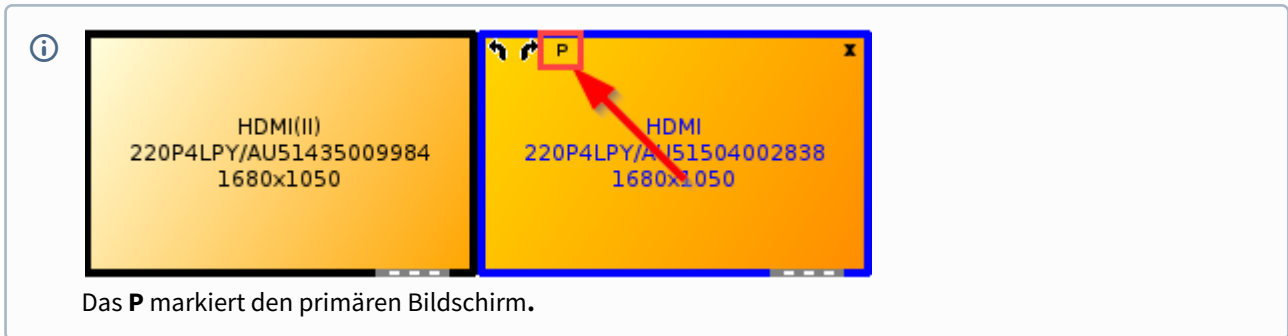


Schaltfläche	Funktion
--------------	----------

<b>Identifizierte Bildschirme</b>	Starten der Monitor Erkennung.
	Benutzt nur Display 1.
	Zeigt auf allen Bildschirmen den gleichen Inhalt, z. B. Klonmodus oder Spiegelung.
	Erweitert den Anzeigebereich auf den rechten Bildschirm.
	Erweitert den Anzeigebereich auf den linken Bildschirm.
	Benutzt nur Display 2.

Weitere Informationen finden Sie unter dem Kapitel Funktion "Bildschirm umschalten" verwenden im Handbuch.





## Multimonitor

Das Arbeiten mit zwei oder mehr Bildschirmen wird in professionellen Arbeitsumgebungen immer beliebter.


Wie Sie mehrere Bildschirme und einen erweiternden Desktop mit dem IGEL Setup konfigurieren, erfahren Sie hier.

Es gibt verschiedene Optionen, Bildschirme zu konfigurieren:

- [Automatische Konfiguration](#) (see page 571)
- [Manuelle Konfiguration](#) (see page 573)
- [Zusätzliche Einstellungen](#) (see page 575)
- [Konfiguration des Auto-Switch-Monitors für Laptops](#) (see page 580)

Wenn Sie mit dem IGEL Universal Desktop oder der unterstützten UDC3 Hardware arbeiten, ist die Multi-Monitor-Unterstützung garantiert.

Es könnte zu Schwierigkeiten kommen, wenn Sie mit einer von IGEL nicht voll unterstützten Hardware arbeiten.

 Die Multimonitor-Konfiguration für nicht unterstützte Hardware funktioniert nur, wenn die native Grafiktreiberunterstützung ordnungsgemäß funktioniert. Sie müssen sicherstellen, dass der native Treiber wirklich funktioniert, da der Fallback-VESA-Treiber keine Multimonitor-Konfiguration erlaubt. Klicken Sie im **Starter für Sitzungen** auf **Informationen**, um festzustellen, mit welchem Grafik-Chipsatz Sie arbeiten. Wenn VESA dort aufgeführt ist, funktioniert der native Treiber nicht und eine Multimonitor-Konfiguration ist nicht möglich.

- Eine Liste unterstützter Grafikkarten finden Sie unter: [Linux 3rd party hardware database](#)<sup>51</sup>.

---


<sup>51</sup> <https://www.igel.com/linux-3rd-party-hardware-database/>

## Automatische Konfiguration

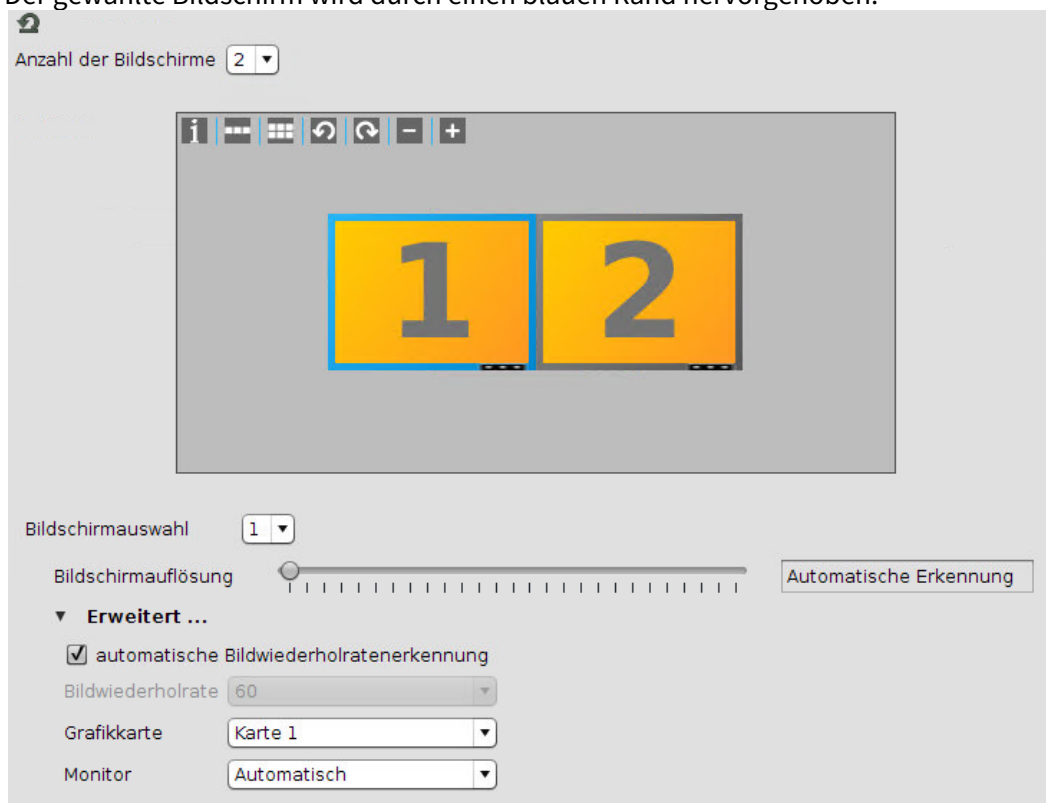
Die Firmware erkennt den nativen Grafiktreiber und verwendet die Bildschirme standardmäßig automatisch.

Zwei oder mehr Monitore definieren:


1. Gehen Sie im Strukturbaum unter **Benutzeroberfläche > Bildschirm**.
2. Wählen Sie **2** (oder mehr) unter **Anzahl der Bildschirme**.

 Die Anzahl der Bildschirme, die Sie auswählen können hängt von Ihrer Hardware ab. Benutzen Sie die Universal Management Suite (UMS), können sie bis zu 8 Monitore auswählen.

3. Wählen Sie den Bildschirm unter **Bildschirmauswahl** oder per Anklicken mit der Maus. Der gewählte Bildschirm wird durch einen blauen Rand hervorgehoben.



4. Setzen Sie **Bildschirmauflösung** auf **Automatische Erkennung** (Standardeinstellung). Das Betriebssystem liest die EDID (Extended Display Identification Data) aus.

 Wenn die **Automatische Erkennung** nicht verfügbar ist, überprüfen Sie **Monitoreerkennung (DDC)** unter **Benutzeroberfläche > Bildschirm > Optionen**. Die **Monitoreerkennung (DDC)** muss aktiviert sein (Standardeinstellung).

⚠ Bei mehr als 2 Monitoren muss die Bildschirmauflösung für jeden Bildschirm manuell angepasst werden.

5. Aktivieren Sie **automatische Bildwiederholratenerkennung** (Standardeinstellung) unter **Erweitert**.
6. Setzen Sie **Monitor** auf **Automatisch**.  
Der ausgewählte Bildschirm wird automatisch dem Grafikanschluss (Monitor) zugeordnet.
7. Ziehen Sie die Rechtecke per Drag & Drop, um die Bildschirme zu positionieren.

ℹ Bildschirm 1 ist immer der primär Bildschirm, auf dem sich die Taskleiste befindet.

8. Klicken Sie **Übernehmen** oder **Ok** um die Einstellungen zu speichern.

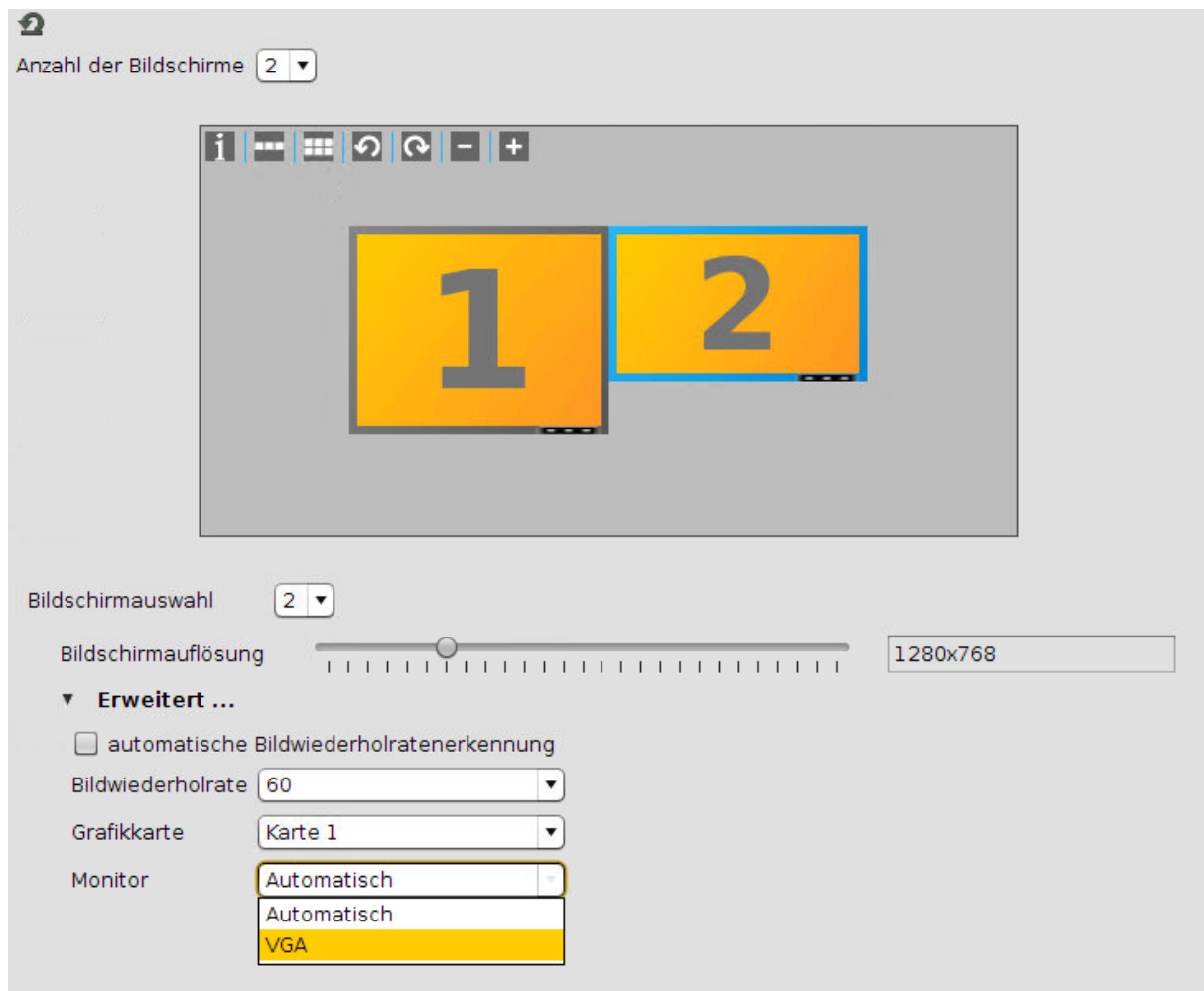
## Manuelle Konfiguration

Während der automatischen Konfiguration, können folgende Probleme auftreten:

- Einer der Bildschirme bleibt schwarz.
- Der gleiche Display wird auf allen Bildschirmen angezeigt.

In diesem Fall können Sie die Bildschirme manuell einstellen:

1. Gehen Sie im Strukturbaum unter **Benutzeroberfläche > Bildschirm**.



2. Wählen Sie eine Bildschirm-Nummer unter **Bildschirmauswahl**.
3. Geben Sie die Auflösung manuell unter **Bildschirmauflösung** ein.

 Die Einstellung der Standardauflösung ist **Automatische Erkennung**.

**i** Ab IGEL Linux Version 10.03.100, haben Sie die Möglichkeit Ihre Eigene Auflösung über **Registry** zu definiere (`x.xserver0.custom_resolution`). Damit die dort eingestellten Werte wirksam werden, muss die Auflösung auf Autodetect (der Schieberegler ganz links) eingestellt sein. Die folgenden Parameter gelten für den Eintrag in der Registry:

- **WxH:** W = width, H = height (example: 1920x1080)
- **WxH@R :** W = width, H = height, R = refresh rate (Beispiel: 1920x1080@60 oder 1920x1200@59.8)

4. Wählen Sie für alle Bildschirme den entsprechenden Anschluss unter **Monitor** aus. Die manuelle Konfiguration kann nur wirksam werden, wenn Sie den Monitoranschluss allen Bildschirmen zuweisen.

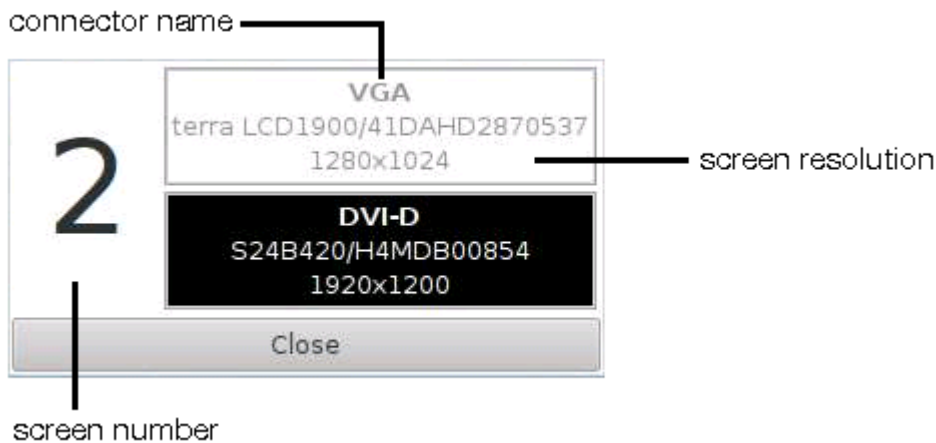
**i** Wenn Sie die Einstellungen direkt in IGEL Setup anpassen, sind nur die angeschlossenen Monitore in der Auswahlliste verfügbar sein. Wenn Sie Bildschirme mit Hilfe des UMS Profils konfigurieren möchten, werden alle möglichen Anschlüsse in der Auswahlliste angezeigt und Sie werden nicht wissen, welcher davon für Ihr Gerät relevant ist.

**Tip:**

► Klicken Sie **i** in Ihrem Geräte Setup um Informationen über die Namen der Anschlüsse, Bildschirmauflösungen und Bildschirm-Nummern zu erhalten.

**i** Auf diese Konfiguration kann nicht über die UMS zugegriffen werden.

Das Schwarze Feld gehört zu der Bildschirm-Nummer auf der linken Seite:





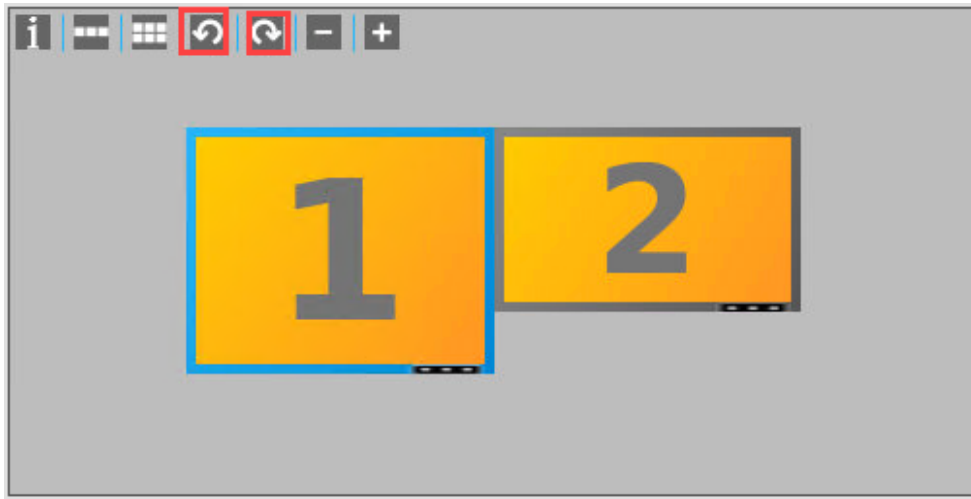
## Zusätzliche Einstellungen


Nachfolgend finden Sie einige nützliche Hinweise:

- [Bildschirm drehen \(Pivot\)](#) (see page 576)
- [Verschiedene Hintergründe einstellen](#) (see page 577)
- [Nützliche Fenster-Einstellungen](#) (see page 578)


## Bildschirm drehen (Pivot)

1. Klicken Sie auf ein Bildschirmfeld.
2. Wählen Sie  (Dreht den ausgewählten Bildschirm gegen den Uhrzeigersinn) oder  (Dreht den ausgewählten Bildschirm im Uhrzeigersinn).



 Zwei Bildschirme mit automatischer Bildwiederholratenerkennung werden automatisch nach oben ausgerichtet.

► **Ausrichtung:** Wenn Sie die richtige Auflösung eingeben, sehen Sie die tatsächliche Größe der Bildschirme und können sie nach Ihren Wünschen ausrichten.

 Die einzelnen Bildschirmbereiche müssen jedoch an einer Kante und Ecke miteinander in Kontakt stehen und dürfen sich nicht überlappen.



## Verschiedene Hintergründe einstellen

Sie können ganz einfach verschiedene Hintergründe für Ihren Bildschirm einstellen:

► Klicken Sie im Setup unter **Benutzeroberfläche > Desktop > Hintergrund**. Für jeden Bildschirm gibt es eine Konfigurationsseite.









► Wählen Sie das Hintergrundbild aus und definieren Sie den Stil.

**i** Sie können auch Ihr eigenes **Eigenes Hintergrundbild** hochladen, z. B. einen Hintergrund mit Ihrem firmeneigenen Design. Sehen Sie hierzu [Hintergrundbild festlegen](#) (see page 634).

## Nützliche Fenster-Einstellungen

Startmonitor oder Vollbildmodus einstellen:





1. Klicken Sie auf den Namen Ihrer Sitzung unter **Sitzungen** im IGEL Setup, z. B. **RDP > RDP Sitzungen**.
2. Klicken Sie **[Sitzungsname] > Fenster** um die Fenstereinstellungen zu konfigurieren.

Anzahl an Farben	 Globale Einstellung
Fenstergröße	 <b>Vollbild</b>
Desktop Skalierungsfaktor	 Globale Einstellung
Bildschirmauflösung	 Entspricht Fenstergröße
Startmonitor	 Keine Konfiguration
Multi-Monitor-Vollbildmodus	 Globale Einstellung

 Für die Funktion "**2. Monitor als Startmonitor**" muss die **Fenstergröße** auf **Vollbild** eingestellt sein.

Multi-Monitor-Vollbildmodus einstellen













1. Klicken Sie **Fenster** in globalen Ordner Ihrer Sitzung, z. B. **RDP > RDP Global > Window**.
2. Konfigurieren Sie die Fenstereinstellungen.


Anzahl an Farben	 Millionen
Fenstergröße	 <b>Vollbild</b>
Desktop Skalierungsfaktor	 Automatisch
<input checked="" type="checkbox"/> Display Control aktivieren	
<input type="checkbox"/> Steuerleiste für RDP-Sitzungen	
<b>Multi Monitor</b>	
Multi-Monitor-Vollbildmodus	 Vollbildsitzung auf einen Monitor beschränken.

Taskleiste definieren

1. Klicken Sie **Benutzeroberfläche > Desktop > Taskleiste**.

## 2. Definieren Sie die Einstellungen der **Taskleiste**.

 <input checked="" type="checkbox"/> Aktiviere Taskleiste	
Position der Taskleiste	 Unten
Modus der vertikalen Taskleiste	 Deskbar
Höhe/Breite der Taskleiste	 40
Anzahl der Zeilen/Spalten in der Taskleiste	 Automatisch
Taskleistengröße in Multi Monitor	 Taskleiste auf einen Monitor beschränken
Monitor	 1. Monitor
 <input type="checkbox"/> Taskleiste über allen Fenstern halten	
 <input type="checkbox"/> Taskleiste automatisch ausblenden	
Verhalten beim automatischen Ausblenden	 Intelligent
Taskleisten-Einblendverzögerung	 600
Taskleisten-Ausblendverzögerung	 400

 Wenn Sie die Taskleiste auf alle Monitore erweitern möchten, müssen Sie sicherstellen, dass alle Bildschirme nach unten ausgerichtet sind. Andernfalls, sehen Sie nur die Hälfte der Taskleiste an einem Bildschirm.

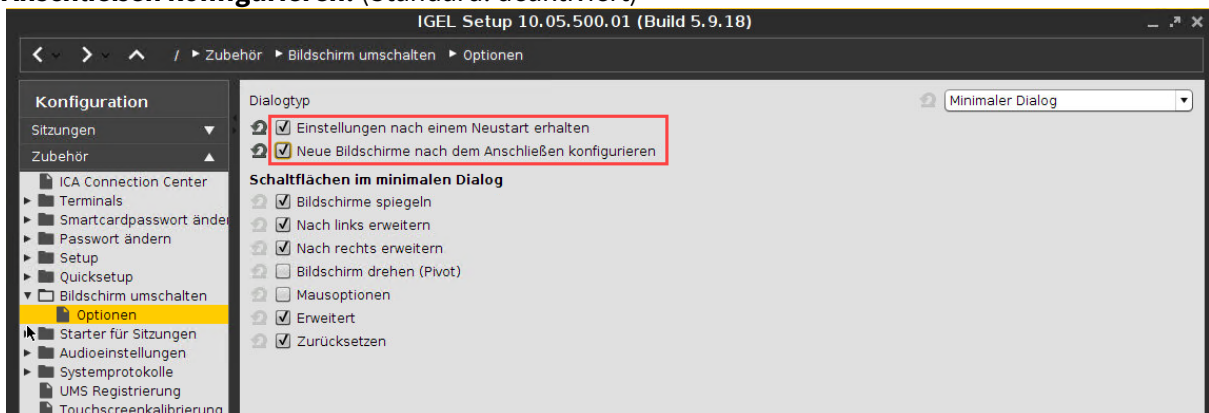
## Konfiguration des Auto-Switch-Monitors für Laptops

Dies ist ein Beispiel dafür, wie man den Auto-Switch-Monitor für Laptops konfiguriert.

1. Schließen Sie das Gerät an und öffnen/schließen Sie den Deckel.
2. Öffnen Sie das Dienstprogramm **Bildschirm umschalten**.



3. Im erweiterten Modus können Sie die Bildschirme per Drag & Drop für Ihre gewünschte Konfiguration verschieben.  
Der Bildschirm wird an die anderen angefügt.
4. Soll ein Bildschirm nicht verwendet werden, kann es in den **Deaktiviert**-Bereich oben rechts gezogen werden - der Bildschirm wird beim Zurückziehen in den aktiven Bereich wieder aktiviert.
5. Um den gleichen Inhalt auf mehreren Bildschirmen anzuzeigen, sollte ein Bildschirm auf einen anderen aktiven Bildschirm gezogen werden.  
Die Oberfläche zeigt eine Spiegelung an. Der Spiegelungsmonitor wird unten rechts unter **Spiegelnd** angezeigt.
6. Drücken Sie **Übernehmen** um die Einstellung zu speichern.
7. Drücken Sie im Konfigurationsdialogfeld **Konfiguration beibehalten** auf **Ja**, damit die aktuellen Einstellungen im persistenten Speicher gespeichert und dem Profil zugeordnet werden.  
Sie können erweiterte Funktionen (z. B. Schwenken, Skalieren und Auflösungen) in Dropdown-Boxen konfigurieren (versteckt in einem Fach auf der rechten Seite).
  - Klicken Sie auf > am rechten Rand.
8. Gehen Sie im IGEL Setup unter **Zubehör > Bildschirm umschalten > Optionen**.
9. Aktivieren Sie **Einstellungen nach einem Neustart erhalten** und **Neue Bildschirme nach dem Anschließen konfigurieren**. (Standard: deaktiviert)



10. Das Dienstprogramm **Bildschirm umschalten** wird nun auch für NVIDIA-Grafikgeräte verwendet.

## Konfiguration der Anzeigeeinstellung für die Handhabung des Notebookdeckels

Sie können die Handhabung des Deckels eines Notebooks so konfigurieren, dass das Notebook durch Schließen des Deckels in den Standby-Modus geht, unabhängig davon, ob das Notebook eingesteckt ist oder nicht.

### Einstellungen des Standby-Modus

Wenn Sie möchten, dass Ihr Notebook durch Schließen des Deckels in den Standby-Modus wechselt, während Ihr Notebook angeschlossen ist, müssen Sie folgende Einstellungen vornehmen:

1. Gehen Sie unter **IGEL Setup** unter **System > Registry > system > actions > lid > ac**.
2. Stellen Sie **Schließen des Deckels im angeschlossenen Zustand** auf **vorrübergehend aussetzen**. (Standard: Bildschirm ausschalten)
3. Klicken Sie **Übernehmen** oder **Ok** um die Einstellung zu speichern.

Wenn Sie möchten, dass Ihr Notebook durch Schließen des Deckels in den Standby-Modus wechselt, während Ihr Notebook nicht angeschlossen ist, müssen Sie folgende Einstellungen vornehmen:

1. Gehen Sie unter **IGEL Setup** unter **System > Registry > system > actions > lid > battery**.
2. Stellen Sie **Schließen des Deckels im angeschlossenen Zustand** auf **vorrübergehend aussetzen**. (Standard: Display ausschalten)
3. Klicken Sie **Übernehmen** oder **Ok** um die Einstellung zu speichern.

**i** Wenn Sie möchten, dass das Notebook nach dem Schließen des Deckels den **Bildschirm ausschaltet**, ist es sinnvoll, die folgende Einstellung vorzunehmen, um das Notebook intern auszuschalten:

1. Gehen Sie im **IGEL Setup** unter **System > Registry > sessions > user\_display0 > options > lid\_events**.
2. Aktivieren Sie **Reagiere auf Auf- und Zuklappereignis**.
3. Klicken Sie **Übernehmen** oder **Ok** um die Einstellung zu speichern.

## Bildschirmtastatur automatisch einblenden und ausblenden

Sie können die Bildschirmtastatur so konfigurieren, dass sie automatisch eingeblendet oder ausgeblendet wird je nachdem, ob ein Textfeld ausgewählt oder verlassen wird (z. B. Firefox oder Bildschirmsperre).

### Automatisch einblenden

Mit der folgenden Einstellung wird die Bildschirmtastatur automatisch angezeigt, wenn ein Eingabefeld im Fokus ist.

1. Gehen Sie im IGEL Setup unter **System > Registry > userinterface > softkeyboard > autoshow** (Parameter: `userinterface.softkeyboard.autoshow`).
2. Aktivieren Sie **Bildschirmtastatur automatisch anzeigen, wenn Eingabefeld angetippt wird**.

### Automatisch ausblenden

Mit der folgenden Einstellung wird die Bildschirmtastatur automatisch ausgeblendet, sobald ein Eingabefeld nicht mehr im Fokus ist.

1. Gehen Sie im IGEL Setup unter **System > Registry > userinterface > softkeyboard > autohide**. (Parameter: `userinterface.softkeyboard.autohide`)
2. Aktivieren Sie **Bildschirmtastatur automatisch verstecken, wenn das Textfeld verlassen wird**.

Bei Problemen, z. B. wenn sich die Tastatur nicht automatisch verbirgt, müssen Sie **Bildschirmtastatur automatisch verstecken, wenn das Textfeld verlassen wird** deaktivieren und sicherstellen, dass folgende Parameter deaktiviert sind:

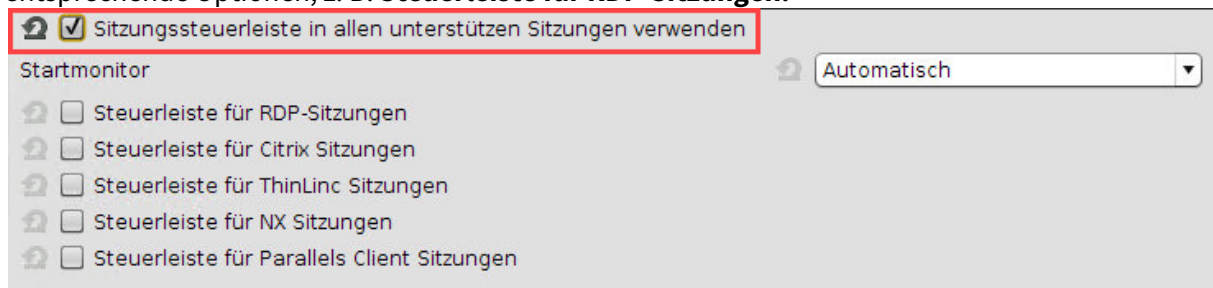
- **Zubehör > Bildschirmtastatur > Autostart**
- **Zubehör > Bildschirmtastatur > Neustart**

## Sitzungssteuerleiste in einer Vollbildsitzung

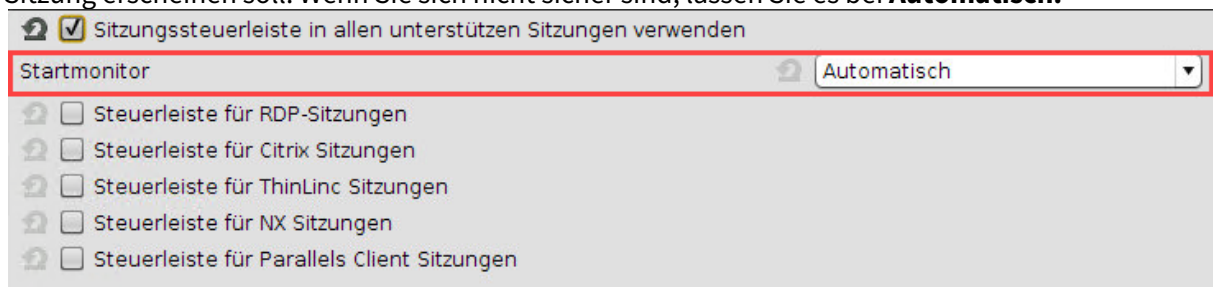
Wenn Sie eine Sitzung im Vollbildmodus ausführen, haben Sie den Vorteil, dass die gesamte Nutzungsfläche Ihres Monitors für diese Sitzung zur Verfügung steht. Möglicherweise möchten Sie jedoch trotzdem ein Hotplug-Laufwerk auswerfen oder die aktuelle Sitzung minimieren oder beenden. Die von IGEL Linux bereitgestellte Lösung heißt Sitzungssteuerleiste.

### Sitzungssteuerleiste aktivieren:

1. Öffnen Sie Setup und gehen Sie auf **Benutzeroberfläche > Desktop > Sitzungssteuerleiste**.
2. Aktivieren Sie **Sitzungssteuerleiste in allen unterstützten Sitzungen verwenden**, wenn Sie eine Sitzungssteuerleiste in allen Sitzungstypen haben möchten, für die sie unterstützt wird. Wenn Sie eine Sitzungssteuerleiste nur in Sitzungen bestimmter Typen haben möchten, aktivieren Sie die entsprechende Optionen, z. B. **Steuerleiste für RDP-Sitzungen**.



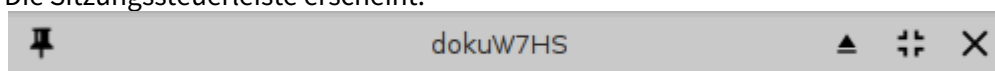
3. Wählen Sie in der Auswahl **Startmonitor** den Desktop aus, auf dem die In-Session Control Bar der Sitzung erscheinen soll. Wenn Sie sich nicht sicher sind, lassen Sie es bei **Automatisch**.



4. Klicken Sie **Übernehmen** oder **Ok**.

### Sitzungssteuerleiste verwenden:

1. Bewegen Sie die Maus bis zum oberen Rand des Desktops. Die Sitzungssteuerleiste erscheint.



2. Um die gewünschte Aktion auszuführen, klicken Sie auf das entsprechende Symbol:

- Um ein USB-Gerät auszuwerfen, klicken Sie ▲
- Um eine Sitzungsansicht zu minimieren, klicken Sie ⇄
- Um eine Sitzung zu beenden, klicken Sie ✕
- Um die In-Session Control Bar in der Sitzung dauerhaft sichtbar zu machen, klicken Sie ↗ .



## Externe NVIDIA-Grafikkarte verwenden

### Ziel

Sie möchten eine externe NVIDIA-Grafikkarte für Ihr Endgerät verwenden und müssen diese mit allen Grafikausgängen verknüpfen.

### Umgebung


- IGEL OS 11.04.100 oder höher

### Lösung


1. Gehen Sie im IGEL Setup zu **System > Registry**.
2. Setzen Sie den Registry Key **x.drivers.preferred\_driver** auf `nvidia`.
3. Aktivieren Sie den Registry Key **x.drivers.nvidia.use\_modeset**. Dieser Registry Key sollte verwendet werden, wenn Sie PRIME verwenden möchten.
4. Starten Sie das Gerät manuell neu, z. B. über den Netzschalter.
5. Richten Sie unter **Benutzeroberfläche > Bildschirm** Ihre Monitore aus und positionieren Sie sie.
6. Für die Feineinstellung verwenden Sie die Funktion **Bildschirm umschalten**, die unter **Zubehör > Bildschirm umschalten** aktiviert werden kann. Siehe Funktion "Bildschirm umschalten" verwenden und Bildschirm umschalten.

Dann können sowohl die Onboard-Grafikanschlüsse als auch die Anschlüsse der NVIDIA-Karte verwendet werden, was der empfohlene Modus ist, da alles auf der NVIDIA GPU gerendert wird.

## Bluelight Filter for Nighttime Display

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Screen Flickers on Intel Devices, Error Log Shows " [drm] \*ERROR\* CPU pipe C FIFO underrun "

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.


## Anpassung

- [Custom Partition Tutorial](#) (see page 589)
- [Benutzerdefinierte PKCS#11-Bibliothek verwenden](#) (see page 623)
- [Startsymbol für Dateimanager für Wechseldatenträger erstellen](#) (see page 625)
- [Symbol für den Bildbetrachter hinzufügen](#) (see page 626)
- [Getimtes Kommando erstellen \(Ersatz für Cron\)](#) (see page 628)
- [Den IGEL OS Desktop individuell anpassen](#) (see page 630)
- [How to Change the Font Color of the Desktop Icons](#) (see page 652)
- [Wie richte ich einen Countdown ein, um eine unerwünschte Bildschirmsperre in IGEL OS zu verhindern?](#) (see page 653)
- [Tastenkombinationen zur Verwaltung von Windows](#) (see page 660)
- [Vereinfachung häufiger Benutzeraktionen durch die Definition von Hotkeys](#) (see page 661)
- [Ein Gerät bei Beendigung einer Sitzung automatisch herunterfahren/ausschalten](#) (see page 664)
- [Standbybetrieb - Wecken mit der USB-Maus](#) (see page 665)
- [Screenshots in IGEL Linux erstellen](#) (see page 666)
- [Systemzeit des Geräts einstellen](#) (see page 668)
- [Aktualisierung der Zeitoneninformationen](#) (see page 669)
- [Einen Handler für MIME-Typen hinzufügen oder ändern](#) (see page 672)
- [Regionale Einstellungen in Sitzungen](#) (see page 676)


## Custom Partition Tutorial

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## A First Simple Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Development Environment


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Activating the Custom Partition Functionality


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## "Hello World" Program

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Creating the Custom Application

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Using a Partition Parameter

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Packaging the Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Development Environment

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Compressing the Custom Partition Contents

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Writing the \*.inf Metadata File


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Uploading the Files to UMS


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## Creating a Profile for the Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Assigning the Profile

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Zoom as a Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Development Environment

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Getting the Packages

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Unpacking the Packages

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Creating the Initialization Script


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Compressing the Custom Partition Contents


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## Writing the \*.inf Metadata File

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Uploading the Files to the UMS

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Creating a Profile for the Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Assigning the Profile and Testing the Application

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Microsoft Teams as a Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Development Environment

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Getting the Packages


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Unpacking the Packages


 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.




## Creating the Initialization Script

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Compressing the Custom Partition Contents

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Writing the \*.inf Metadata File

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.


## Uploading the Files to the UMS

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Creating a Profile for the Custom Partition

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Assigning the Profile and Testing the Application

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Benutzerdefinierte PKCS#11-Bibliothek verwenden


### Anliegen

Sie möchten eine eigene PKCS#11-Bibliothek verwenden.

### Problem

Sie wissen nicht, wie Sie im Setup eine benutzerdefinierte PKCS#11-Bibliothek aktivieren können.

### Lösung

-  Wenn Sie eine benutzerdefinierte PKCS#11-Bibliothek verwenden möchten, muss die Datei(en) entweder per UMS Dateiübertragung oder [Custom Partition \(see page 589\)](#) auf dem Endgerät platziert werden. Die Verwendung des Ordners `/wfs` wird wegen des begrenzten Speicherplatzes NICHT empfohlen.

### Mit Kerberos und/oder Citrix StoreFront Logon verwenden

Um eine benutzerdefinierte PKCS#11-Bibliothek mit Kerberos und/oder Citrix StoreFront Logon zu verwenden:

- Gehen Sie im Setup auf **Sicherheit > Smartcard > Middleware**.
- Wählen Sie **Benutzerdefiniertes PKCS#11-Modul**.
- Unter **Pfadname der Bibliothek** geben Sie den Pfad zu Ihrer PKCS#11-Bibliothek ein. Beispiel: `/usr/lib/pkcs11/[Name der Bibliothek].so`

### Mit VMware Horizon verwenden

Um eine benutzerdefinierte PKCS#11-Bibliothek mit VMware Horizon zu verwenden:

- Gehen Sie im Setup auf **System > Registry**.
- Aktivieren Sie den Registry Key `vmware.view.pkcs11.use_custom`.
- Suchen Sie nach dem Registry Key `vmware.view.pkcs11.custom_path` und geben Sie den Pfad zu Ihrer PKCS#11-Bibliothek an. Beispiel: `/usr/lib/pkcs11/[Name der Bibliothek].so`

### Mit Firefox Browser verwenden

Um eine benutzerdefinierte PKCS#11-Bibliothek mit dem Firefox Browser zu verwenden:

- Gehen Sie im Setup auf **System > Registry**.
- Aktivieren Sie den Registry Key `browserglobal.security_device.custom.enable`.

- Suchen Sie nach dem Registry Key `browserglobal.security_device.custom.device_name` und geben Sie den Namen Ihrer PKCS#11-Bibliothek an.
- Suchen Sie nach dem Registry Key `browserglobal.security_device.custom.lib_path` und geben Sie den Pfad zu Ihrer PKCS#11-Bibliothek an. Beispiel: `/usr/lib/pkcs11/[Name der Bibliothek].so`

## Mit Chromium Browser verwenden

Um eine benutzerdefinierte PKCS#11-Bibliothek mit dem Chromium Browser zu verwenden:

- Gehen Sie im Setup auf **Sitzungen > Chromium Browser > Chromium Browser Global > Smartcard Middleware**.
- Aktivieren Sie **Verwende benutzerdefiniertes Security Device**.
- Unter **Name des Security Device** geben Sie einen willkürlichen Namen für die Bibliothek ein.
- Unter **Pfad zur Bibliothek** geben Sie den Pfad zu Ihrer PKCS#11-Bibliothek ein. Beispiel: `/usr/lib/pkcs11/[Name der Bibliothek].so`



## Startsymbol für Dateimanager für Wechseldatenträger erstellen

So erstellen Sie eine **Eigene Anwendung**, die Ihnen ermöglicht, den Inhalt von Wechseldatenträgern wie z. B. USB-Sticks direkt auf dem Gerät zu betrachten.

### Schritte

1. Gehen Sie in IGEL Setup zu **System > Firmwareanpassung > Eigene Anwendung**.
2. Klicken Sie , um eine **Eigene Anwendung** zu erstellen.
3. Geben Sie bei **Sitzungsname** einen passenden Namen ein, z. B. "Wechseldatenträger", und wählen Sie die Optionen für die Desktopintegration.
4. Klicken Sie **Übernehmen**.
5. Gehen Sie zu **[Name der gerade angelegten Applikation] > Einstellungen**.
6. Geben Sie `thunar` bei **Name des Icons** sowie bei **Startkommando** ein.
7. Klicken Sie **Übernehmen** oder **Ok**.  
Das Startsymbol steht zur Verfügung.

Sie können jetzt z. B. einen USB-Stick mit dem Gerät verbinden und den Dateimanager starten. Im Ordner `/media` wird der USB-Stick angezeigt.

## Symbol für den Bildbetrachter hinzufügen

### Thema

Sie möchten Bilder lokal auf dem Gerät anzeigen.

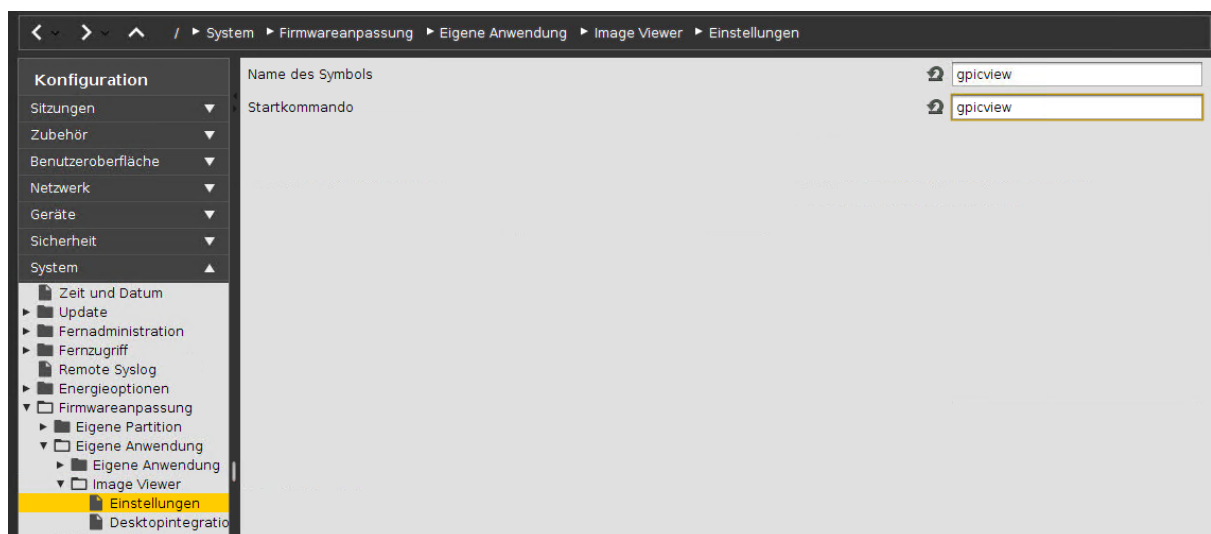
### Problem

Der in IGEL Linux ab Version 5.06.100 enthaltene Bildbetrachter hat kein Desktop-Symbol und keinen Menüeintrag.

### Lösung

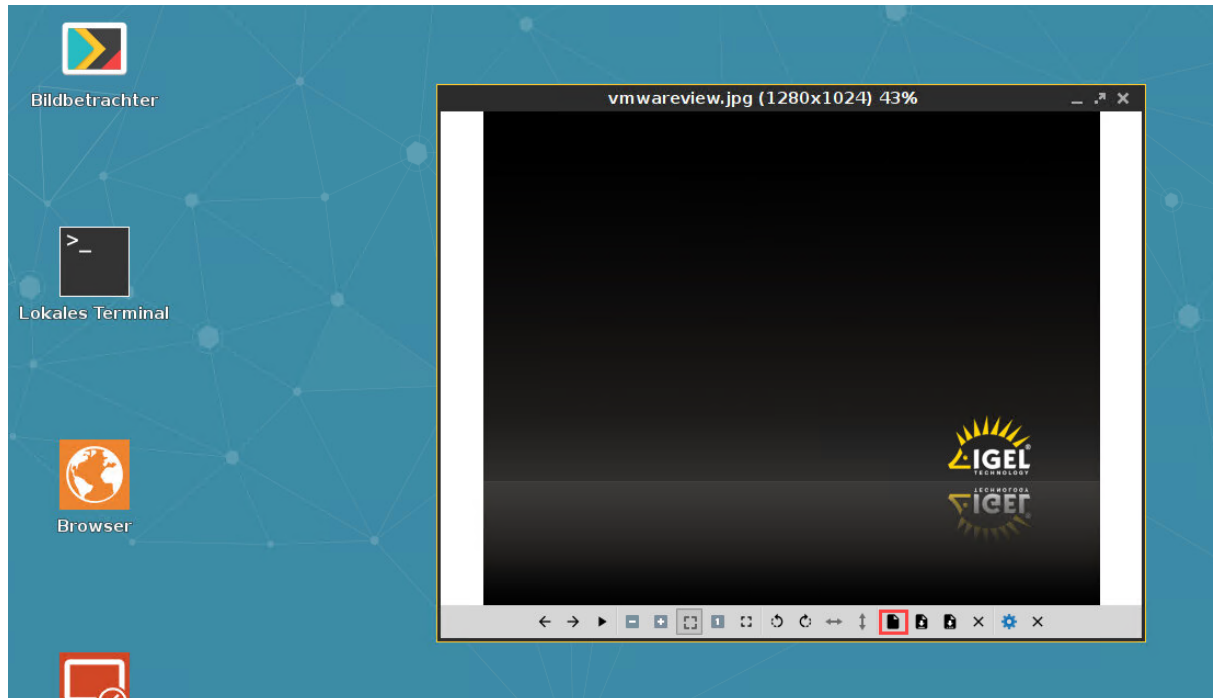
Erstellen Sie eine benutzerdefinierte Anwendung, die den Bildbetrachter öffnet.

1. Gehen Sie im Setup auf **System > Firmwareanpassung > Eigene Anwendung**.
2. Klicken Sie, um eine **Eigene Anwendung** zu erstellen.
3. Geben Sie bei **Sitzungsname** einen passenden Namen ein, z. B. "Bildbetrachter", und wählen Sie die Optionen für die Desktopintegration.
4. Gehen Sie zu **Bildbetrachter > Einstellungen**:



5. Geben Sie in **Name des Symbols** sowie bei **Startkommando** `gpicview` ein.
6. Sichern Sie die Einstellungen.
7. Klicken Sie auf das neu erstellte Symbol für **Bildbetrachter**.
8. Der **Bildbetrachter** öffnet sich.

9. Klicken Sie auf das **Datei öffnen** Symbol um eine Datei zu öffnen.



## Getimtes Kommando erstellen (Ersatz für Cron)

Sie können ein oder mehrere Kommandos definieren, die zu einer bestimmten Zeit ausgeführt werden. Die Konfiguration ist ähnlich wie bei einem `cron` Job. Die Implementierung in IGEL OS verwendet `systemd`, um das Kommando auszuführen.

So definieren Sie ein getimtes Kommando:

1. Gehen Sie im Setup auf **System > Registry > system > cron > cronjob%**
2. Aktivieren Sie **enable\_cron**.
3. Wenn Sie weitere Pfade zu ausführbaren Dateien festlegen wollen, zusätzlich zur existierenden Pfad-Umgebungsvariable, fügen Sie diese unter **path** hinzu, getrennt durch ":".
4. Klicken Sie **Instanz hinzufügen**.  
Die Instanz "cronjob1" wird erzeugt; diese wird nach dem Neustart des Geräts zu "cronjob0" umbenannt.
5. Setzen Sie die Parameter für Ihre getimtes Kommando nach Ihren Bedürfnissen:
  - **command:** Auszuführendes Kommando. Beispiel für Testzwecke: `gtkmessage -m "Hier ist Ihr Cron-Ersatz"`
  - **day\_of\_month:** Tag im Monat  
Mögliche Werte:
    - "1" ... "31": Das Kommando wird am angegebenen Tag ausgeführt. Um eine Liste von Tagen für die Ausführung auszuwählen, geben Sie eine durch Kommas getrennte Liste ein, z. B. "1,8". Um einen Bereich von Tagen anzugeben, verwenden Sie einen Bindestrich, z. B. "1-3".
    - "\*": Das Kommando wird an jedem Tag des Monats ausgeführt.
  - **day\_of\_week:** Tag in der Woche  
Mögliche Werte;
    - "1" ... "7": Das Kommando wird am angegebenen Tag ausgeführt. Sowohl "0" als auch "7" bedeuten Sonntag. Um eine Liste von Tagen für die Ausführung auszuwählen, geben Sie eine durch Kommas getrennte Liste ein, z. B. "1,3". Um einen Bereich von Tagen anzugeben, verwenden Sie einen Bindestrich, z. B. "1-3".
    - "\*": Das Kommando wird an jedem Tag des Monats ausgeführt.
  - **hour**  
Mögliche Werte:
    - "0" ... "23": Das Kommando wird zur angegebenen Stunde ausgeführt. Beispiel: "15" bedeutet 15:00, zuzüglich der unter **minute** angegebenen Minuten. Um eine Liste von Stunden für die Ausführung auszuwählen, geben Sie eine durch Kommas getrennte Liste ein, z. B. "9,17". Um einen Bereich von Stunden anzugeben, verwenden Sie einen Bindestrich, z. B. "9-17".
    - "\*": Das Kommando wird jede Stunde ausgeführt.
  - **minute**  
Mögliche Werte:
    - "0" ... "59": Das Kommando wird in der angegebenen Minute ausgeführt. Um eine Liste von Minuten für die Ausführung auszuwählen, geben Sie eine durch Kommas getrennte Liste ein, z. B. "15,45". Um einen Bereich von Minuten anzugeben, verwenden Sie einen Bindestrich, z. B.

"5-10".

- "\*": Das Kommando wird jede Minute ausgeführt.

- **month**

Mögliche Werte:

- "1" ... "12"; Das Kommando wird im angegebenen Monat ausgeführt. Um eine Liste von Monaten für die Ausführung auszuwählen, geben Sie eine durch Kommas getrennte Liste ein, z. B. "1,4". Um einen Bereich von Monaten anzugeben, verwenden Sie einen Bindestrich, z. B. "1-3".

- "\*": Das Kommando wird jeden Monat ausgeführt.

- **user**: Der Benutzer, unter dem das Kommando ausgeführt wird

Mögliche Werte:

- "root"

- "user"

- **year**: Jahr im 4-Ziffern-Format. Beispiel: "2019". Um eine Liste von Jahren für die Ausführung auszuwählen, geben Sie eine durch Kommas getrennte Liste ein, z. B. "2019,2020". Um einen Bereich von Jahren anzugeben, verwenden Sie einen Bindestrich, z. B. "2019-2021". Wenn das Kommando jedes Jahr ausgeführt werden soll, geben Sie "\*" ein.

6. Klicken Sie **Übernehmen** oder **Ok**.


7. Starten Sie das Gerät neu.

Wenn das Gerät neu gestartet ist, wird das Kommando wie konfiguriert ausgeführt.

## Den IGEL OS Desktop individuell anpassen

In diesem How-To erfahren Sie, wie Sie mithilfe der Universal Management Suite (UMS) Ihren IGEL OS Desktops einen individuelleren Look-and-Feel geben. Dafür gibt es zwei Wege:

- über eine Firmwareanpassung;
- über ein Profil.

 Der Weg über eine Firmwareanpassung ist viel einfacher und schneller.  
Für ein Beispiel siehe [Ein eigenes Hintergrundbild über eine Firmwareanpassung erstellen](#) (see page 635).  
Siehe auch Firmwareanpassung und Firmwareanpassung erstellen im UMS Referenzhandbuch.

Für Informationen über die Desktopanpassung über ein Profil siehe:

- [Grundschr](#)itte (see page 631)
- [Hintergrundbild festlegen](#) (see page 634)
- [Wie kann ich einen eigenen Bootsplash für IGEL OS-Geräte über die UMS festlegen?](#) (see page 638)
- [Einen Bildschirmschoner konfigurieren](#) (see page 643)
- [Eigene Firmenlogos festlegen](#) (see page 648)
- [Eigene Taskleiste erstellen](#) (see page 650)
- [Eigene Desktopsymbole erstellen](#) (see page 651)

## IGEL Tech Video



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=qFQttefMIX8>

## Grundschrirte

Um Ihr komplettes Corporate Design auf mehreren Geräten einzurichten, können Sie ein Profil für alle Einstellungen erstellen.

Bevor Sie das Profil definieren, müssen Sie folgende Schritte ausführen:

- [Eine Grafik hochladen](#) (see page 632)
- [Ein Profil erstellen](#) (see page 633)


## Eine Grafik hochladen

Sie können Grafikdateien auf den UMS-Server hochladen, um sie dann Profilen zuzuordnen. Die Profile können Sie dann Ihren Geräten zuweisen.


Folgende Grafikformate werden unterstützt: BMP, JPG, GIF, TIF, PNG und SVG. Der Dateiname der Grafik darf keine Leerzeichen enthalten. Für Ihre Grafiken stehen 25 MB Speicherplatz zur Verfügung.

So laden Sie Grafikdateien hoch:

1. Klicken Sie mit der rechten Maustaste das Verzeichnis **Dateien** in der UMS Konsole und wählen Sie im Kontextmenü **Neue Datei**.  
Das Fenster **Neue Datei** öffnet sich.
2. Wählen Sie eine **Lokale Datei**.

 Seit UMS 5 können Sie nur das Verzeichnis `/ums-filetransfer/` und in diesem enthaltene Unterordner als Speicherort auf dem UMS-Server verwenden.

3. Wählen Sie einen **Speicherort im UMS Server (URL)**
4. Geben Sie einen **Speicherpfad des Thin Clients** ein.  
Wenn Sie ein Verzeichnis eingeben, das nicht existiert, dann wird dieses automatisch erstellt.  
Wenn Sie keinen bestimmtes Verzeichnis angeben, dann wird die Grafik im Wurzelverzeichnis gespeichert.
5. Klicken Sie **Ok**.  
Die Grafik wird jetzt im Verzeichnis **Dateien** aufgeführt.
6. Weisen Sie die Grafik per Drag & Drop oder im Bereich **Zugeordnete Objekte** Ihren Geräten zu.

 Wenn Sie mehrere Grafiken im Speicherpfad des Thin Clients ablegen, dann werden die Grafiken vom **Bildschirmschoner** (see page 643) abwechselnd nacheinander angezeigt.



## Ein Profil erstellen

Dieser Schritt setzt voraus, dass Sie [eine Grafik hochgeladen haben](#). (see page 632)

Wenn Sie mit der UMS mehrere Thin Clients verwalten, dann sollten Sie ein Profil erstellen, um mithilfe des Profils neue Einstellungen an die Thin Clients zu übertragen.

So erstellen Sie ein Profil:

1. Starten Sie die UMS Konsole.
2. Klicken Sie mit der rechten Maustaste das Verzeichnis **Profile**.
3. Wählen Sie im Kontextmenü **Neues Profil**.  
Das Fenster **Neues Profil öffnet** sich.
4. Geben Sie einen **Profilname** ein.
5. Geben Sie ein **Beschreibung** ein.
6. Wählen Sie aus **Basiert auf** die Firmware Ihres Thin Clients.
7. Klicken Sie **Ok**.

## Hintergrundbild festlegen

Es gibt zwei Wege, ein eigenes Hintergrundbild zu bauen:

- [Über eine Firmwareanpassung](#) (see page 635)
- [Über ein Profil](#) (see page 636)

Wir empfehlen Ihnen den Weg über die Firmwareanpassung, dieser ist sehr viel einfacher.

## Ein eigenes Hintergrundbild über eine Firmwareanpassung erstellen

So erzeugen Sie ein eigenes Hintergrundbild mit Hilfe einer UMS Funktion "Firmwareanpassung":

1. In der UMS rechtsklicken Sie **Firmwareanpassungen > Neue Firmwareanpassung erstellen**.  
Der Dialog **Firmwareanpassung Details** öffnet sich.
2. Geben Sie den **Name** für die Hintergrundbild-Firmwareanpassung ein.
3. Unter **Anwendungsfall** wählen Sie **Hintergrundbild**.
4. Wählen Sie die Bilddatei aus:
  - Klicken Sie **Datei auswählen**, wenn Sie Ihre Bilddatei bereits in die UMS hochgeladen haben.
  - Klicken Sie **Datei hochladen**, wenn Sie eine neue Datei hochladen möchten.

 Der Dateiname soll keine Sonderzeichen wie %, \$ oder Umlaute enthalten.

5. Wählen Sie Ihre Datei aus und klicken Sie **Öffnen**.
6. Prüfen Sie den Speicherort und klicken Sie **OK**.
7. Optional können Sie auf **Weiter** klicken, um die neue Firmwareanpassung direkt einem Gerät oder einem Ordner zuzuweisen.
8. Klicken Sie **Fertig**, um Ihre neue Firmwareanpassung zu speichern.

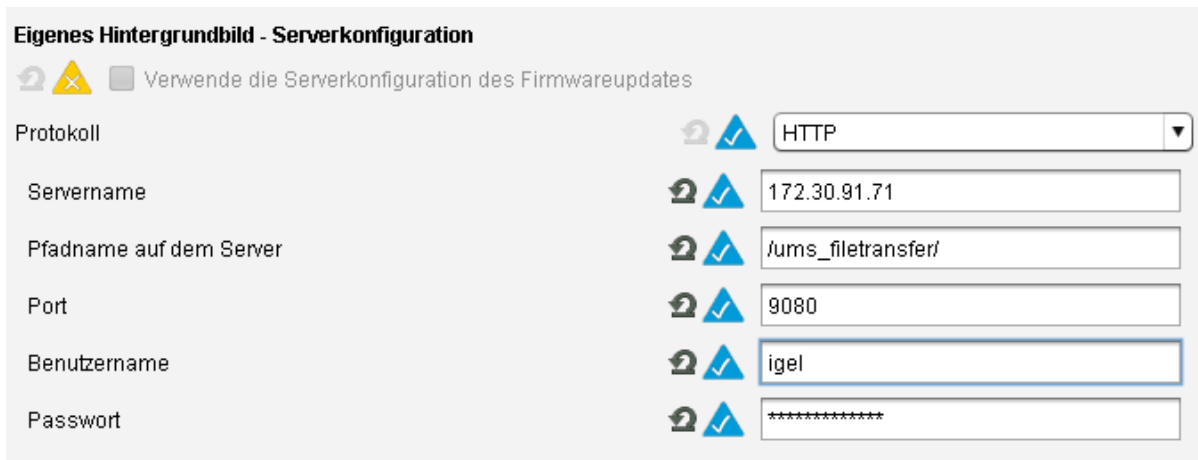
## Ein eigenes Hintergrundbild über ein Profil erstellen

Dieser Schritt setzt voraus, dass Sie eine Grafik für das Hintergrundbild hochgeladen haben; siehe [Eine Grafik hochladen](#) (see page 632).

1. Erstellen Sie ein Profil und geben Sie ihm einen Namen, z. B. **Wallpaper**; siehe [Ein Profil erstellen](#) (see page 633).  
Das **Konfigurationsfenster** des Profils öffnet sich.
2. Konfigurieren Sie den Hintergrundbildserver, siehe unten "Den Serverstandort des Hintergrundbilds einstellen".
3. Legen Sie das Hintergrundbild fest, siehe unten "Den Hintergrund konfigurieren".

Den Serverstandort des Hintergrundbilds einstellen

1. Öffnen Sie das Profil.
2. Gehen Sie zu **System > Firmwareanpassung > Corporate Design > Hintergrund (1. Monitor) > Hintergrundbildserver**.



**Eigenes Hintergrundbild - Serverkonfiguration**

Verwende die Serverkonfiguration des Firmwareupdates


Protokoll	HTTP
Servername	172.30.91.71
Pfadname auf dem Server	/ums_filetransfer/
Port	9080
Benutzername	igel
Passwort	*****

3. Wählen Sie bei **Protokoll** den Wert **HTTP**.
4. Geben Sie bei **Servername** Ihren UMS-Server ein.
5. Geben Sie als **Pfadname auf dem Server** den Pfad des Verzeichnisses mit dem Hintergrundbildern ein.
6. Normalerweise können Sie **Port** auf der Portnummer 9080 belassen (Standardport).
7. Geben Sie den **Benutzername** und das **Passwort** des UMS-Administrators ein.
8. Klicken Sie **Übernehmen und an Thin Client senden** oder **Speichern**, um die Einstellungen zu speichern.

Den Hintergrund konfigurieren

1. Öffnen Sie das Profil.
2. Klicken Sie **System > Firmwareanpassung > Corporate Design > Hintergrund (1. Monitor)**.
3. Aktivieren Sie **Eigenes Hintergrundbild**.

4. Geben Sie unter **Dateiname des eigenen Hintergrundbilds** den Namen des Bildes ein, das Sie als Hintergrundbild definieren möchten.

 Wenn Sie mehr als einen Bildschirm verwenden, müssen Sie das Hintergrundbild jedem einzeln zuweisen.

5. Weisen Sie das Profil Ihrem Gerät zu, indem Sie es per Drag & Drop unter **Zugewiesene Objekte** hinzufügen.

#### Das Ergebnis überprüfen

1. Wählen Sie das Gerät unter **Geräte** im Strukturbaum.
2. Gehen Sie zu **Benutzeroberfläche > Desktop > Hintergrund**.  
Sie werden sehen, dass das Hintergrundbild dem Gerät von dem Profil zugewiesen wurde. Sie können das Hintergrundbild manuell nicht mehr festlegen.  
Alternativ können Sie auch Ihr Gerät spiegeln und das neue Hintergrundbild ansehen.

Auf die Weise können Sie die Hintergrundbilder Ihren Geräten automatisch zuweisen. Falls Sie ein anderes Bild wählen möchten, reicht es, dieses Bild nur im Profil zu ändern.

## Wie kann ich einen eigenen Bootsplash für IGEL OS-Geräte über die UMS festlegen?

Dieses Dokument zeigt, wie Sie mithilfe der Universal Management Suite (UMS) einen eigenen Bootsplash für Ihre Endgeräte erstellen können. Dafür gibt es zwei Wege:

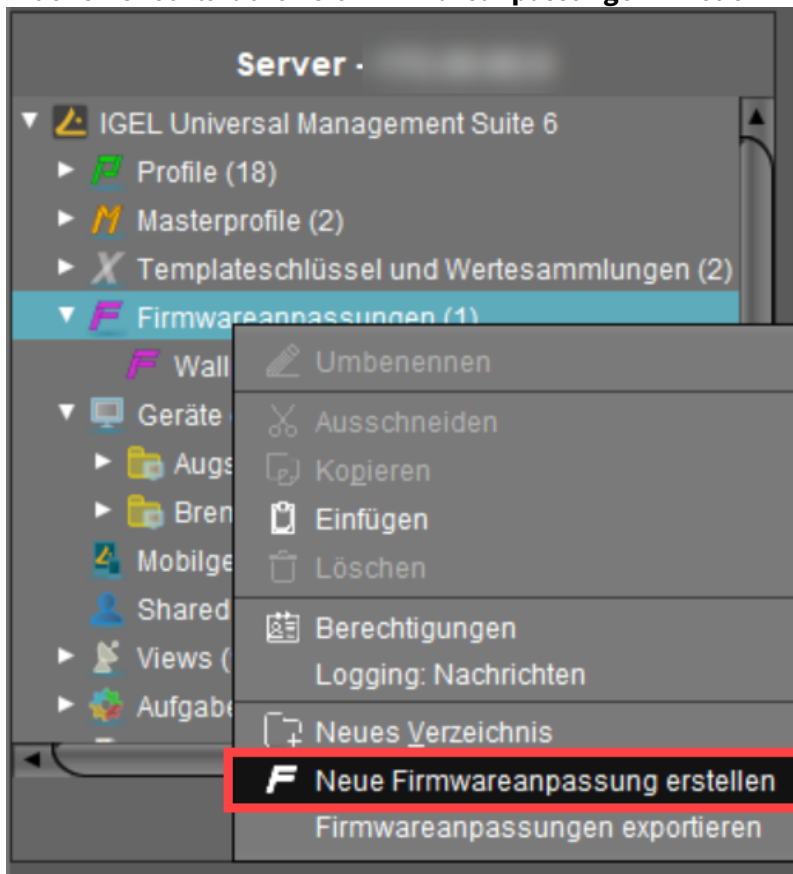
- über eine Firmwareanpassung (empfohlen, da dieser Weg einfacher und schneller ist)
- über ein Profil

**!** Wenn Sie die Bootsplash-Grafik oder ein andere Einstellung eines existierenden Bootsplash ändern, muss der Bootsplash-Code neu erzeugt werden. Diesen Vorgang können Sie in der UMS unter **Aufgaben > Neue Aufgabe** mit dem Befehl **Desktopanpassungen aktualisieren** oder über **Geräte > [Kontextmenü] > Weitere Befehle > Desktopanpassungen aktualisieren** auslösen.

### Einen eigenen Bootsplash über eine Firmwareanpassung erstellen

So erzeugen Sie einen eigenen Bootsplash mithilfe einer UMS Funktion "Firmwareanpassung":

1. In der UMS rechtsklicken Sie **Firmwareanpassungen > Neue Firmwareanpassung erstellen**.



Der Dialog **Firmwareanpassung Details** öffnet sich.

2. Geben Sie den **Name** für Ihre Bootsplash-Firmwareanpassung ein.
3. Unter **Anwendungsfall** wählen Sie **Bootsplash**.

**Firmwareanpassungen**

**Firmwareanpassung Details**

Name:

Anwendungsfall: Anwendungsfall auswählen

Startmenüsymbol

Startmenü

Hintergrund der Taskleiste

Bildschirmschoner

Bildschirmschoner (Custom Partition)

Bootsplash

Hintergrundbild

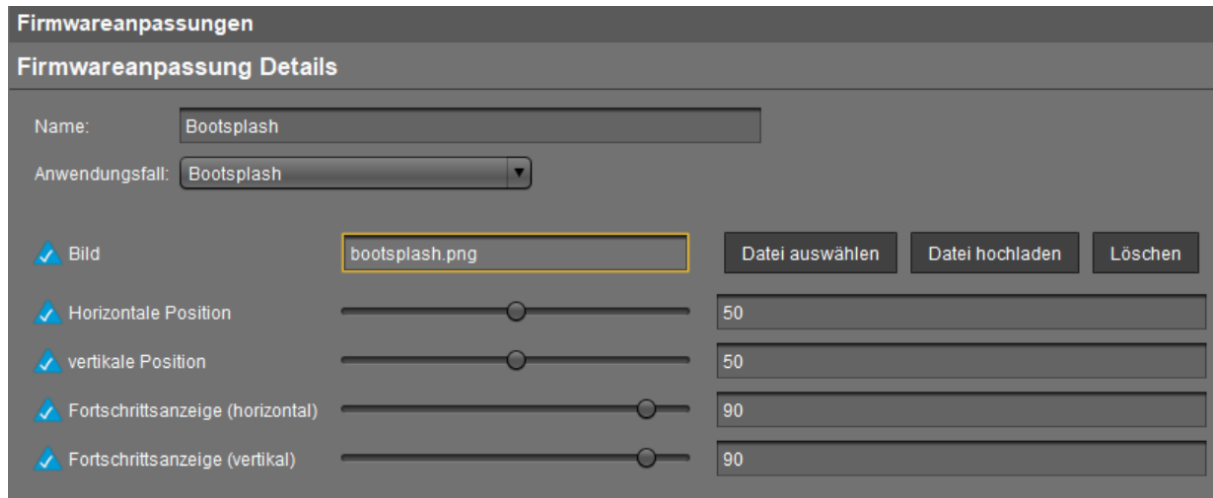
Bitte beachten:  
**Wenn mehrere Anwendungsfälle desselben Typs dem Gerät zugewiesen werden, wird nur der Anwendungsfall mit der höchsten Priorität wirksam.**

Beispiel:  
 Es ist möglich, eine Hintergrundbild-Anpassung und eine Bildschirmschoner-Anpassung einem Gerät zuzuweisen. Beide Anpassungen werden angewendet.  
 Es ist weiterhin möglich zwei Bildschirmschoner-Anpassungen einem Gerät zuzuweisen. Die Firmwareanpassung mit der niedrigeren ID wird dann allerdings ignoriert.

4. Wählen Sie die Bilddatei für Ihren Bootsplash aus:
  - Klicken Sie **Datei auswählen**, wenn Sie Ihre Bilddatei bereits in die UMS hochgeladen haben.
  - Klicken Sie **Datei hochladen**, wenn Sie eine neue Datei hochladen möchten.

- i

  - Der Dateiname soll keine Sonderzeichen wie %, \$, Umlaute, usw. enthalten.
  - Die folgenden Dateitypen sind unterstützt: JPG, JPEG, BMP und PNG.
  - Die optimale Größe des Bildes beträgt 800 x 600 Pixel.



5. Bestimmen Sie die Position Ihrer Bootsplash-Grafik.
6. Klicken Sie **Weiter**, um die neue Firmwareanpassung einem Gerät oder einem Geräteverzeichnis zuzuweisen.  
Oder weisen Sie sie später per Drag & Drop oder über **Zugewiesene Objekte** zu.
7. Klicken Sie **Fertig**, um Ihre neue Firmwareanpassung zu speichern.

### Einen eigenen Bootsplash über ein Profil erstellen

So können Sie Ihren eigenen Bootsplash mittels eines Profils in der UMS erstellen:

1. Laden Sie Ihre Bootsplash-Grafik auf den UMS Server hoch; siehe [Eine Grafik hochladen](#) (see page 632).

- i**

  - Der Dateiname soll keine Sonderzeichen wie %, \$, Umlaute, usw. enthalten.
  - Die folgenden Dateitypen können verwendet werden: JPG, JPEG, BMP, PNG, SVG, GIF und TIFF.
  - Die optimale Größe des Bildes beträgt 800 x 600 Pixel.

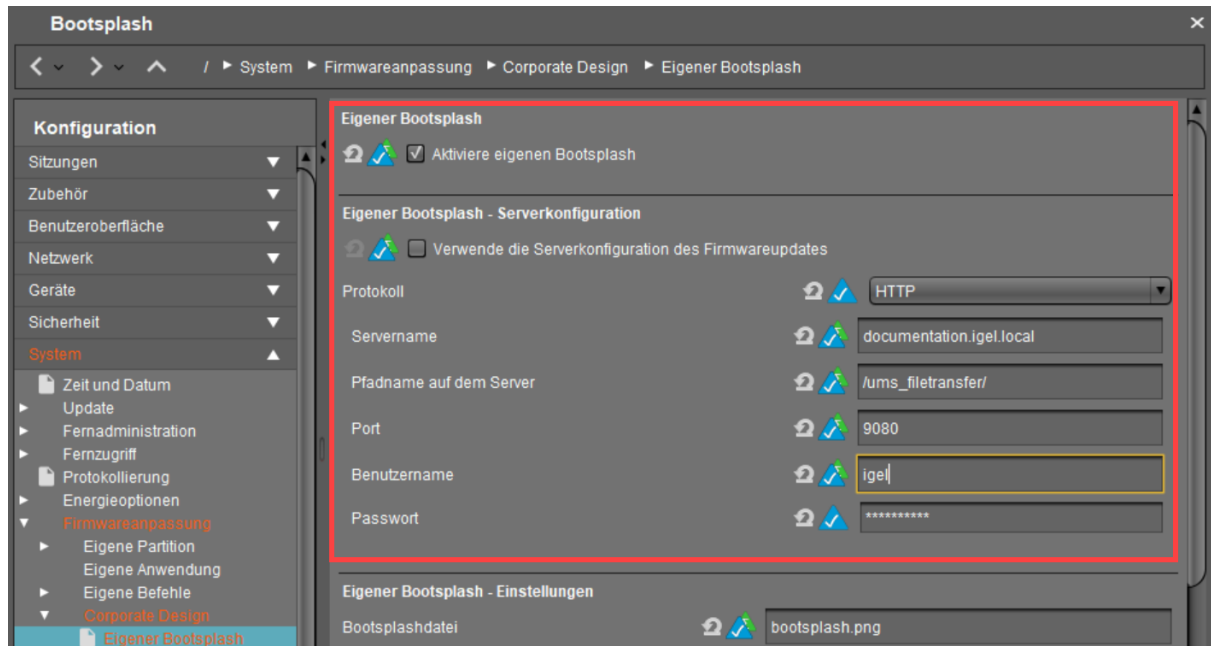
2. Erstellen Sie ein neues Profil, z. B. mit einem Namen "Bootsplash"; siehe [Ein Profil erstellen](#) (see page 633).
3. Gehen Sie in den Profileinstellungen zu **System > Firmwareanpassung > Corporate Design > Eigener Bootsplash**.
4. Aktivieren Sie die Einstellung **Aktiviere eigenen Bootsplash**.
5. Wählen Sie bei **Protokoll** den Wert **HTTP**.
6. Geben Sie bei **Servername** den Namen oder die IP-Adresse Ihres UMS Servers ein.



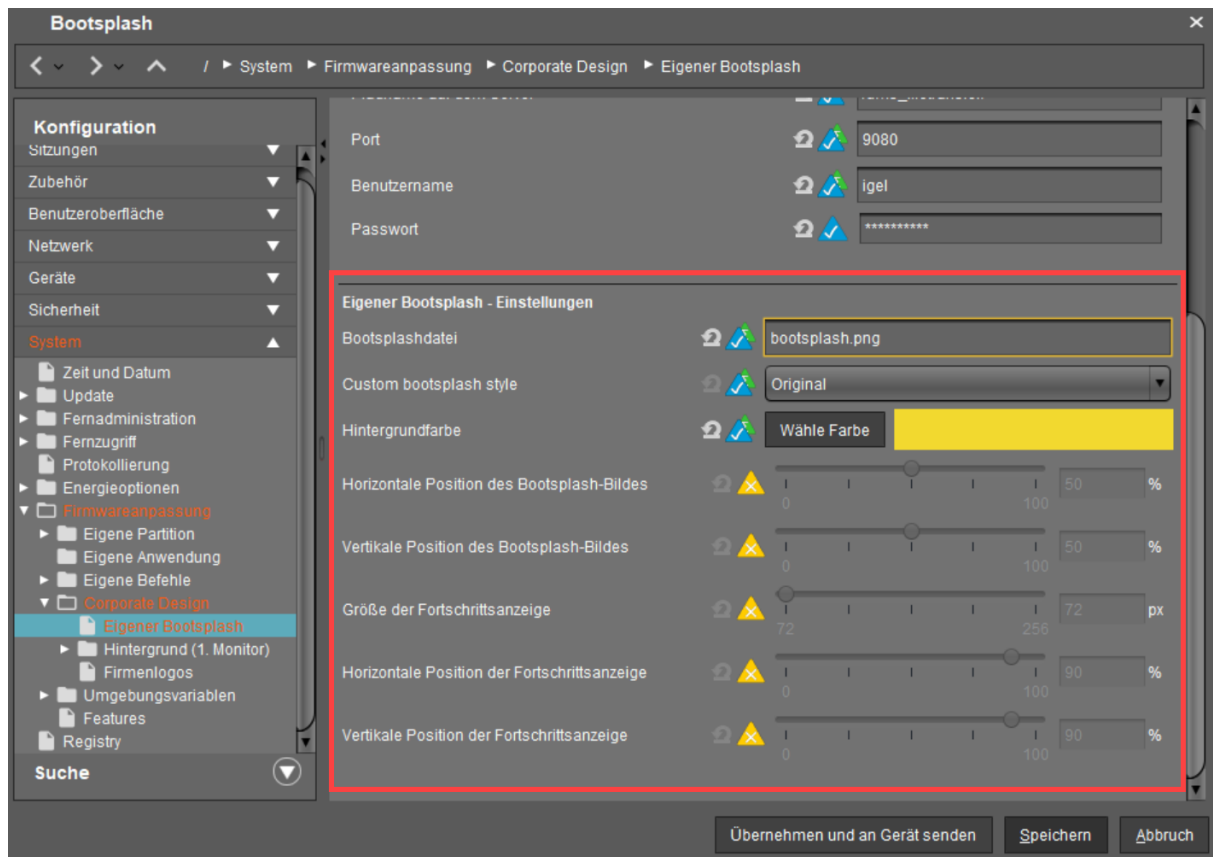
- Geben Sie bei **Pfadname auf dem Server** den Pfad des Verzeichnisses mit Ihrer Bootsplash-Grafik ein.
- Geben Sie bei **Port** die Portnummer von Ihrem HTTP-Server ein.

 Ein Standardport für UMS HTTP-Server ist 9080.

- Geben Sie den **Benutzername** und das **Passwort** Ihres UMS Administrators an.



- Geben Sie bei **Bootsplashdatei** den Namen der Grafikdatei mit Ihrem Bootsplash ein.
- Legen Sie unter **Custom bootsplash style** einen Stil für Ihren Bootsplash und eine **Hintergrundfarbe** fest.
- Legen Sie einen Wert für die **horizontale** und **vertikale Position** der Bootsplash-Grafik sowie der Fortschrittsanzeige fest. Der Wertebereich beträgt 0 (links) bis 100 (rechts). 50 bedeutet "zentriert".




13. **Speichern** Sie die Einstellungen.
14. Weisen Sie dem erstellten Profil Ihre Bootsplash-Grafik zu.
15. Weisen Sie das Profil Ihren Geräten per Drag & Drop oder unter **Zugewiesene Objekte** zu. Weitere Informationen über die Profilzuweisung finden Sie unter [Wie kann ich IGEL UMS Profile zuweisen?](#)

## Einen Bildschirmschoner konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie mit der UMS einen Bildschirmschoner konfigurieren, der automatisch startet und ein von Ihnen festgelegtes Bild verwendet.

Führen Sie die gleichen Schritte wie beim Festlegen eines Hintergrundbildes aus:


1. Laden Sie die gewünschte Grafik auf den UMS-Server hoch, siehe [Eine Grafik hochladen](#) (see page 632).

 Die Größe des Bildes ist irrelevant, da es automatisch auf 200 x 150 Pixel reduziert wird.

2. Erstellen Sie ein neues Profil und geben Sie ihm einen Namen, z. B. "Bildschirmschoner". Siehe [Ein Profil erstellen](#) (see page 633).
3. Konfigurieren Sie die Profileinstellungen.  
Im Profil müssen Sie in vier Bereichen Einstellungen treffen:
  - [Zeitverzögerung bei Systemstart festlegen](#) (see page 644)
  - [Timeout für Autostart festlegen](#) (see page 645)
  - [Eigenes Logo festlegen](#) (see page 646)
  - [Eigene Bildschirmschoneruhr zuweisen](#) (see page 647)
4. Weisen Sie das Profil Ihren Geräten zu. Nutzen Sie dafür Drag & Drop oder fügen Sie sie dem Bereich **Zugeordnete Objekte** hinzu.


## Zeitverzögerung bei Systemstart festlegen

1. Öffnen Sie das Profil.
2. Gehen Sie zu **Benutzeroberfläche > Bildschirmsperre/-schoner**.
3. Aktivieren Sie **Autostart**.
4. Legen Sie einen Wert für **Verzögerung** fest.

 Diese Einstellung bestimmt, dass die Sitzung bei Systemstart mit einer bestimmten Verzögerung gestartet wird.


## Timeout für Autostart festlegen

1. Gehen Sie zu **Benutzeroberfläche > Bildschirmsperre/-schoner > Optionen**.
2. Aktivieren Sie **Automatisch starten**.
3. Legen Sie einen Wert für **Zeitlimit in Minuten** fest.

 Die Einstellung bestimmt, wie lange nach der letzten Eingabe bis zum Start des Bildschirmschoners gewartet wird.

## Eigenes Logo festlegen

1. Gehen Sie zu **System > Firmwareanpassung > Corporate Design > Firmenlogos**.
2. Aktivieren Sie **Bild anzeigen**.
3. Geben Sie bei **Bilddatei / Bildverzeichnis** den Pfad ein, den Sie unter **Speicherpfad des Thin Clients** festgelegt haben. Siehe [Eine Grafik hochladen](#) (see page 632).

 Wenn Sie statt einer einzelnen Datei den Pfad eines Verzeichnisses angeben, dann werden die sich in dem Verzeichnis befindenden Grafiken abwechselnd nacheinander angezeigt. In dem Fall können Sie eine **Bildanzeigedauer** festlegen.

4. Aktivieren Sie **Ein Bild pro Monitor**, falls Sie mehrere Monitore verwenden und auf jedem Monitor ein anderes Bild angezeigt werden soll.
5. Legen Sie bei **Bildanzeigedauer** fest, nach wie vielen Sekunden das Bild wechseln soll.
6. Bei **Bildanzeigemodus** können Sie verschiedene Anzeigemodi festlegen:
  - **Klein springend**: Kleine Bilder werden mit wechselnder Position angezeigt.
  - **Mittelgroß springend**: Mittelgroße Bilder werden mit wechselnder Position angezeigt.
  - **Vollbild Center-cut-out**: Die Bilder werden im Vollbildmodus angezeigt. Möglicherweise werden Sie am Rand abgeschnitten.
  - **Vollbild Letterbox**: Die Bilder werden im Vollbildmodus so groß wie möglich angezeigt.

## Eigene Bildschirmschoneruhr zuweisen

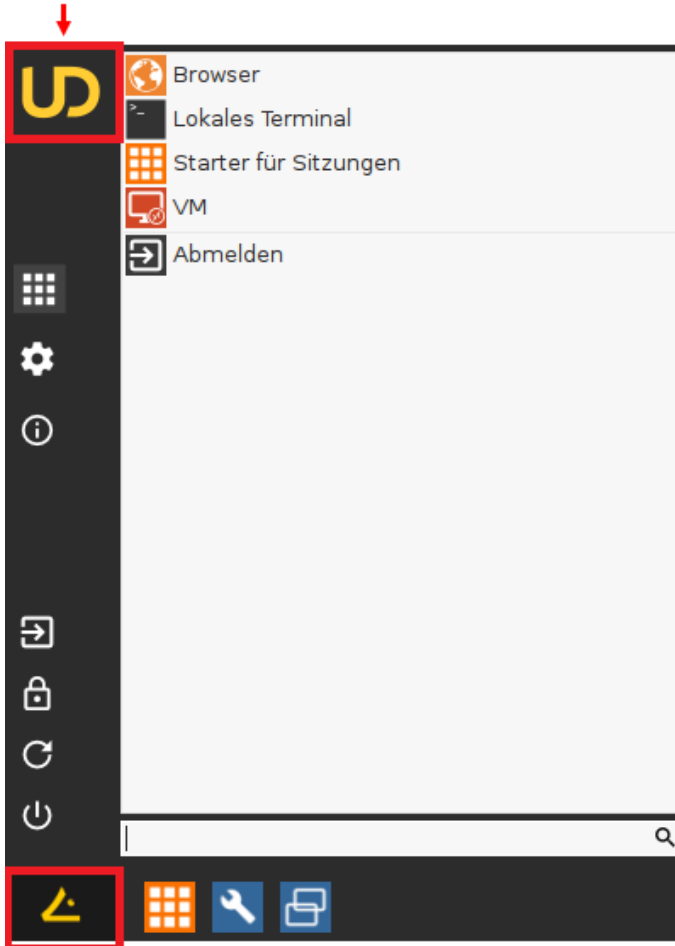
Sie können auch eine digitale Bildschirmschoneruhr konfigurieren, die unabhängig auf einem bestimmten Monitor angezeigt wird.

1. Gehen Sie zu **Benutzeroberfläche > Bildschirmsperre/-schoner > Bildschirmschoner**.
2. Wählen Sie bei **Monitor für die Uhrenanzeige**, wo die Uhr angezeigt werden soll.
3. Aktivieren Sie **Sekunden anzeigen**, wenn Sie möchten, dass die Sekundenzahl der Uhrzeit angezeigt wird.
4. Definieren Sie **Größe, Position** und **Farbe** Ihrer Bildschirmschoneruhr.

## Eigene Firmenlogos festlegen

Sie können das **Firmenlogo** und das **Startmenüsymbol** durch eigene Grafiken ersetzen.

**Firmenlogo**



**Startmenüsymbol**

**i** Das **Startmenüsymbol** kann seit IGEL Linux 5.08.100 angepasst werden.

**i** Um das eigene Logo im Startmenü zu sehen, müssen Sie **Erweitert** unter **Benutzeroberfläche > Desktop > Startmenü > Startmenütyp** auswählen.  
Falls unter **Startmenütyp Automatisch** aktiviert ist und das Gerät die Taktfrequenz von 1 GHz hat, wählt das System den erweiterten Startmenütyp aus.

So legen Sie eigene Grafiken als Startmenüsymbol und -logo fest:



1. Laden Sie die gewünschten Bilder auf den UMS-Server hoch; siehe [Eine Grafik hochladen](#) (see page 632).  
Die Grafiken müssen folgende Abmessungen haben.
2. Erstellen Sie ein neues Profil; siehe [Ein Profil erstellen](#) (see page 633).  
Das Konfigurationsfenster des Profils öffnet sich.
3. Gehen Sie zu **System > Firmwareanpassung > Corporate Design > Firmenlogos > Startmenü**.
4. Geben Sie bei **Startmenüsymbol** den vollständigen Pfad einer entsprechenden Bilddatei ein.
5. Geben Sie bei **Firmenlogo im Startmenü** den vollständigen Pfad einer entsprechenden Bilddatei ein.
6. Klicken Sie **Übernehmen und an Thin Client senden** oder **Speichern**, um die Einstellungen zu speichern.
7. Weisen Sie das Profil Ihren Geräten per Drag & Drop oder unter **Zugewiesene Objekte** zu.

 Eine Alternative hierzu gibt es das Kapitel "Firmwareanpassung erstellen" im UMS Handbuch. Hier finden Sie weitere Konfigurationsmöglichkeiten, wie Sie die UMS nach Ihren Wünschen anpassen können.

## Eigene Taskleiste erstellen

So legen Sie ein eigenes Bild für die Taskleiste fest:

1. Laden Sie das gewünschte Bild auf den UMS-Server hoch; siehe [Eine Grafik hochladen \(see page 632\)](#).
2. Erstellen Sie ein neues Profil; siehe [Ein Profil erstellen \(see page 633\)](#).
3. Weisen Sie das Bild dem Profil per Drag & Drop oder unter **Zugewiesene Objekte** zu.
4. Gehen Sie im Konfigurationsfenster des Profils zu **Benutzeroberfläche > Desktop > Hintergrund der Taskleiste**.
5. Wählen Sie bei **Hintergrundstil** den Wert **Hintergrundbild**.
6. Geben Sie bei **Pfad des Hintergrundbilds** den vollständigen Pfad der Bilddatei ein.
7. Weisen Sie das Profil Ihren Geräten per Drag & Drop oder unter **Zugewiesene Objekte** zu.

## Eigene Desktopsymbole erstellen

- i** Sie können nur das Desktopsymbol einer Sitzung individuell gestalten. Das Taskleistensymbol einer Sitzung ist nicht veränderbar. Die vollständige Anpassung ist nicht möglich.

### Voraussetzungen

Sie können folgende Formate und Auflösungen für ein Desktopsymbol verwenden:

- PNG - übliche Auflösungen sind 128x128, 96x96, 64x64, 48x48, 32x32, 24x24, 22x22, 16x16. Andere Auflösungen werden akzeptiert und entsprechend skaliert.

- i** Wir empfehlen eine Auflösung von mindestens 64x64 Pixel.

- SVG - keine Auflösungen, da SVG mit frei skalierbaren Vektorgrafiken arbeitet.

- i** Obwohl andere Formate wie BMP oder JPEG akzeptiert werden, empfehlen wir PNG- und SVG-Formate, weil sie Transparenz unterstützen.

### Schritte


So erstellen Sie ein eigenes Desktopsymbol für eine Sitzung:

1. Gehen Sie im IGEL Setup zu **System > Registry**.
2. Navigieren Sie zu **sessions.[session name].icon**.

- i** Aus technischen Gründen unterscheiden sich einige Registry-Keys vom Sitzungsnamen. Der RDP-Sitzung entspricht zum Beispiel der Registry-Key `winconnect [0- . . . ]`.

3. Geben Sie bei **Name des Symbols** den absoluten Pfad zur entsprechenden Bilddatei ein.
4. Klicken Sie Ok, um die Einstellungen zu speichern.

## How to Change the Font Color of the Desktop Icons

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Wie richte ich einen Countdown ein, um eine unerwünschte Bildschirmsperre in IGEL OS zu verhindern?

In manchen Situationen kann eine Bildschirmsperre, die ohne Warnung auftritt, zu Störungen führen. Dies ist in der Regel der Fall, wenn ein Benutzer, der bei einer Remote-Sitzung angemeldet ist, einige Zeit lang nicht mit dem Gerät interagiert, so dass die Bildschirmsperre ausgelöst wird. Um dieses Problem zu umgehen, können Sie einen sichtbaren Countdown einstellen, der gestartet wird, bevor der Bildschirm gesperrt wird; der Benutzer kann somit rechtzeitig reagieren.

**i** Überprüfen Sie die Timeouts in den Energieeinstellungen Ihres Geräts, um sicherzustellen, dass das Display nicht schwarz wird, bevor der Countdown startet; siehe System-Energieoptionen in IGEL OS und Bildschirm

Die Konfiguration ist in den folgenden Abschnitten beschrieben:

- [Verhalten des Countdowns definieren](#) (see page 653)
- [Erscheinungsbild des Countdowns festlegen](#) (see page 655)

Für spezielle Zwecke, z. B. das Schließen einer Remote-Sitzung, um zu verhindern, dass sie unbeaufsichtigt läuft, können Sie einen zusätzlichen Satz von Befehlen konfigurieren. Dieser besteht aus einem Befehl, der festlegt, ob der Countdown gestartet werden soll (typischerweise wird geprüft, ob die Remote-Sitzung läuft) und einem Befehl, der ausgeführt wird, wenn der Countdown 0 erreicht (typischerweise wird die Remote-Sitzung geschlossen). Die Konfiguration wird im folgenden Abschnitt beschrieben:

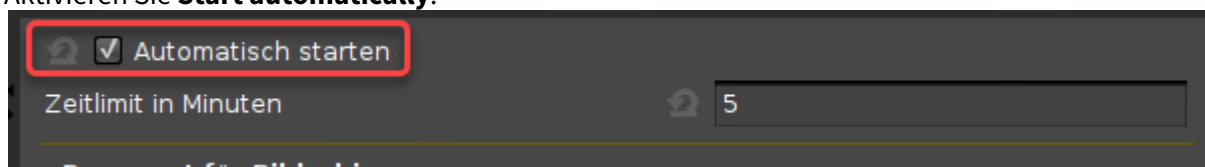
- [Bedingten Befehl und Kommando konfigurieren](#) (see page 0)

---

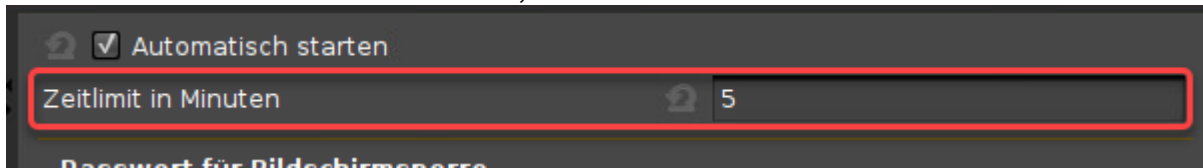
## Verhalten des Countdowns festlegen

Eine Beschreibung aller Optionen finden Sie unter Optionen.

1. Gehen Sie im Setup oder UMS Konfigurationsdialog zu **Benutzeroberfläche > Bildschirmsperre/-schoner > Optionen**.
2. Aktivieren Sie **Start automatisch**.



3. Geben Sie im Feld **Zeitlimit in Minuten** an, nach wievielen Minuten der Countdown starten soll.



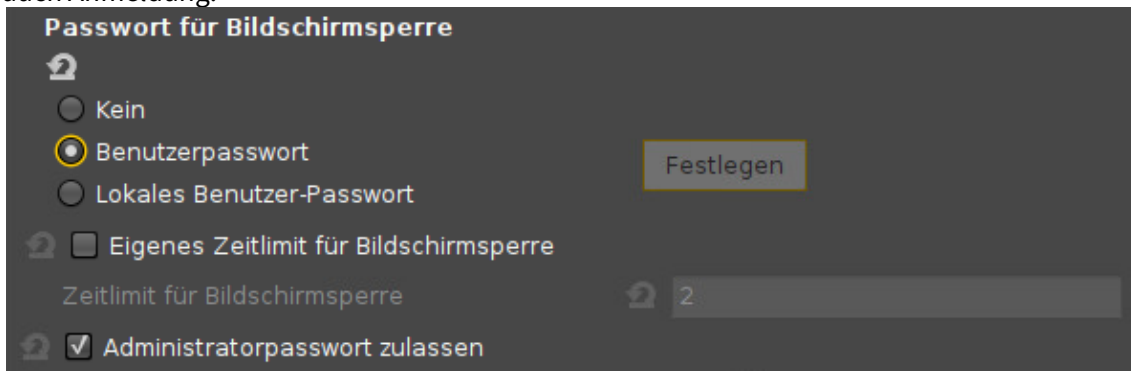
4. Wählen Sie das Passwort zum Entsperren des Bildschirms:

- **Kein:** Der Benutzer kann den Bildschirm ohne Passwort entsperren. Bitte beachten Sie, dass der Countdown nicht startet, wenn diese Option ausgewählt ist!
- **Benutzerpasswort:** Der Benutzer muss das Passwort eingeben, um den Bildschirm zu entsperren. Wenn Sie Microsoft Active Directory (AD) bzw. Kerberos zur Authentifizierung verwenden, was dringend empfohlen wird, wird hier das AD/Kerberos-Passwort des Benutzers verwendet. Weitere Informationen finden Sie unter Active Directory/Kerberos. Wenn Sie nicht AD/Kerberos verwenden, wird das Passwort des Benutzers im Bereich **Sicherheit > Passwort** unter **Benutzer** konfiguriert. Bitte beachten Sie, dass das Passwort auf keinen Fall über ein UMS Profil gesetzt werden sollte, da sonst alle betroffenen Geräte das gleiche Passwort hätten!
- **Lokales Benutzer-Passwort:** Der Benutzer muss ein spezielles Passwort für die Bildschirmsperre eingeben, um den Bildschirm zu entsperren; klicken Sie auf **Festlegen**, um dieses Passwort zu definieren. Bitte beachten Sie, dass das Passwort auf keinen Fall über ein UMS-Profil gesetzt werden sollte, da sonst alle betroffenen Geräte das gleiche Passwort hätten!

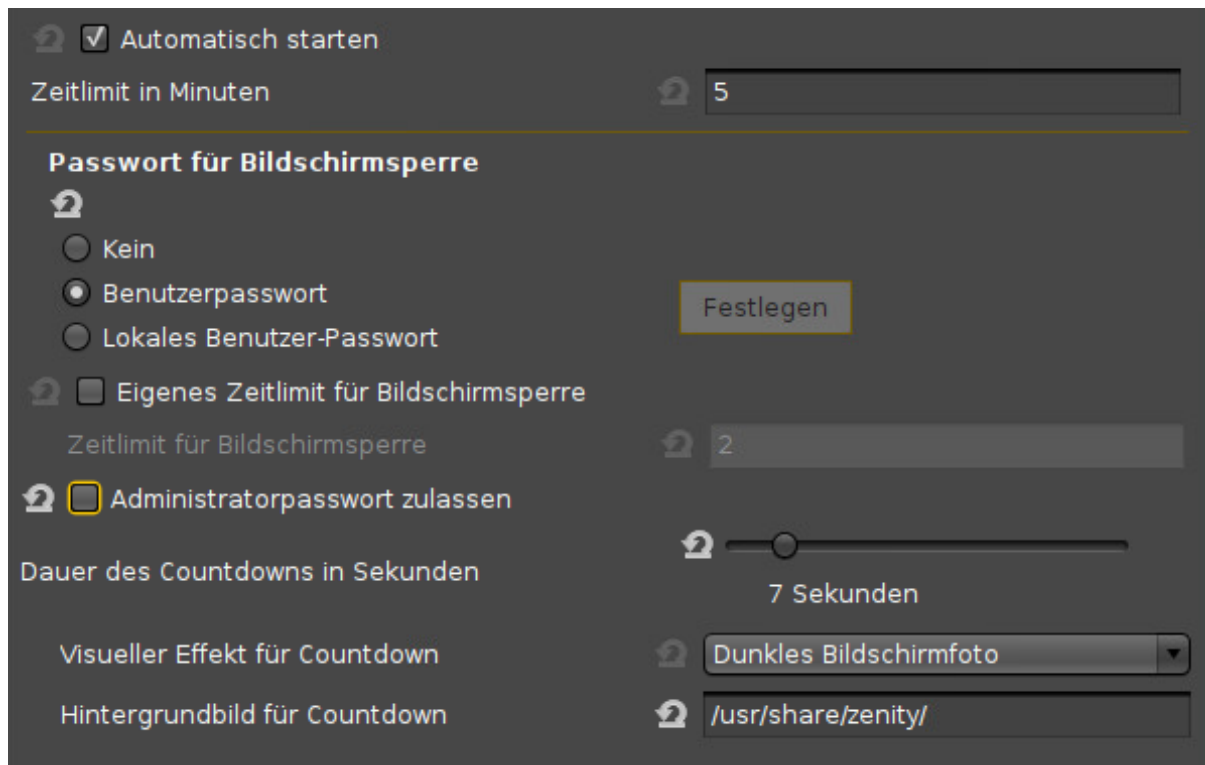
Dieses Passwort wird auch für **Sicherheit > Anmeldung > Lokaler Benutzer > Anmeldung mit Passwort für normalen Benutzer** verwendet; siehe Lokaler Benutzer.

Wenn der Benutzer über Active Directory (AD) angemeldet ist, werden die AD-Anmeldeinformationen anstelle dieses Passworts für das Aufheben der Bildschirmsperre verwendet.

Wenn Sie Citrix Storefront verwenden, kann dieses Passwort mit dem Citrix Sitzungspasswort synchronisiert werden, indem Sie **Citrix Passwort für Bildschirmsperre übernehmen** unter **Sitzungen > Citrix > Citrix StoreFront > Anmeldung** aktivieren; siehe auch Anmeldung.



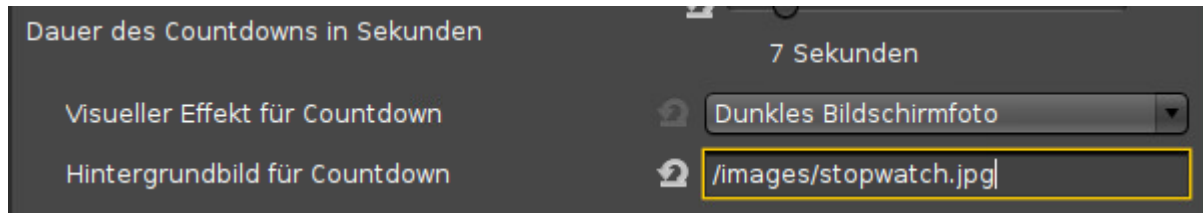
5. Legen Sie die **Dauer des Countdowns in Sekunden** fest. Der Wertebereich liegt zwischen 1 und 60. Konfigurationsbeispiel:



6. Übernehmen Sie die Einstellungen für Ihre Geräte oder für Ihr Profil.

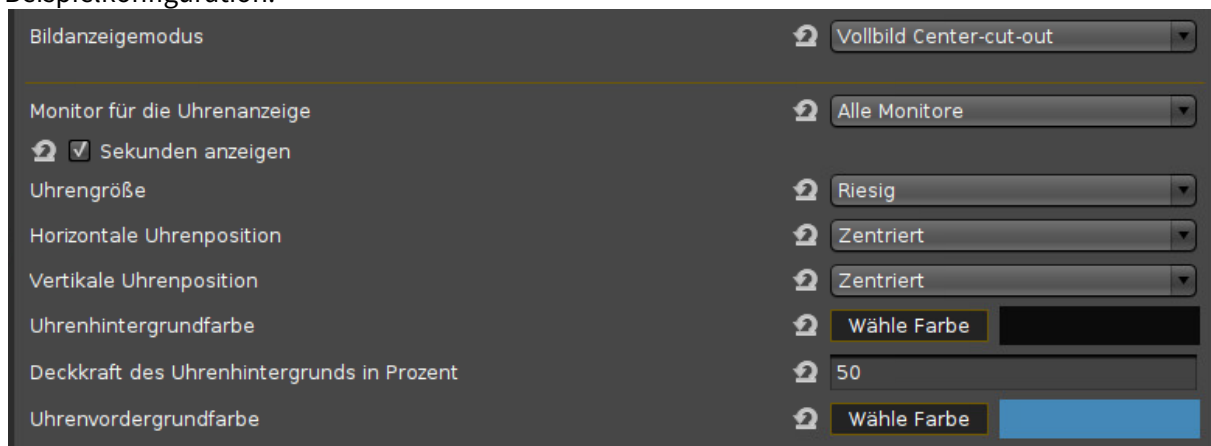
## Erscheinungsbild des Countdowns festlegen

1. Gehen Sie im Setup auf **Benutzeroberfläche > Bildschirmsperre/-schoner > Optionen**.
2. Wenn Sie den aktuellen Desktop als Hintergrundbild während des Countdowns verwenden möchten, wählen Sie den visuellen Effekt:
  - **Dunkles Bildschirmfoto:** Der Desktop-Screenshot ist abgedunkelt.
  - **Graues Bildschirmfoto:** Der Desktop-Screenshot ist ausgegraut.
3. Wenn Sie ein benutzerdefiniertes Bild als Hintergrundbild während des Countdowns verwenden möchten, geben Sie einen gültigen Pfad und Dateinamen ein. Beispiel: `/images/`. Wenn sich das Bild nicht bereits auf Ihrem Gerät befindet, können Sie es über die UMS hochladen; siehe [Eine Grafik hochladen](#) (see page 632).  
Konfigurationsbeispiel mit benutzerdefiniertem Bild:



4. Gehen Sie auf **Benutzeroberfläche > Bildschirmsperre/-schoner > Bildschirmschoner**.
5. Passen Sie das Erscheinungsbild des Countdowns mit den folgenden Parametern an; diese Parameter bestimmen das Erscheinungsbild sowohl der Uhr des Bildschirmschoners als auch des Countdowns. Weitere Informationen finden Sie unter Bildschirmschoner.
  - **Bildanzeigemodus:** Position und Skalierung für das Hintergrundbild
  - **Monitor für die Uhrenanzeige:** Wählen Sie den/die Bildschirm(e), auf denen der Countdown angezeigt werden soll.
  - **Sekunden anzeigen:** Legen Sie fest, ob die Sekunden auf der Uhr angezeigt werden sollen.
  - **Uhrengöße:** Größe der Countdown-Ziffern
  - **Horizontale Uhrenposition:** Horizontale Position der Countdown-Ziffern
  - **Vertikale Uhrenposition:** Vertikale Position der Countdown-Ziffern
  - **Uhrenhintergrundfarbe:** Farbe des Hintergrundbereichs des Countdowns. Der Hintergrundbereich des Countdowns ist ein Rechteck mit abgerundeten Ecken.
  - **Deckkraft des Uhrenhintergrunds in Prozent:** Legen Sie die Deckkraft für den Hintergrundbereich der Uhr fest (definiert durch die **Uhrenhintergrundfarbe**),
  - **Uhrenvordergrundfarbe:** Farbe der Countdown-Ziffern

Beispielkonfiguration:





6. Übernehmen Sie die Einstellungen für Ihr Gerät oder für Ihr Profil.  
Hier ist ein Beispiel für einen Countdown mit einem benutzerdefinierten Bild:



## Bedingten Countdown und Befehl konfigurieren

In unserem Beispiel läuft eine Citrix Sitzung (z. B. im Appliance-Modus), und das Endgerät war eine Zeit lang inaktiv. Nach dem Timeout prüft das System, ob eine Citrix-Sitzung läuft; dies soll verhindern, dass die Sitzung unbeaufsichtigt läuft. Wenn eine Citrix Sitzung erkannt wird, startet der Countdown. Der Benutzer interagiert nicht mit dem Gerät, so dass der Countdown nicht angehalten wird. Wenn der Countdown 0 erreicht hat, beendet das System den Citrix Client; der Benutzer wird abgemeldet..

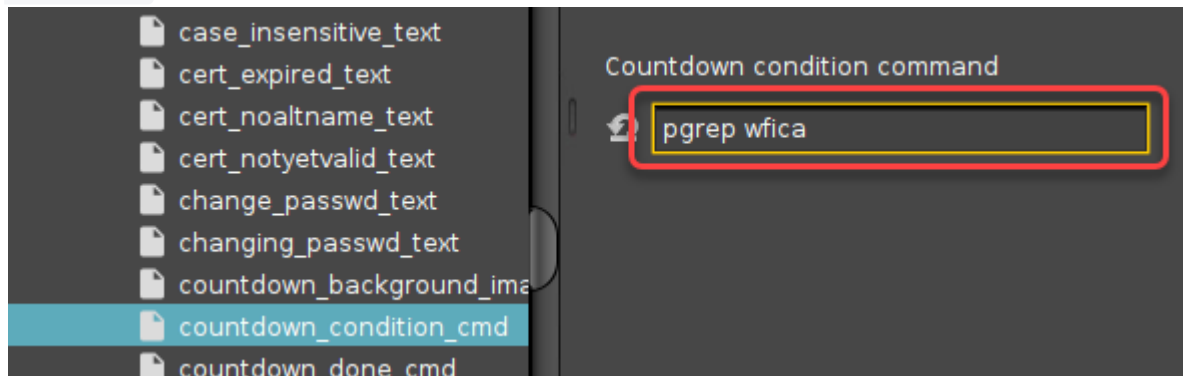
Im Folgenden geben wir zunächst den Befehl an, der bestimmt, ob der Countdown gestartet werden soll. Dann geben wir den Befehl an, der ausgeführt wird, wenn der Countdown 0 erreicht hat.

Befehl, der die Bedingung festlegt, unter der der Countdown gestartet werden soll

**⚠** Dieser Befehl ist nur in Kombination mit einem Befehl sinnvoll, der nach Ablauf des Countdowns ausgeführt werden soll; siehe [Befehl, der nach dem Countdown ausgeführt werden soll](#) (see page 658).

1. Gehen Sie im Setup auf **System > Registry** und öffnen Sie den Registry-Schlüssel **sessions > xlock0 > options > countdown\_condition\_cmd**  
( `sessions.xlock0.options.countdown_condition_cmd` ).

2. Geben Sie dem Befehl im Feld **Befehl für bedingten Start des Countdowns** ein. Der Benutzer, der den Befehl ausführt, ist `user`. Wenn hier kein Befehl angegeben ist, wird der Countdown gestartet. Beispiele: `pgrep wfica` (gibt 0 zurück, wenn eine Citrix Sitzung aktiv ist), `pgrep igelrdp2`




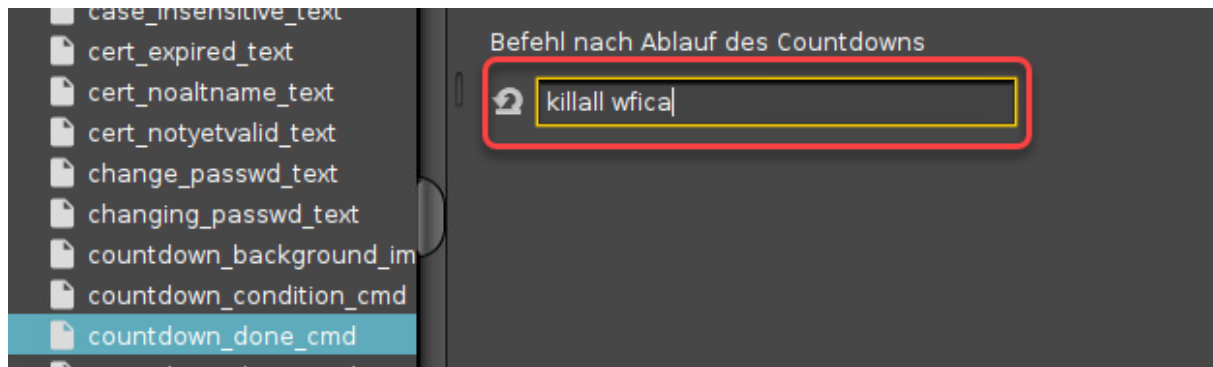
3. Klicken Sie **Übernehmen** oder **Ok**.  
Wenn der Befehl 0 zurückgibt, wird der Countdown gestartet. Wenn der Countdown 0 erreicht hat, wird der unter **System > Registry > sessions > xlock0 > options > countdown\_done\_cmd** angegebene Befehl ausgeführt (siehe [Befehl, der nach dem Countdown ausgeführt werden soll](#) (see page 658)).  
Wenn der Befehl einen von 0 verschiedenen Wert zurückgibt, wird der Countdown nicht gestartet. Ein Befehl, der für die Ausführung nach dem Countdown konfiguriert ist, wird daher nicht ausgeführt. Die Bildschirmsperre oder der Bildschirmschoner wird gestartet.

#### Befehl, der nach dem Countdown ausgeführt werden soll


1. Gehen Sie im Setup auf **System > Registry** und öffnen Sie den Registry-Schlüssel **sessions > xlock0 > options > countdown\_done\_cmd** (`sessions.xlock0.options.countdown_done_cmd`).

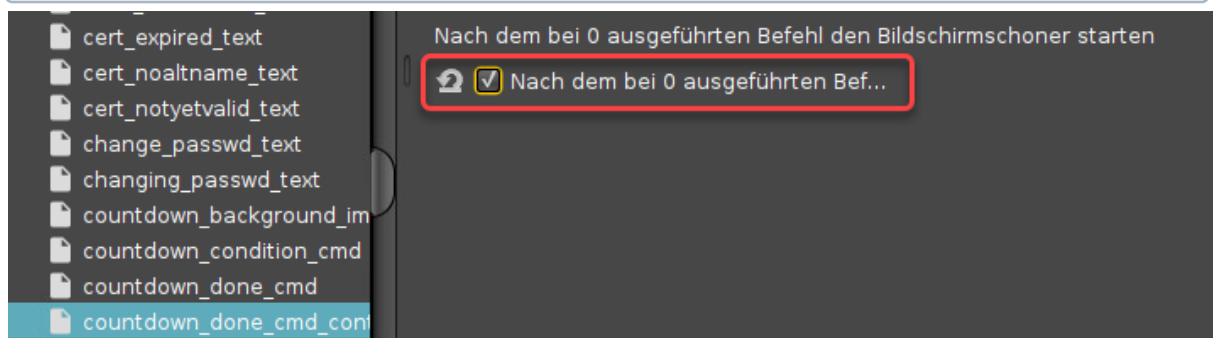
2. Geben Sie den Befehl im Feld **Befehl nach Ablauf des Countdowns** ein. Der Benutzer, der den Befehl ausführt, ist `user`. Beispiele: `killall wfica` (beendet den Citrix ICA Client),  
`logoff`

 Der Befehl wird synchron ausgeführt, bevor der Countdown abläuft. Wenn der Befehl nicht schnell beendet wird, muss er durch Anhängen von " & " in den Hintergrund versetzt werden.



3. (Optional) Wenn Sie den Start des Bildschirmschoners nach dem **Befehl nach Ablauf des Countdowns** erzwingen wollen, öffnen Sie den Registry-Schlüssel **sessions > xlock0 > options > countdown\_done\_cmd\_continue** ( `sessions.xlock0.options.countdown_done_cmd_continue` ) und aktivieren Sie **Nach dem bei 0 ausgeführten Befehl den Bildschirmschoner starten**.

 Einige Anwendungen beenden den Bildschirmschoner, wenn sie neu gestartet werden, so dass dies nicht immer die gewünschte Wirkung hat.



4. Klicken Sie **Übernehmen** oder **Ok**.

## Tastenkombinationen zur Verwaltung von Windows


Das Hin- und Herwechseln zwischen offenen Anwendungsfenstern mit Hilfe von Tastaturkombinationen ist eine gängige Methode, um Fenster zu verwalten.

Wenn Sie in einer Vollbildumgebung arbeiten, benötigen Sie auch eine Möglichkeit, auf den Desktop zu wechseln.

Mit IGEL Linux OS Version 10.03.500 wurde der Geräte-Desktop in den Fensterzyklus des Windowsmanagers aufgenommen.

Benutzen sie folgende Standard-Verknüpfungen um zwischen den Anwendungsfenstern auf den Desktop zu wechseln:

Task	Standard-Verknüpfung
Umschalten zwischen aktiven Fenstern im Task Switcher	Ctrl + Alt + Tab
Umschalten zwischen aktiven Fenstern im Task Switcher (Zurück)	Ctrl + Alt + Shift + Tab
Fokus auf das nächste Fenster umschalten	Ctrl + Esc
Fokus auf das nächste Fenster umschalten (2)	Ctrl + Alt + Pfeil hoch
Fokus auf das nächste Fenster umschalten (umgekehrte Reihenfolge)	Ctrl + Alt + Pfeil runter

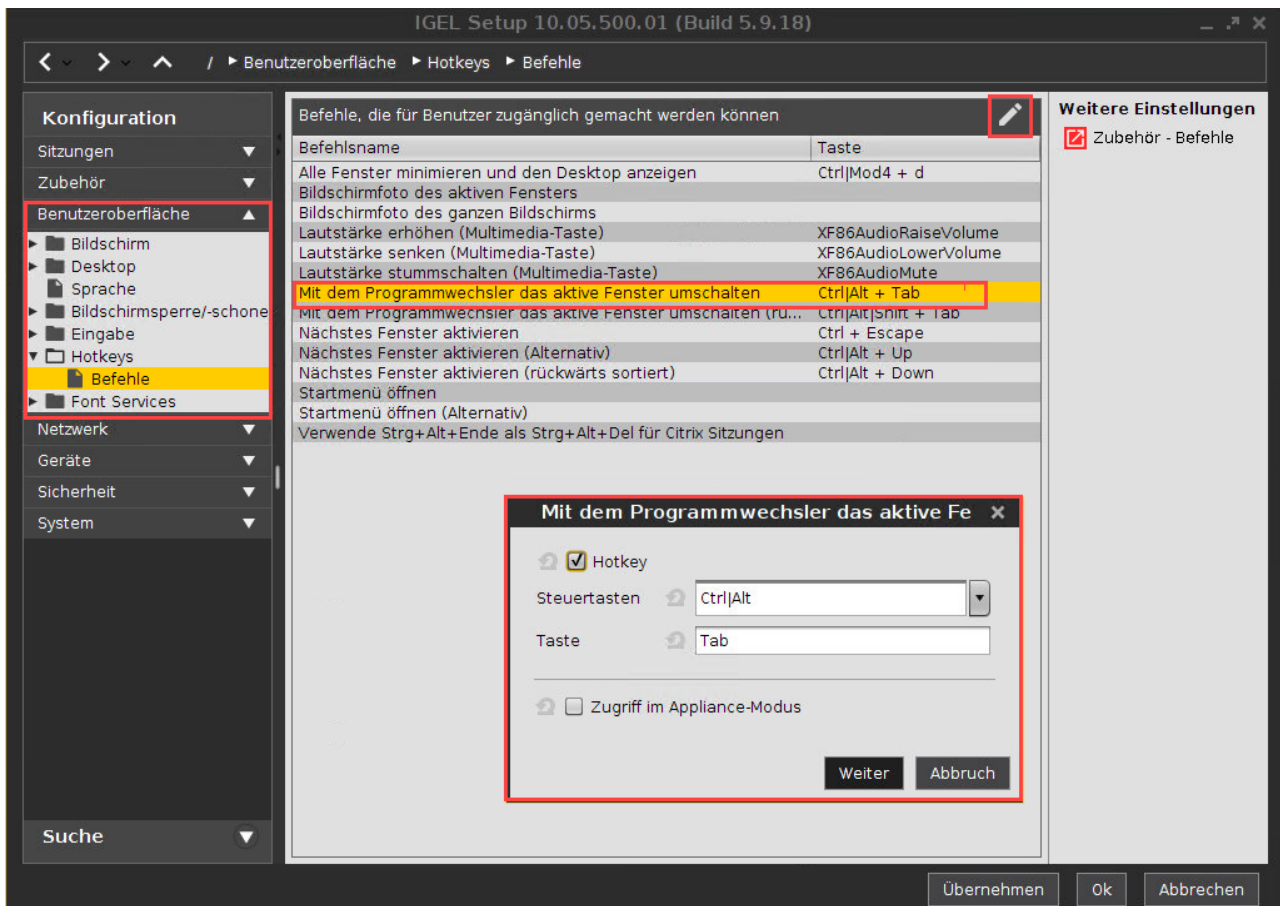
 Gehen Sie auf IGEL Setup > Benutzeroberfläche > Hotkeys > Befehle um die Tastenkombinationen zu ändern.

 Umschalten auf den Desktop minimiert alle Fenster. Wenn Sie danach direkt zu einem Fenster zurückkehren, werden alle Fenster wiederhergestellt.

## Vereinfachung häufiger Benutzeraktionen durch die Definition von Hotkeys

Für allgemeine Aktionen, wie das Umschalten zwischen verschiedenen Fenstern oder das Sperren des Bildschirms, können Sie einen Hotkey verwenden. Auch wenn einige Hotkeys bereits vorkonfiguriert sind, können Sie diese jederzeit aktivieren, deaktivieren und ändern.

Das folgende Beispiel zeigt, wie Sie den Hotkey zum Umschalten zwischen den Fenstern herausfinden oder ändern können:

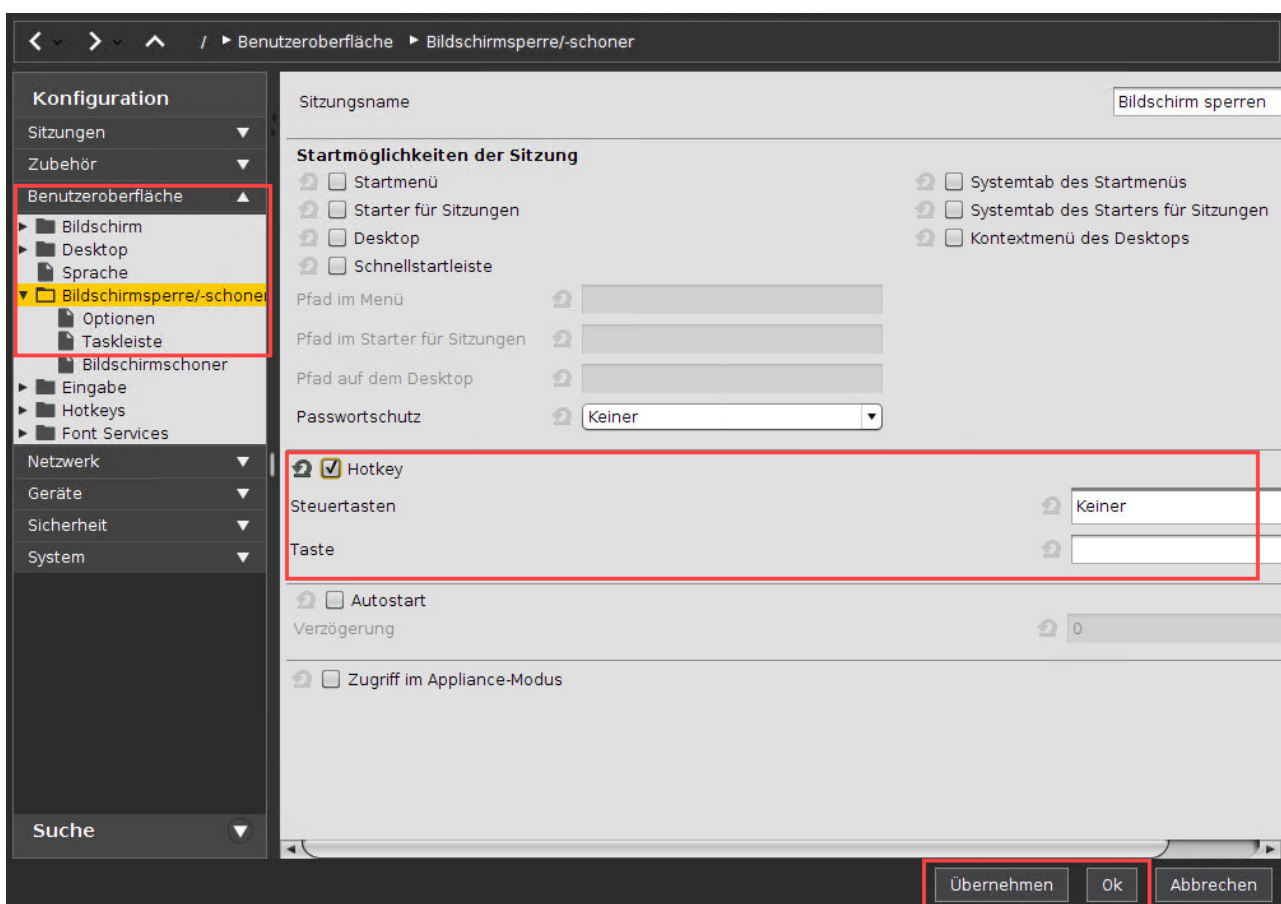


1. Öffnen Sie Setup und gehen Sie zu **Benutzeroberfläche > Hotkeys > Befehle**.
2. Wählen Sie **Mit dem Programmwechsler das aktive Fenster umschalten**.
3. Klicken Sie auf **Bearbeiten**.  
Es öffnet sich ein Dialog Fenster
4. **Hotkey** aktivieren, falls nicht bereits aktiviert.
5. Wählen Sie unter **Steuertasten** einen Steuertasten-Schlüssel oder eine Kombination von Steuertasten-Schlüsseln aus.
6. Geben Sie eine **Taste** ein.

**i** Wenn Sie einen Schlüssel eingeben möchten, dem kein sichtbares Zeichen zugeordnet ist, gehen Sie wie folgt vor, z. B. den [Tab], öffnen sie ein Terminal, melden Sie sich als Benutzer an und geben sie `xev -event keyboard` ein. Drücken Sie die für den Hotkey vorgesehene Taste. Der Text in Klammern beginnend mit `keysym` enthält die gewünschte Zeichenkette für das Feld Key;  
Beispiel: Tab in (`keysym 0xff09`, Tab)

7. Klicken Sie auf **Weiter**
8. Klicken Sie auf **Übernehmen** oder **Ok**.  
Der Hotkey kann nun benutzt werden.

Das folgende Beispiel zeigt, wie man einen Hotkey definiert, um den Bildschirm zu sperren:



1. Öffnen Sie Einstellungen und gehen Sie zu **Benutzeroberfläche > Bildschirmsperre/-schoner**.
2. **Hotkey** aktivieren.
3. Wählen Sie unter **Steuertasten** einen Steuertasten-Schlüssel oder eine Kombination von Steuertasten-Schlüsseln aus.
4. Geben Sie eine **Taste** ein.

5. Klicken Sie auf **Übernehmen** oder **Ok**.  
Der Hotkey kann nun benutzt werden.

## Ein Gerät bei Beendigung einer Sitzung automatisch herunterfahren/ ausschalten

### Problem

Sie möchten, dass das Gerät nach Beendigung einer Sitzung automatisch herunterfährt, neustartet, sich abmeldet oder in den Standbymodus versetzt wird.

### Lösung

Sie können eine "After-Logoff-Aktion" abhängig vom Sitzungstyp definieren. Diese Aktion wird ausgeführt, nachdem die letzte Instanz des definierten Sitzungstyps beendet wurde.

Gehen Sie wie folgt vor:

1. Navigieren Sie im lokalen Setup des Geräts (oder seiner UMS Konfiguration oder seinem Profil) zu den folgenden Punkten **System > Firmwareanpassung > Eigene Befehle > Nach Sitzungsende**.
2. Wählen Sie einen **Sitzungstyp**.
3. Wählen Sie einen **Kommando nach Sitzungsende**.
4. Speichern Sie die Änderungen mit **Übernehmen** oder **OK**.

Wenn die letzte Instanz des gewählten Sitzungstyps beendet wird, wird der Befehl zur automatischen Abmeldung ausgeführt.

Sehen Sie auch im IGEL OS Handbuch das Kapitel Nach Sitzungsende-Befehle in IGEL OS.

**i** Der Befehl **Herunterfahren/Standbymodus** führt die unter **System > Energieoptionen > Herunterfahren > Standardverhalten** definierte Standardaktion aus. Bitte überprüfen Sie diesen Parameter, bevor Sie den Befehl verwenden.


**i** Der Befehl **Abmelden** ist sinnlos, es sei denn, Sie definieren unter **Sicherheit > Anmeldung** eine Anmeldemethode (Smartcard, Active Directory/Kerberos oder IGEL Shared Workplace). Der Abmeldebefehl kann auch nicht mit einer Appliance verwendet werden – in diesem Fall funktionieren nur die Befehle **Herunterfahren/Standbymodus** oder **Neustart**.

**i** Wenn Sie Befehle zur automatischen Abmeldung mit einer Appliance verwenden, stellen Sie sicher, dass Sie den entsprechenden Sitzungstyp definieren – z.B. **Horizon View** bei Verwendung der VMware Horizon View Appliance.



## Standbybetrieb - Wecken mit der USB-Maus

Sie können Ihr Gerät per Mausklick oder Tastatureingabe aus dem Standbymodus wecken.

 Die Aufweckfunktion ist stark von der verwendeten Hardware und BIOS-Version abhängig. Wir empfehlen, die Funktion zu testen, bevor sie verwendet wird. Bei mit UDC3/OS Creator oder UD Pocket konvertierten Geräten funktioniert das Aufwecken nur mit vollständig unterstützter Hardware.

### Standbymodus als Standardverhalten setzen

1. Gehen Sie im Setup zu **System > Energieoptionen > Herunterfahren**.
2. Aktivieren Sie **Herunterfahren erlauben**.
3. Wählen Sie unter **Standardverhalten** "Standbymodus".
4. Speichern Sie die Einstellung, indem Sie **Übernehmen** oder **Ok** klicken.

Um die Aufweckfunktion zu benutzen, müssen die folgenden Schritte durchgeführt werden:

### BIOS für PS/2-Maus und -Tastatur konfigurieren



1. Öffnen Sie das BIOS Ihres Geräts und prüfen Sie, ob der Bereich Energiemanagement Parameter mit der Bezeichnung "PS/2 Wake up from S3" oder ähnlich enthält.
2. Aktivieren Sie die Parameter, soweit vorhanden.
3. Speichern Sie die BIOS-Konfiguration und fahren Sie mit dem Booten fort.

### BIOS für USB-Maus und -Tastatur konfigurieren

1. Öffnen Sie das BIOS Ihres Geräts und prüfen Sie, ob der Bereich Energiemanagement Parameter mit der Bezeichnung "USB Wake Up from S3" oder ähnlich enthält.
2. Aktivieren Sie die Parameter, soweit vorhanden.
3. Speichern Sie die BIOS-Konfiguration und fahren Sie mit dem Booten fort.

### Die Aufweckfunktion aktivieren

1. Im IGEL Setup aktivieren Sie **System > Registry > system > acpi\_wakeup > enabled > Mittels USB-Geräten aus dem Standbymodus aufwachen**.
2. Klicken Sie **Übernehmen** oder **Ok**.

Um zu überprüfen, ob das Aufwecken funktioniert, klicken Sie  > , warten Sie einige Minuten, und versuchen Sie, das Gerät mit der Maus oder dem Drücken einer Taste aufzuwecken.

## Screenshots in IGEL Linux erstellen

### Problem

Zu Support- und Dokumentationszwecken möchte der Nutzer einen Screenshot in IGEL Linux machen, ohne über VNC auf den Client zuzugreifen.

### Lösung

Verwenden Sie unter IGEL Linux 5.08.100 und neuer oder IGEL Linux 10.01.100 das vorinstallierte Bildschirmfoto.

Auf früheren Versionen:

1. Laden Sie sich das Tool [Rapid Screenshot](#)<sup>52</sup> herunter.

 Der Standard-Download-Speicherort des lokalen Firefox ist `/tmp/`.

2. Öffnen Sie einen **lokalen Terminal** und melden Sie sich als root an.
3. Kopieren Sie die heruntergeladene `.jar`-Datei aus dem Verzeichnis `/tmp/` nach `/wfs/screenshot.jar`:

```
cp /tmp/ /wfs/screenshot.jar
```


Es ist wichtig, die Datei nach `/wfs` zu kopieren, da die Datei bei einem Neustart gelöscht würde.

4. Öffnen Sie IGEL Setup und erstellen Sie eine neue **Eigene Anwendung: System > Firmwareanpassung > Eigene Anwendung > Einstellungen**
5. Geben Sie in die **Einstellungen** das **Startkommando** `java -jar /wfs/screenshot.jar` ein.
6. Klicken Sie das neue Symbol auf Ihrem Desktop um die **Eigenen Anwendungen** zu starten.

Um diese Anwendungen auf mehreren Geräten zu verteilen, verwenden Sie die Option Dateiübertragung in IGEL UMS und richten Sie ein Profil mit der benutzerdefinierten Anwendungskonfiguration ein.

1. ANWENDUNG des Easy Screenshot Maker:
  - a. Start der Anwendung.
  - b. Screenshot erstellen.
  - c. Sichern der Datei, zum Beispiel als `test.png`.
2. ANWENDUNG des Rapid Screenshot:
  - a. Start der Anwendung.
  - b. Auf **Speichern unter** klicken, um den Pfad zum Speichern von Screenshots zu konfigurieren.
  - c. **Aufnahme** drücken.  
Screenshot wird automatisch als `.jpg` gespeichert.

<sup>52</sup> <https://sourceforge.net/projects/screenshot/?source=directory>

 Bitte beachten Sie die Lizenzen der beiden Screenshot-Erfassungstools, die auf den Websites dieser spezifischen Tools erwähnt werden!

## Systemzeit des Geräts einstellen

### Problem

Die Systemzeit des Geräts stimmt nicht.

### Lösung

1. Öffnen Sie die Gerätekonfiguration entweder lokal oder in der UMS.
2. Gehen Sie unter **System > Zeit und Datum**.
3. Wählen Sie Ihren **Kontinent/Bereich** (z. B. Deutschland).
4. Wählen Sie Ihren **Standort** (z. B. Berlin).
5. Stellen Sie die Zeit und das Datum ein
  - a. entweder manuell indem Sie auf **Zeit und Datum speichern** klicken
  - b. oder automatisch über die Option **NTP-Zeitserver verwenden**.
6. Klicken Sie **Übernehmen** oder **Ok** um Ihre Einstellungen zu speichern.

#### **Notiz**

Wenn Sie **Allgemein** als **Zeitzonebereich** wählen, müssen Sie Ihre GMT-Zeitzone (**Standort**) nach dem POSIX-Standard (wie unter Linux üblich) einstellen - das heißt, Sie müssen den Offset Ihrer gemeinsamen UTC-Zeitzone umkehren! (Siehe auch Tooltipp für Standort.) Daher ist es besser, die Zeitzone des Systems einzustellen, indem Sie den entsprechenden Bereich und Standort auswählen, als den GMT-Offset zu definieren.

Beispiel für America/New Your: Im POSIX-Standard ist **GMT+5** die Zeitzone **5 Stunden westlich** von Greenwich und entspricht **UTC-5**.

## Aktualisierung der Zeitzoneinformationen

### Symptom

Das Gerät zeigt eine falsche Tageszeit für Ihren Standort an, obwohl Sie die richtige Zeitzone eingestellt haben.

### Problem

Die Zeitzone oder die Regelung für die Sommerzeit für Ihren Standort hat sich geändert.

### Lösung

- ▶ Aktualisieren Sie die Zeitzone-Informationsdateien über die IGEL Universal Management Suite (UMS).

#### Abrufen der aktuellen Zeitzone-Informationsdateien

##### Auf Windows

- Verwenden Sie Ihren Webbrowser, um die folgenden Paketdateien herunterzuladen:
  - <http://packages.ubuntu.com/xenial-updates/all/tzdata/download> (for IGEL Linux version 10.x)
  - <http://packages.ubuntu.com/trusty-updates/all/tzdata/download> (for IGEL Linux version 5.x)
  - <http://packages.ubuntu.com/precise-updates/all/tzdata/download> (for IGEL Linux version 4.x)
- Entpacken Sie den Lieferumfang mit dem Programm 7-Zip (kostenlos erhältlich unter <http://www.7-zip.org>).
- Suchen Sie die Datei für Ihren Standort im extrahierten Verzeichnis in `usr/share/zoneinfo/`, z.B. `usr/share/zoneinfo/Africa/Casablanca` für Marokko.

##### Auf Linux

- Aktualisieren Sie Ihre Systemzeitzoneinformationen mit folgenden Befehlen: `sudo apt-get update sudo apt-get update sudo apt-get install tzdata`
- Suchen Sie die Datei für Ihren Standort im Systemverzeichnis `/usr/share/zoneinfo/`, z.B. `/usr/share/zoneinfo/Africa/Casablanca` für Marokko.

#### Verteilung der Dateien aus der IGEL Universal Management Suite

- Wählen Sie **System > Neu > Neue Datei** in der Menüleiste der UMS Konsole oder gehen Sie zu **Dateien** in der Baumstruktur und wählen Sie **Neue Datei** aus dem Kontextmenü.
- Wählen Sie unter **Lokale Datei** die Zeitzoneendatei für Ihren Standort aus.

- Wählen Sie **Nicht definiert** unter **Klassifizierung**.
- Geben Sie `/wfs/zoneinfo/` als **Speicherpfad des Gerätes** an.
- Setzen Sie die **Zugriffsrechte** auf "Lesen" und "Schreiben" für den Besitzer und "Lesen" für Andere.
- Wählen Sie **Root** als **Besitzer**.
- Klicken Sie auf **Ok**, um die Einstellungen zu bestätigen.

### Neue Datei ✕

**Dateiursprung**

Lokale Datei zu UMS Server hochladen

Lokale Datei

Speicherort im UMS Server (URL)

Bestehende Datei aus UMS Server verwenden

Speicherort der Datei (URL)

**Dateiziel**

Klassifizierung

Speicherpfad des Gerätes

**Zugriffsrechte**

	Lesen	Schreiben	Ausführen
Besitzer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Andere	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Besitzer

Auf einem Gerät können Sie die Übertragung und Aktivierung der neuen Zeitzonen-Informationsdateien überprüfen:

- Geben Sie im **lokalen Terminal** `grep 'timezone_config' /var/log/messages` ein.

i Auf IGEL Linux Version 10.x, verwenden Sie: `journalctl | grep 'timezone_config'`.

- Die Ausgabe sollte wie folgt aussehen:

```
Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/
Casablanca to /usr/share/zoneinfo/Africa/Casablanca
```

```
Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/  
Casablanca to /usr/share/zoneinfo/posix/Africa/Casablanca
```

```
Feb 27 11:28:13 (none) timezone_config: configure timezone Africa/  
Casablanca
```

## Einen Handler für MIME-Typen hinzufügen oder ändern

### Symptom

Dateien oder Protokolle werden mit der falschen Applikation geöffnet.

### Problem

Der Handler für MIME-Typen für den Dateityp oder das Protokoll fehlt oder ist falsch konfiguriert.

### Lösung

Ändern sie den Handler für MIME-Typen oder fügen Sie einen neuen ein.

Handler für MIME-Typen werden durch \*.desktop-Dateien im Verzeichnis `/usr/share/applications.mime/` definiert.

Um eine neue \*.desktop- Datei hinzuzufügen, verwenden Sie das folgende Beispiel und bearbeiten Sie es nach Ihren Wünschen:

```
[Desktop Entry]
Version=1.0
Encoding=UTF-8
Type=Application
Name=Browser//A name for the MIME type handler
Categories=Application
Exec=/usr/bin/firefox %u//The binary to execute on opening an associated file
MimeType=x-scheme-handler/http;x-scheme-handler/https;text/html,application/
xhtml+xml;//A list of MIME types separated by semicolon
Terminal=false
StartupNotify=false
NoDisplay=true
```

Mehr über \*.desktop -Dateien erfahren Sie in einer Spezifikation unter [freedesktop.org](http://freedesktop.org)<sup>53</sup>.

Dies sind die Standardhandler unter IGEL Linux:

Bilder (geöffnet mit gpicview)

- image/bmp;

---

<sup>53</sup> <http://freedesktop.org>



- image/gif;
- image/jpeg;
- image/jpg;
- image/png;
- image/x-bmp;
- image/x-pcx;
- image/x-tga;
- image/x-portable-pixmap;
- image/x-portable-bitmap;
- image/x-targa;
- image/x-portable-greymap;
- application/pcx;
- image/svg+xml;
- image/svg+xml;

Videos und Musik (geöffnet über `/services/mplr/bin/mediaplayer` )

Beachten Sie, dass `/services/mplr/bin/mediaplayer` entweder `/config/sessions/mediaplayer0` , falls vorhanden, oder `totem` aufruft, wenn dies nicht der Fall ist.

- application/mxf;
- application/ogg;
- application/ram;
- application/sdp;
- application/smil;
- application/smil+xml;
- application/vnd.ms<sup>54</sup>-wpl;
- application/vnd.rn-realmedia;
- application/x-extension-m4a;
- application/x-extension-mp4;
- application/x-flac;
- application/x-flash-video;
- application/x-matroska;
- application/x-netshow-channel;
- application/x-ogg;
- application/x-quicktime-media-link;
- application/x-quicktimeplayer;
- application/x-shorten;
- application/x-smil;
- application/xspf+xml;
- audio/3gpp;
- audio/ac3;
- audio/AMR;
- audio/AMR-WB;
- audio/basic;
- audio/midi;

---

<sup>54</sup> <http://vnd.ms>

- audio/mp4;
- audio/mpeg;
- audio/mpegurl;
- audio/ogg;
- audio/prs.sid;
- audio/vnd.rn-realaudio;
- audio/x-ape;
- audio/x-flac;
- audio/x-gsm;
- audio/x-it;
- audio/x-m4a;
- audio/x-matroska;
- audio/x-mod;
- audio/x-mp3;
- audio/x-mpeg;
- audio/x-mpegurl;
- audio/x-ms-asf;
- audio/x-ms-asx;
- audio/x-ms-wax;
- audio/x-ms-wma;
- audio/x-musepack;
- audio/x-pn-aiff;
- audio/x-pn-au;
- audio/x-pn-realaudio;
- audio/x-pn-realaudio-plugin;
- audio/x-pn-wav;
- audio/x-pn-windows-acm;
- audio/x-realaudio;
- audio/x-real-audio;
- audio/x-sbc;
- audio/x-scpls;
- audio/x-speex;
- audio/x-tta;
- audio/x-wav;
- audio/x-wavpack;
- audio/x-vorbis;
- audio/x-vorbis+ogg;
- audio/x-xm;
- image/vnd.rn-realpixmap;
- image/x-pict;
- misc/ultravox;
- text/google-video-pointer;
- text/x-google-video-pointer;
- video/3gpp;
- video/dv;
- video/fli;
- video/flv;

- video/mp4;
- video/mp4v-es;
- video/mpeg;
- video/msvideo;
- video/ogg;
- video/quicktime;
- video/vivo;
- video/vnd.divx;
- video/vnd.rn-realvideo;
- video/vnd.vivo;
- video/x-anim;
- video/x-avi;
- video/x-flc;
- video/x-fli;
- video/x-flic;
- video/x-flv;
- video/x-m4v;
- video/x-matroska;
- video/x-mpeg;
- video/x-ms-asf;
- video/x-ms-asx;
- video/x-msvideo;
- video/x-ms-wm;
- video/x-ms-wmv;
- video/x-ms-wmx;
- video/x-ms-wvx;
- video/x-nsv;
- video/x-ogm+ogg;
- video/x-theora+ogg;
- video/x-totem-stream;
- x-content/video-dvd;
- x-content/video-vcd;
- x-content/video-svcd;

Dokumente (geöffnet über `/usr/bin/evince`)

- application/pdf;
- image/tiff

Web (geöffnet über `/usr/bin/firefox -remote`)

- x-scheme-handler/http;
- x-scheme-handler/https;
- text/html;
- application/xhtml+xml;

## Regionale Einstellungen in Sitzungen

### Symptom

Im IGEL Setup gibt es mehrere Eingabefelder für regionale Einstellungen. Sie möchten wissen, welche Einstellungen welchen Effekt auf die Sitzungen haben.

### Problem

Wenn Sie eine bestimmte Tastatursprache einstellen, hat dies keinen Einfluss auf die regionalen Einstellungen.


### Lösung

Allgemeine regionale Einstellungen definieren:

- ▶ Gehen Sie auf **IGEL Setup > Benutzeroberfläche > Sprache**.
  - **Sprache:** Wählen Sie eine der angebotenen Sprachen für die grafische Benutzeroberfläche.
  - **Tastaturbelegung:** Wählen Sie die länderspezifische Zuordnung der Tasten, z. B. Englisch(US).
  - **Eingabegebietsschema:** Stellen Sie die Sprache ein, in der Sie schreiben werden, z. B. Englisch (Australien).
  - **Standards und Formate:** Wählen Sie die länderspezifischen Formate, z. B. für Datum und Zeit oder Währung.

Sitzungsspezifische regionale Einstellungen definieren:

- ▶ Gehen Sie in die Einstellungen Ihrer Sitzung, z. B. Citrix: **IGEL Setup > Sitzungen > Citrix > Citrix Global > Tastatur**

 Die Standardeinstellungen sind die, die Sie unter **Benutzeroberfläche > Sprache** definiert haben.

- ▶ Geben Sie die **Tastaturbelegung** und das **Eingabegebietsschema** für Ihre Citrix-Sitzung an.

## Geräte


- [Monitor \(see page 678\)](#)
- [Cherry SECURE BOARD verwenden \(see page 697\)](#)
- [Webcam-Umleitung und Optimierung in IGEL OS \(see page 726\)](#)
- [Webcam-Information \(see page 739\)](#)
- [Bluetooth-Tool \(see page 741\)](#)
- [Jabra Xpress Pakete bereitstellen \(see page 744\)](#)
- [Unterschriftenpads anschließen \(see page 748\)](#)
- [Ein Kofax / Wacom Unterschriftenpad verwenden \(see page 749\)](#)
- [Ein StepOver Unterschriftenpad verwenden \(see page 750\)](#)
- [eGK/KVK - Kartenlesegerät \(see page 756\)](#)
- [Mobilgeräte-Zugriff verwenden \(see page 773\)](#)
- [Austauschen der Funktion von Maustasten \(z. B. Verwendung einer Evoluent Maus\) \(see page 783\)](#)
- [Natürliches Scrollen \(umgekehrte Scrollrichtung\) in IGEL OS verwenden \(see page 785\)](#)
- [Einen seriellen Barcodescanner verbinden \(see page 788\)](#)
- [DriveLock mit IGEL Geräten verwenden \(see page 790\)](#)
- [Einschränkung der Montage von Hotplug-Speichergeräten auf IGEL Linux \(see page 791\)](#)
- [When to Use USB Redirection \(see page 792\)](#)
- [USB-Zugriffskontrolle konfigurieren \(see page 793\)](#)
- [Probleme mit USB-IDs in den USB-Geräteregeln \(see page 796\)](#)
- [Fixing Touchpad Issues \(see page 798\)](#)
- [How Do I Configure a Fujitsu PalmSecure Vein Scanner with IGEL OS? \(see page 799\)](#)
- [Virtual Background for Unified Communication Apps in IGEL OS \(see page 800\)](#)

## Monitor

- [Kalibrierung eines Touchscreens \(see page 679\)](#)
- [Touchscreen in Multimonitor-Umgebung \(see page 691\)](#)
- [USB-betriebener ASUS-Monitor und IGEL OS 11 \(see page 692\)](#)
- [Probleme von Hotplugging mit DisplayPort-Monitoren beheben \(see page 693\)](#)
- [Kein Ton bei Verwendung eines DisplayPort-Monitors \(see page 694\)](#)
- [Drei DVI-Monitore an den UD7 mit passivem DisplayPort-Adaptern anschließen \(see page 696\)](#)

## Kalibrierung eines Touchscreens

Um einen Touchscreen einzurichten, müssen Sie die Touchscreenfunktion aktivieren und einen bestimmten Touchscreentreiber auswählen.

 Die Erstkonfiguration sollte mit angeschlossener Maus oder Tastatur erfolgen, um sicherzustellen, dass Sie das Setup öffnen und darin navigieren können.

Um einen Touchscreen einzurichten:

1. Gehen Sie im IGEL Setup auf **Benutzeroberfläche > Eingabe > Touchscreen**.
2. Aktivieren Sie **Touchscreen aktivieren**.
3. Wählen Sie Ihren **Touchscreentreiber**.

Je nach dem gewählten Treiber haben Sie verschiedene Konfigurationsmöglichkeiten. Für weitere Informationen klicken Sie auf den entsprechenden Link:

- [EvTouch \(USB\) \(see page 680\)](#)
- [eGalax \(see page 683\)](#)
- [Elo Multitouch \(USB\) \(see page 685\)](#)
- [Elo Singletouch \(USB\) \(see page 687\)](#)
- [TSHARC \(USB\) \(see page 689\)](#)

## EvTouch (USB)

## Unterstützte Geräte

## Unterstützte Touch-Monitore und Touchscreen-Controller:

Hersteller	Produkt	Name
0x16FD	0x5453	Reakin, TS2005F USB TouchController
0x7374	0x0001	
0x04E7	0x0020	Elo TouchSystems, Touchscreen Interface (2700)
0x1870	0x0001	Nexio Co., Ltd, iNexio Touchscreen Controller
0x10F0	0x2002	Nexio Co., Ltd, iNexio Touchscreen Controller
0x0664	0x0306	ET&T Technology Co., Ltd., Groovy Technology Corp. GTouch Touch Screen
0x0664	0x0309	ET&T Technology Co., Ltd. Groovy Technology Corp. GTouch Touch Screen
0x14C8	0x0003	Zytronic, Unbekanntes Gerät
0x1AC7	0x0001	
0x0F92	0x0001	
0x08F2	0x00F4	Gotop Information Inc., Unbekanntes Gerät
0x08F2	0x00CE	Gotop Information Inc., Unbekanntes Gerät
0x08F2	0x007F	Gotop Information Inc., Super Q2 Tablet
0x0DFC	0x0001	GeneralTouch Technology Co., Ltd, Touchscreen
0x1391	0x1000	IdealTEK, Inc., URTC-1000
0x6615	0x0001	IRTOUCHSYSTEMS Co. Ltd., Touchscreen
0x595A	0x0001	IRTOUCHSYSTEMS Co. Ltd., Touchscreen
0x0AFA	0x03E8	
0x0637	0x0001	
0x1234	0x5678	Brain Actuated Technologies, Unbekanntes Gerät
0x16E3	0xF9E9	
0x0403	0xF9E9	Future Technology Devices International, Ltd, Unbekanntes Gerät



Hersteller	Produkt	Name
0x0596	0x0001	MicroTouch Systems, Inc., Touchscreen
0x134C	0x0004	PanJit International Inc., Touch Panel Controller
0x134C	0x0003	PanJit International Inc., Touch Panel Controller
0x134C	0x0002	PanJit International Inc., Touch Panel Controller
0x134C	0x0001	PanJit International Inc., Touch Panel Controller
0x1234	0x0002	Brain Actuated Technologies, Unbekanntes Gerät
0x1234	0x0001	Brain Actuated Technologies Unbekanntes Gerät
0x0EEF	0x0002	D-WAV Scientific Co., Ltd, Touchscreen Controller(Professional)
0x0EEF	0x0001	D-WAV Scientific Co., Ltd, eGalax TouchScreen
0x0123	0x0001	
0x3823	0x0002	
0x3823	0x0001	

## Einstellungsparameter

- **Touchscreentreiber**

Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

- **X- und Y-Werte vertauschen**

Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; X- und Y-Werte vertauschen</b>	userinterface.touchscreen.swapxy	aktiviert / <u>deaktiviert</u>

- **Treiberspezifische Voreinstellungen laden** für das Zurücksetzen der Kalibrierwerte.

## Kalibrierung / Zurücksetzung

Um den Touchscreen zu kalibrieren:

1. Gehen Sie zu **IGEL Setup > Benutzeroberfläche > Eingabe > Touchscreen**.
2. Deaktivieren Sie **Touchscreen ist bereits kalibriert**.

Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreen ist bereits kalibriert</b>	userinterface.touchscreen.calibrated	aktiviert / <a href="#">deaktiviert</a>

3. Setzen Sie **Touchscreentreiber** auf **EvTouch (USB)**.  
**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

4. Starten Sie Ihr Gerät neu und klicken Sie auf **Setup > Zubehör > Touchscreenkalibrierung**, um das IGEL Tool für Touchscreenkalibrierung zu verwenden. Dadurch wird das Tool für Kalibrierung *xinput\_calibrator* aufgerufen, das sich unter `/usr/bin/xinput_calibrator` befindet. Die Kalibrierungsparameter werden im IGEL Setup gespeichert.

Funktion 'Halten für Rechtsklick'

Um die Funktion zu aktivieren:

1. Aktivieren Sie die Option **Emuliere rechte Maustaste** unter **Benutzeroberfläche > Eingabe > Touchscreen**.  
**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Emuliere rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbutton	aktivieren / <a href="#">deaktivieren</a>

2. Stellen Sie unter **Zeitlimit für rechte Maustaste** die Zeit ein, nach der ein Rechtsklick erzeugt werden soll.  
**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Zeitlimit für rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbuttontimeout	Standard: 1000 ms

Multimonitor

Multimonitorkonfiguration wird nicht unterstützt.

## eGalax

## Unterstützte Geräte

EETI eGalax eMPIA USB Touchscreens.

## Einstellungsparameter

- **Touchscreentreiber**

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

## Kalibrierung / Zurücksetzung

Um den Touchscreen zu kalibrieren:

1. Gehen Sie im IGEL Setup unter **Benutzeroberfläche > Eingabe > Touchscreen**.
2. Deaktivieren Sie **Touchscreen ist bereits kalibriert**.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreen ist bereits kalibriert</b>	userinterface.touchscreen.calibrated	aktiviert / <u>deaktiviert</u>

3. Wählen Sie **eGalax** als **Touchscreentreiber**.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

4. Starten Sie das Gerät neu oder klicken Sie im IGEL Setup **Zubehör > Touchscreenkalibrierung**, um das IGEL Tool für Touchscreenkalibrierung zu verwenden. Dies ruft das proprietäre EETI Kalibrierungstool auf, das sich unter `/usr/bin/eCaLib` befindet. Der Kalibrierparameter wird in `/wfs/egtouch.d` gespeichert.

## Funktion 'Halten für Rechtsklick'

Um diese Funktion zu aktivieren:

1. Aktivieren Sie die Option **Emuliere rechte Maustaste** unter **Benutzeroberfläche > Eingabe > Touchscreen**.

**Mehr**

IGEL Setup > Benutzeroberfläche > Eingabe > Touchscreen		
> <b>Emuliere rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbutton	aktiviert / <u>deaktiviert</u>

2. Stellen Sie unter **Zeitlimit für rechte Maustaste** die Zeit ein, nach der ein Rechtsklick erzeugt wird.

**Mehr**

IGEL Setup > Benutzeroberfläche > Eingabe > Touchscreen		
> <b>Zeitlimit für rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbutton	Standard: <u>1000 ms</u>

Multimonitor

Multimonitorkonfiguration wird nicht unterstützt.

## Elo Multitouch (USB)

### Unterstützte Geräte

IntelliTouch Plus/iTouch Plus 2515-07(non HID), 2521 (HID), 2515-00(HID) PCAP 2 Touch, 4 Touch und 10 Touch Controller.

### Einstellungsparameter

- Touchscreentreiber

#### Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

### Kalibrierung / Zurücksetzung

Um den Touchscreen zu kalibrieren:

1. Gehen Sie auf **IGEL Setup > Benutzeroberfläche > Eingabe > Touchscreen**.
2. Deaktivieren Sie **Touchscreen ist bereits kalibriert**.

#### Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreen ist bereits kalibriert</b>	userinterface.touchscreen.calibrated	aktiviert / <u>deaktiviert</u>

3. Wählen Sie **Elo Multitouch (USB)** als **Touchscreentreiber**.

#### Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

4. Starten Sie das Gerät neu oder klicken Sie im IGEL Setup auf **Zubehör > Touchscreenkalibrierung**, um das IGEL Tool für Touchscreenkalibrierung zu verwenden. Dies ruft das proprietäre Kalibrierungstool ELO Multitouch auf, das sich unter `/etc/opt/elo-mt-usb/elo-va` befindet. Der Kalibrierparameter wird in `/wfs/elo-usb.d/MT-USBConfigData` gespeichert.

### Funktion 'Halten für Rechtsklick'

Um diese Funktion zu aktivieren:

1. Aktivieren Sie die Option **Emuliere rechte Maustaste** unter **Benutzeroberfläche > Eingabe > Touchscreen**.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Emuliere rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbutton	aktiviert / <u>deaktiviert</u>

2. Stellen Sie unter **Zeitlimit für rechte Maustaste** die Zeit ein, nach der ein Rechtsklick erzeugt wird.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Zeitlimit für rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbutton	Standard: <u>1000 ms</u>

## Multimonitor

Es werden mehrere Touchscreens ELO Multitouch (USB) auf einem IGEL Gerät unterstützt. Die Kalibrierung eines zweiten Touchscreens ELO Multitouch USB kann über die Befehlszeile mithilfe von `/etc/opt/elo-mt-usb/eloVa --videoscreen=2` erfolgen, wobei 2 für den zweiten Touchscreen ELO Multitouch steht, der mit dem IGEL Gerät verbunden ist.

- i** Um eine Liste der für die Kalibrierung verfügbaren Video- und USB-Touchscreenegeräte anzuzeigen, verwenden Sie den Befehl: `/etc/opt/elo-mt-usb/eloVa --viewdevices`.

## Elo Singletouch (USB)

### Unterstützte Geräte

#### Elo Smartset USB-Controller:

- IntelliTouch(R) 2701, 2700, 2600, 2500U
- CarrollTouch(R) 4500U, 4000U
- Accutouch(R) 2216, 3000U, 2218
- Surface Capacitive 5020, 5010, 5000
- Accoustic Pulse Recognition(APR) Smartset 7010
- Andere Elo Smartset USB-Controller

### Einstellungsparameter

- Touchscreentreiber

#### Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

### Kalibrierung / Zurücksetzung

Um den Touchscreen zu kalibrieren:

1. Gehen Sie auf **IGEL Setup > Benutzeroberfläche > Eingabe > Touchscreen**.
2. Deaktivieren Sie **Touchscreen ist bereits kalibriert**.

#### Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreen ist bereits kalibriert</b>	userinterface.touchscreen.calibrated	aktiviert / <u>deaktiviert</u>

3. Wählen Sie **Elo Singletouch (USB)** als **Touchscreentreiber**.

#### Mehr

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	


4. Starten Sie das Gerät neu oder klicken Sie im IGEL Setup auf **Zubehör > Touchscreenkalibrierung**, um das IGEL Tool für Touchscreenkalibrierung zu verwenden. Dies ruft das proprietäre Kalibrierungstool ELO Singletouch auf, das sich unter `/etc/opt/elo-usb/elo-usb/e_lova` befindet. Der Kalibrierparameter wird in `/wfs/elo-usb.d/USBConfigData` gespeichert.

### Funktion 'Halten für Rechtsklick'

Diese Funktion wird nicht unterstützt.

### Multimonitor

Es werden mehrere Touchscreens ELO Singletouch USB auf einem IGEL Gerät unterstützt. Die Kalibrierung eines zweiten Touchscreens ELO Singletouch USB kann über die Befehlszeile mithilfe von `/etc/opt/elo-usb/e1ova --videoscreen=2` erfolgen, wobei 2 für den zweiten Touchscreen ELO Singletouch USB steht, der an das IGEL Gerät angeschlossen ist.

 Um eine Liste der für die Kalibrierung verfügbaren Video- und USB-Touchscreengeräte anzuzeigen, verwenden Sie den Befehl: `/etc/opt/elo-usb/e1ova --viewdevices`.



## TSHARC (USB)

## Unterstützte Geräte

Hampshire TSHARC USB Touchscreens.

## Einstellungsparameter

- **Touchscreentreiber**

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

## Kalibrierung / Zurücksetzung

Um den Touchscreen zu kalibrieren:

1. Gehen Sie im IGEL Setup unter **Benutzeroberfläche > Eingabe > Touchscreen**.
2. Deaktivieren Sie **Touchscreen ist bereits kalibriert**.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreen ist bereits kalibriert</b>	userinterface.touchscreen.calibrated	aktiviert / <u>deaktiviert</u>

3. Wählen Sie **TSharc** unter **Touchscreentreiber**.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Touchscreentreiber</b>	userinterface.touchscreen.driver	

4. Starten Sie das Gerät neu oder klicken Sie im **Setup** auf **Zubehör > Touchscreenkalibrierung**, um das IGEL Tool für Touchscreenkalibrierung zu verwenden. Dies ruft das proprietäre Hampshire Kalibrierungstool auf, das sich unter `/usr/bin/tscal` befindet. Der Kalibrierparameter wird in `/wfs/tsharc.d.` gespeichert.

## Funktion 'Halten für Rechtsklick'

Um die Funktion zu aktivieren:

1. Aktivieren Sie die Option **Emuliere rechte Maustaste** unter **Benutzeroberfläche > Eingabe > Touchscreen**.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
---	--	--

<b>&gt; Emuliere rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbutton	aktiviert / <u>deaktiviert</u>
---------------------------------------	--	--------------------------------

2. Stellen Sie unter **Zeitlimit für rechte Maustaste** die Zeit ein, nach der ein Rechtsklick erzeugt werden soll.

**Mehr**

<b>IGEL Setup &gt; Benutzeroberfläche &gt; Eingabe &gt; Touchscreen</b>		
<b>&gt; Zeitlimit für rechte Maustaste</b>	userinterface.touchscreen.emulatethirdbuttontimeout	Standard: 1000 ms

Multimonitor

Multimonitorkonfiguration wird nicht unterstützt.

## Touchscreen in Multimonitor-Umgebung

### Symptom

Sie verwenden einen Touchscreen in einer Multimonitor-Umgebung. In diesem Fall kann es vorkommen, dass sich die Touchscreen-Koordinatenmatrix über beide Monitore ausdehnt, so dass der Monitor den Berührungspunkt falsch interpretiert.

### Problem

Sie berühren den Touchscreen in der Mitte und der Cursor bewegt sich zwischen den beiden Bildschirmen.

### Lösung

Um eine unerwünschte Erweiterung der Touchscreen-Matrix zu vermeiden, müssen Sie im Setup die richtige Touchscreen-Anschlussart auswählen:

1. Klicken Sie auf **Benutzeroberfläche > Eingabe > Touchscreen** im IGEL Setup.
2. Wählen Sie die richtige Touchscreen-Anschlussart unter **Multi Monitor > Touchscreenmonitor**.

## USB-betriebener ASUS-Monitor und IGEL OS 11

### Lösung beruht auf Erfahrungen im Feld

Dieser Artikel stellt eine Lösung bereit, die nicht durch die IGEL Forschungs- und Entwicklungsabteilung geprüft wurde. Daher kann IGEL keinen offiziellen Support leisten. Soweit durchführbar, testen Sie die Lösung, bevor Sie diese in einer Produktivumgebung zum Einsatz bringen.

### Problem

USB-betriebener Monitor

### Umgebung

- IGEL OS 11 (11.03.100)
- UMS 6.01 und neuer

### Beschreibung

Empfehlung für einen USB-betriebenen Monitor

### Lösung

Unter folgenden Link finden Sie den USB-betriebenen ASUS-Monitor, der Plug-and-Play mit IGEL OS funktioniert: <https://www.asus.com/us/Monitors/MB168B/>.

## Probleme von Hotplugging mit DisplayPort-Monitoren beheben

### Symptom

Bei IGEL Linux tritt bei einer Konfiguration mit zwei Ansichten folgendes Problem auf: Wird ein über DisplayPort angeschlossener Monitor erst nach dem Booten des Geräts eingeschaltet, bleibt er schwarz.

### Problem

Der Display Port-Standard ermöglicht es, dass ein ausgeschalteter Monitor von der Grafikkarte nicht erkannt werden kann.

### Lösung

Im Folgenden wird überprüft, ob ein in der Konfiguration enthaltener Monitor fehlt (d.h. ausgeschaltet ist) und sofort wieder betriebsbereit gemacht wird sobald er angezeigt wird (d.h. eingeschaltet ist):

1. Wenn Sie IGEL Linux 5 verwenden, stellen Sie sicher, dass Sie Version 5.10.410 oder neuer verwenden.  
Wenn Sie IGEL Linux 10 verwenden, benötigen Sie kein Upgrade.
2. Gehen Sie im Setup unter **System > Registry > Parametersuche** > `session.user_display` > `%.options.enhanced_hotplug`
3. Stellen Sie sicher, dass der Parameter auf `true` gesetzt ist. (Standard)

- i** Eine weitere Einstellung können Sie verwenden, wenn Sie nicht möchten, dass IGEL Linux die Anzeigeeinstellungen bei jedem Ein- und Ausschalten eines Display Port-Monitors ändert:
- Gehen Sie zu **System > Registry > Parametersuche**  
> `sessions.user_display%.options.disable_hotplug`
  - Stellen Sie **Nur\_DP\_Trennen** ein.

## Kein Ton bei Verwendung eines DisplayPort-Monitors

### Symptom

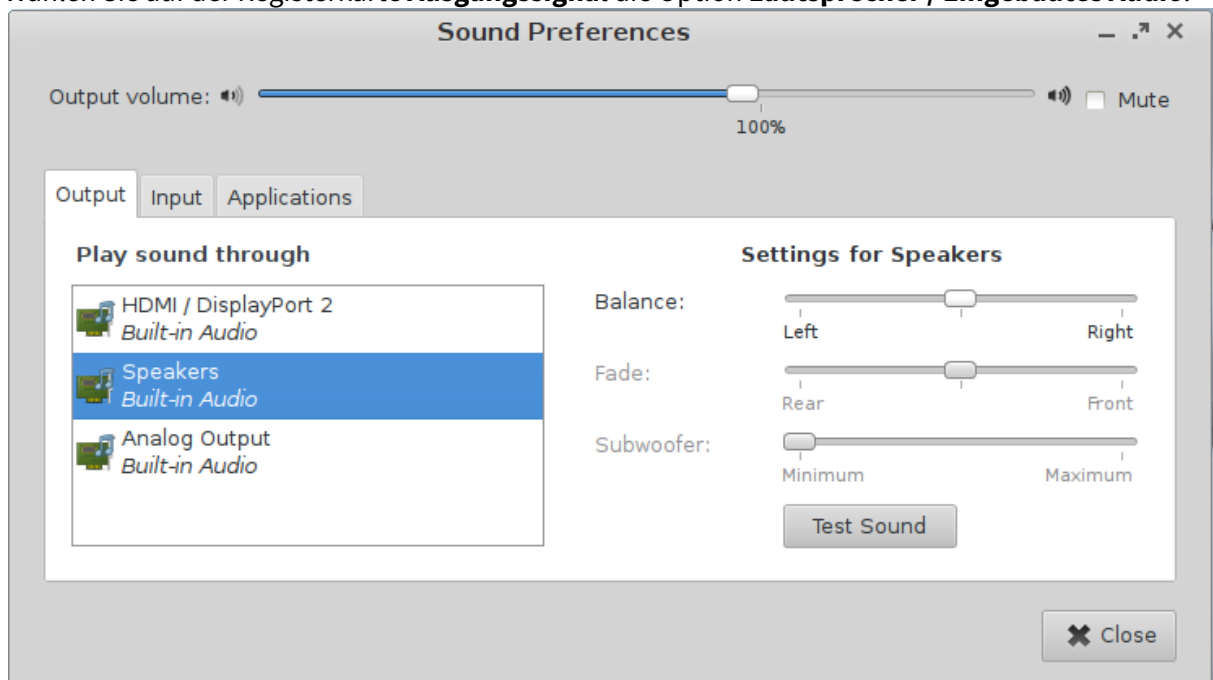
Sie hören keinen Ton Ihres IGEL UD 5 oder UD 6 Geräts. Sie verwenden einen Monitor der über den DisplayPort verbunden ist.

### Problem

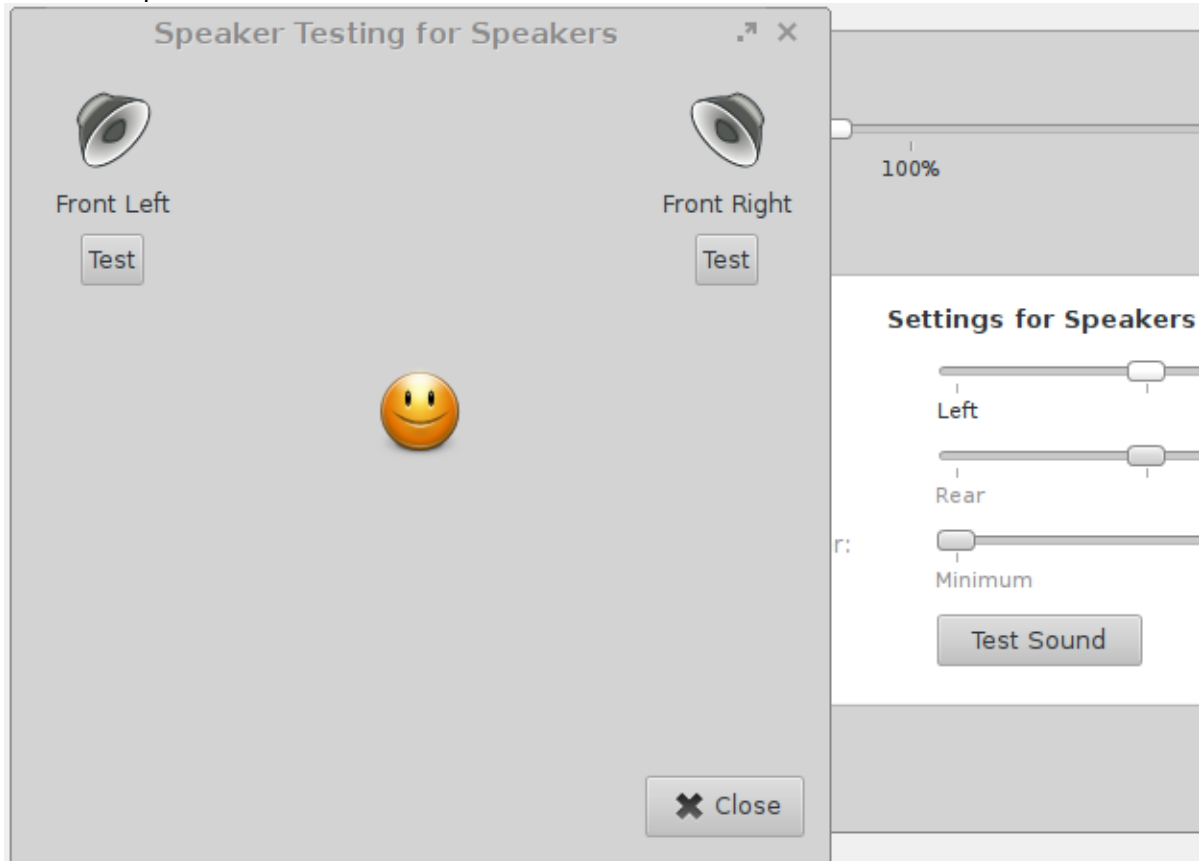
Manche DisplayPort-Monitore melden irreführend die Unterstützung für Display-Audio, obwohl sie keine Lautsprecher haben. IGEL Linux wird daher versuchen, Audio über den Monitor wiederzugeben.

### Lösung

1. Klicken Sie mit der rechten Maustaste auf das Lautsprechersymbol im Bedienfeld und öffnen Sie **Audioeinstellungen**.
2. Wählen Sie auf der Registerkarte **Ausgangssignal** die Option **Lautsprecher / Eingebautes Audio**.



3. Klicken Sie **Testton** um die neue Einstellung zu testen. Überprüfen Sie, ob Sie auf den Gerätausprechern eine Stimme mit den Worten "Vorne Links" und "Vorne Rechts" hören.




## Drei DVI-Monitore an den UD7 mit passivem DisplayPort-Adaptern anschließen

### Problem

Wenn drei DVI-Monitore an den UD7 mit passiven DisplayPort-Adaptern angeschlossen sind, werden nur ein oder zwei Monitore erkannt.

### Lösung

 Diese Lösung ist nur dann nachhaltig, wenn die Energieeinsparung ausgeschaltet ist.

1. Öffnen Sie das Geräte-Setup.
2. Gehen Sie unter **System > Registry > x > xserver0 > force\_reconfig** (Parametersuche: `x.xserver0.force_reconfig`) und stellen Sie den Wert auf **Nie**.
3. Klicken Sie **Ok** um die Einstellungen zu speichern und das Setup zu schließen.
4. Starten Sie das Gerät neu.  
Alle drei Monitore sollten erkannt werden.



## Cherry SECURE BOARD verwenden

### Überblick

Cherry SECURE BOARD 1.0 bietet einen sicheren Tastatureingabemodus, der gegen Hardware Keylogging und "Bad USB"-Angriffe schützt.

Die folgenden Sicherheitsfunktionen stehen zur Verfügung, wenn ein IGEL OS 11-Gerät im Sicherheitsmodus an ein Cherry SECURE BOARD 1.0 angeschlossen wird:

- Ihre IGEL OS 11-Geräte akzeptieren Tastatureingaben nur von einem personalisierten Cherry SECURE BOARD mit aktiviertem Sicherheitsmodus.
- Der Tastaturverkehr zwischen der Tastatur und dem Endgerät wird über eine TLS 1.3-verschlüsselte Verbindung übertragen.
- Optional kann die Tastatur so konfiguriert werden, dass sie nur Endgeräte akzeptiert, die über die richtigen Zertifikate verfügen.

Weitere Einzelheiten über das Cherry SECURE BOARD finden Sie unter <https://www.cherry-world.com/cherry-secure-board-1-0.html>.

### Voraussetzungen

- Geräte mit IGEL OS 11.03 oder höher
- UMS 6.01 oder höher

## Das Cherry SECURE BOARD im sicheren Modus arbeiten lassen

Um eine Reihe von Cherry SECURE BOARD-Tastaturen einzurichten, müssen Sie zunächst ein Endgerät konfigurieren, der für die Personalisierung der Tastaturen verwendet wird. Der Personalisierungsprozess setzt voraus, dass für jede Cherry SECURE BOARD-Tastatur, die im Sicherheitsmodus verwendet werden soll, die entsprechenden Zertifikate bereitgestellt werden.

Darüber hinaus müssen die Endgeräte, die an die Cherry SECURE BOARD-Tastaturen angeschlossen werden sollen, mit den entsprechenden Zertifikaten ausgestattet werden.

Um Cherry SECURE BOARD-Tastaturen einzurichten und zu verwenden, führen Sie die folgenden Schritte durch:

1. [Zertifikate erhalten](#) (see page 698)
2. [Die Personalisierungsmaschine einrichten](#) (see page 714)
3. [Personalizing the Cherry SECURE BOARD](#) (see page 716)
4. [Setting Up the Endpoints](#) (see page 720)

Wenn Sie eine Cherry SECURE BOARD-Tastatur in den Originalzustand zurückversetzen möchten, lesen Sie den Abschnitt [Zurücksetzen der Tastatur in den Originalzustand](#) (see page 725).

## Zertifikate erhalten

Der Sicherheitsmodus erfordert eine Reihe von Zertifikaten, die sowohl auf dem Endgerät als auch auf der Tastatur vorhanden sein müssen. Zunächst werden alle erforderlichen Zertifikate an das Endgerät übertragen. Dann installiert das Endgerät ein Benutzerzertifikat und den entsprechenden Schlüssel auf der Tastatur; optional wird auch das Root-CA-Zertifikat des Clients installiert. Diese Installation von Zertifikaten wird als Personalisierung bezeichnet.

## Gerätezertifikate herunterladen

- ▶ Laden Sie alle Zertifikate herunter von <https://github.com/secureboard10/secureboard-ca>:
  - Geräte-Root-CA-Zertifikat: `SecureboardRootCA.pem`
  - Geräte-Zwischen-CA-Zertifikate: `p-20190712.pem`, `p-20191030` usw.

## Erstellen der benutzerdefinierten Zertifikate

Gemäß "CHERRY SECUREBOARD 1.0, Software Developer's Guide", Kapitel 9.5, müssen alle Zertifikate und Schlüsselpaare, die an die Tastatur gesendet werden, die folgenden Anforderungen erfüllen:

- X509 Version 3 unter Verwendung der ECDSA-über-NIST-Kurve prime256v1 mit entsprechenden Tasten
  - Größe: Maximal 572 Byte bzw. 475 Byte im DER-Format
- ▶ Erstellen Sie die folgenden benutzerdefinierten Zertifikate:

- ✓ Eine Beispielanleitung für OpenSSL finden Sie in "CHERRY SECUREBOARD 1.0, Software Developer's Guide", Kapitel 9.5; Siehe [https://www.cherry.de/files/manual/SECUREBOARD\\_SwDev\\_Guide\\_en-0.4.pdf](https://www.cherry.de/files/manual/SECUREBOARD_SwDev_Guide_en-0.4.pdf). Außerdem enthält das SECURE BOARD 1.0 Quick Installation Package ein fertiges Skript, das Beispielzertifikate erzeugt. Laden Sie das Paket von [https://www.cherry.de/files/software/Cherry\\_Secureboard\\_1.0\\_Quick\\_Installation\\_Package\\_V1.0.zip](https://www.cherry.de/files/software/Cherry_Secureboard_1.0_Quick_Installation_Package_V1.0.zip) herunter, entzippen Sie die Datei und verwenden Sie `Cherry Secureboard 1.0 cert-package V1.0/secureboard_linux/create_certs.sh` (Linux) oder `Cherry Secureboard 1.0 cert-package V1.0/secureboard_windows/create_certs.bat` (Windows).

Zertifikat	Erforderlich/optional	Anforderungen	Kodierung/Endung	Max. Größe	Dateiname	Anmerkungen
Root-CA-Zertifikat des Benutzers	erforderlich	keine Angabe	PEM	keine Angabe	keine Angabe	Wenn dieses Zertifikat auch als Root-CA-Zertifikat des Benutzers für die wechselseitige Authentifizierung dienen soll, muss es die Anforderungen für an die Tastatur gesendete Zertifikate erfüllen: X509 Version 3 unter Verwendung von ECDSA über die NIST-Kurve prime256v1 mit dazugehörigen Schlüsseln; max. 475 Bytes
CA-Zwischenzertifikate	optional (je nach Verwendung Zertifikatskette)	keine Angabe	PEM	keine Angabe	keine Angabe	
Benutzerzertifikat (Tastatur)	erforderlich	X509 Version 3 unter Verwendung von ECDSA über die NIST-Kurve prime256v1 mit dazugehörigen Schlüsseln	DER (binär)	572 Bytes	user-cert.der	
Entsprechender Benutzer Schlüssel (Tastatur)	erforderlich	X509 Version 3 unter Verwendung von ECDSA über die NIST-Kurve prime256v1 mit dazugehörigen Schlüsseln	PEM (ohne Passphrase)	keine Angabe	user-key.pem	

Zertifikat	Erforderlich/optional	Anforderungen	Kodierung/Endung	Max. Dateigröße*	Dateiname	Anmerkungen
Root-CA-Zertifikat des Clients (Tastatur)	optional; für wechselseitige Authentifizierung <a href="#">** (see page 700)</a>	X509 Version 3 unter Verwendung von ECDSA über die NIST-Kurve prime256v1 mit dazugehörigen Schlüsseln	PEM	475 Bytes	kein Angabe	Kann mit dem Root-CA-Zertifikat des Benutzers identisch sein
Zertifikat des Clients (Endgerät)	optional; für wechselseitige Authentifizierung <a href="#">** (see page 700)</a>	X509 Version 3 unter Verwendung von ECDSA über die NIST-Kurve prime256v1 mit dazugehörigen Schlüsseln	PEM	475 Bytes	clients-cert.pem	
Schlüssel des Clients (Endgerät)	optional; für wechselseitige Authentifizierung <a href="#">** (see page 700)</a>	X509 Version 3 unter Verwendung von ECDSA über die NIST-Kurve prime256v1 mit dazugehörigen Schlüsseln	PEM (ohne Passphrase)	keine Angabe	clients-key.pem	

\* Der relevante Wert ist die Dateigröße, die das Zertifikat hat, wenn es im Binärformat gespeichert wird.

\*\* Wenn diese Zertifikate installiert sind, kann die Tastatur überprüfen, ob das Endgerät authentisch ist. Ohne die optionalen Zertifikate wird nur die Überprüfung der Authentizität der Tastatur durch das Endgerät durchgeführt.

## Bereitstellung der Personalisierungsmaschine

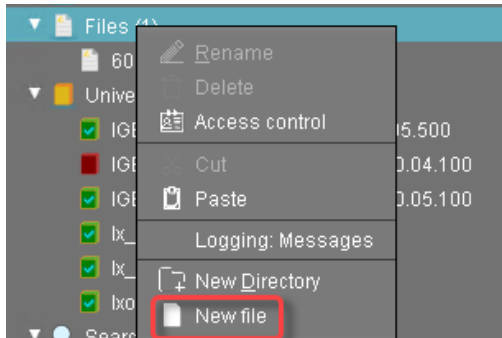
Die folgenden Anweisungen beschreiben, wie die erforderlichen Zertifikate auf die Personalisierungsmaschine übertragen werden. Der Personalisierungscomputer stellt die Zertifikate auf der Tastatur bereit. Zu diesem Zweck wird das UMS verwendet.

Zunächst wird für jedes Zertifikat oder jede Schlüsseldatei ein Dateiobjekt erstellt, damit die Dateien vom UMS verarbeitet werden können.

Zweitens werden die Dateiobjekte der Personalisierungsmaschine zugeordnet, was dazu führt, dass die Dateien auf diese Maschine übertragen werden.

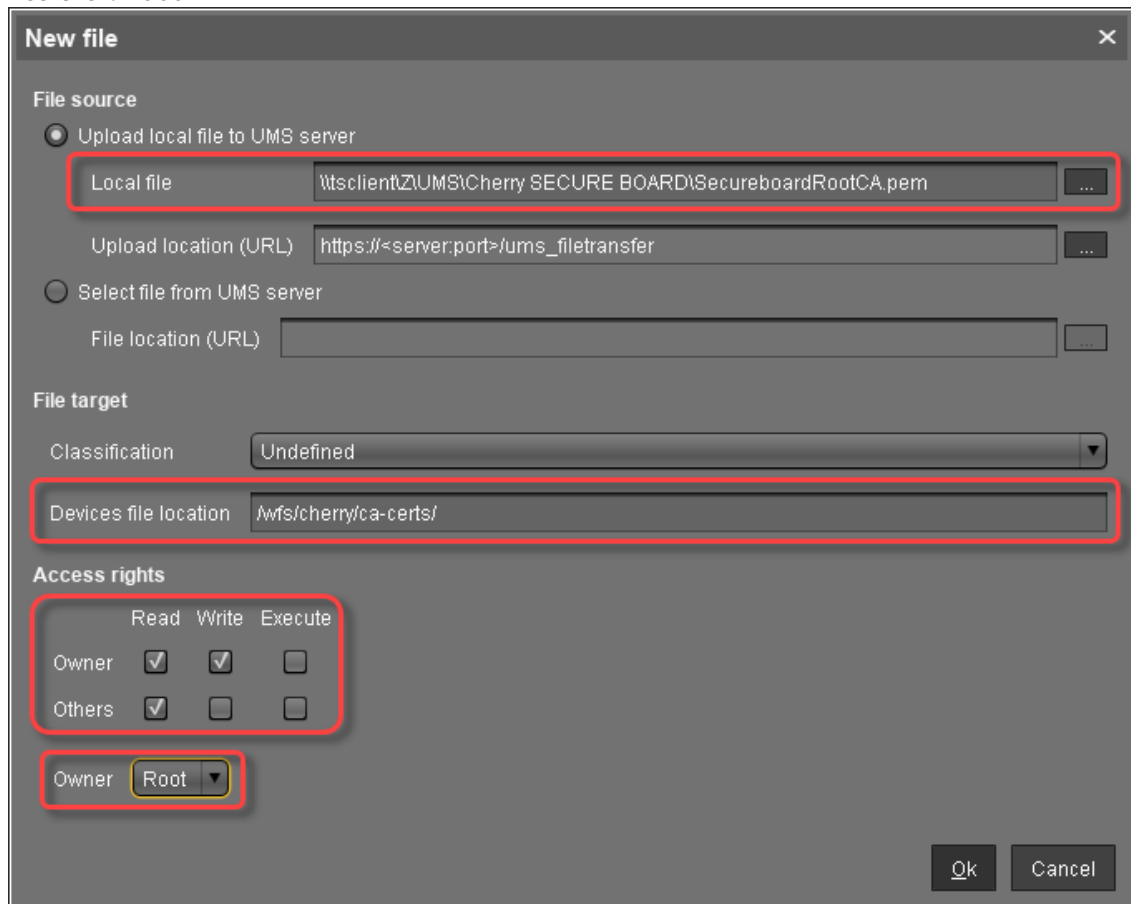
### Erstellen des Dateiobjekts für das Geräte-Root-CA-Zertifikat

- Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



- Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:
  - **Lokale Datei:** Lokaler Dateipfad von SecureboardRootCA.pem. Verwenden Sie die Dateiauswahl durch Klicken auf **...**.
  - **Speicherort der Gerätedatei:** /wfs/cherry/ca-certs/
  - **Zugriffsrechte - Besitzer:** Lesen, Schreiben
  - **Zugangsrechte - Andere:** Lesen

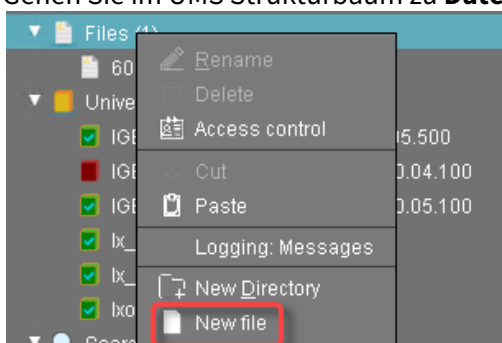
- **Besitzer:** Root



- Klicken Sie **Ok**.  
In der UMS wird die Datei **SecureBoardRootCA.pem** erzeugt.

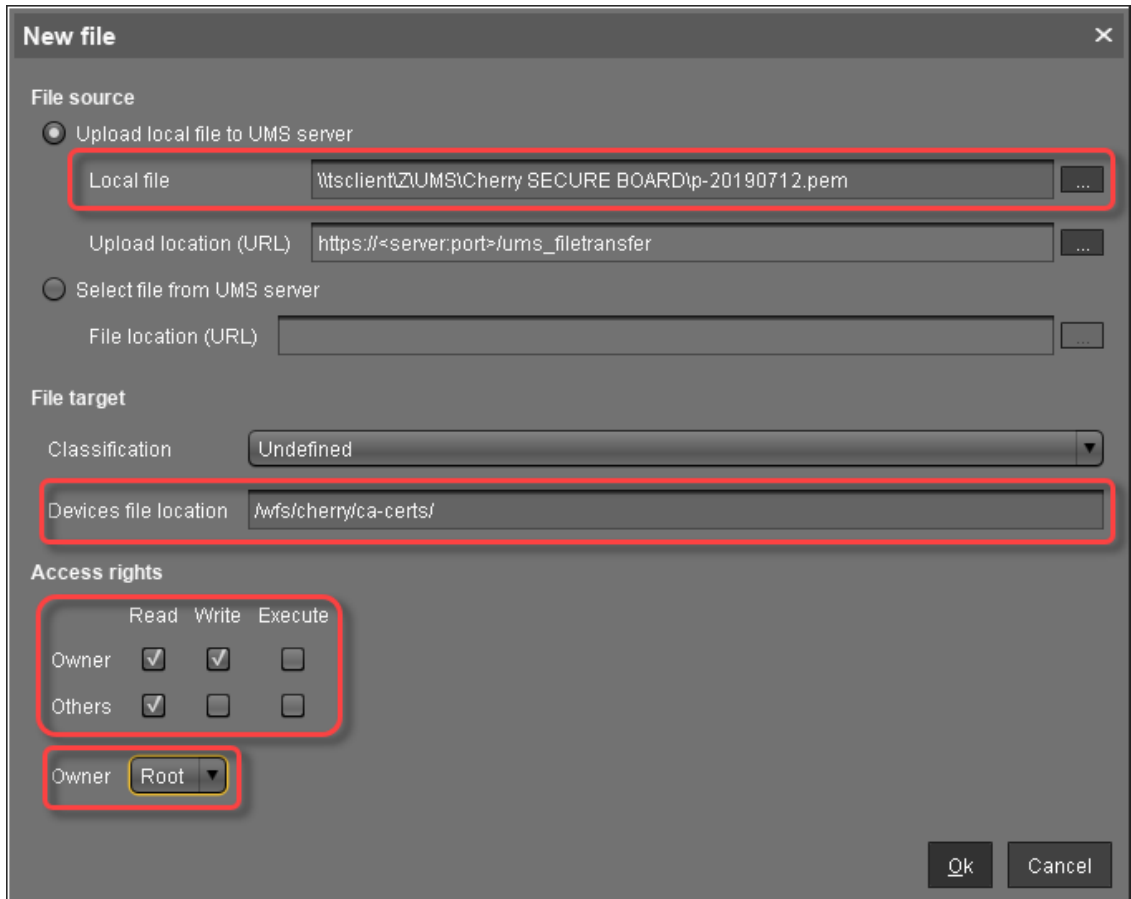
Erstellen des Dateiobjekts für das Geräte-Zwischen-CA-Zertifikat

1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:
  - **Lokale Datei:** Lokaler Dateipfad von `SecureboardRootCA.pem`. Verwenden Sie die Dateiauswahl durch Klicken auf `...`.

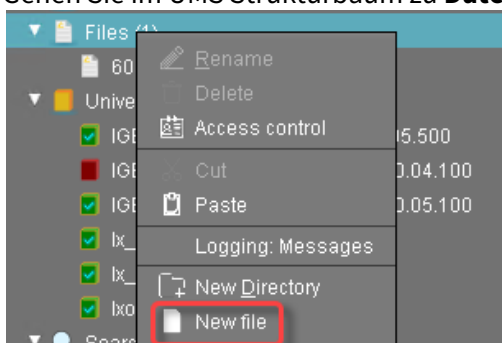
- **Speicherort der Gerätedatei:** /wfs/cherry/ca-certs/
- **Zugriffsrechte - Besitzer:** Lesen, Schreiben
- **Zugangsrechte - Andere:** Lesen
- **Besitzer:** Root



3. Klicken Sie **Ok**.  
In der UMS wird die Datei **p-20190712.pem** erzeugt.

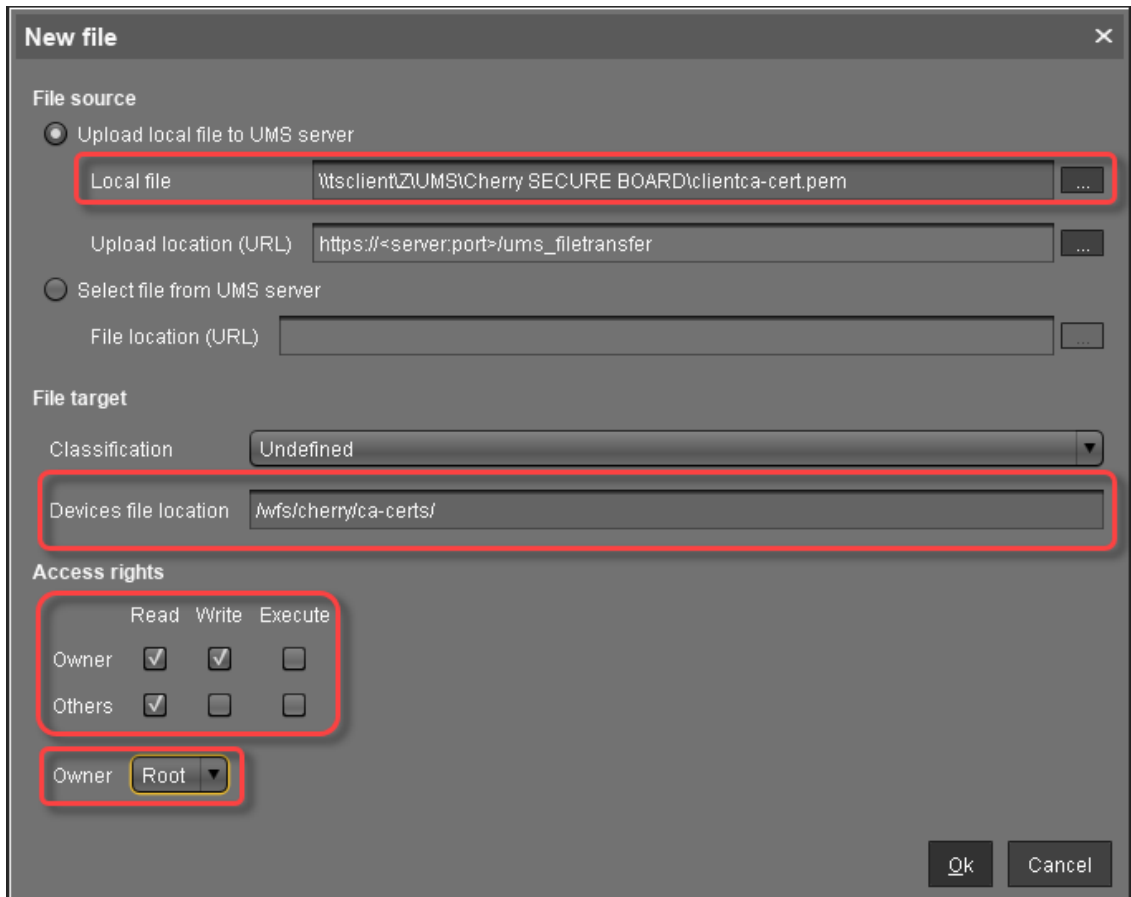
Erstellen des Dateiobjekts für das Geräte-Client-CA-Zertifikat (optional)

1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:

- **Lokale Datei:** Lokaler Dateipfad von `SecureboardRootCA.pem`. Verwenden Sie die Dateiauswahl durch Klicken auf `...`.
- **Speicherort der Gerätedatei:** `/wfs/cherry/ca-certs/`
- **Zugriffsrechte - Besitzer:** Lesen, Schreiben
- **Zugangsrechte - Andere:** Lesen
- **Besitzer:** Root



3. Klicken Sie **Ok**.

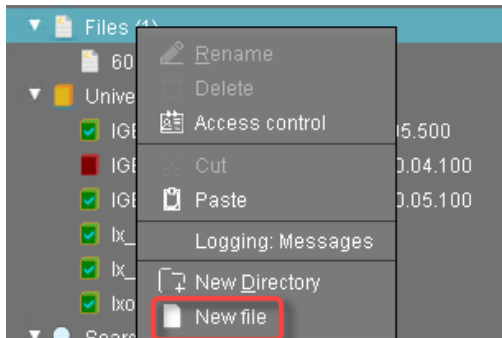
In der UMS wird das Dateiojekt **clientca-cert.pem** erzeugt.

Erstellen des Dateiobjekts für das Benutzerzertifikat (Tastatur)

Um die Zertifikatsdatei `user-cert.der` in das Verzeichnis `/wfs/cherry/client-certs/` auf der Personalisierungsmaschine zu übertragen, gehen Sie wie folgt vor:

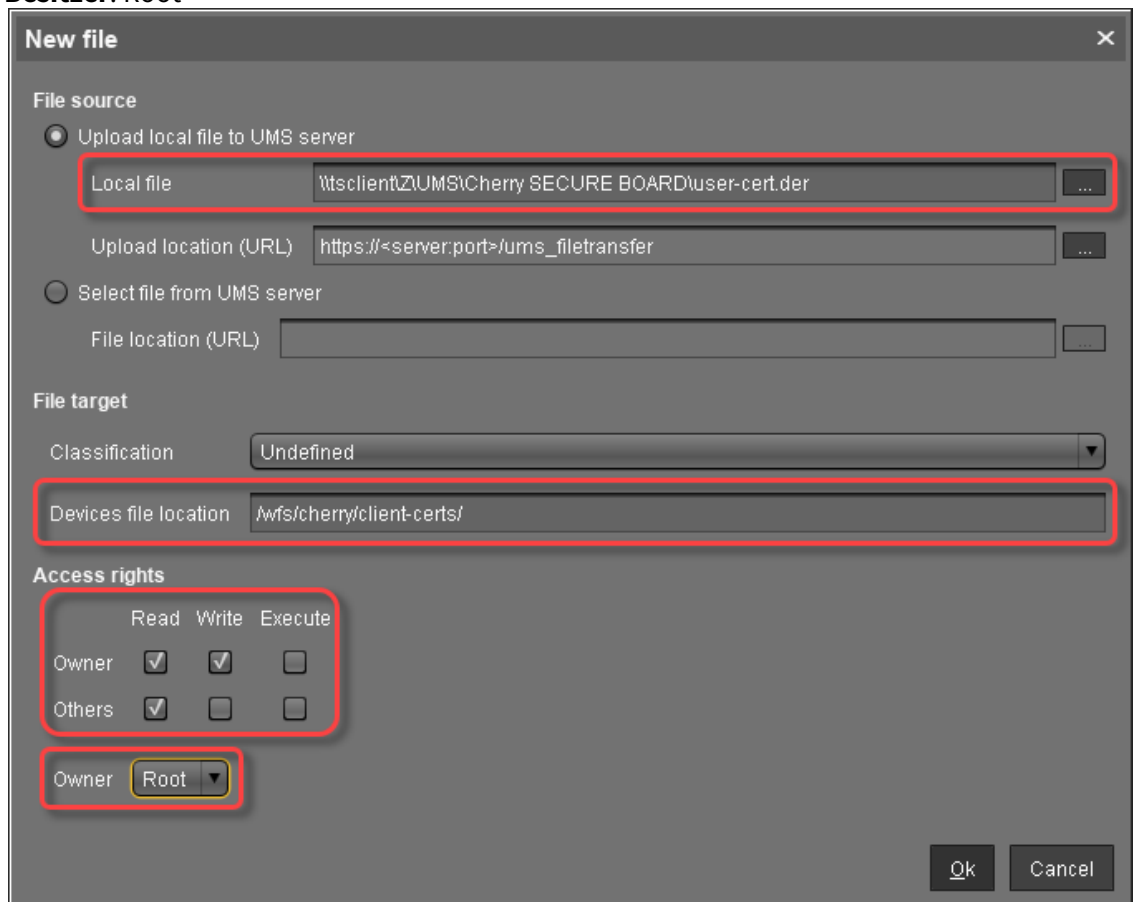


1. Gehen Sie im UMS-Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:

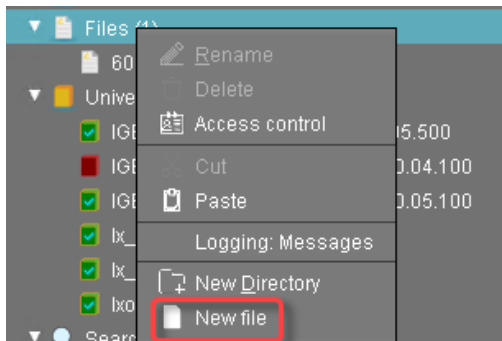
- **Lokale Datei:** Lokaler Dateipfad von `SecureboardRootCA.pem`. Verwenden Sie die Dateiauswahl durch Klicken auf `...`.
- **Speicherort der Gerätedatei:** `/wfs/cherry/ca-certs/`
- **Zugriffsrechte - Besitzer:** Lesen, Schreiben
- **Zugangsrechte - Andere:** Lesen
- **Besitzer:** Root



3. Klicken Sie **Ok**.  
In der UMS wird die Datei **user-cert.der** erzeugt.

Erstellen des Dateiobjekts für die Benutzertaste (Tastatur)

1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:
  - **Lokale Datei:** Lokaler Dateipfad von `SecureboardRootCA.pem`. Verwenden Sie die Dateiauswahl durch Klicken auf `...`.
  - **Speicherort der Gerätedatei:** `/wfs/cherry/ca-certs/`
  - **Zugriffsrechte - Besitzer:** Lesen, Schreiben
  - **Zugangsrechte - Andere:** Lesen

- **Besitzer:** Root

**New file**

File source

Upload local file to UMS server

Local file: \\tsclient\ZUMS\Cherry SECURE BOARD\user-key.pem

Upload location (URL): https://<server:port>/ums\_filetransfer

Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/cherry/client-certs/

Access rights

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Owner: Root

Ok Cancel

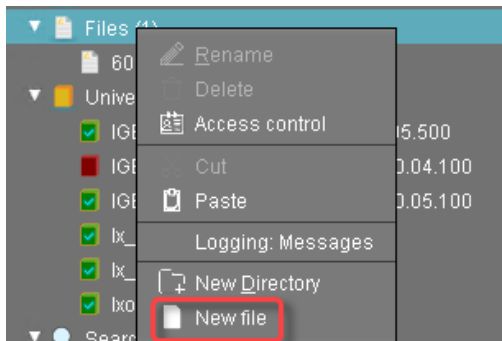
3. Klicken Sie **Ok**.  
In der UMS wird die Datei **user-key.pem** erzeugt.

## Bereitstellen der Endgeräte für die Verwendung des SECURE BOARD

Die folgenden Anweisungen beschreiben, wie die erforderlichen Zertifikate an die Endgeräte übertragen werden, die im sicheren Modus mit dem SECURE BOARD verbunden werden.

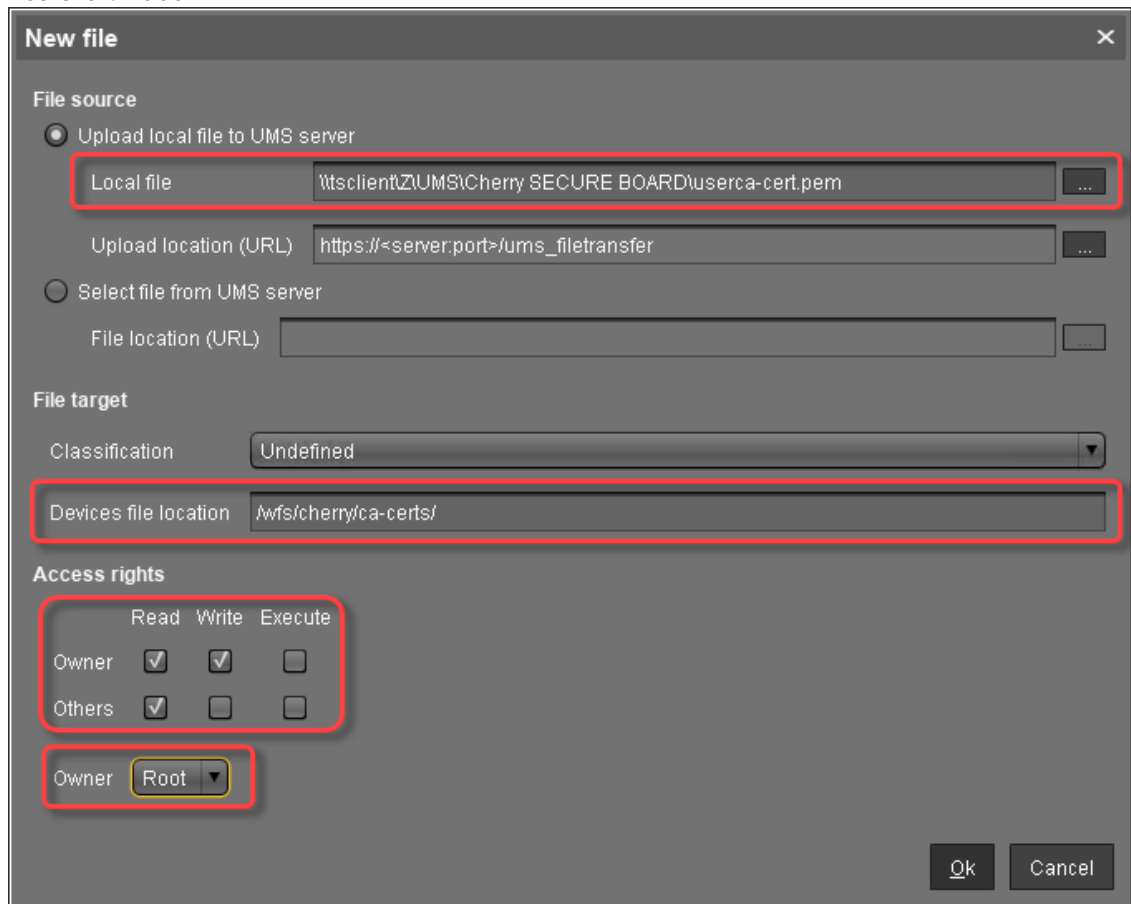
Erstellen des Dateiobjekts für das Benutzer-Root-CA-Zertifikat

1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:
  - **Lokale Datei:** Lokaler Dateipfad von `SecureboardRootCA.pem`. Verwenden Sie die Dateiauswahl durch Klicken auf `...`.
  - **Speicherort der Gerätedatei:** `/wfs/cherry/ca-certs/`
  - **Zugriffsrechte - Besitzer:** Lesen, Schreiben
  - **Zugangsrechte - Andere:** Lesen

- **Besitzer:** Root

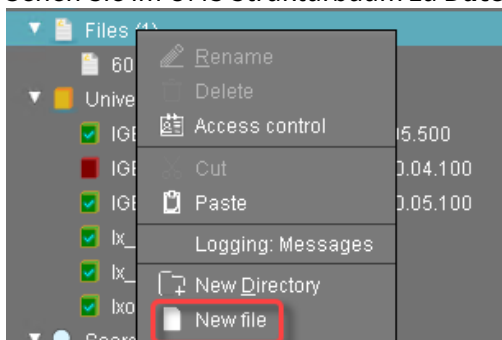


3. Klicken Sie **Ok**.

In der UMS wird das Dateiojekt erzeugt. Der Name des Dateiojekts wird vom Dateinamen abgeleitet.

Erstellen des Dateiojekts für das Client-Root-CA-Zertifikat (optional)

1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Konfigurieren Sie im Dialogfeld **Neue Datei** die Einstellungen wie folgt:

- **Lokale Datei:** Lokaler Dateipfad von `SecureboardRootCA.pem`. Verwenden Sie die Dateiauswahl durch Klicken auf `...`.

- **Speicherort der Gerätedatei:** /wfs/cherry/ca-certs/
- **Zugriffsrechte - Besitzer:** Lesen, Schreiben
- **Zugangsrechte - Andere:** Lesen
- **Besitzer:** Root

**New file** [X]

**File source**

Upload local file to UMS server

Local file: \\tsclient\ZUMS\Cherry SECURE BOARD\clientca-cert.pem

Upload location (URL): https://<server:port>/ums\_filetransfer

Select file from UMS server

File location (URL):

**File target**

Classification: Undefined

Devices file location: /wfs/cherry/ca-certs/

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

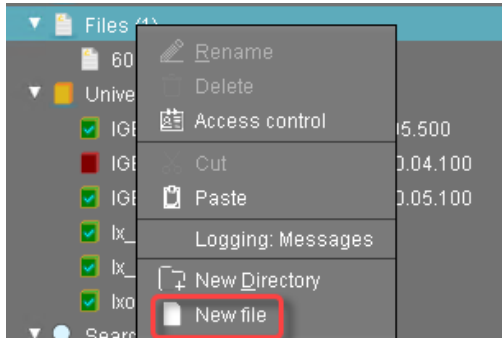
Owner: Root

Ok Cancel

3. Klicken Sie **Ok**.  
In der UMS wird das Dateiojekt erzeugt. Der Name des Dateiojekts wird vom Dateinamen abgeleitet.

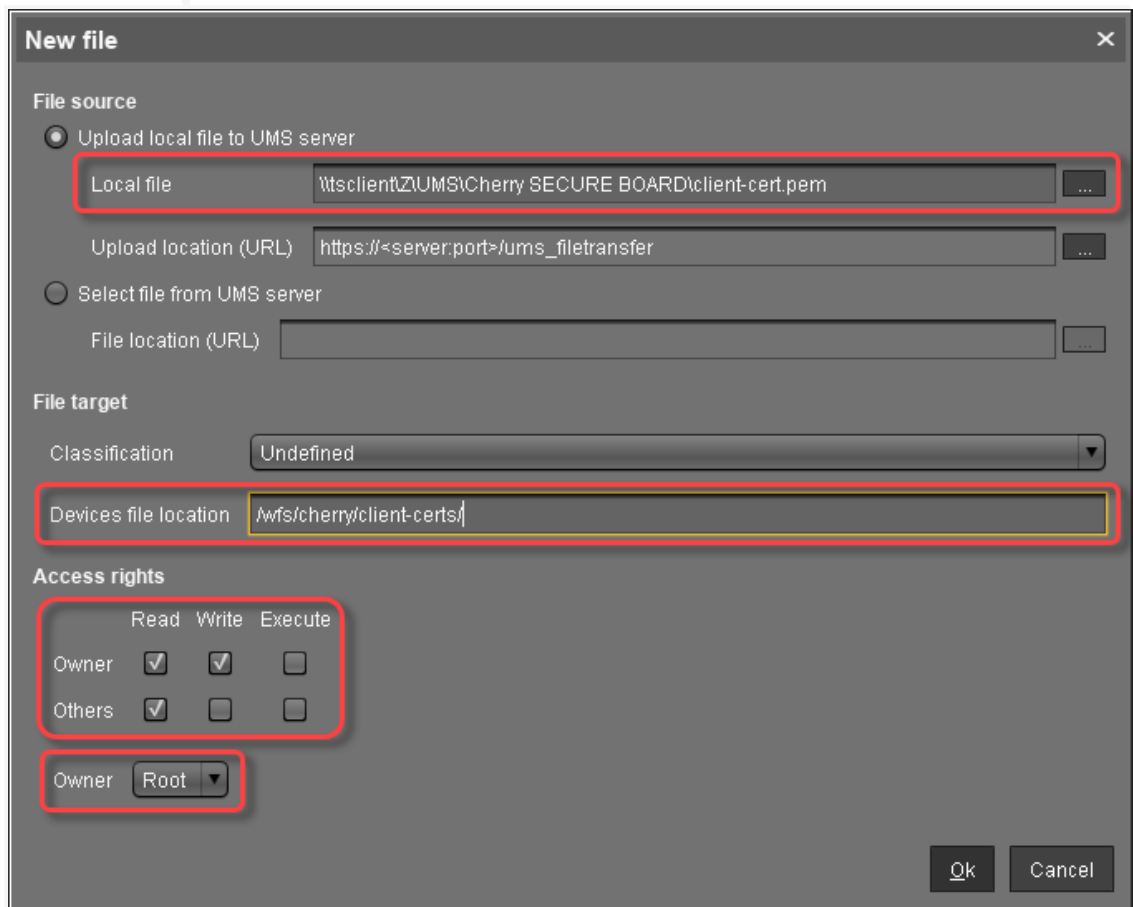
Dateiobjekt für das Client-Zertifikat erzeugen (optional)

1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Bearbeiten Sie die Einstellungen im Dialog **Neue Datei** wie folgt:
  - **Lokale Datei:** Lokaler Dateipfad von `client-cert.pem`. Verwenden Sie die Dateiauswahl, indem Sie `...` klicken.
  - **Speicherort der Gerätedatei:** `/wfs/cherry/client-certs/`
  - **Zugriffsrechte - Besitzer:** Lesen, schreiben
  - **Zugangsrechte - Andere:** Lesen

- **Besitzer:** Root

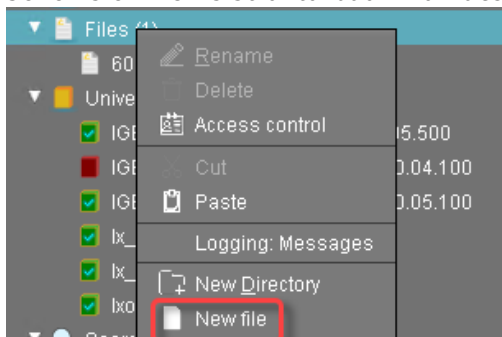


3. Klicken Sie **Ok**.

In der UMS wird eine Datei erzeugt. Der Name des Dateiobjekts wird aus dem Dateinamen abgeleitet.

Erstellen des Dateiobjekts für den Client-Schlüssel (Endgerät) (optional)

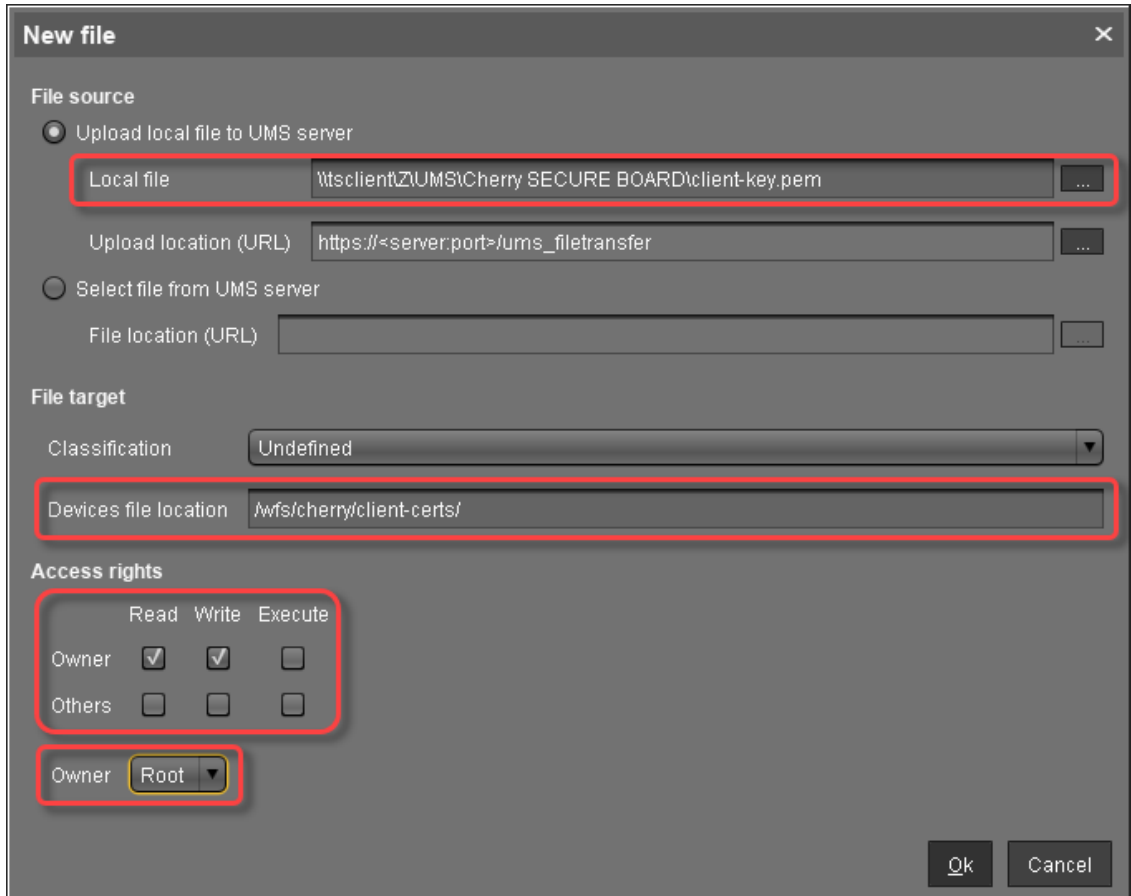
1. Gehen Sie im UMS Strukturbaum zu **Dateien** und wählen Sie im Kontextmenü **Neue Datei**.



2. Bearbeiten Sie die Einstellungen im Dialog **Neue Datei** wie folgt:



- **Lokale Datei:** Lokaler Dateipfad von `client-cert.pem`. Verwenden Sie die Dateiauswahl, indem Sie `...` klicken.
- **Speicherort der Gerätedatei:** `/wfs/cherry/client-certs/`
- **Zugriffsrechte - Besitzer:** Lesen, schreiben
- **Zugangsrechte - Andere:** Lesen
- **Besitzer:** Root



**New file** [X]

**File source**

Upload local file to UMS server

Local file: `\\tsclient\ZUMS\Cherry SECURE BOARD\client-key.pem` [...]

Upload location (URL): `https://<server:port>/ums_filetransfer` [...]

Select file from UMS server

File location (URL): [...]

**File target**

Classification: `Undefined` [v]

Devices file location: `/wfs/cherry/client-certs/`

**Access rights**

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


Owner: `Root` [v]

[Ok] [Cancel]

### 3. Klicken Sie **Ok**.


In der UMS wird eine Datei erzeugt. Der Name des Dateiobjekts wird aus dem Dateinamen abgeleitet.

## Die Personalisierungsmaschine einrichten

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.



### Setting Up the Local Terminal

If a local terminal session has already been configured on the designated personalization machine, you can skip this step.

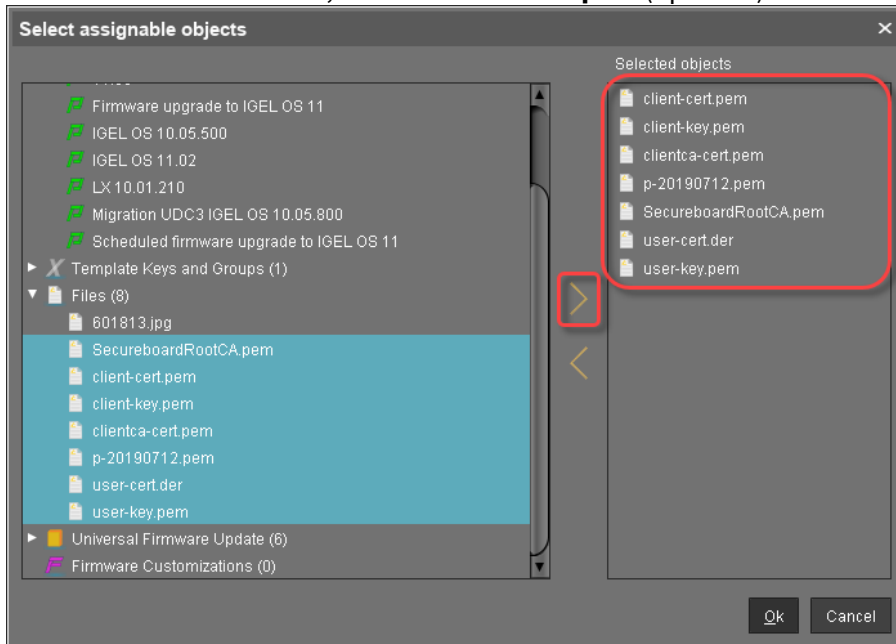
1. Open the device's Setup and go to **Accessories >Terminals**.
2. Select .
3. Click **Ok**.

On the desktop and in the Application Starter, a starter for the terminal session is created.

### Assigning the File Objects to the Personalization Machine

1. In the UMS structure tree, select the endpoint that will act as the personalization machine.
2. In the **Assigned objects** area, click .
3. Under **Files**, select the file objects using the  button:
  - **SecureboardRootCA.pem**
  - Device intermediate CA certificates; here: **p-20190712.pem**
  - **user-cert.der**
  - **user-key.pem**
  - **client-cert.pem** (optional)
  - **client-key.pem** (optional)

- Device client CA certificate; here: **clientca-cert.pem** (optional)



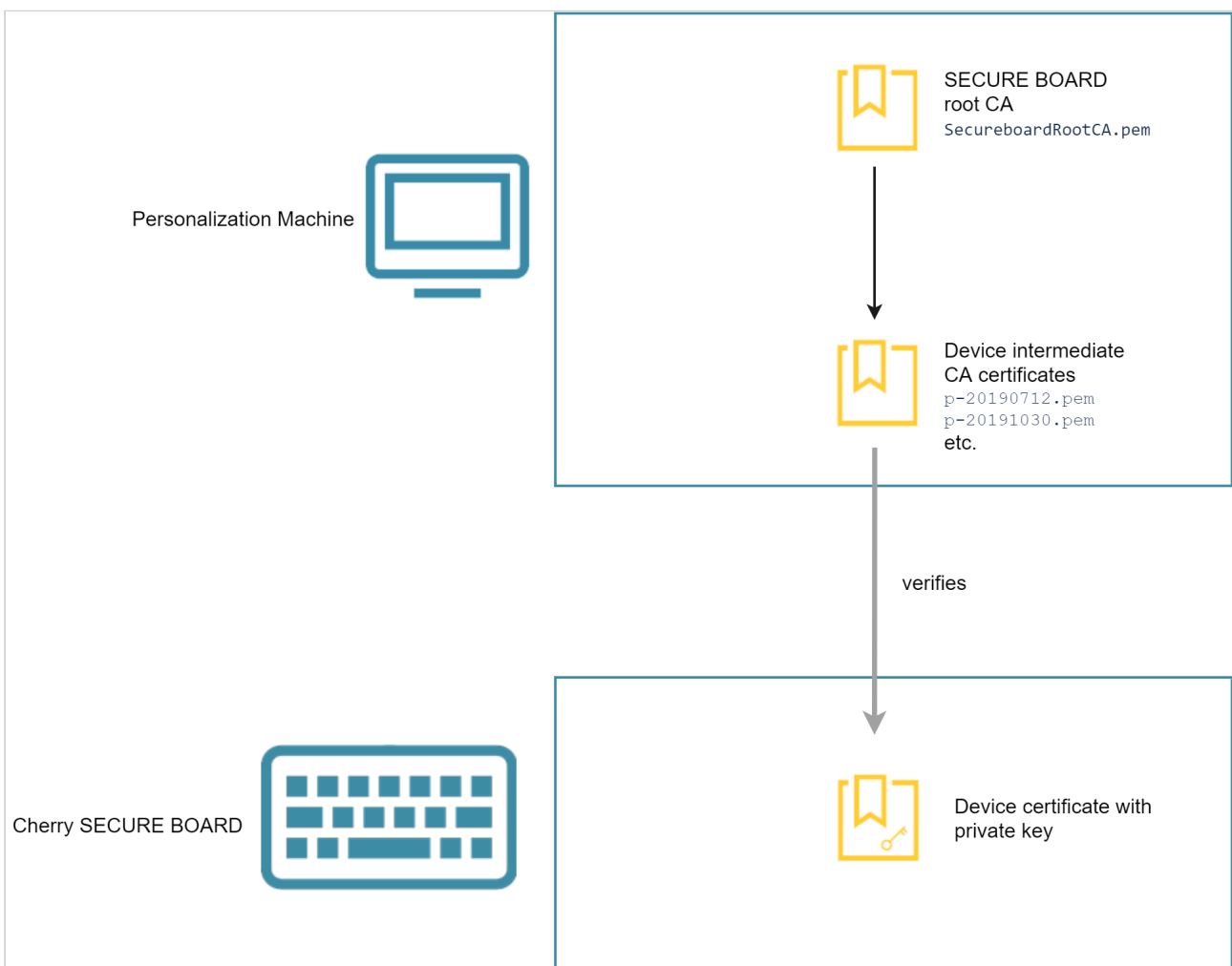
4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.  
The certificate and key files are transferred to the personalization machine. The personalization machine is ready for operation.

## Personalizing the Cherry SECURE BOARD

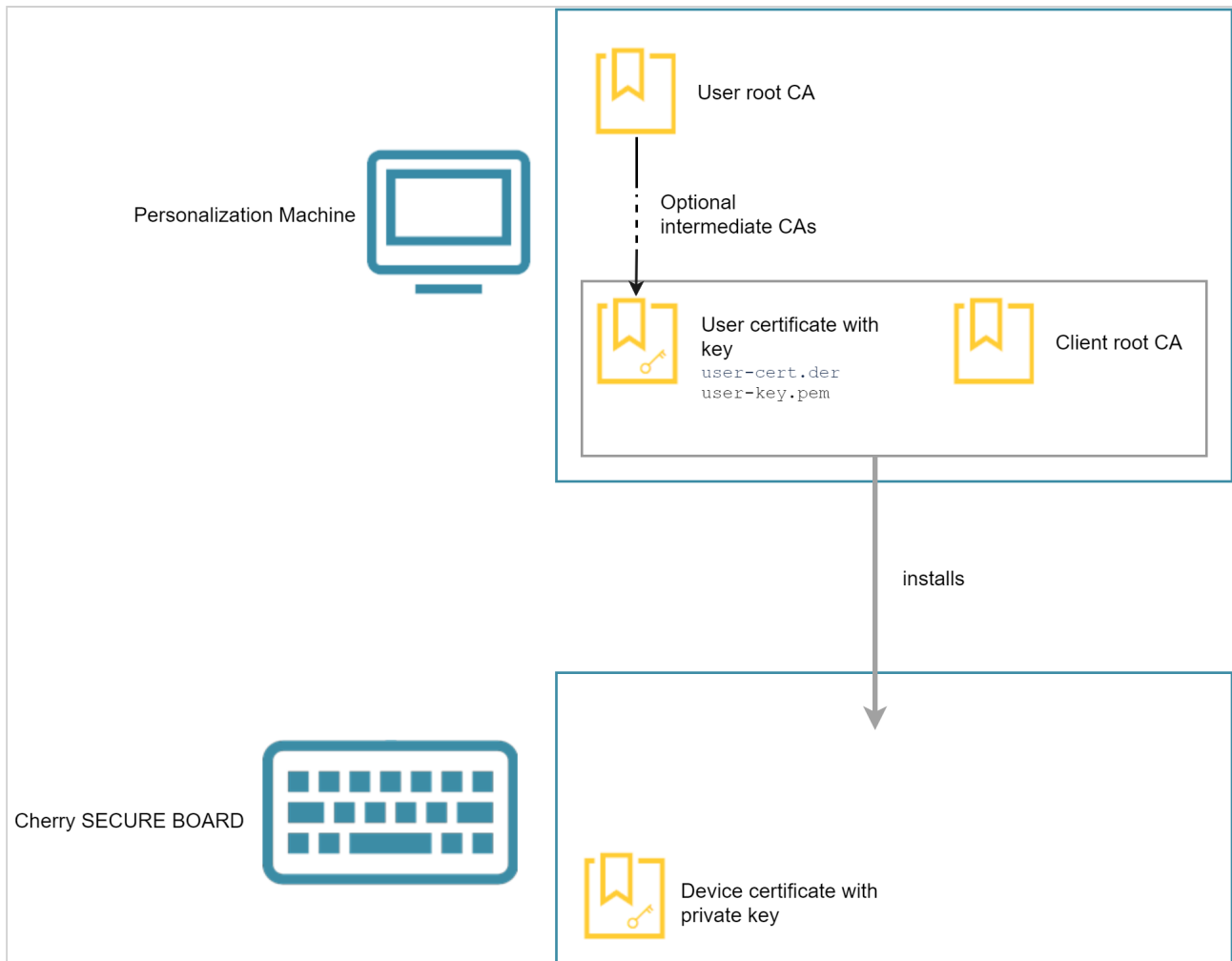
**i** Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

### Overview

#### Personalization Machine Verifies if the Keyboard Is a Genuine Cherry SECURE BOARD



#### Personalization Machine Installs the Certificates on the Keyboard



## Prerequisites

- The machine has been prepared as described under [Die Personalisierungsmaschine einrichten](#) (see [page 714](#)).
- The Cherry SECURE BOARD keyboards are in factory state or have been reset (see [Resetting the Cherry SECURE BOARD to Its Original State](#) (see [page 725](#))).

## Instructions

1. Start the local terminal and log in as `root`.

```
Local Terminal
login as "user" or "root": root
```

2. Enter the command `secureboard_personalize`

```
Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# secureboard_personalize
```

If all required certificates and the optional certificates for mutual authentication are present, the personalization facility is ready.

```
Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem client-key.pem user-cert.der user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0 570b05fc.0 d81e5d09.0 ece45aca.0 SecureboardRootCA.pem
46c284d6.0 clientca-cert.pem dce0a93b.0 p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.
```

In case only the required certificates are present, the personalization facility is ready, but a message stating the absence of the optional certificates for mutual authentication is shown:

```
Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# secureboard_personalize
Optional Client Root certificate /wfs/cherry/ca-certs/clientca-cert.pem is missing.
Certificate check succeeded.
Personalization without (optional) Client Root certificate!

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CCOGLI2.

Personalize SECURE BOARD 1.0 (y/n)?
```

### 3. Plug in a Cherry SECURE BOARD.

A message confirms that the keyboard has been detected; you are prompted to start the personalization.

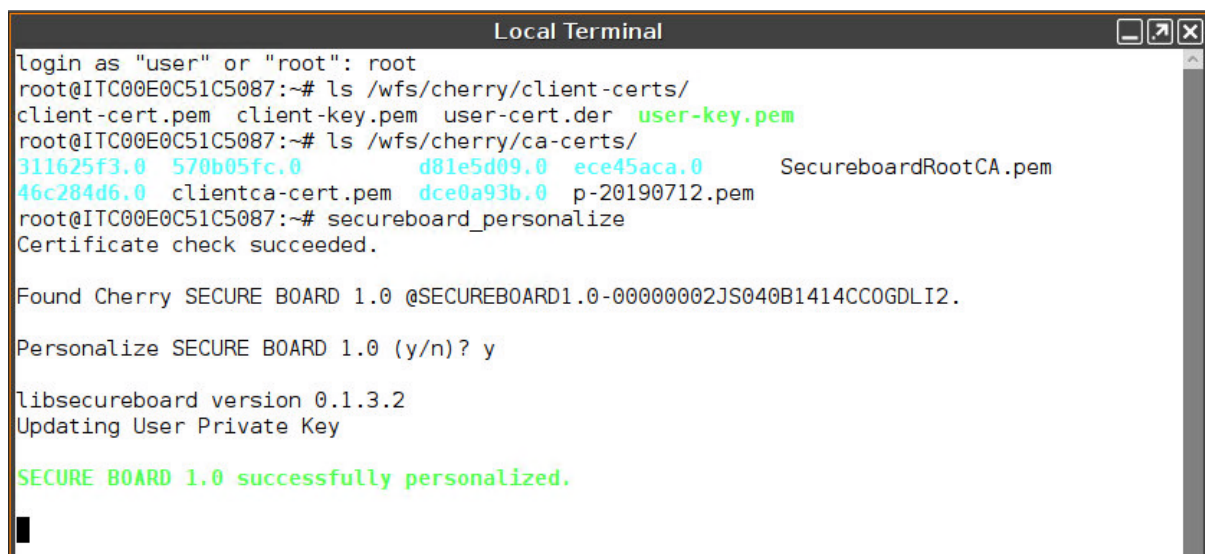


```
Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem client-key.pem user-cert.der user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0 570b05fc.0 d81e5d09.0 ece45aca.0 SecureboardRootCA.pem
46c284d6.0 clientca-cert.pem dce0a93b.0 p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CCOGLI2.
Personalize SECURE BOARD 1.0 (y/n)? █
```

### 4. Enter `y` to start the personalization process.

During the personalization process, a few messages are shown. If everything has gone well, a message about the successful personalization appears.



```
Local Terminal
login as "user" or "root": root
root@ITC00E0C51C5087:~# ls /wfs/cherry/client-certs/
client-cert.pem client-key.pem user-cert.der user-key.pem
root@ITC00E0C51C5087:~# ls /wfs/cherry/ca-certs/
311625f3.0 570b05fc.0 d81e5d09.0 ece45aca.0 SecureboardRootCA.pem
46c284d6.0 clientca-cert.pem dce0a93b.0 p-20190712.pem
root@ITC00E0C51C5087:~# secureboard_personalize
Certificate check succeeded.

Found Cherry SECURE BOARD 1.0 @SECUREBOARD1.0-00000002JS040B1414CCOGLI2.

Personalize SECURE BOARD 1.0 (y/n)? y

libsecureboard version 0.1.3.2
Updating User Private Key

SECURE BOARD 1.0 successfully personalized.
█
```

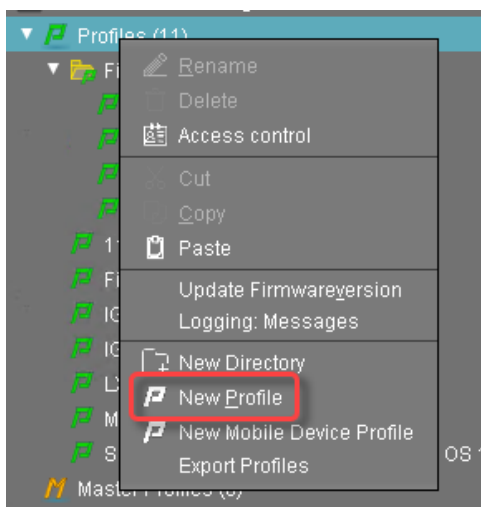
### 5. Unplug the personalized Cherry SECURE BOARD and proceed with the next Cherry SECURE BOARD.

## Setting Up the Endpoints

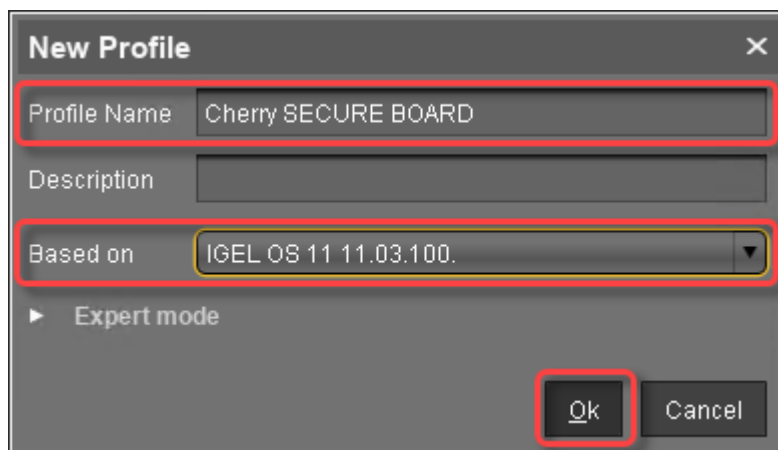
**i** Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

### Creating a Profile for the Endpoints

1. In the UMS structure tree, open the context menu for **Profiles** and select **New Profile**.

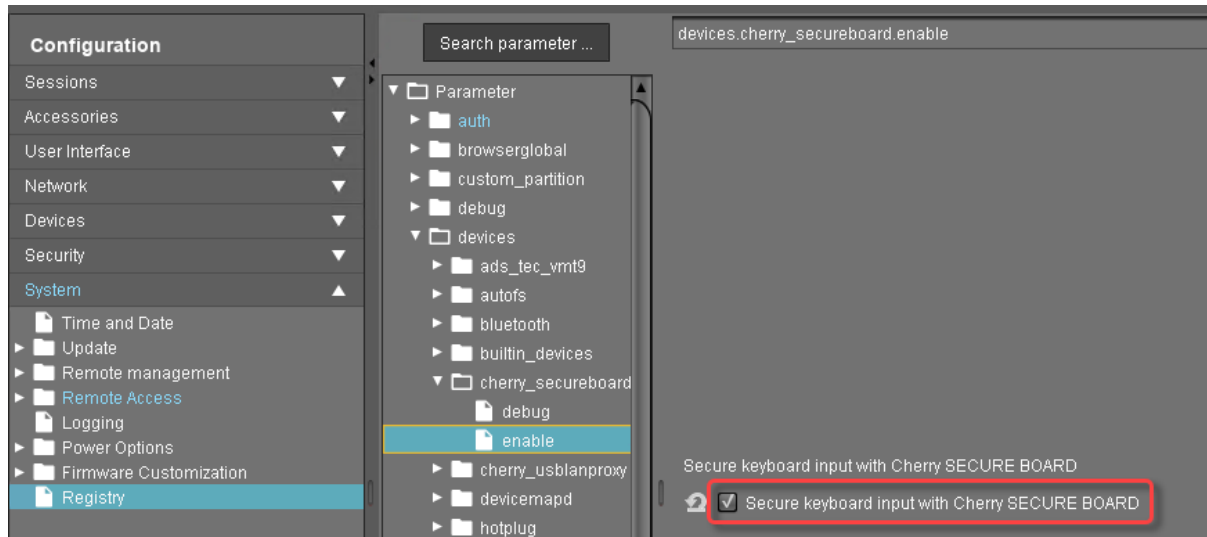




2. In the **New Profile** dialog, enter the required data and click **Ok**:
  - **Profile Name**: Name for the profile
  - **Based on**: Select the version of IGEL OS that is installed on your devices (IGEL OS 11.03.100 or higher).

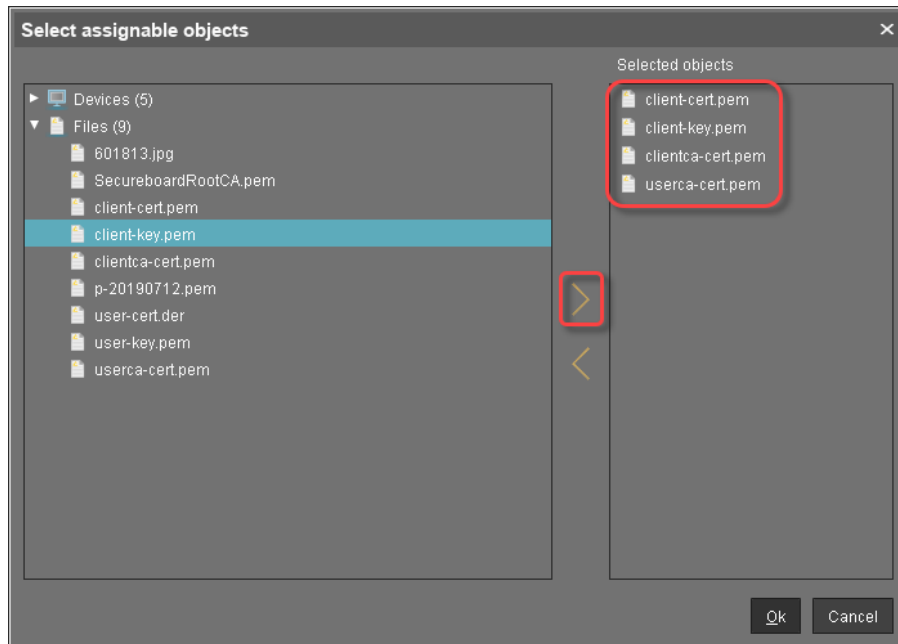




- In the configuration dialog of the profile, go to **System > Registry > devices > cherry\_secureboard > enable** and activate **Secure keyboard input with Cherry SECURE BOARD** (registry key: `devices.cherry_secureboard.enable`). (From UMS 6.03.130 or higher, the parameter can be found under **User Interface > Input > Keyboard**)





- Click **Ok** to save and close the profile.
- Make sure that the profile is selected in the UMS structure tree.
- In the **Assigned objects** area, click .
- Under **Files**, select the file objects using the  button:
  - User root CA certificate; here: **userca-cert.pem**
  - Client root CA certificate; here: **clientca-cert.pem** (optional)
  - Client certificate; here: **client-cert.pem**
  - Client key; here: **client-key.pem**



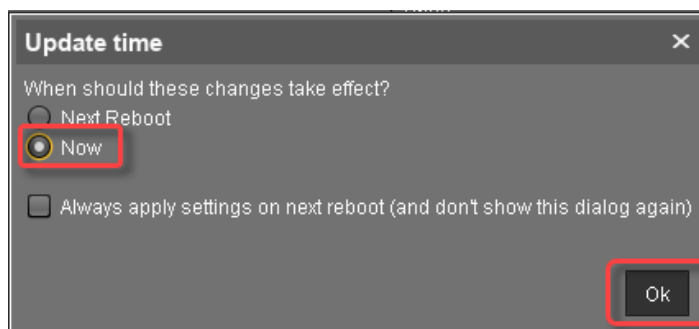
8. Click **Ok**.
9. In the **Update time** dialog, select **Now** and click **Ok**.  
The certificate and key files are assigned to the profile.

### Assigning the Profile to the Endpoints

1. In the UMS structure tree, select the devices that are to be connected to the Cherry SECURE Board keyboards.
2. In the **Assigned objects** area, click .
3. Under **Profiles**, select the appropriate profile using the  button.



4. Click **Ok**.
5. In the **Update time** dialog, select **Now** and click **Ok**.

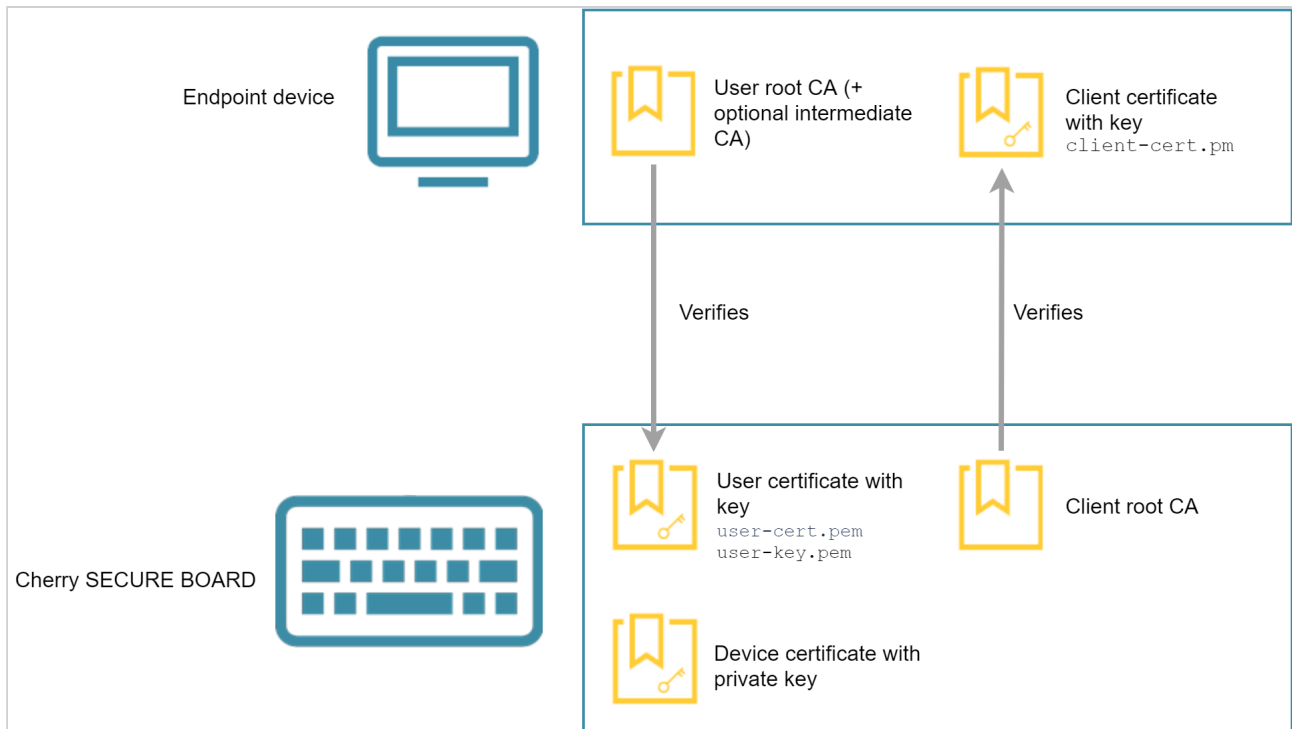


The settings and certificate and key files are transferred to the endpoints. The endpoints are ready for connecting to the Cherry SECURE BOARD keyboards.


## Operation

The endpoint verifies if the Cherry SECURE BOARD has the right certificates. When the optional client certificates have been installed, too, the Cherry SECURE BOARD verifies if the endpoint has the right certificates. When everything went well, the endpoint and the Cherry SECURE BOARD work in secure mode.

On the keyboard side, the secure mode is indicated by the red light next to the lock symbol. On the endpoint side, the secure mode is indicated by an icon on the system tray.



## Resetting the Cherry SECURE BOARD to Its Original State

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

To reset the Cherry SECURE BOARD to its factory settings:

1. Disconnect the keyboard from the endpoint.
2. Hold the keys [D], [J] and [RGUI] (right Windows key) and, at the same time, connect the keyboard to the endpoint.

When the reset has been successful, all LEDs flash for about 1 second. After that, the keyboard starts normally, and the certificate store is emptied. The keyboard can be personalized again.

## Webcam-Umleitung und Optimierung in IGEL OS


Dieser Artikel bietet einen Überblick und Best-Practice-Empfehlungen für den Gebrauch von Webcams in IGEL OS innerhalb von Remotesitzungen wie Citrix, VMware Horizon und RDP.

### Überblick

Generell lässt sich die Webcam-Unterstützung in IGEL OS in drei Kategorien einteilen:

Nicht optimiert	<p>Die Rohdaten von der Webcam werden per USB-Umleitung über das Netzwerk gesendet. Die Rohdaten von der Webcam sind stark von der Netzwerklatenz zwischen dem Client und Server betroffen und beanspruchen viel Bandbreite, erfordern auf der Serverseite die richtigen Treiber und erhöhen die CPU- und RAM-Auslastung des Servers.</p> <p>Beispiel: <b>Native USB Redirection</b> für RDP-Sitzungen</p>
Optimierungstyp 1	<p>In diesem Fall werden die Video- und Audiodaten auf der Seite des Clients komprimiert. Dieser Optimierungstyp macht den Datenstrom der Webcam wesentlich effizienter und zuverlässiger, obwohl der Datenstrom zusätzlich zu den Cloud-Servern der jeweiligen Kommunikationssoftware (Teams, Zoom, usw.) noch über den VDI-Server laufen muss.</p> <p>Beispiele: <b>HDX RealTime Webcam Redirection</b> für Citrix Sitzungen, <b>Real Time Audio Video (RTAV)</b> für VMware Horizon Sitzungen</p>

Optimierungstyp 2	<p>In diesem Fall werden die Video- und Audiodaten auch auf der Seite des Clients komprimiert. Jedoch wird bei diesem Optimierungstyp im Gegensatz zu Typ 1 der Datenstrom vom VDI-Server ausgelagert und direkt an Teams/Zoom/usw. in der Cloud, d.h. "single-hop", gesendet. Dies ermöglicht die beste Leistung und entlastet auch den Server, setzt aber voraus, dass das richtige Optimierungspack auf dem Client vorhanden ist, und ist spezifisch für jede Kommunikationssuite. Dies kann auch eine komplexere Netzwerkkonfiguration erfordern, da das Endgerät in der Lage sein muss, direkt mit dem Kommunikations-Cloud-Server und nicht nur mit dem VDI-Server zu kommunizieren.</p> <p>Beispiele: <b>Microsoft Teams Optimierung</b> und <b>Zoom Media Plugin</b> für Citrix Sitzungen</p>
-------------------	---

 Im Falle von Optimierungstyp 1 oder 2 ist es wichtig, sicherzustellen, dass der Agent/die Komponente auf der Serverseite installiert und mit der clientseitigen Version kompatibel ist. Einzelheiten zu letzterer finden Sie im Abschnitt "Component Versions" der IGEL OS Release Notes.

## Allgemeine Empfehlungen

Für eine optimale Leistung von Webcams in IGEL OS muss das richtige Optimierungspack für die jeweilige Anwendung aktiviert sein, z.B. **Microsoft Teams Optimierung**, **Zoom VDI Media Plugin**, **Cisco Webex VDI** usw. Optimierungspacks sind jedoch nicht für alle Sitzungstypen verfügbar.

### **USB Redirection**

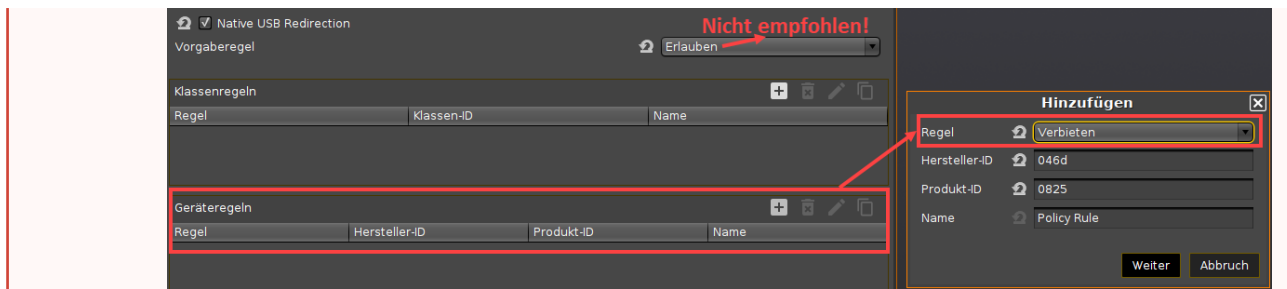
Wenn für Ihren Sitzungstyp kein Optimierungspack vorhanden ist oder das vorhandene Optimierungspack nicht richtig funktioniert, können Sie versuchen, die USB-Umleitung zu verwenden - entweder die **Native USB Redirection** oder die weniger häufig verwendete **Fabulatech USB Redirection** (nicht beide zusammen), - aber NUR als LETZTER AUSWEG, wenn keine andere Lösung möglich ist.

Im Allgemeinen, wenn die USB-Umleitung als Option innerhalb der VDI-Sitzungsoptionen verfügbar ist, sollte sie für die Webcam-Geräte deaktiviert werden.

- Setzen Sie **Vorgaberegeln** auf "Verbieten"
- ODER, wenn die **Vorgaberegeln** "Erlauben" ist (NICHT empfohlen), gehen Sie auf **Geräteregeln** und fügen Sie "Verbieten"-Regeln für die spezifische Hersteller-ID und Produkt-ID der Webcam hinzu.

#### **Hersteller- und Produkt-IDs herausfinden**

Um Hersteller-/Produkt-IDs zu ermitteln, verwenden Sie im Terminal den Befehl `lsusb`. Sie können auch das Tool **Systeminformationen** verwenden, siehe Using "System Information" Function.



Dies ist notwendig, weil die USB-Umleitung die korrekte Optimierung der Webcam behindert (falls die Optimierung möglich ist).

**⚠** Vergessen Sie nicht, die Einstellungen und Richtlinien auf der Serverseite zu überprüfen und anzupassen. Andernfalls funktioniert Ihre Webcam möglicherweise nicht, selbst wenn alle Einstellungen in IGEL OS korrekt konfiguriert wurden.

**✓** Schauen Sie immer in den IGEL OS Release Notes nach spezifischen Anmerkungen, insbesondere bei Private Builds. Versuchen Sie immer, die neueste Firmware zu verwenden, siehe [IGEL Downloadserver](https://www.igel.com/software-downloads/workspace-edition/)<sup>55</sup>.

**i** In bestimmten Fällen können einige der weiter unten in diesem Artikel beschriebenen Einstellungen nicht sichtbar sein, obwohl Sie die richtige Firmwareversion für das Profil in der UMS ausgewählt haben. Aktualisieren Sie in diesem Fall die UMS auf die neueste Version.

<sup>55</sup> <https://www.igel.com/software-downloads/workspace-edition/>



## Citrix

## Option 1: Unified Communications (Beste Wahl)

<p><b>Microsoft Teams Optimierung</b></p>	<p>Pfad: <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI-Lösungen &gt; Microsoft Teams Optimierung</b> (standardmäßig aktiviert)</p> <ul style="list-style-type: none"> <li>• Verfügbar ab IGEL OS-Version 11.04.100</li> <li>• Hängt von der verwendeten Version der Citrix Workspace App ab. Für die besten Ergebnisse sollte die neueste Version bevorzugt werden. Die enthaltenen Versionen der Citrix Workspace App finden Sie in den IGEL OS Release Notes.</li> </ul> <p>Die serverseitigen Anforderungen für die Microsoft Teams Optimierung finden Sie unter <a href="#">Microsoft Teams installation</a><sup>56</sup>.</p> <p>Informationen zur Fehlerbehebung bei der Microsoft Teams Optimierung in Citrix finden Sie unter:</p> <ul style="list-style-type: none"> <li>• <a href="#">Troubleshooting HDX Optimization for Microsoft Teams</a><sup>57</sup></li> <li>• <a href="#">Peripherals in Microsoft Teams</a><sup>58</sup></li> </ul>
<p><b>Zoom VDI Media Plugin</b></p>	<p>Pfad: <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; VDI-Lösungen &gt; Zoom VDI Media Plugin</b></p> <ul style="list-style-type: none"> <li>• Verfügbar ab IGEL OS-Version 11.04.100</li> <li>• Die enthaltenen Versionen des Zoom Media Plugins finden Sie in den IGEL OS Release Notes.</li> <li>• Ab IGEL OS 11.06 können Sie die Version des Zoom VDI Media Plugins unter <b>Sitzungen &gt; Unified Communications &gt; Zoom Client-Auswahl</b> ändern.</li> </ul> <p>Weitere Informationen über das Zoom Media Plugin, einschließlich der serverseitigen Anforderungen, finden Sie unter <a href="#">Getting started with VDI</a><sup>59</sup>.</p>

<sup>56</sup> <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#microsoft-teams-installation>

<sup>57</sup> <https://support.citrix.com/article/CTX253754>

<sup>58</sup> <https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/opt-ms-teams.html#peripherals-in-microsoft-teams>

<sup>59</sup> <https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI>

<p><b>Cisco Webex Meetings VDI / Cisco Webex VDI</b></p>	<p>Pfad: <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco &gt; Cisco Webex Meetings VDI</b> oder <b>Cisco Webex VDI</b></p> <ul style="list-style-type: none"> <li>• Verfügbar ab IGEL OS-Version 11.04.100</li> <li>• Die enthaltenen Versionen der Cisco Webex Meetings VDI / Cisco Webex VDI finden Sie in den IGEL OS Release Notes.</li> <li>• Ab IGEL OS 11.06 können Sie die Version des Cisco Webex Meetings VDI Clients unter <b>Sitzungen &gt; Unified Communications &gt; Cisco Webex Meetings VDI-Auswahl</b> ändern.</li> </ul> <p>Weitere Informationen über Cisco Webex Produkte für VDI, einschließlich der unterstützten Umgebungen, finden Sie unter:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Webex Meetings Virtual Desktop Software</a><sup>60</sup></li> <li>• <a href="#">Overview of Webex App for VDI</a><sup>61</sup></li> </ul>
<p><b>Cisco JVDI Client</b></p>	<p>Pfad: <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Cisco &gt; Cisco JVDI Client</b></p> <ul style="list-style-type: none"> <li>• Die enthaltenen Versionen des Cisco JVDI Clients finden Sie in den IGEL OS Release Notes.</li> </ul> <p>Weitere Informationen über Cisco JVDI Client finden Sie unter <a href="#">Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0</a><sup>62</sup>.</p>

<sup>60</sup> <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>

<sup>61</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT\\_chapter\\_00.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT_chapter_00.html)

<sup>62</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jvdi/14\\_0/dig/jvdi\\_b\\_deploy-install-jvdi-14-0/jvdi\\_b\\_deploy-install-jvdi-12-9\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html)

<b>Skype for Business</b>	<p>Pfad: <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; Unified Communications &gt; Skype for Business &gt; HDX RealTime Media Engine</b> (standardmäßig aktiviert)</p> <ul style="list-style-type: none"> <li>• Die Umleitung für Skype for Business basiert auf <b>Citrix HDX Realtime Media Engine</b> (clientseitiges Gegenstück zum Lync Optimization Pack).</li> <li>• Diese Einstellung ist die gleiche wie <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia &gt; HDX RealTime Media Engine</b>.</li> </ul> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p><b>!</b> <b>WICHTIG:</b> <a href="#">Skype for Business Online</a> wird von Microsoft am 31. Juli 2021 abgeschaltet<sup>63</sup>. Stattdessen muss danach Microsoft Teams verwendet werden.</p> </div>
---------------------------	--


Option 2: HDX RealTime Webcam Redirection (sollte nur verwendet werden, wenn Optimierungspacks unter Option 1 nicht anwendbar sind)

Für andere VDI-Programme, die den Gebrauch einer Webcam erfordern (z.B. den Browser), kann HDX RealTime Webcam Redirection verwendet werden. Diese Option ermöglicht die clientseitige Komprimierung von Audio- und Videodaten, die auf eine virtuelle HDX-Webcam auf der Serverseite umgeleitet werden. Sie ermöglicht es auch, die Auflösung der Webcam manuell zu definieren.

**!** **Jeweils nur eine Option für ein Gerät**

- Die **HDX RealTime Webcam Redirection** und **HDX RealTime Media Engine (Skype for Business)** sollten nicht gleichzeitig aktiviert sein.
- Wenn Sie HDX oder ein anwendungsspezifisches Optimierungspack (z.B. **Zoom VDI Media Plugin**) verwenden, sollte **Native USB Redirection / Fabulatech USB Redirection** deaktiviert sein.

<sup>63</sup> <https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833>

Serverseitige Einstellungen	Clientseitige Einstellungen
<p>Die folgenden Richtlinieneinstellungen müssen aktiviert sein:</p> <ul style="list-style-type: none"> <li>• Multimediakonferenzen (standardmäßig aktiviert)</li> <li>• Windows Media-Umleitung (standardmäßig aktiviert)</li> </ul> <p>Für Details siehe <a href="https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/webcam-compression.html">https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/multimedia/webcam-compression.html</a>.</p>	<ol style="list-style-type: none"> <li>1. Gehen Sie auf <b>Sitzungen &gt; Citrix &gt; Citrix Global &gt; HDX Multimedia</b>.</li> <li>2. Aktivieren Sie <b>Aktiviere Multimedia Redirection</b> (standardmäßig aktiviert).</li> <li>3. Aktivieren Sie <b>HDX RealTime Webcam Redirection</b>.</li> <li>4. Konfigurieren Sie die Auflösung für die Webcam, standardmäßig 352 x 288, und bei Bedarf weitere Einstellungen. <div style="border: 1px solid #ffc107; padding: 5px; margin: 5px 0;"> <p> Einige Webcammodelle können nur bestimmte Auflösungen unterstützen.</p> </div> </li> <li>5. Wenn die USB-Umleitung aktiviert ist (nicht empfohlen), verwenden Sie die <b>Geräteregeln</b>, um die Weiterleitung der Webcam per USB-Umleitung zu verbieten. Siehe <a href="#">den obigen Abschnitt</a> (see page 727).</li> </ol>

#### Abhängigkeiten

- **HDX RealTime Webcam Redirection** wird für 32-Bit-Anwendungen auf der Serverseite unterstützt (Einschränkung von Citrix Receiver/Workspace App für Linux). Verwenden Sie einen 32-Bit-Browser, um die Webcam-Umleitung online zu überprüfen, z.B. [www.webcamtests.com](http://www.webcamtests.com)<sup>64</sup>. Siehe auch <https://support.citrix.com/article/CTX223199>.

Die Webcam-Umleitung für 64-Bit-Anwendungen wird seit CWA 2203 unterstützt; zur Konfiguration siehe <https://virtualbrat.com/2023/02/23/citrix-hdx-webcam-redirection-for-64-bit-applications-how-to-guide/>. Davor war diese noch nicht in der Phase der allgemeinen Verfügbarkeit, siehe <https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#webcams>.


- Die Webcam-Umleitung funktioniert im Allgemeinen mit oder ohne **HDX RealTime Media Engine (RTME)**. Zur Vermeidung von Konflikten und für eine bessere Leistung der Webcam-Umleitung wird jedoch die Deaktivierung von **RTME** (standardmäßig aktiviert) dringend empfohlen.
- Die Nutzung der Webcam ist auf eine Anwendung beschränkt. Wenn z.B. Skype mit einer Webcam läuft und GoToMeeting gestartet wird, müssen Sie Skype schließen, um die Webcam mit GoToMeeting verwenden zu können.

#### Unterstützte Videokonferenz-Anwendungen

- Adobe Connect

<sup>64</sup> <http://www.webcamtests.com>

- Cisco Webex und Webex für Teams (Geben Sie dem Optimierungspack für Cisco Webex Meetings / Teams VDI den Vorzug, [siehe oben \(see page 729\)](#))
- GoToMeeting
- Google Hangouts und Hangouts Meet
- IBM Sametime
- Microsoft Skype for Business 2015, 2016, und 2019 (Geben Sie dem Optimierungspack für Skype for Business den Vorzug, [siehe oben \(see page 729\)](#))
- Microsoft Lync 2010 und 2013
- Microsoft Skype 7 oder höher
- Media Foundation-basierte Videoanwendungen auf Windows 8.x oder höher und Windows Server 2012 R2 oder höher

 **HDX RealTime Webcam Redirection** wird für Microsoft Teams NICHT unterstützt. Verwenden Sie stattdessen **Microsoft Teams Optimierung**, [siehe oben \(see page 729\)](#).

 **Funktioniert Audio bei der Webcam, aber kein Video?**

 Versuchen Sie, den Grafikspeicher im BIOS auf 512 MB zu erhöhen.

Nähere Informationen über HDX RealTime Webcam finden Sie unter:

- <https://support.citrix.com/article/CTX132764>
- <https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/configure-xenapp.html#webcams>

## VMware Horizon

### Option 1 (Beste Wahl)

<p><b>Microsoft Teams Optimierung</b></p>	<p>Pfad: <b>Sitzungen &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; VDI-Lösungen &gt; Microsoft Teams Optimierung</b> (standardmäßig aktiviert)</p> <ul style="list-style-type: none"> <li>• Verfügbar ab IGEL OS-Version 11.06.100</li> </ul> <p>Weitere Informationen über Microsoft Teams finden Sie unter <a href="#">Microsoft Teams Optimization with VMware Horizon<sup>65</sup></a> und <a href="#">Configuring Media Optimization for Microsoft Teams<sup>66</sup></a>.</p>
---	--

<sup>65</sup> <https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon>

<sup>66</sup> <https://docs.vmware.com/en/VMware-Horizon/2106/horizon-remote-desktop-features/GUID-F68FA7BB-B08F-4EFF-9BB1-1F9FC71F8214.html>

<p><b>Zoom VDI Media Plugin</b></p>	<p>Pfad: <b>Sitzungen &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; VDI-Lösungen &gt; Zoom VDI Media Plugin</b></p> <ul style="list-style-type: none"> <li>• Die enthaltenen Versionen des Zoom VDI Media Plugins finden Sie in den IGEL OS Release Notes.</li> <li>• Ab IGEL OS 11.06 können Sie die Version des Zoom VDI Media Plugins unter <b>Sitzungen &gt; Unified Communications &gt; Zoom Client-Auswahl</b> ändern.</li> </ul> <div style="border: 1px solid orange; padding: 5px; background-color: #fff9c4;"> <p><b>⚠</b> Zoom Media Plugin wird NICHT funktionieren, wenn Sie <b>HTML5 Multimedia Redirection</b> aktivieren (<b>Sitzungen &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; VDI-Lösungen</b>, standardmäßig aktiviert).</p> </div> <p>Weitere Informationen über das Zoom Media Plugin, einschließlich der serverseitigen Anforderungen, finden Sie unter <a href="#">Getting started with VDI</a><sup>67</sup>.</p>
<p><b>Cisco Webex Meetings VDI / Cisco Webex VDI</b></p>	<p>Pfad: <b>Sitzungen &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; Cisco &gt; Cisco Webex Meetings VDI</b> oder <b>Cisco Webex VDI</b></p> <ul style="list-style-type: none"> <li>• Die enthaltenen Versionen der Cisco Webex Meetings VDI / Cisco Webex VDI finden Sie in den IGEL OS Release Notes.</li> <li>• Ab IGEL OS 11.06 können Sie die Version des Cisco Webex Meetings VDI Clients unter <b>Sitzungen &gt; Unified Communications &gt; Cisco Webex Meetings VDI-Auswahl</b> ändern.</li> </ul> <p>Weitere Informationen über Cisco Webex Produkte für VDI, einschließlich der unterstützten Umgebungen, finden Sie unter:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Webex Meetings Virtual Desktop Software</a><sup>68</sup></li> <li>• <a href="#">Overview of Webex App for VDI</a><sup>69</sup></li> </ul>

<sup>67</sup> <https://support.zoom.us/hc/en-us/articles/360031096531-Getting-Started-with-VDI>


<sup>68</sup> <https://help.webex.com/en-us/nfjsqzbb/Cisco-Webex-Meetings-Virtual-Desktop-Software>

<sup>69</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT\\_chapter\\_00.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/wbxt/vdi/wbx-teams-vdi-deployment-guide/wbx-teams-vdi-deployment-wbx-calling-EFT_chapter_00.html)


<b>Cisco JVDI Client</b>	<p>Pfad: <b>Sitzungen &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; Cisco &gt; Cisco JVDI Client</b></p> <ul style="list-style-type: none"> <li>Die enthaltenen Versionen des Cisco JVDI Clients finden Sie in den IGEL OS Release Notes.</li> </ul> <p>Weitere Informationen über Cisco JVDI Client finden Sie unter <a href="#">Deployment and Installation Guide for Cisco Jabber Softphone for VDI Release 14.0</a><sup>70</sup>.</p>
<b>Skype for Business</b>	<p>Pfad: <b>Sitzungen &gt; Horizon Client &gt; Horizon Client Global &gt; Unified Communications &gt; Skype for Business &gt; Virtualization Pack für Skype for Business</b> (standardmäßig aktiviert)</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p><b>⚠ WICHTIG:</b> <a href="#">Skype for Business Online</a> wird von Microsoft am 31. Juli 2021 abgeschaltet<sup>71</sup>. Stattdessen muss danach Microsoft Teams verwendet werden.</p> </div>


## Option 2: Real-Time Audio-Video (RTAV)

Real-Time Audio-Video (RTAV) ist das Optimierungspack für Audio- und Videoanrufe innerhalb von VMware Horizon Sitzungen. RTAV komprimiert Audio- und Videodaten auf der Seite des Clients und sendet sie an den Horizon-Server, wo eine Instanz für VMware Virtual Webcam erstellt wird.

 Wie bei Citrix Sitzungen sollte die USB-Umleitung deaktiviert werden, wenn RTAV verwendet werden soll.

► Aktivieren Sie **Sitzungen > Horizon Client > Horizon Client Global > Multimedia > Real Time Audio Video (RTAV)**.

 RTAV ist nur bei Verbindungen über PCoIP oder VMware Blast verfügbar.

 Beachten Sie, dass nur eine Webcam umgeleitet wird (Einschränkung von Horizon-Client für Linux). Wenn es mehrere Webcams auf dem Client gibt, kann die bevorzugte Webcam im IGEL Setup unter **System > Registry > vmware.view.rtav-webcam-id** definiert werden. Details finden Sie unter [Select a Preferred Webcam or Microphone on a Linux Client System](#)<sup>72</sup>.

Weitere Informationen über RTAV finden Sie unter [Configuring Real-Time Audio-Video](#)<sup>73</sup>.

<sup>70</sup> [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jvdi/14\\_0/dig/jvdi\\_b\\_deploy-install-jvdi-14-0/jvdi\\_b\\_deploy-install-jvdi-12-9\\_chapter\\_010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jvdi/14_0/dig/jvdi_b_deploy-install-jvdi-14-0/jvdi_b_deploy-install-jvdi-12-9_chapter_010.html)

<sup>71</sup> <https://techcommunity.microsoft.com/t5/microsoft-teams-blog/skype-for-business-online-to-be-retired-in-2021/ba-p/777833>

<sup>72</sup> <https://docs.vmware.com/en/VMware-Horizon-Client-for-Linux/2111/horizon-client-linux-installation/GUID-C8C17975-AA1E-4378-A305-00E02FF93201.html>

<sup>73</sup> <https://docs.vmware.com/en/VMware-Horizon/2111/horizon-remote-desktop-features/GUID-D6FD6AD1-D326-4387-A6F0-152C7D844AA0.html>


### **Microsoft Teams**

Microsoft Teams kann mit RTAV im "Fallback-Modus" verwendet werden. Diese Konfiguration ist nicht optimal, da die Daten einen langen Weg über die Stationen Horizon-Client, Horizon-Server und Microsoft Teams-Server nehmen müssen. Weitere Informationen finden Sie unter [Configuring Microsoft Teams with Real-Time Audio-Video](#)<sup>74</sup>.

Die Medienoptimierung für Microsoft Teams (Single Hop oder "Optimierter Modus") in Horizon-Sitzungen wird derzeit nur mit dem Horizon-Client für Windows 10 in Verbindung mit Horizon 8 (2006) unterstützt. Weitere Informationen finden Sie unter [Microsoft Teams Optimization with VMware Horizon](#)<sup>75</sup>.

## RDP

Derzeit ist keine Optimierung für die Webcam-Umleitung in RDP-Sitzungen verfügbar. Es kann möglich sein, Webcams per USB-Umleitung umzuleiten, z.B. per **Native USB Redirection**. Allerdings muss für jede Webcam einzeln getestet werden, ob sie mit dieser Methode funktioniert. Es hängt oft von der Webcam und ihrem Windows-Treiber ab, ob sie mit den im Vergleich zum echten USB-Bus höheren Latenzen zurechtkommen, die bei USB-Umleitungen auftreten.

 In einigen Situationen können Webcams aufgrund von Netzwerklatenz, Bandbreitenbeschränkungen oder dem Fehlen kompatibler Treiber auf dem Server nicht korrekt umgeleitet werden.

### **Nicht optimierte Webcam-Unterstützung**

- Beachten Sie, dass die Bandbreitennutzung und die CPU-Auslastung des Servers erheblich ansteigen können, da die USB-Umleitung nicht für die Umleitung von Videogeräten ausgelegt ist.
- Aus diesem Grund wird zwecks Reduzierung der Datenvolumen empfohlen, Webcams zu verwenden, die direkt H.264- oder H.265-, und nicht MJPEG-Streams, ausgeben.

## Native USB Redirection

1. Aktivieren Sie **Native USB Redirection** unter **Sitzungen > RDP > RDP Global > Native USB Redirection**.
2. Setzen Sie **Vorgaberegeln** auf "Verbieten".
3. Unter **Geräteregeln** fügen Sie die **Hersteller-ID** und **Produkt-ID** des umzuleitenden Geräts hinzu.

### **Informationen zu USB-Geräten erhalten**

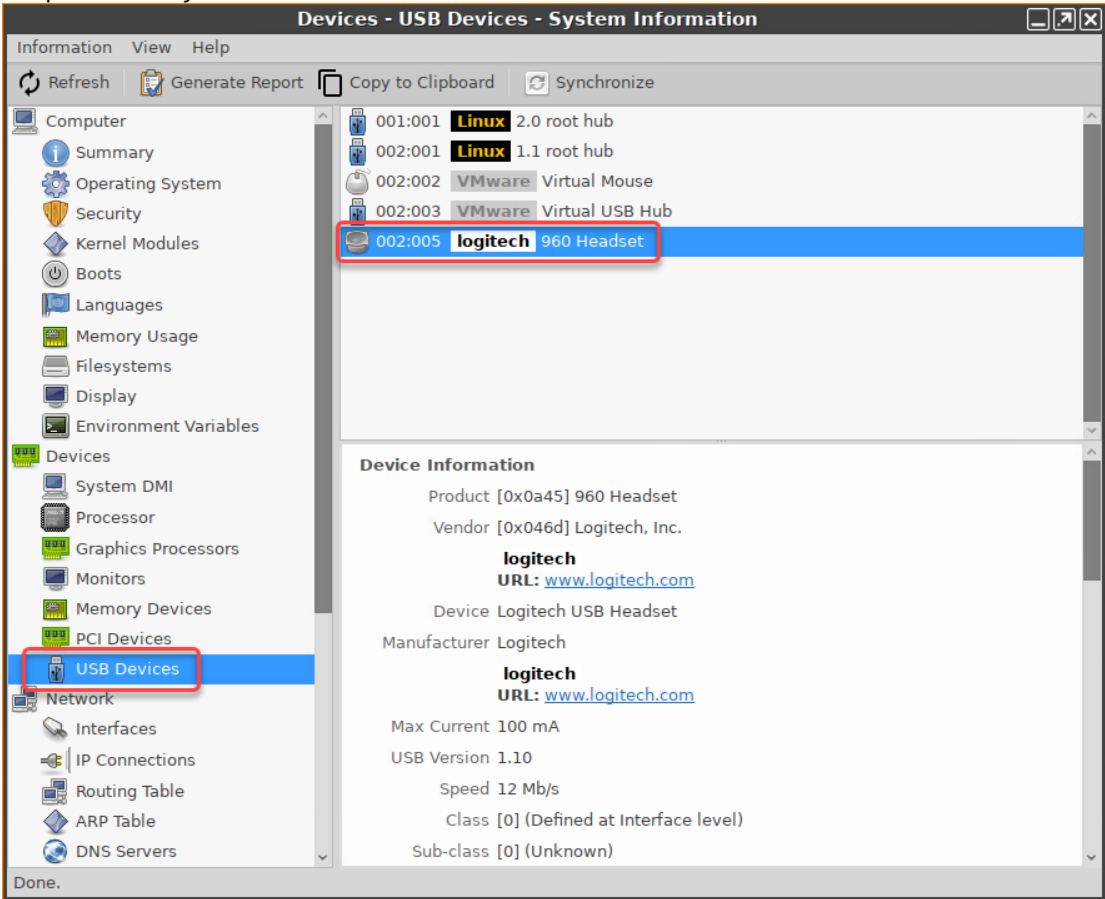
Um die **Klassen-ID**, die **Unterklassen-ID**, die **Hersteller-ID** und die **Produkt-ID** des angeschlossenen USB-Geräts herauszufinden, können Sie die Funktion **Systeminformationen** verwenden. Weitere Informationen finden Sie unter Using "System Information" Function.

<sup>74</sup> <https://docs.vmware.com/en/VMware-Horizon/2006/horizon-remote-desktop-features/GUID-E64B3E85-BA1E-4FB7-9DB4-FF9B7B7A892C.html>

<sup>75</sup> <https://techzone.vmware.com/resource/microsoft-teams-optimization-vmware-horizon>

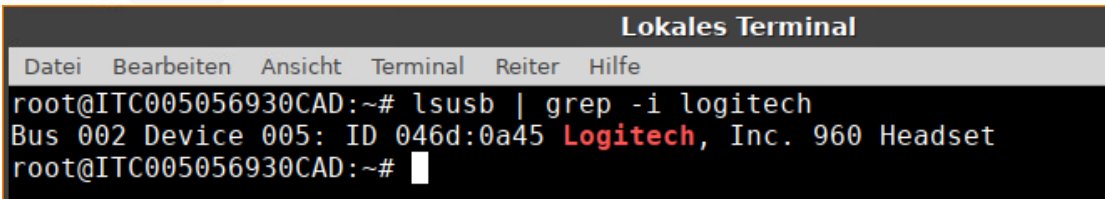


Beispiel für die Systeminformationen:



Alternativ können Sie auch den Befehl `lsusb` (oder `lsusb | grep -i [Suchbegriff]`) im Terminal verwenden.

Beispiel für `lsusb` :



- i Auf RDS-Servern kann das Folgende hilfreich sein:
  - ▶ Deaktivieren Sie die Einstellung **Do not allow supported Plug and Play device redirection** unter **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection**.

- i **Für Mikrofon (z.B. Headset)**
  - ▶ Aktivieren Sie **Sitzungen > RDP > RDP Global > Mapping > Audio > Audioaufnahme**.

**✓ Custom Partition als lokale Alternative**

Sie können auch [Custom Partitions](#) (see page 589) für Microsoft Teams oder Zoom verwenden, z.B. um Backend-Ressourcen zu sparen, was bei langsamen RDP-Backends eine gute Lösung sein kann. Die Custom Partition wird lokal installiert, ist aber in der Remotesitzung leicht zugänglich.

- Details finden Sie unter [Microsoft Teams as a Custom Partition](#) (see page 613) und [Zoom as a Custom Partition](#) (see page 603).
- Wenden Sie sich an das IGEL Support Team, um Unterstützung bei der Bereitstellung von Custom Partitions zu erhalten.

Wie Sie die Webcam in Windows 10 öffnen können, erfahren Sie unter [Open the Camera in Windows 10](#)<sup>76</sup>.

Einen Video-Überblick über die Verwendung von Webcams und anderen USB-Geräten in Remotesitzungen finden Sie unter:

**Englisch**

Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=PYCU1AEfS-g&feature=youtu.be>

**Deutsch**

Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=caNhFib5cuA&feature=youtu.be>

<sup>76</sup> <https://support.microsoft.com/en-us/windows/open-the-camera-in-windows-10-8da044ed-c4a8-2fb4-da51-232362e4126d#:~:text=To%20open%20up%20your%20webcam,Let%20apps%20use%20my%20camera.>

## Webcam-Information

Wenn Sie ein Gerät mit der IGEL Linux Version 5.3.100 oder höher betreiben, können Sie eine Webcam mit integrierten Tool konfigurieren und testen. Dieses Tool nennt sich **Webcam Information**.

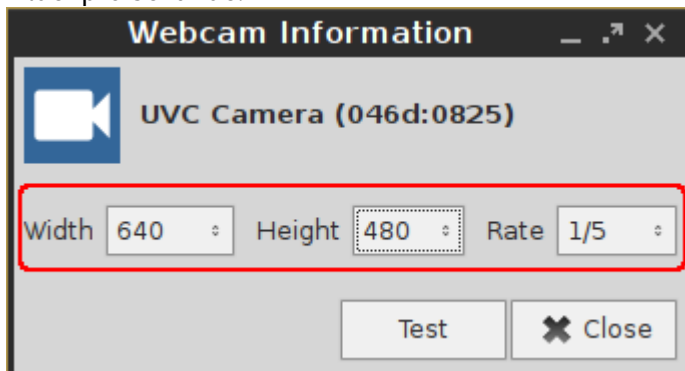
► Um einen Starter für **Webcam Information** zu konfigurieren, öffnen Sie die IGEL Setup und gehen Sie auf **Zubehör > Webcam Information**.

So bestimmen und ändern Sie Breite, Höhe und Bildfrequenz Ihrer Webcam:

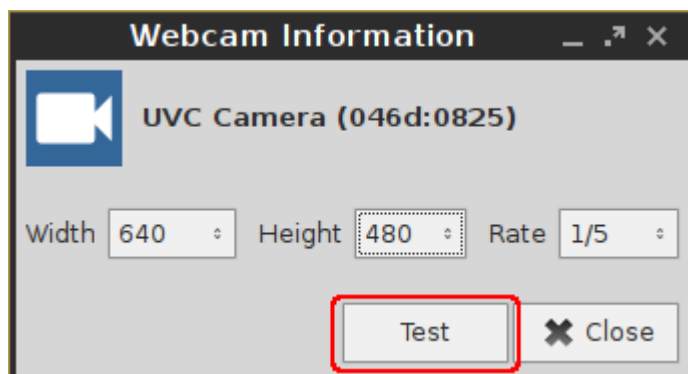
1. Starten Sie das **Webcam Information** Tool.

Die folgenden Werte werden angezeigt:

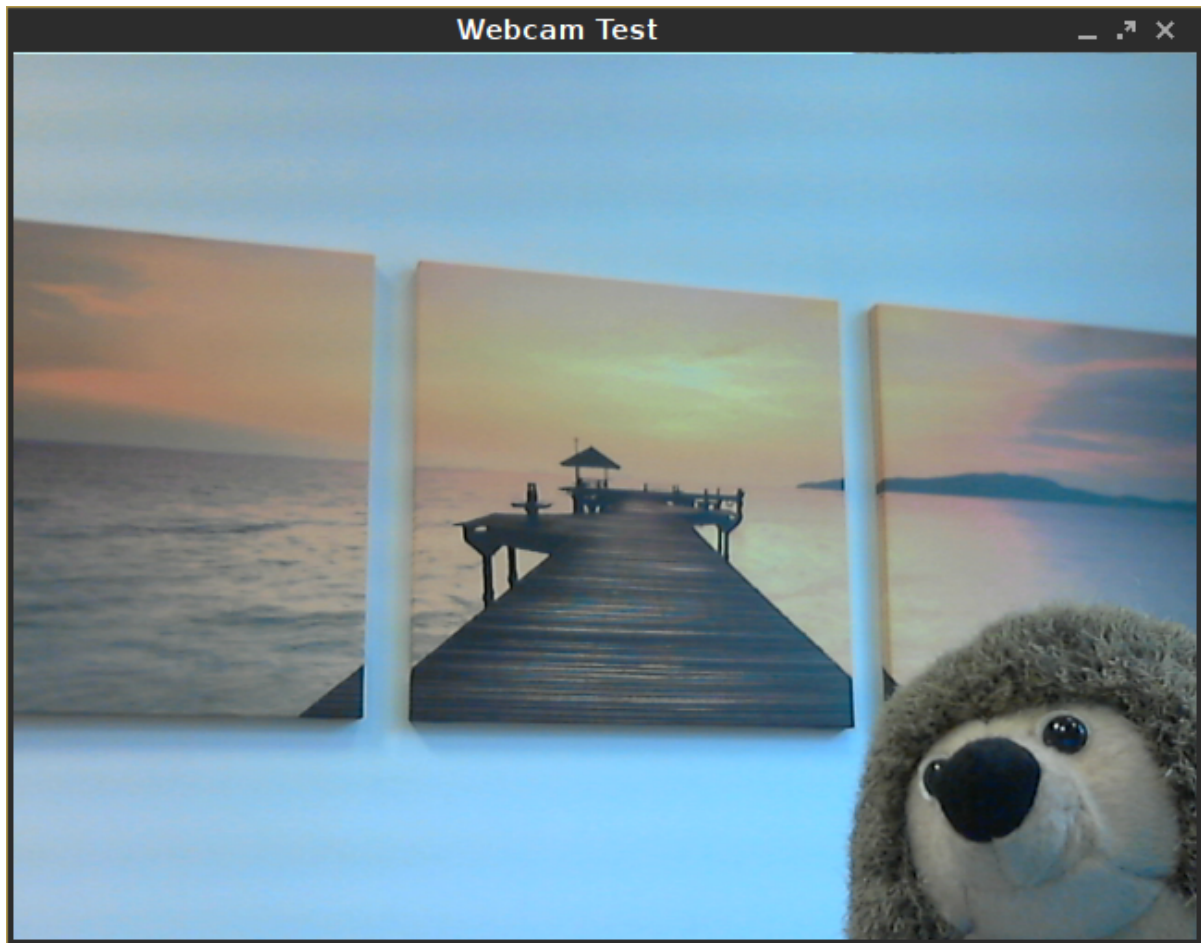
- **Breite:** Bildbreite in Pixel
- **Höhe:** Bildhöhe in Pixel
- **Frequenz:** Bildfrequenz in fps (frequenz pro Sekunde) Beispiel: **1/30** bedeutet 30 einzelne Bilder pro Sekunde.



2. Klicken Sie auf eines der Felder um den Wert zu ändern. Dabei werden die unterstützten Werte angezeigt.
3. Klicken Sie **Test**.



Das mit den aktuellen Einstellungen erzeugten Videobild wird angezeigt.



Um zu testen ob die Webcam in einer Sitzung funktioniert (z. B. via Citrix HDX Webcam-Umleitung), öffnen Sie einen Browser in der Sitzung und gehen Sie zu <https://www.onlinemictest.com/webcam-test/>.


## Bluetooth-Tool

Mit dem Bluetooth-Tool können Sie Bluetooth-Geräte komfortabel verbinden oder trennen. Das Bluetooth-Tool unterstützt folgende Kopplungsmethoden:

- **Automatische PIN-Auswahl:** Kopplung mit automatischer PIN-Zuweisung
- **0000, 1111, 1234:** Kopplung mit fester PIN (bei den meisten Kopfhörern, Mäusen oder GPS-Geräten)
- **Benutzerdefinierte PIN:** Kopplung mit einer vom Benutzer eingegebenen festen PIN  
Weitere Informationen finden Sie in den Handbuch-Kapiteln Bluetooth-Tool verwenden und Bluetooth-Tool.

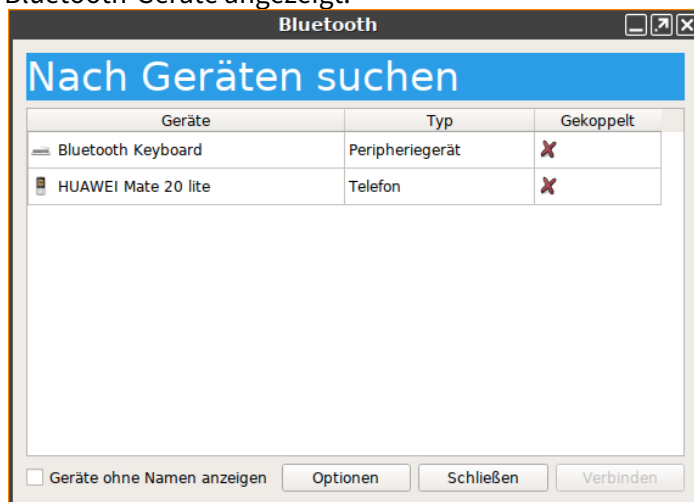
Im folgenden Beispiel verbinden wir eine Bluetooth-Tastatur mittels **Automatischer PIN-Auswahl:**


1. Achten Sie darauf, dass folgende Voraussetzung übereinstimmen:
  - Im IGEL Setup sind die Optionen **Geräte > Bluetooth > Bluetooth** und **Symbol in der Systemleiste** aktiviert.
  - Das Bluetooth-Gerät ist bereit.

 Wenn Ihr Endgerät (z. B. UD2 D220) Bluetooth nicht unterstützt, ist es notwendig, einen Bluetooth-USB-Adapter daran anzuschließen.

2. Starten Sie das Bluetooth-Tool über das IGEL Menü  via **System > Bluetooth-Tool** oder andere verfügbaren Startoptionen.

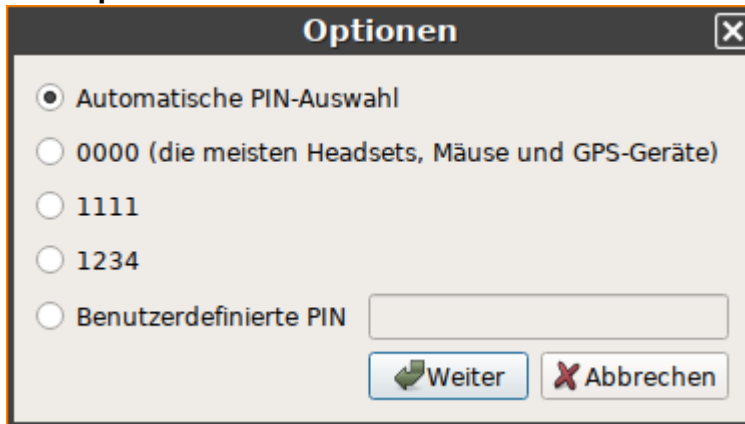
Der Dialog **Nach Geräten suchen** erscheint. Nach einigen Sekunden werden die gefundenen Bluetooth-Geräte angezeigt.



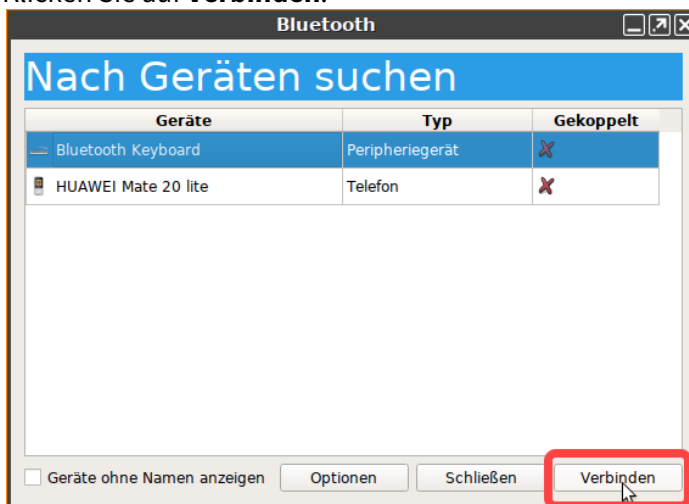
 Wenn keine Geräte gefunden wurden, schalten Sie das Bluetooth-Gerät aus und wieder ein oder drücken Sie die Bluetooth-Kopplungstaste, in unserem Fall **Connect** auf der Rückseite der Tastatur.

3. Markieren Sie das gewünschte Bluetooth-Gerät.

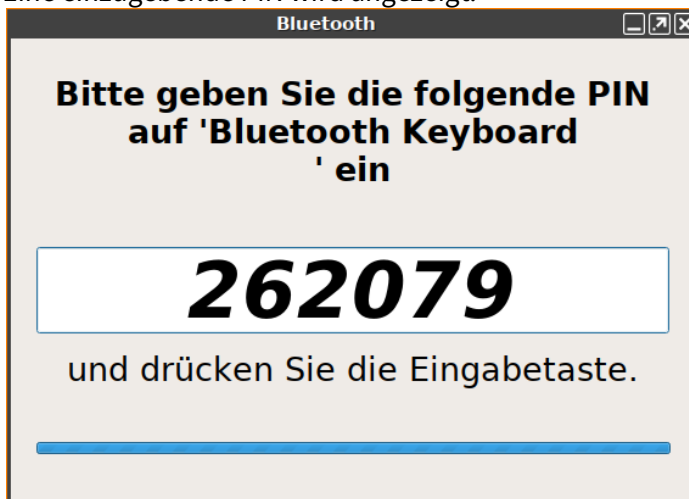
4. Unter **Optionen** wählen Sie **Automatische PIN-Auswahl** aus.



5. Klicken Sie auf **Verbinden**.



Eine einzugebende PIN wird angezeigt.




✓ Wenn keine PIN angezeigt wird, klicken Sie erneut auf die Schaltfläche **Verbinden**.

6. Tippen Sie die PIN in Ihr Bluetooth-Gerät ein.  
Wenn alles gut gelaufen ist, wird der Verbindungsstatus angezeigt.



7. Schließen Sie den Dialog.

Ihr Bluetooth-Gerät kann nun verwendet werden. Per rechten Mausklick auf das Symbol  in der Systemleiste können Sie das Bluetooth-Tool erneut starten, z. B. um ein weiteres Bluetooth-Gerät zu koppeln oder ein Gerät abzukoppeln.

## Jabra Xpress Pakete bereitstellen

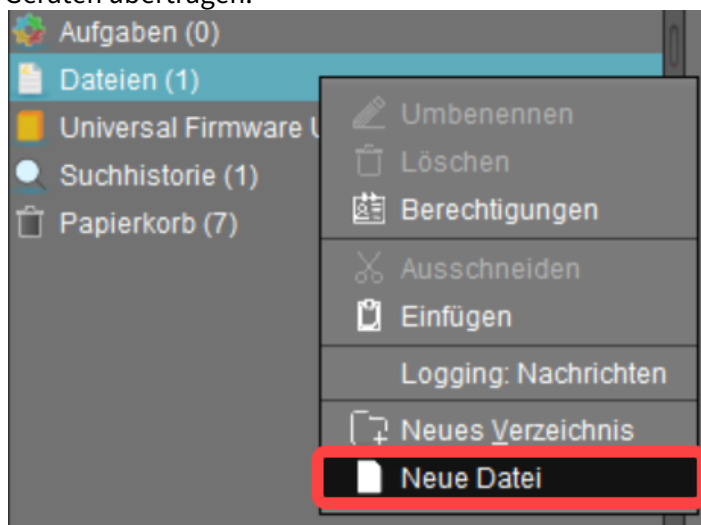
Jabra Xpress ist eine Lösung für die ferngesteuerte Massenbereitstellung von Jabra USB-Headsets, die es ermöglicht, Pakete mit Einstellungen, Firmwareupdates usw. für Jabra Geräte zu erstellen, siehe <https://www.jabra.com/supportpages/jabra-xpress#/>.

Die Bereitstellung eines Jabra Xpress Pakets umfasst die folgenden Schritte:

1. Das Paket zum Herunterladen über das FTP(S)- oder HTTP(S)-Protokoll bereitstellen (see page 744)
2. Die Quell-URL im IGEL Setup konfigurieren (see page 744)
3. Den Bereitstellungsprozess in der UMS auslösen (see page 745)

### Xpress Paket zum Herunterladen über das FTP(S)- oder HTTP(S)-Protokoll bereitstellen

1. Erstellen Sie ein Paket auf dem Jabra Xpress Portal und laden Sie es herunter.
2. Legen Sie das ZIP-Archiv auf Ihrem FTP(S)- oder HTTP(S)-Server ab.  
Wenn Sie die UMS als Ablageort verwenden möchten, registrieren Sie das ZIP-Archiv in der UMS unter **Dateien > [Kontextmenü] > Neue Datei**. Detaillierte Informationen zur Registrierung einer Datei in der UMS finden Sie unter Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen.



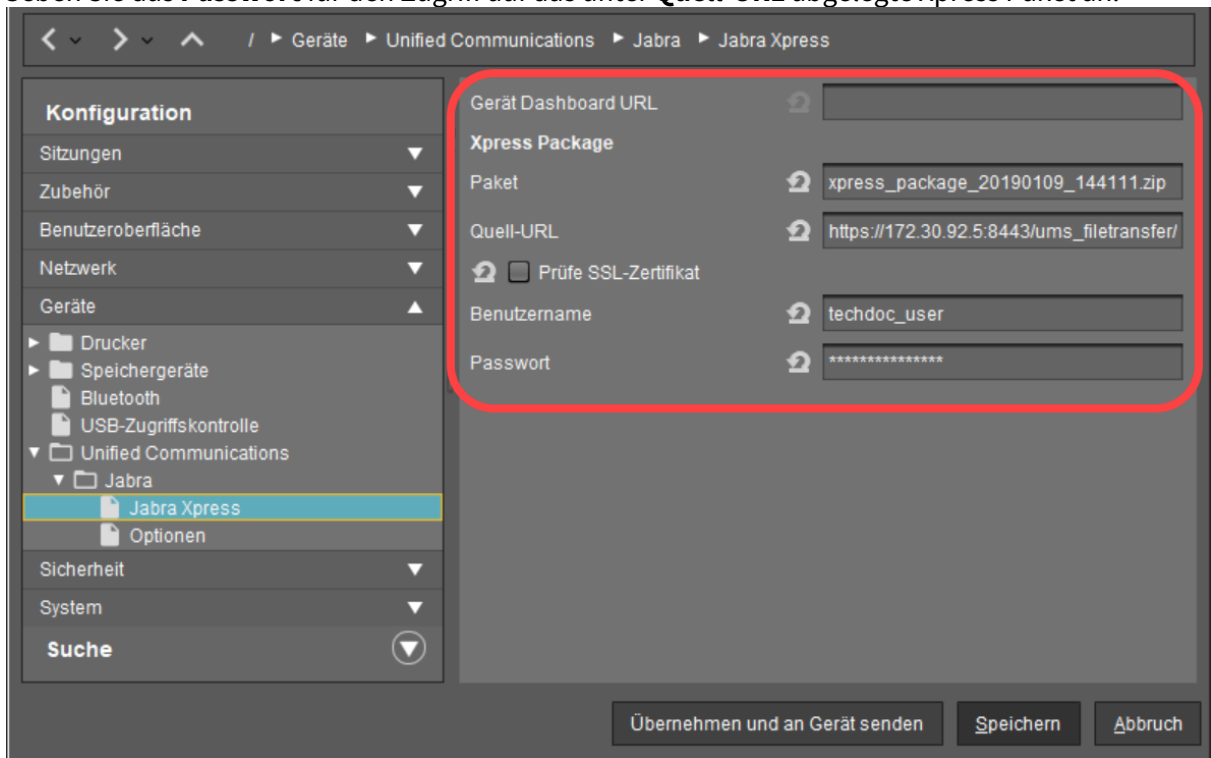
### Quell-URL im IGEL Setup konfigurieren

Als nächstes müssen Sie den Downloadort konfigurieren:

1. Im IGEL Setup oder im Konfigurationsdialog in der UMS gehen Sie auf **Geräte > Unified Communications > Jabra > Jabra Xpress**.



2. Unter **Gerät Dashboard URL** können Sie optional die URL zum Dashboard-Server des Jabra Geräts angeben.
3. Unter **Paket** geben Sie den Dateinamen des Xpress Pakets ein.  
Beispiel: `xpress_package_20190109_144111.zip`.
4. Unter **Quell-URL** geben Sie die URL zum Verzeichnis an, das das Xpress Paket enthält.  
Beispiel: `https://172.30.92.5:8443/ums_filetransfer/`, wenn Sie die UMS als Ablageort verwenden.
5. Deaktivieren Sie das Kästchen **Prüfe SSL-Zertifikat**, wenn Ihr HTTPS- oder FTPS-Server ein selbstsigniertes Zertifikat verwendet.
6. Geben Sie den **Benutzernamen** für den Zugriff auf das unter **Quell-URL** abgelegte Xpress Paket an.
7. Geben Sie das **Passwort** für den Zugriff auf das unter **Quell-URL** abgelegte Xpress Paket an.



The screenshot shows the configuration page for a Jabra Xpress device. The left sidebar contains a navigation menu with categories like 'Konfiguration', 'Geräte', 'Sicherheit', and 'Suche'. The 'Geräte' section is expanded to show 'Jabra Xpress'. The main content area is titled 'Xpress Package' and contains the following fields:

- Gerät Dashboard URL: (empty)
- Xpress Package: (empty)
- Paket: `xpress_package_20190109_144111.zip`
- Quell-URL: `https://172.30.92.5:8443/ums_filetransfer/`
- Prüfe SSL-Zertifikat:
- Benutzername: `techdoc_user`
- Passwort: `*****`

At the bottom of the configuration area, there are three buttons: 'Übernehmen und an Gerät senden', 'Speichern', and 'Abbruch'.

8. Speichern Sie die Einstellungen.

## Bereitstellungsprozess in der UMS auslösen

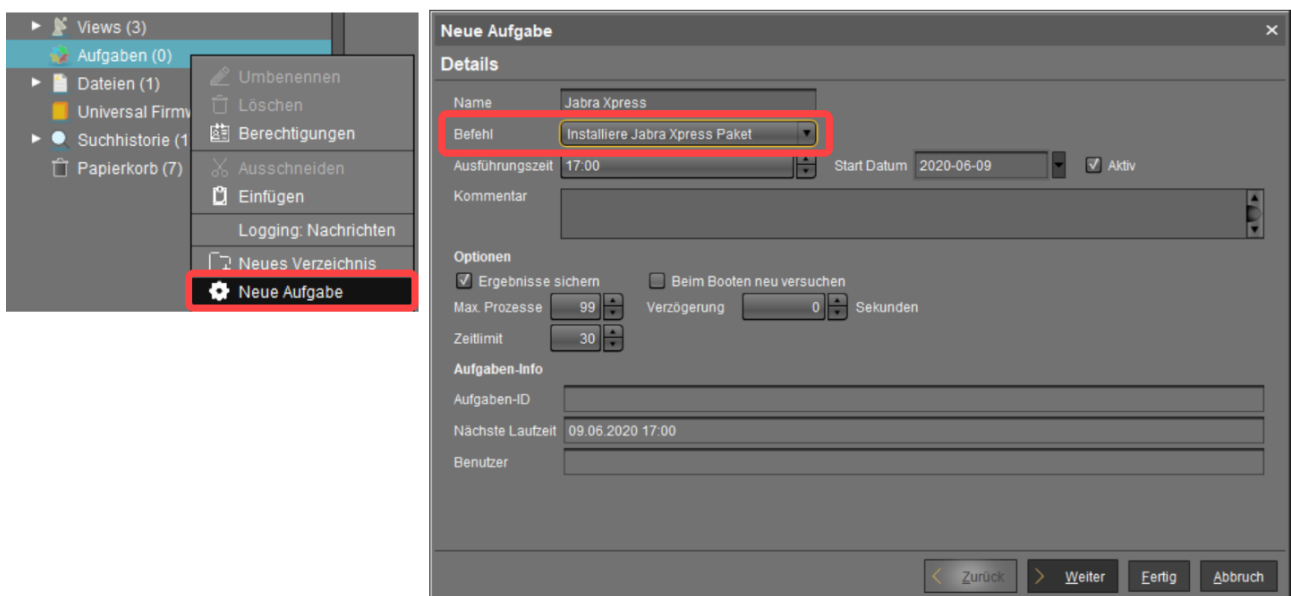
Nun müssen Sie den Bereitstellungsprozess auslösen. Es gibt zwei Möglichkeiten:


- Gehen Sie in der UMS auf **Geräte** > [Kontextmenü des Geräts] > **Spezifische Befehle** und wählen Sie **Installiere Jabra Xpress Paket** aus.



ODER

- Gehen Sie in der UMS auf **Aufgaben** > **Neue Aufgabe** und wählen Sie **Installiere Jabra Xpress Paket** als **Befehl** aus. Weisen Sie die Aufgabe den erforderlichen Geräten zu, siehe Zuordnung.



 Beachten Sie, dass es nicht möglich ist, den Bereitstellungsprozess rückgängig zu machen, z.B. ein Xpress Paket vom Jabra Gerät zu entfernen. Wenn Sie die vorherigen Einstellungen benötigen, müssen Sie ein neues Jabra Xpress Paket mit der alten Headset-Firmware und -Konfiguration konfigurieren und bereitstellen.

Siehe auch Jabra Xpress im IGEL OS Referenzhandbuch.

## Unterschriftenpads anschließen

Sie können Unterschriftenpads der folgenden Hersteller anschließen:


- StepOver;
- signotec.

▶ Um sie zu aktivieren, gehen Sie auf Setup > **Benutzeroberfläche** > **Eingabe** > **Unterschriftenpad**.

▶ Um USB-Unterschriftenpads dieser Hersteller verwenden zu können, muss eine serielle Verbindung konfiguriert werden. Gehen Sie wie folgt vor:

1. Aktivieren Sie **COM Port Mapping** unter:

- Setup > **Sitzungen** > **Citrix** > **Citrix Global** > **Mapping** > **Serielle Anschlüsse** für Citrix Sitzungen;
- Setup > **Sitzungen** > **RDP** > **RDP Global** > **Mapping** > **Serielle Anschlüsse** für RDP-Sitzungen.

2. Klicken Sie auf **Hinzufügen** .

3. Klicken Sie auf **Geräte suchen...**

4. Wählen Sie Ihr Gerät.

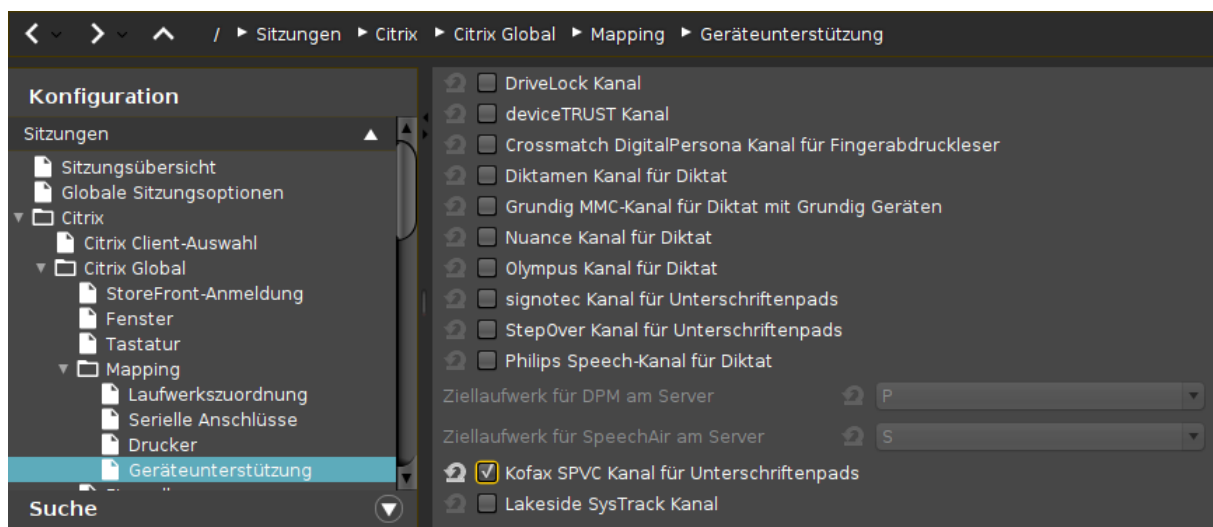
Ihr Unterschriftenpad kann nun benutzt werden.

## Ein Kofax / Wacom Unterschriftenpad verwenden

Sie können ein Kofax / Wacom Unterschriftenpad in Citrix Sitzungen über den Kofax SPVC Kanal für Unterschriftenpads verwenden. Die Virtual-Serial-Sign-Pad-Methode wird nicht länger unterstützt.

### Auf dem Gerät

1. Verbinden Sie das Unterschriftenpad mit einem der USB-Ports Ihres Geräts.
2. Gehen Sie zu **Sitzungen > Citrix > Citrix Global > Mapping > Geräteunterstützung**.
3. Aktivieren Sie **Kofax SPVC Kanal für Unterschriftenpads**.



### Auf dem VDI Server (Windows)

- ▶ Installieren Sie die erforderliche Software von Kofax / Wacom.

Der in dieser Software enthaltene Treiber wartet auf Unterschriftenpads auf einem virtuellen Kanal. Anwendungen wie SignDoc können das Unterschriftenpad verwenden.

## Ein StepOver Unterschriftenpad verwenden

Sie können ein StepOver Unterschriftenpad in einer Citrix oder RDP-Sitzung verwenden. Es gibt dafür zwei verschiedene Möglichkeiten:

- [Mit StepOver TCP Client \(see page 751\)](#)
- [Mit StepOver Kanal für Unterschriftenpads \(see page 755\)](#)

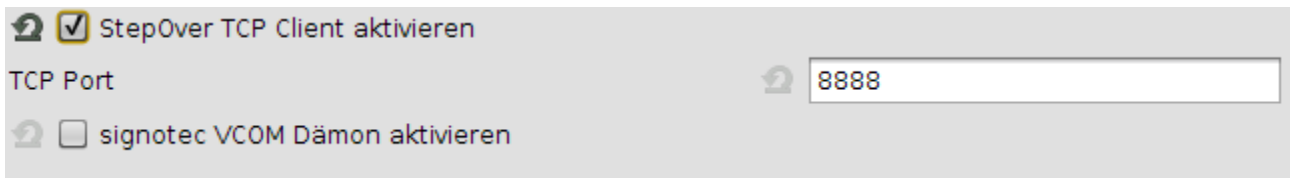
Nur eine der Methoden kann zu einem bestimmten Zeitpunkt verwendet werden. Welche der beiden Sie benötigen, wird von Ihren Anwendungen auf der Serverseite bestimmt.

Siehe auch Kompatibilität mit StepOver Unterschriftenpads.

## Mit StepOver TCP Client

### Auf dem Gerät

- ▶ Verbinden Sie das Unterschriftenpad mit einem der USB-Ports des Geräts.
- ▶ Gehen Sie im IGEL Setup unter **Benutzeroberfläche > Eingabe > Unterschriftenpad**.
- ▶ Aktivieren Sie **StepOver TCP Client aktivieren**.
- ▶ Ändern Sie bei Bedarf den **TCP Port**. (Standard: 8888)

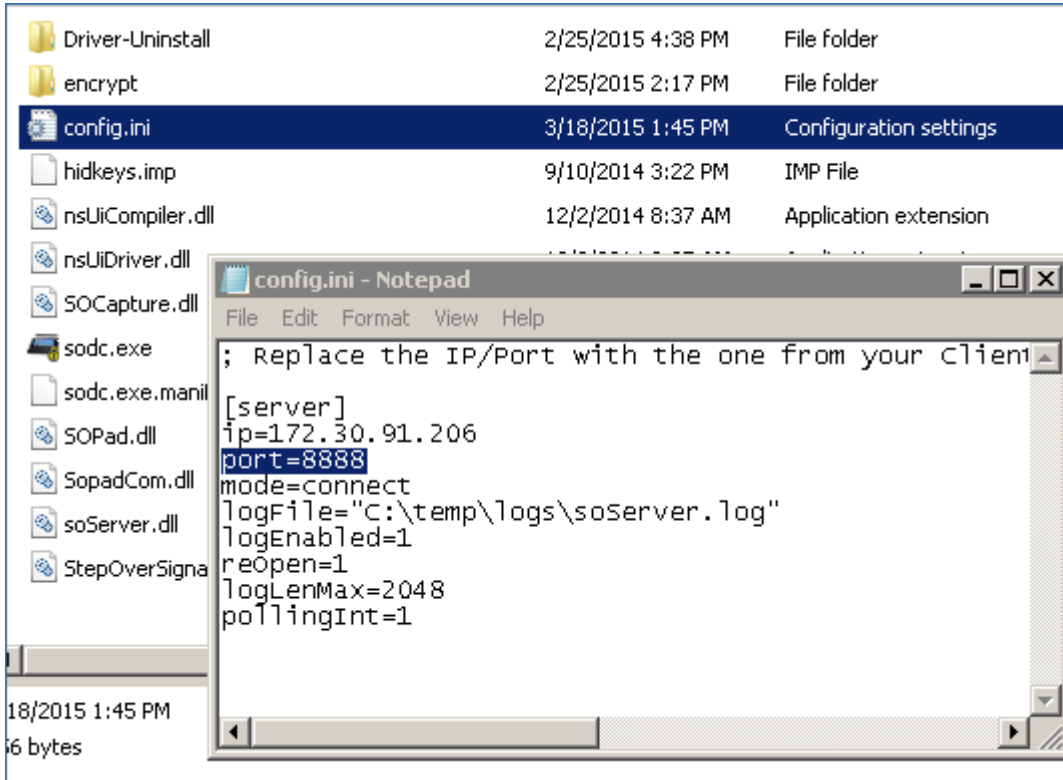


**i** Sie können überprüfen, ob der StepOver TCP Client auf dem Gerät läuft, indem Sie in einem lokalen Terminal Folgendes eingeben: `ps waux | grep sotcp`. Das Ergebnis sollte einen `sotcp`-Prozess enthalten.

### Auf dem VDI Server (Windows)

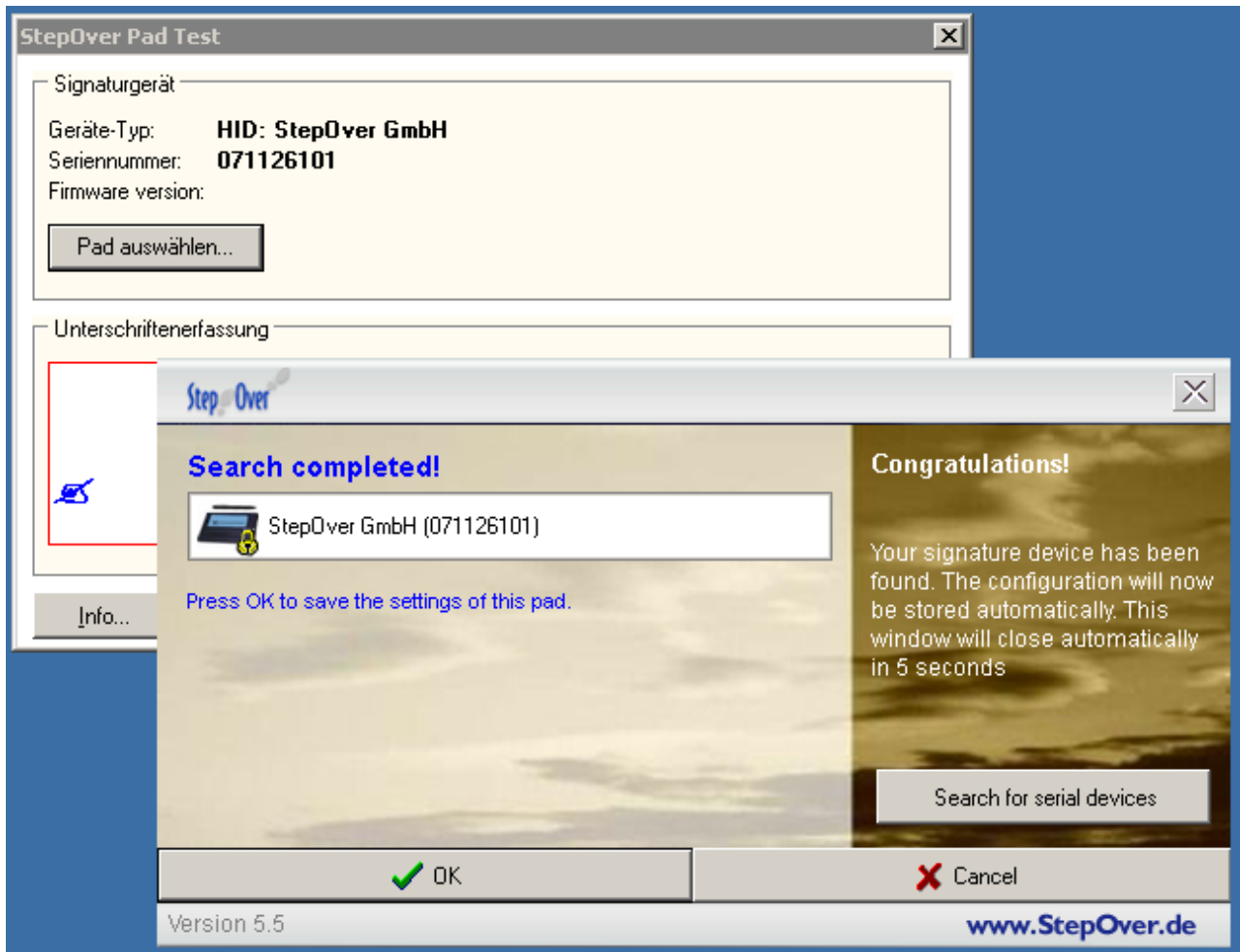
- ▶ Suchen Sie das Programm `sodc.exe` auf dem Server. Es ist ein Teil von StepOver eSignature Office und ist unter `[Your Program Files Directory]\StepOver\eSignatureOffice [version]\driver\` zu finden.

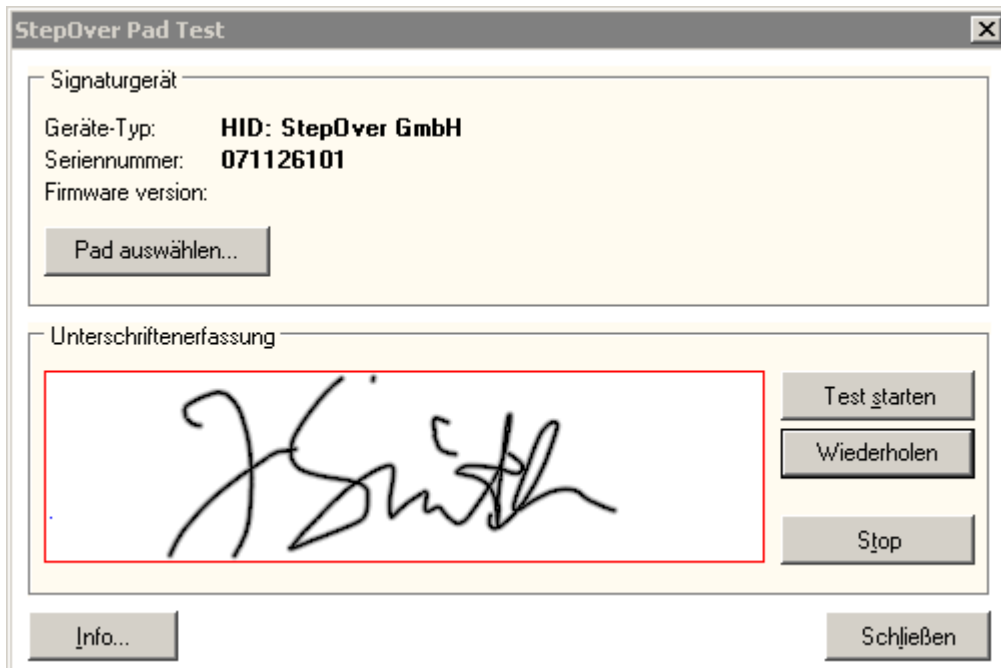
- Falls Sie einen anderen TCP-Port verwenden, ändern Sie ihn in der Datei `config.ini`, die sich im selben Verzeichnis befindet.



- Führen Sie `sodc.exe` aus. Das **StepOver Pad Test**-Fenster öffnet sich. Verwenden Sie die Tasten, um Ihr Unterschriftenpad zu suchen und auszuwählen, und versuchen Sie, in das dafür vorgesehene Feld zu schreiben.







Die Status-LED des Pads leuchtet Grün, wenn die Verbindung erfolgreich ist. Das Unterschriftenpad ist nun bereit für die Verwendung mit aktivierten Anwendungen wie StepOver eSignature Office.

## Mit StepOver Kanal für Unterschriftenpads

**StepOver Kanal für Unterschriftenpads** ist nur für Citrix Sitzungen anwendbar. Er aktiviert StepOver Citrix Client und ermöglicht die Umleitung über Citrix virtuellen Kanal.

### Auf dem Gerät

- ▶ Gehen Sie im IGEL Setup unter **Sitzungen > Citrix > Citrix Global > Mapping > Geräteunterstützung**.
- ▶ Aktivieren Sie **StepOver Kanal für Unterschriftenpads**.

### Auf dem Server

- ▶ Wählen Sie bei der Installation der StepOver Software die Option "Citrix".

## eGK/KVK - Kartenlesegerät

IGEL OS Geräte unterstützen das Lesen von deutschen elektronischen Gesundheitskarten (eGK), Krankenversicherungskarten (KVK) und den deutschen Heilberufsausweis (HBA) durch eine Vielzahl von Lesegeräten, die über RDP oder ICA verbunden sind. Die Konfiguration und Funktionalitäten variieren je nach Lesertyp.

Die folgenden getesteten Lösungen sind verfügbar:


Kartelesegerät	Schnittstelle	Gerät-/Server-Anbindung
Cherry G80-1502	seriell	COM port mapping
Cherry ST-2052	USB	Smartcard mapping
Cherry ST-1506	USB	USB RNDIS. IGEL OS Gerät agiert als NAT-Router.
Cherry ST-1503 und Cherry G87-1504	USB	Cherry Virtual Channel (IGEL Linux v5 only)
SICCT via LAN über den Cherry USB2LAN Proxy. (IGEL Linux Version 5.12.100 und IGEL Linux Version 10.03.100 oder höher)		
ORGA 910/920 M	USB	COM port mapping
ORGA 6041 L eGK eHealth-BCS	USB	COM port mapping
SCM Microsystems eHealth200	USB	Smartcard mapping
SCM Microsystems eHealth500	USB	COM port mapping
celectronic CARD STAR /medic2	seriell	COM port mapping
celectronic CARD STAR /memo3	USB	COM port mapping

- [Cherry G80-1502 an der seriellen Schnittstelle \(see page 757\)](#)
- [Cherry ST-2052 \(see page 759\)](#)
- [Cherry ST-1503 und G87-1504 \(USB\)](#)
- [Cherry eHealth Kartenterminal ST-1506 im USB-RNDIS-Modus mit IGEL OS verwenden \(see page 760\)](#)
- [Orga 910/920 M \(see page 765\)](#)
- [Orga 6041 L eGK eHealth-BC S \(see page 767\)](#)
- [celectronic CARD STAR / medic2 \(see page 769\)](#)
- [celectronic CARD STAR/ memo3 \(see page 771\)](#)

## Cherry G80-1502 an der seriellen Schnittstelle

### Tastatur anschließen

- ▶ Verbinden Sie die Tastatur sowohl mit dem PS/2-Anschluss als auch mit dem seriellen Anschluss des Gerätes.

 Die Tastatur muss mindestens in Firmware Version 1.19 vorliegen und im Modus S1 sein. Siehe dazu [http://www.cherry.de/files/manual/Cherry\\_G80-1502\\_mit\\_eGK.pdf](http://www.cherry.de/files/manual/Cherry_G80-1502_mit_eGK.pdf) ([http://www.cherry.de/files/manual/Cherry\\_G80-1502\\_mit\\_eGK.pdf](http://www.cherry.de/files/manual/Cherry_G80-1502_mit_eGK.pdf)).

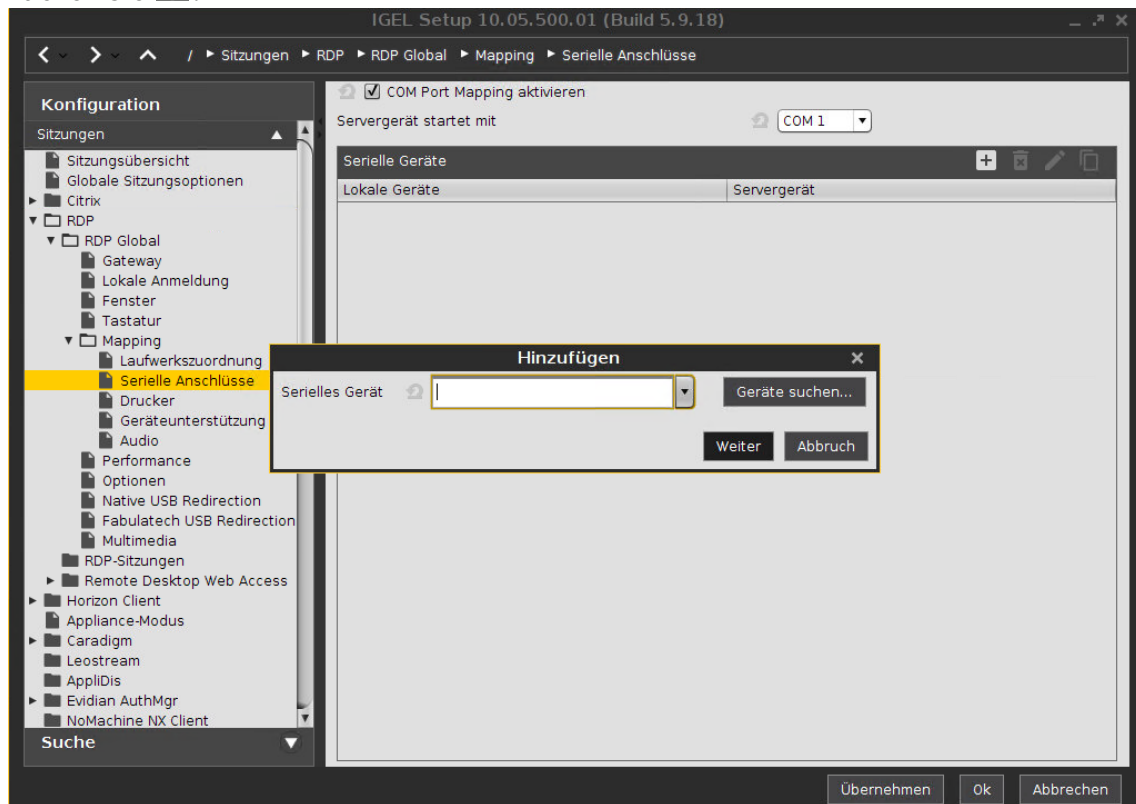
Funktionalität	
Software:	Cherry eHealth eGK/KVK Software
Gerät/Server-Anbindung	COM Port Mapping

### Gerät konfigurieren

Fügen Sie im IGEL-Setup das serielle Gerät hinzu, mit dem die Tastatur verbunden ist:

1. Klicken Sie **Sitzungen > RDP > RDP Global > Mapping > Serielle Anschlüsse**

## 2. Klicken Sie .



## 3. Wählen Sie ein Serielles Gerät (COM1, COM2,...).

### Server konfigurieren

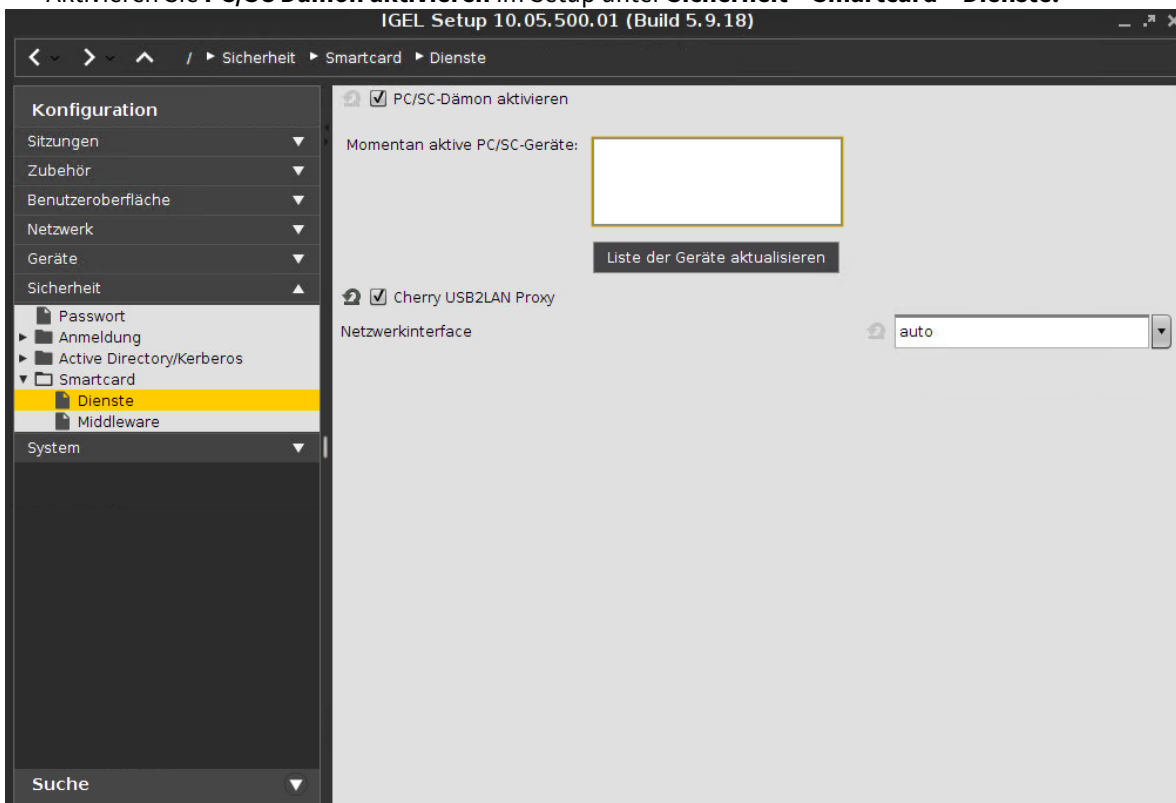
1. Installieren Sie die eGK-KVK-Software von Cherry.  
Siehe auch: [http://www.cherry.de/files/manual/eHealth\\_Client-Server\\_Einbindung.pdf](http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf)
2. Starten Sie das Programm CT-API Konfiguration.
3. Wählen Sie die entsprechende Portnummer für das G80-1502.

## Cherry ST-2052

Funktionalität	
USB ID:	046a:003e
Software:	Cherry eHealth eGK/KVK Software
Gerät/Server-Anbindung:	Smartcard (PC/SC) Mapping

## Gerät konfigurieren

► Aktivieren Sie **PC/SC Dämon aktivieren** im Setup unter **Sicherheit > Smartcard > Dienste**:



## Server konfigurieren

1. Installieren Sie die eGK-KVK-Software von Cherry.  
Siehe auch [http://www.cherry.de/files/manual/eHealth\\_Client-Server\\_Einbindung.pdf](http://www.cherry.de/files/manual/eHealth_Client-Server_Einbindung.pdf)
2. Starten Sie das Programm CT-API Konfiguration.
3. Wählen Sie die Portnummer 1 für das ST-2052.

## Cherry eHealth Kartenterminal ST-1506 im USB-RNDIS-Modus mit IGEL OS verwenden

Wenn Sie beispielsweise keine freie Netzwerkdose haben, können Sie Ihr Cherry eHealth Kartenterminal ST-1506 über ein Endgerät im USB-RNDIS-Modus (Remote Network Driver Interface Specification) betreiben. In diesem Fall agiert das IGEL OS Endgerät als NAT-Router. Das Kartenterminal nutzt die Netzwerkschnittstelle Ihres IGEL OS Geräts.

Weitere Informationen zu ST-1506 finden Sie unter:

- CHERRY eHealth Terminal ST-1506 Handbuch für Administratoren:  
<https://cherry.saas.contentsev.com/admin/ImageServer.php?ID=c9d5ca123973@iko249&rand=7fd8bfba76d6640e20fb48013ada6fe&lang=1&force=true&download=1>
- Benutzerhandbuch CHERRY ST-1506 USB-LAN Proxy:  
<https://cherry.saas.contentsev.com/admin/ImageServer.php?ID=fa222a123000@iko249&rand=ecdbe080457ef3f85ef67ef99515bbf2&lang=32&force=true&download=1>
- Konfiguration im USB-Modus (RNDIS):  
<https://cherry.saas.contentsev.com/admin/ImageServer.php?ID=b95fba122999@iko249&rand=4184538cb599fac797ec81076c31e366&lang=1&force=true&download=1>
- Für weitere Downloads, siehe:  
<https://www.cherry.de/service/downloads#15239>

### Voraussetzungen

- IGEL OS 11.08.100 oder höher
- Cherry ST-1506 muss eine statische IP-Konfiguration haben

### Konfiguration auf Ihrem Cherry ST-1506

1. Schließen Sie Ihr Kartenterminal an das IGEL OS Gerät an.
2. Geben Sie im **Menü > Admin-Menü** Ihre Admin-PIN ein.
3. Gehen Sie auf **Verbindung > USB Ethernet**.
4. Aktivieren Sie **RNDIS**.
5. Deaktivieren Sie **DHCP**.
6. Konfigurieren Sie eine statische **IP-Adresse**.
7. Geben Sie als **Gateway** die Host-IP-Adresse an, die Sie auf Ihrem IGEL OS Gerät mit dem Registry Key `devices.cherry.terminal%.rndis.host_ipaddress` (Standard: 192.168.42.1)



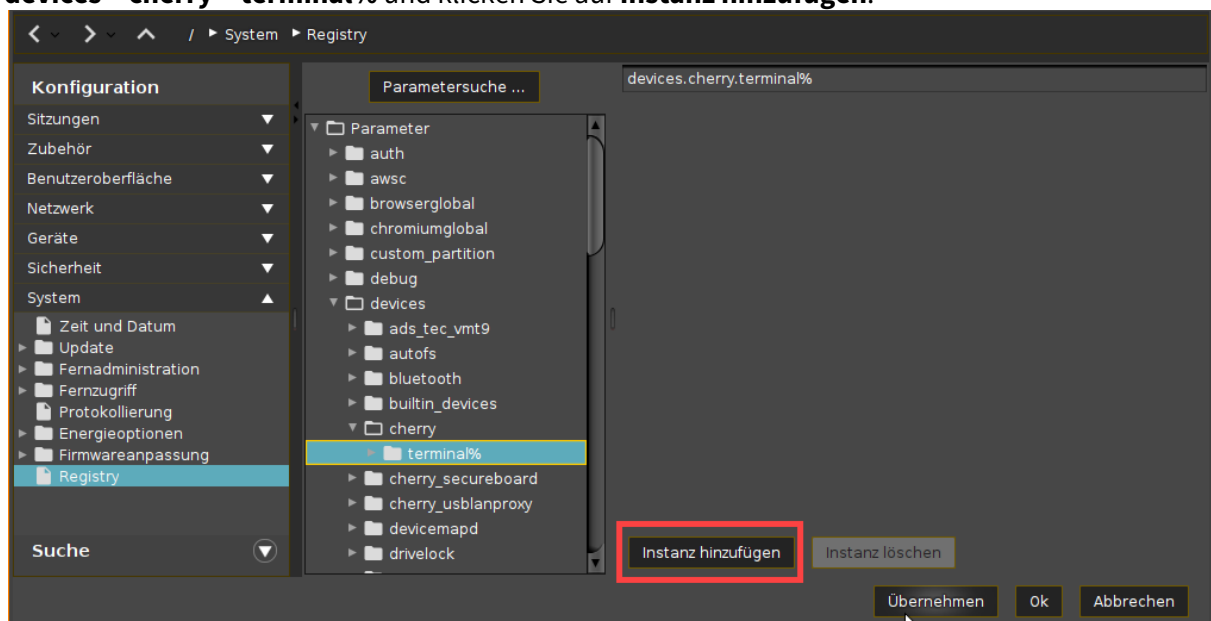
konfigurieren. Siehe dazu die Anleitung unten.

## 8. Speichern Sie die Einstellungen.

## Konfiguration auf Ihrem IGEL OS Gerät

Für jedes Kartenterminal muss eine Instanz der Vorlage `devices.cherry.terminal%` erstellt und konfiguriert werden. Standardmäßig ist keine konfiguriert, so dass die Funktion im Grunde deaktiviert ist. Um eine Instanz hinzuzufügen und zu konfigurieren, gehen Sie wie folgt vor:

1. Gehen Sie im IGEL Setup oder im Konfigurationsdialog in der UMS auf **System > Registry > devices > cherry > terminal%** und klicken Sie auf **Instanz hinzufügen**.

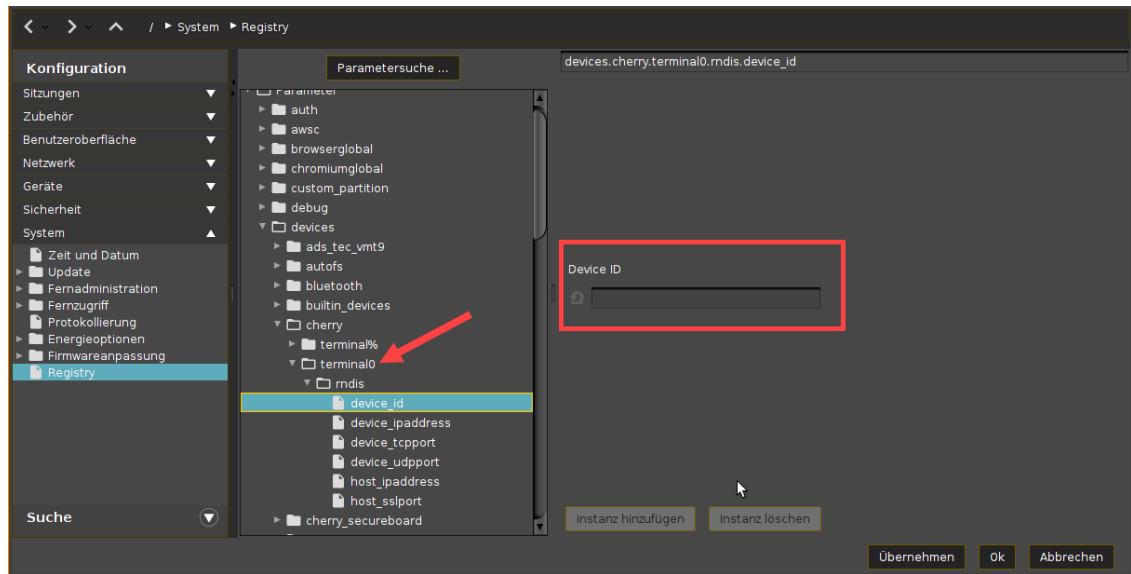


Für die hinzugefügte Instanz konfigurieren Sie Folgendes:

2. Wenn mehrere ST-1506-Geräte angeschlossen sind, konfigurieren Sie zu Unterscheidungszwecken den Registry Key `devices.cherry.terminal%.rndis.device_id`. Er kann leer bleiben, wenn nur ein Kartenterminal unterstützt werden soll.

Geben Sie hier an:

- eine MAC-Adresse des Kartenterminals (Um sie herauszufinden, können Sie z. B. den Befehl `ifconfig` im lokalen Terminal verwenden oder sie direkt auf dem ST-1506 im Admin-Menü einsehen)  
ODER
- den Wert der udev-Eigenschaft `ID_NET_NAME_PATH` (Um ihn herauszufinden, können Sie z. B. den Befehl `udevadm info --export-db | less` verwenden)



3. Konfigurieren Sie die **IP-Adresse des Geräts:**

<b>Parameter</b>	Device IP address
<b>Registry</b>	devices.cherry.terminal%.rndis.device_ipaddress
<b>Typ</b>	string
<b>Wert</b>	192.168.42.42 (Standard)
<b>Hinweis</b>	<p>Hier geben Sie eine statische IP an, die Sie auf Ihrem ST-1506 über das Admin-Menü konfiguriert haben.</p> <ul style="list-style-type: none"> <li>• Sie können den Standardwert unverändert lassen, wenn Sie ihn auch auf Ihrem ST-1506 verwenden.</li> <li>• Wenn Sie mehrere ST-1506-Geräte angeschlossen haben, müssen Sie für jedes Kartenterminal eine andere IP konfigurieren.</li> </ul>

4. Konfigurieren Sie die **Host-IP-Adresse:**

<b>Parameter</b>	Host IP address
<b>Registry</b>	devices.cherry.terminal%.rndis.host_ipaddress
<b>Typ</b>	string

<b>Wert</b>	192.168.42.1 (Standard)
<b>Hinweis</b>	Dies ist die IP-Adresse, die Sie als <b>Gateway</b> auf Ihrem ST-1506 über das Admin-Menü angeben müssen.

5. Konfigurieren Sie bei Bedarf die folgenden Registry Keys:

<b>Parameter</b>	Device TCP port
<b>Registry</b>	devices.cherry.terminal%.rndis.device_tcpport
<b>Typ</b>	string
<b>Wert</b>	4742 (Standard)
<b>Hinweis</b>	<p>Dieser Port auf dem Host wird an denselben Port auf dem Gerät weitergeleitet.</p> <ul style="list-style-type: none"> <li>• Wenn Sie mehrere ST-1506-Geräte angeschlossen haben, müssen Sie für jedes Kartenterminal einen anderen Port konfigurieren.</li> </ul>
<b>Parameter</b>	Passed through device UDP port
<b>Registry</b>	devices.cherry.terminal%.rndis.device_udpport
<b>Typ</b>	string
<b>Wert</b>	4742 (Standard)
<b>Hinweis</b>	<p>Dieser Port auf dem Host wird an denselben Port auf dem Gerät weitergeleitet.</p> <ul style="list-style-type: none"> <li>• Wenn Sie mehrere ST-1506-Geräte angeschlossen haben, müssen Sie für jedes Kartenterminal einen anderen Port konfigurieren.</li> </ul>
<b>Parameter</b>	Host SSL port
<b>Registry</b>	devices.cherry.terminal%.rndis.host_sslport
<b>Typ</b>	string
<b>Wert</b>	leer (Standard)

**Hinweis**

Dieser Port auf dem Host wird an den Port 443 des Geräts weitergeleitet. Konfigurieren Sie diesen Registry Key, wenn Sie einen Webbrowser für die Fernverwaltung Ihrer ST-1506 Geräte verwenden.

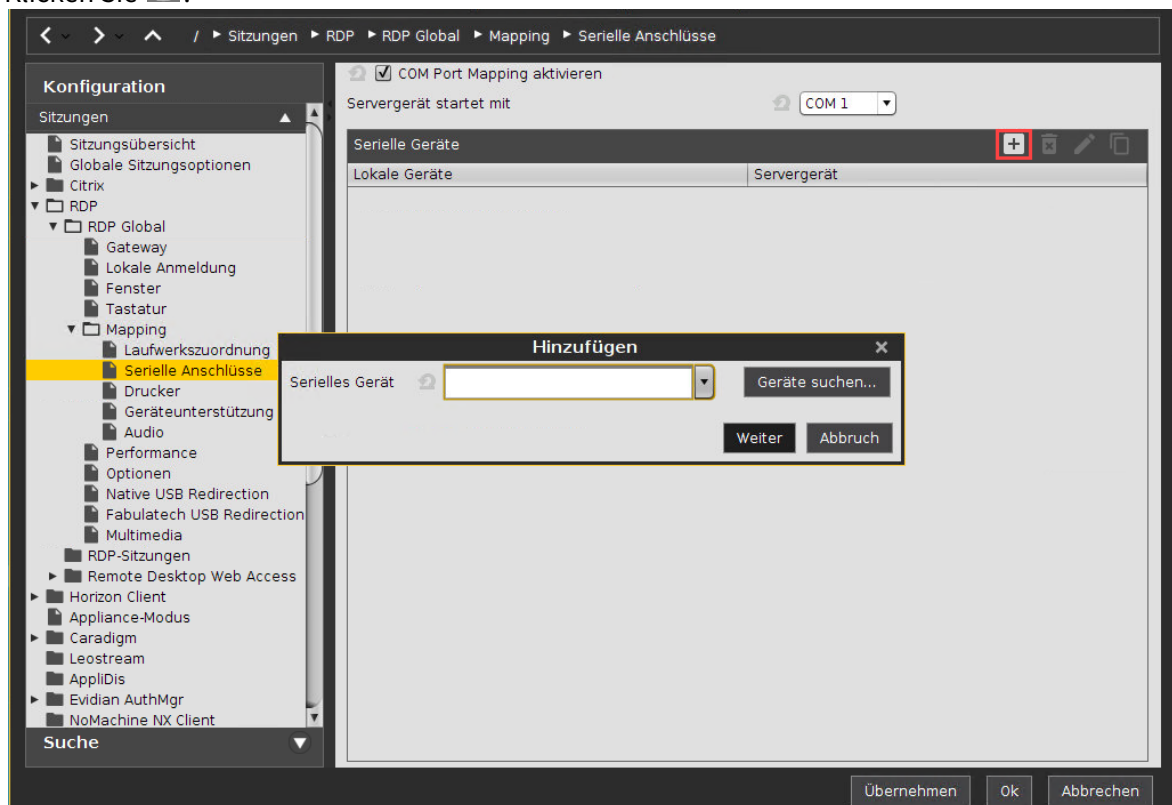
- Wenn Sie mehrere ST-1506-Geräte angeschlossen haben, müssen Sie für jede hinzugefügte Instanz einen anderen Port konfigurieren.

## Orga 910/920 M

Funktionalität	
USB ID:	0780:1202
Software:	CT-API von Orga
Gerät/Server-Anbindung:	COM Port Mapping

## Gerät konfigurieren

1. Klicken Sie **Sitzungen > RDP > RDP Global > Mapping > Serielle Anschlüsse** für RDP.
2. Wählen Sie **COM Port Mapping aktivieren**.
3. Klicken Sie .



4. Wählen Sie als neues serielles Gerät USB COM 1 ( `/dev/ttyUSB0` ).

## Server konfigurieren


1. Laden Sie den entsprechenden Treiber für Orga 910/920 M herunter von der Downloadseite: [http://healthcare-eid.ingenico.com/de/treiber\\_anleitungen.aspx](http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx)

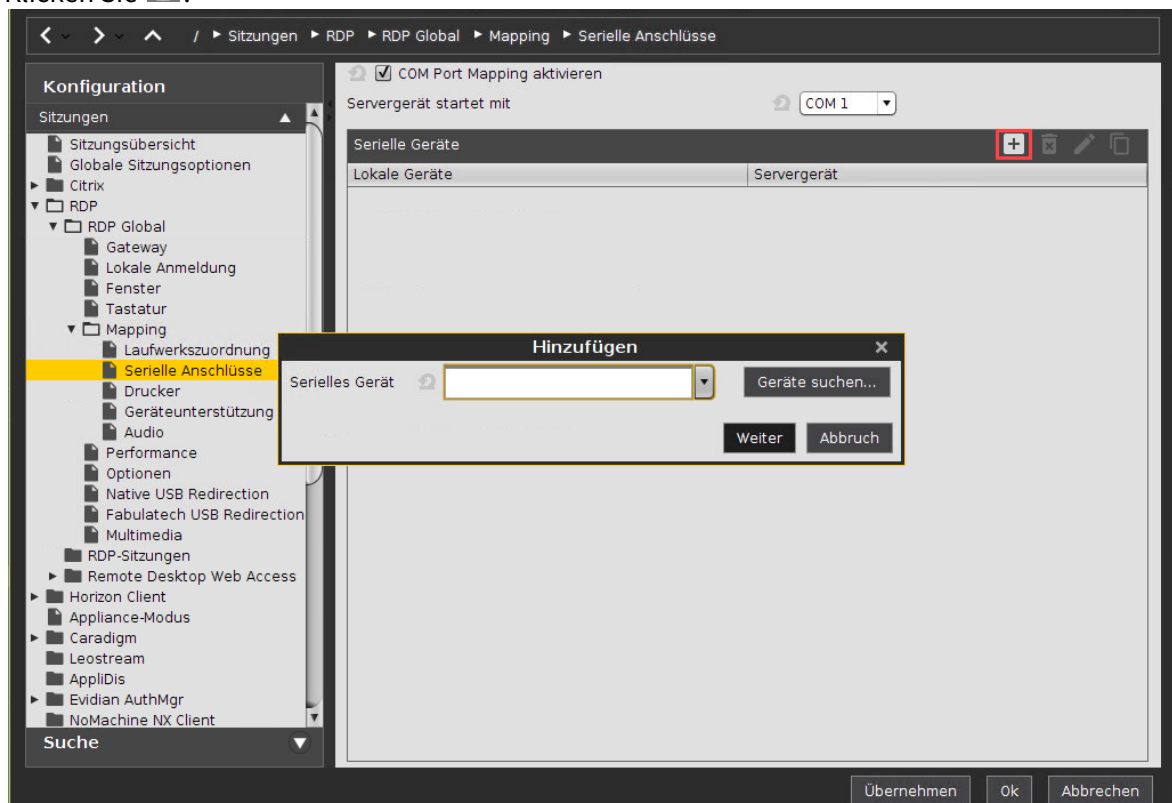
2. Installieren Sie den Treiber.

## Orga 6041 L eGK eHealth-BC S

Funktionalität	
USB ID:	0780:1302
Software:	CT-API von Orga
Gerät/Server-Anbindung:	COM Port Mapping

## Gerät konfigurieren

1. Klicken Sie **Sitzungen > RDP > RDP Global > Mapping > Serielle Anschlüsse** für RDP
2. Wählen Sie **Com Port Mapping aktivieren**.
3. Klicken Sie .



4. Wählen Sie als neues serielles Gerät USB COM 1 ( `/dev/ttyUSB0` ).

## Server konfigurieren


1. Laden Sie den entsprechenden Treiber für Orga 6041 L eGK eHealth-BC S herunter von der Downloadseite:  
[http://healthcare-eid.ingenico.com/de/treiber\\_anleitungen.aspx](http://healthcare-eid.ingenico.com/de/treiber_anleitungen.aspx)
2. Installieren Sie den Treiber.



## celectronic CARD STAR / medic2

### Kartenleser anschließen

- Schließen Sie den Kartenleser an den seriellen Anschluss des Geräts an.

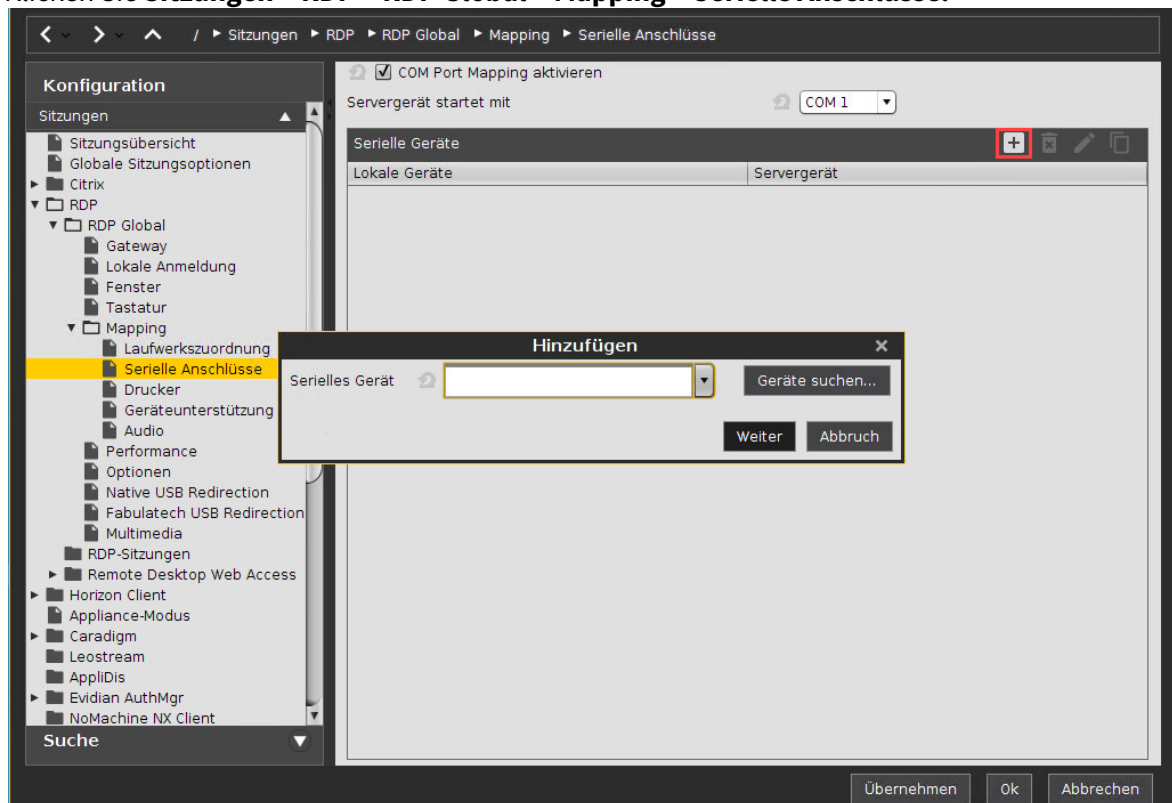
 Der Kartenleser muss auf den seriellen Anschluss eingestellt sein.

Funktionalität	
Software:	CT-API by celectronic
Gerät/Server-Anbindung:	COM Port Mapping

### Gerät konfigurieren

Fügen Sie den seriellen Anschluss hinzu, mit dem der Kartenleser verbunden ist:

1. Klicken Sie **Sitzungen > RDP > RDP Global > Mapping > Serielle Anschlüsse**.



2. Klicken Sie .
3. Wählen Sie ein **Serielles Gerät** (COM1, COM2,...).

## Server konfigurieren

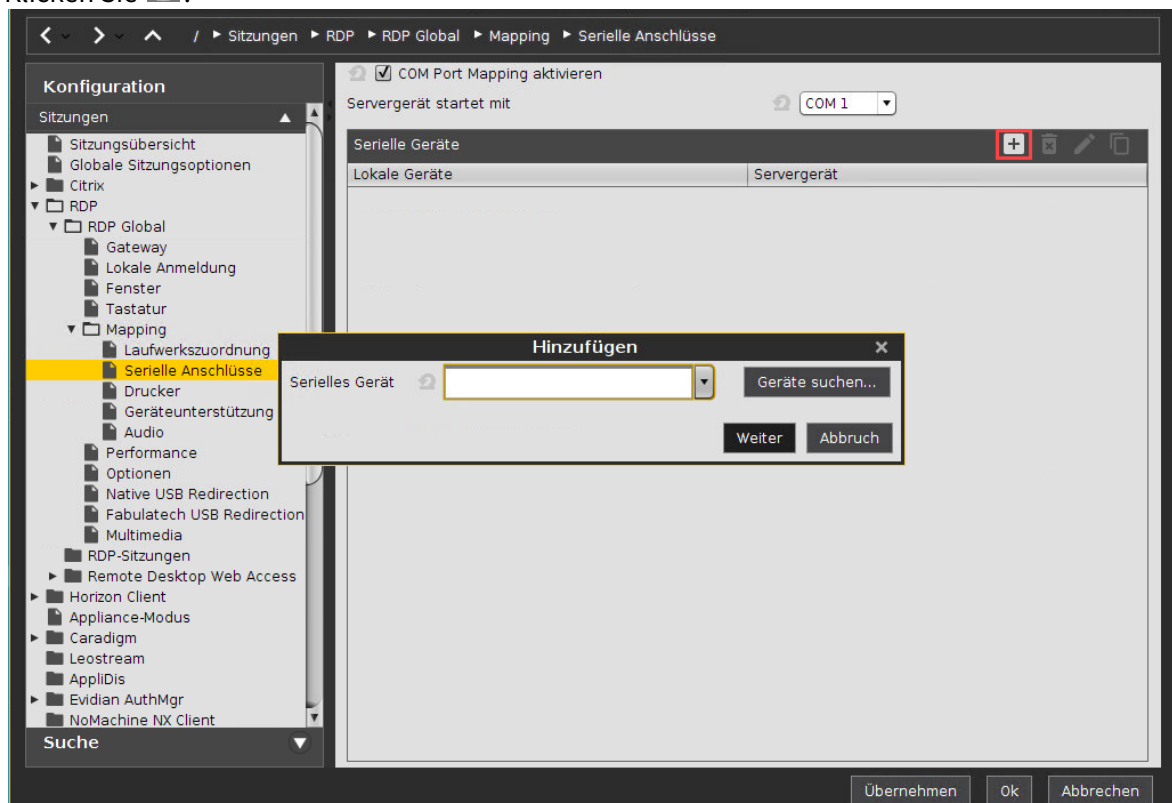
1. Laden Sie den passenden Treiber celectronic CARD STAR /medic2 von der Download-Seite herunter:  
<https://www.ccv.eu/>
2. Installieren Sie den Treiber.

## celectronic CARD STAR/ memo3

Funktionalität	
USB ID:	152a:8180
Software:	CT-API von celectronic
Gerät/Server-Anbindung:	COM Port Mapping

### Gerät konfigurieren

1. Klicken Sie **Sitzungen > RDP > RDP Global > Mapping > Serielle Anschlüsse** für RDP
2. Wählen Sie **Com Port Mapping aktivieren**.
3. Klicken Sie **+**.



4. Wählen Sie als neues serielles Gerät USB COM 1 ( `/dev/ttyUS0` ).


### Server konfigurieren.

1. Laden Sie den CT-API-Treiber für celectronic CARD STAR memo3 herunter von der Downloadseite: <https://www.ccv.eu/>

2. Installieren Sie den Treiber.


## Mobilgeräte-Zugriff verwenden

Sie können auf Daten, die sich auf Mobilgeräten befinden, via USB zugreifen, etwa um die Daten in einer Sitzung bereitzustellen.

 **Feature mit eingeschränktem Support!** Das Feature "Mobilgeräte-Zugriff" hat eingeschränkten Support. Es wird ohne Mangelgewähr angeboten. Support für diese Funktion erfolgt ausschließlich unverbindlich und auf "Best-Effort-Basis" (nach bestem Wissen und Gewissen).

Die folgenden Gerätearten können verwendet werden:

- Smartphones mit Android (via MTP / PTP) oder iOS
- Tablet mit Android (via MTP / PTP) oder iOS
- Digitalkameras

 Die Funktionalität kann je nach Geräteversion und Version des Betriebssystems abweichen.


## Umgebung

- IGEL Universal Desktop (UD) mit IGEL OS 10.04.100 oder höher
- IGEL Universal Desktop Converter 3 (UDC3) mit IGEL OS 10.04.100 oder höher
- UD Pocket mit IGEL OS 10.04.100 oder höher
- Um das Feature via UMS zu konfigurieren, ist UMS 5.08.110 oder höher erforderlich


- 
- [Mobilgeräte-Zugriff aktivieren \(see page 774\)](#)
  - [Mobilgeräte-Zugriff deaktivieren \(see page 775\)](#)
  - [Ein Mobilgerät in einer Sitzung bereitstellen \(see page 776\)](#)
  - [Mobilgeräte anschließen \(see page 777\)](#)
  - [Fenster "Mobilgeräte-Zugriff USB" in Sitzung öffnen \(see page 778\)](#)
  - [Verzeichnisse und Dateien lokal betrachten \(see page 780\)](#)
  - [Mobilgeräte sicher entfernen \(see page 782\)](#)

## Mobilgeräte-Zugriff aktivieren

1. Stellen Sie sicher, dass in IGEL Setup alle Einstellungen unter **System > Update > Firmwareupdate** korrekt sind.  
Der **Pfadname auf dem Server** muss auf die aktuelle Firmwareversion zeigen. Dies ist erforderlich, da das Softwarepaket für Mobilgeräte-Zugriff zuerst heruntergeladen werden muss, bevor das Feature installiert werden kann.
2. Gehen Sie zu **System > Firmwareanpassung > Features** und aktivieren Sie **Mobilgeräte-Zugriff USB**.
3. Bestätigen Sie den Warndialog mit **Ok**.
4. Klicken Sie **Ok**, um die Einstellung zu speichern.
5. Starten Sie das Gerät neu.  
Nach dem Neustart wird das Softwarepaket für das Feature "Mobilegeräte-Zugriff" heruntergeladen und installiert.
6. Wenn der Mobilgeräte-Zugriff dauerhaft aktiviert sein soll, stellen Sie sicher, dass unter **Zubehör > Mobilgeräte-Zugriff** die Einstellung **Autostart** aktiviert ist. Weitere Startoptionen sind im Handbuch unter Mobilgeräte-Zugriff beschrieben.

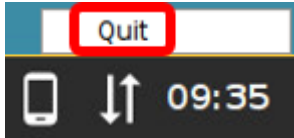
 Wenn Sie den Mobilgeräte-Zugriff im Appliance-Modus verwenden möchten, müssen Sie Autostart aktivieren oder einen Hotkey festlegen. Autostart wird empfohlen.

7. Konfigurieren Sie die Startoptionen für Mobilgeräte-Zugriff gemäß Ihren Anforderungen.
8. Wenn Sie als einzige Startoption **Autostart** ausgewählt haben, starten Sie das Gerät neu.

Wenn der Mobilgeräte-Zugriff aktiviert ist, wird in der Taskleiste das Smartphone-Symbol  angezeigt. Bei Sitzungen im Appliance-Modus ist die Sitzungssteuerleiste verfügbar; siehe [Fenster "Mobilgeräte-Zugriff USB" in Sitzung öffnen](#) (see page 778).

## Mobilgeräte-Zugriff deaktivieren

► Klicken Sie mit der rechten Maustaste auf das Smartphone-Symbol in der Taskleiste, und wählen Sie im Kontextmenü **Beenden**.



## Ein Mobilgerät in einer Sitzung bereitstellen

Die Zuordnung eines Laufwerks zu einem Mobilgerät kann in einer Sitzung auf zwei Weisen erfolgen:

- Per dynamischer Laufwerkszuordnung
- Per statischer Laufwerkszuordnung

### Dynamische Laufwerkszuordnung

Bei der dynamischen Laufwerkszuordnung wird Ihrem Mobilgerät automatisch ein Laufwerk zugewiesen. Die Verzeichnisse und Dateien auf Ihrem Mobilgerät sind dann unter diesem Laufwerk zugänglich.

1. Gehen Sie in IGEL Setup zu **Geräte > Speichergeräte > Hotplug-Speichergerät** und aktivieren Sie **Hotplug-Speichergerät**.
2. Setzen Sie **Laufwerkszuordnung** auf 'Dynamisch'.
3. Klicken Sie **Ok**.

Sie können auf die Verzeichnisse und Dateien auf Ihrem Mobilgerät wie mit einem normalen Hotplug-Speichergerät zugreifen.

Weitere Informationen finden Sie im Handbuchkapitel Hotplug-Speichergerät.

### Statische Laufwerkszuordnung

Bei der statischen Laufwerkszuordnung wird dem Mobilgerät ein benutzerdefinierter Laufwerksbuchstabe zugeordnet.

1. Wenn die Sitzung im Vollbildmodus ausgeführt werden soll, gehen Sie in IGEL Setup zu **Benutzeroberfläche > Desktop** und aktivieren Sie **Sitzungssteuerleiste**.
2. Wenn die Sitzung im Vollbildmodus oder im Appliance-Modus ausgeführt werden soll, stellen Sie sicher, dass unter **Zubehör > Mobilgeräte-Zugriff** die Einstellung **Autostart** aktiviert ist.
3. Gehen Sie zum Bereich **Mapping** der jeweiligen Sitzungsart. Beispiel: Bei RDP-Sitzungen wäre der Pfad **Sitzungen > RDP > RDP Global > Mapping > Laufwerkszuordnung**.
4. Aktivieren Sie **Laufwerkszuordnung aktivieren**.
5. Klicken Sie , um das Fenster **Hinzufügen Laufwerksordnung** zu öffnen.
6. Aktivieren Sie das Kontrollkästchen **Aktiv**, um die Verbindung zum Laufwerk aktivieren.
7. Wählen Sie ein **Ziellaufwerk**.
8. Geben Sie im Feld **Lokaler Laufwerkpfad** den Pfad `/media` ein.
9. Klicken Sie **Ok**.

Sie können auf die Verzeichnisse und Dateien auf Ihrem Mobilgerät wie mit einem normalen Hotplug-Speichergerät zugreifen.



## Mobilgeräte anschließen

1. Wenn der Mobilgeräte-Zugriff nicht schon gestartet wurde, konfigurieren Sie eine der in IGEL Setup unter **Zubehör > Mobilgerätezugriff** verfügbaren Startoptionen.
2. Schließen Sie Ihr Mobilgerät an Ihren Thin Client an.
3. Erlauben Sie auf Ihrem Mobilgerät die Dateiübertragung, z. B. **Transfer Files** (Android-Smartphones) oder **Trust The Computer** (Apple iPhones).  
Die Verzeichnisse von Ihrem Mobilgerät werden eingebunden.

Weiterführende How-tos:

- [Verzeichnisse und Dateien lokal betrachten](#) (see page 780)
- [Mobilgeräte sicher entfernen](#) (see page 782)

## Fenster "Mobilgeräte-Zugriff USB" in Sitzung öffnen

### Bei Sitzungen ohne Vollbildmodus

► Klicken Sie auf das Symbol , um das Fenster **Mobilgeräte-Zugriff USB** zu öffnen. Sie haben die Möglichkeit, die Verzeichnisse und Dateien auf Ihrem Mobilgerät zu betrachten oder das Mobilgerät sicher zu entfernen; siehe [Mobilgeräte sicher entfernen](#) (see page 782).

### Bei Sitzungen im Vollbildmodus

Bei Sitzungen, die im Vollbildmodus laufen, können Sie die Sitzungssteuerleiste verwenden, um das Fenster **Mobilgeräte-Zugriff USB** zu öffnen.

1. Bewegen Sie den Mauszeiger an den oberen Bildschirmrand. Die Sitzungssteuerleiste erscheint.

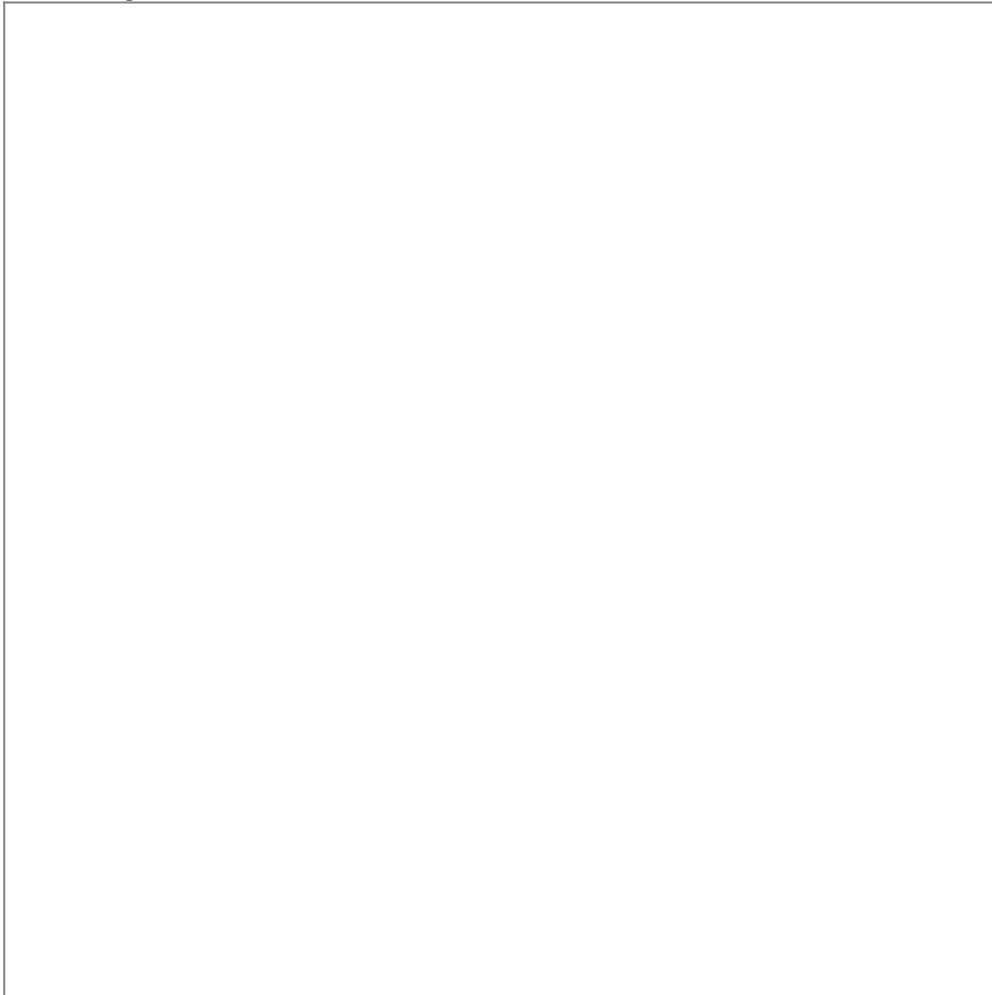


2. Klicken Sie auf das Smartphone-Symbol. Das Fenster **Mobilgeräte-Zugriff USB** erscheint. Sie haben die Möglichkeit, die Verzeichnisse und Dateien auf Ihrem Mobilgerät zu betrachten oder das Mobilgerät sicher zu entfernen.

### Bei Sitzungen im Appliance-Modus

Bei Sitzungen, die im Appliance-Modus laufen, können Sie die Sitzungssteuerleiste verwenden, um das Fenster **Mobilgeräte-Zugriff USB** zu öffnen.

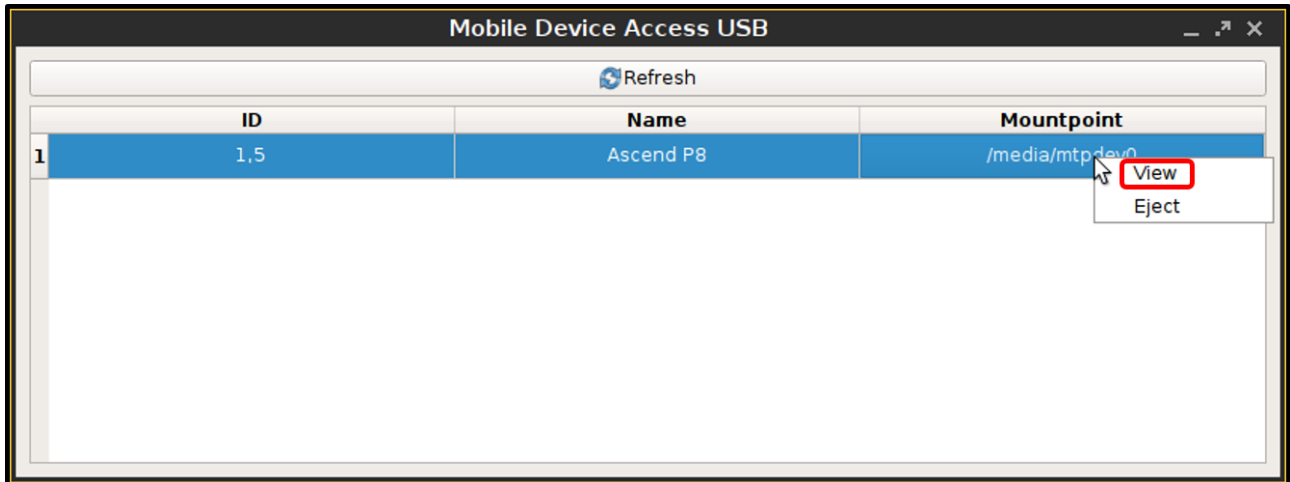
1. Bewegen Sie den Mauszeiger an den oberen Bildschirmrand.  
Die Sitzungssteuerleiste erscheint.



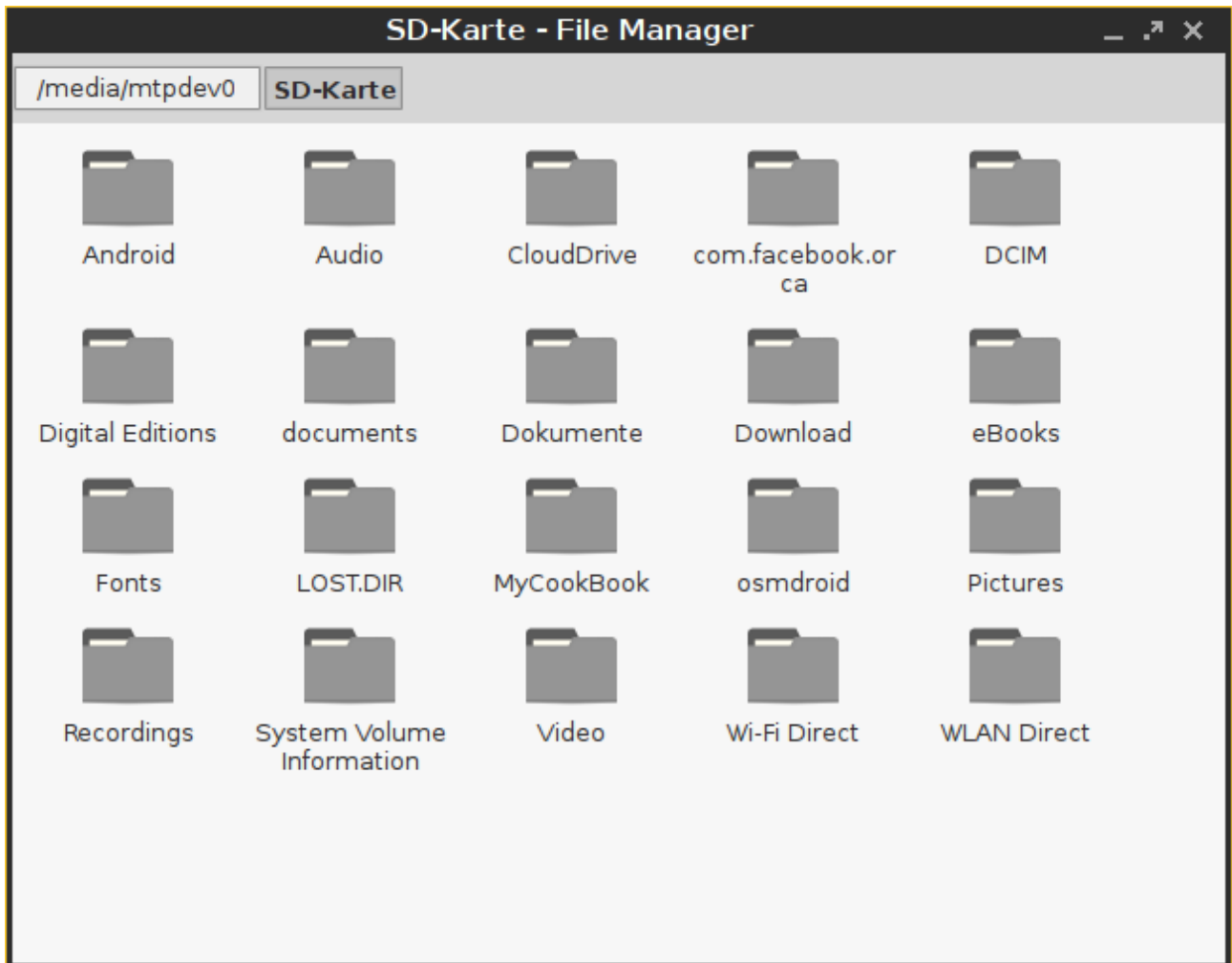
2. Klicken Sie auf das Smartphone-Symbol.  
Das Fenster **Mobilgeräte-Zugriff USB** erscheint.  
Sie haben die Möglichkeit, die Verzeichnisse und Dateien auf Ihrem Mobilgerät zu betrachten oder das Mobilgerät sicher zu entfernen.

## Verzeichnisse und Dateien lokal betrachten

- Wählen Sie im Kontextmenü die Option **Anzeigen**.



Die Verzeichnisse, die sich auf Ihrem Smartphone befinden, werden angezeigt. Der Zugriff ist rein lesend, das heißt Sie können die Verzeichnisse und Dateien nur ansehen, aber nicht verändern.



## Mobilgeräte sicher entfernen

- ▶ Wählen Sie im Kontextmenü des betreffenden Geräts die Option **Auswerfen**.



## Austauschen der Funktion von Maustasten (z. B. Verwendung einer Evoluent Maus)

Die Zuordnung der Maustasten für *Evoluent Mouse 3* ändert sich zwischen Firmware Version 5.04.130 und 5.05.100.

### Problem

Benutzer haben sich an die Zuordnung gewöhnt, da sie bis zur Version 5.04.130 bestand, deswegen möchten Sie die Zuordnung in Version 5.05.100.0 beibehalten.

### Lösung

#### A. Manuelle Analyse der Zuordnung und Festlegung, wie sie angepasst werden muss:

1. Öffnen Sie einen lokalen Terminal.
2. Finden Sie die Maus-ID: `xinput list`

Die Ausgabe sollte ungefähr wie folgt aussehen: | `Virtual core pointerid=2[master pointer (3)]` | `- Virtual core XTEST pointer id=4[slave pointer (2)]` | `- Logitech USB Optical Mouse id=10[slave pointer (2)]` - `Virtual core keyboardid=3[master keyboard (2)]` - `Virtual core XTEST keyboard id=5[slave keyboard (3)]` - `Power Buttonid=6[slave keyboard (3)]` - `Video Busid=7[slave keyboard (3)]` - `Power Buttonid=8[slave keyboard (3)]` - `Sleep Buttonid=9[slave keyboard (3)]` - `Logitech USB Keyboardid=11[slave keyboard (3)]` - `Logitech USB Keyboardid=12[slave keyboard (3)]`

3. Finden Sie Ihre Maus und ihre ID in der Ausgabe (hier: Logitech USB Optical Mouse, id=10).
4. Überprüfen Sie die Anzahl der Tasten in der Tastenbelegung: `xinput get-button-map [ID]` (wobei ID die ID Ihrer Mausvorrichtung ist).
5. Überprüfen Sie nun, welche Tastennummer für die entsprechende Taste eingestellt ist: `xev`  
Es erscheint ein Testfenster.
6. Klicken Sie mit der Taste, die Sie austauschen möchten, in das Fenster. Suchen Sie nach der Tastennummer in der Terminal Ausgabe: `ButtonPress event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25542794, (114,113), root:(2884,634), state 0x10, button 1, same_screen YES` `ButtonRelease event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw 0x0, time 25542898, (114,113), root:(2884,634), state 0x110, button`

```
1, same_screen YES ButtonPress event, serial 39, synthetic NO,
window 0x3200001, root 0xae, subw 0x0, time 25543218, (114,113),
root:(2884,634), state 0x10, button 3, same_screen YES ButtonReleas
e event, serial 39, synthetic NO, window 0x3200001, root 0xae, subw
0x0, time 25543330, (114,113), root:(2884,634), state 0x410, button
3, same_screen YES
```

Im oberen Beispiel wurden die Tastennummern 1 und 3 verwendet.

#### B. Die Zuordnung der Maustasten auf dem lokalen Gerät ändern:

1. Legen Sie eine neue Tastenbelegung für die Maus in **Setup > System > Firmwareanpassung > Eigene Kommandos > Desktop > Finales Desktopkommando** fest.
2. Tauschen Sie die Tasten in der Übersicht. Um z. B. die Tasten 1 und 3 zu tauschen, ändern Sie die Einstellungen von `xinput set-button-map [ID] 1 2 3 4 5 6 7` zu `xinput set-button-map [ID] 3 2 1 4 5 6 7`

#### C. Die Zuordnung automatisch über ein UMS Profil ändern:

Da die ID der Maus auf jedem Client unterschiedlich sein kann, können Sie den Befehl nicht wie in B 2. gezeigt verwenden, sondern müssen ein Skript verwenden, das automatisch das richtige Eingabegerät zuordnet.

1. Führen Sie den folgenden Befehl in einem lokalen Terminal aus: `xinput --list`
2. Notieren Sie sich den kompletten Namen der Maus.
3. Erstellen Sie ein Profil in **Setup > System > Firmwareanpassung > Eigene Kommandos > Desktop > Finales Desktopkommando** mit einem **Eigenen Kommando**: `MouseID=$(xinput --list --id-only 'NAME OF MOUSE') xinput set-button-map $MouseID 3 2 1 4 5 6 7`
4. Ersetzen Sie NAME DER MAUS mit dem Namen der Maus, wie in Schritt C 1. festgelegt.



## Natürliches Scrollen (umgekehrte Scrollrichtung) in IGEL OS verwenden

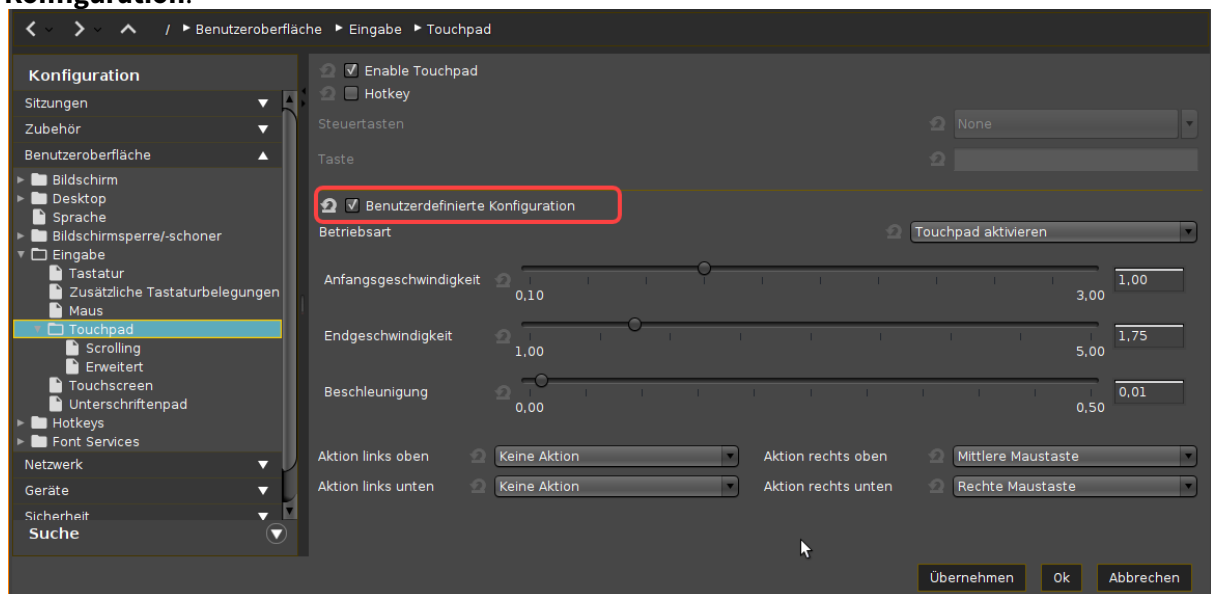
Auf IGEL OS Geräten verwenden Sie statt einer Maus ein Touchpad und möchten die Scrollrichtung umkehren, um ein natürliches Scrollen zu ermöglichen – wobei sich der Bildschirminhalt synchron zur Bewegung der Finger auf dem Touchpad bewegt.

### Problem

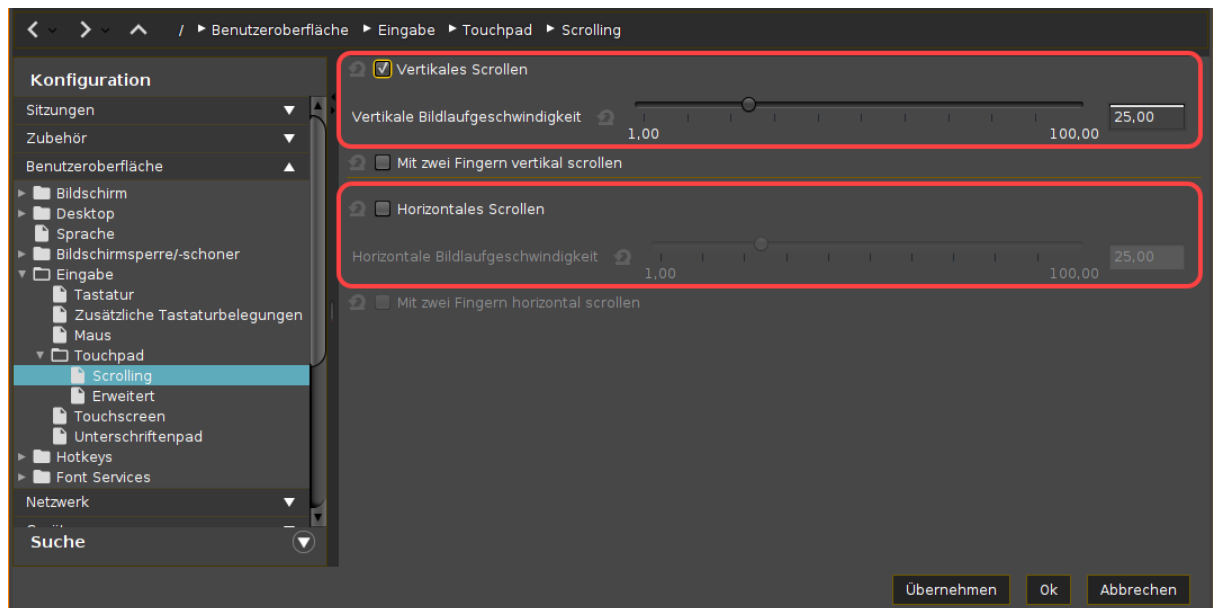
Im IGEL Setup gibt es keinen Parameter "Reverse Scrolling".

### Lösung

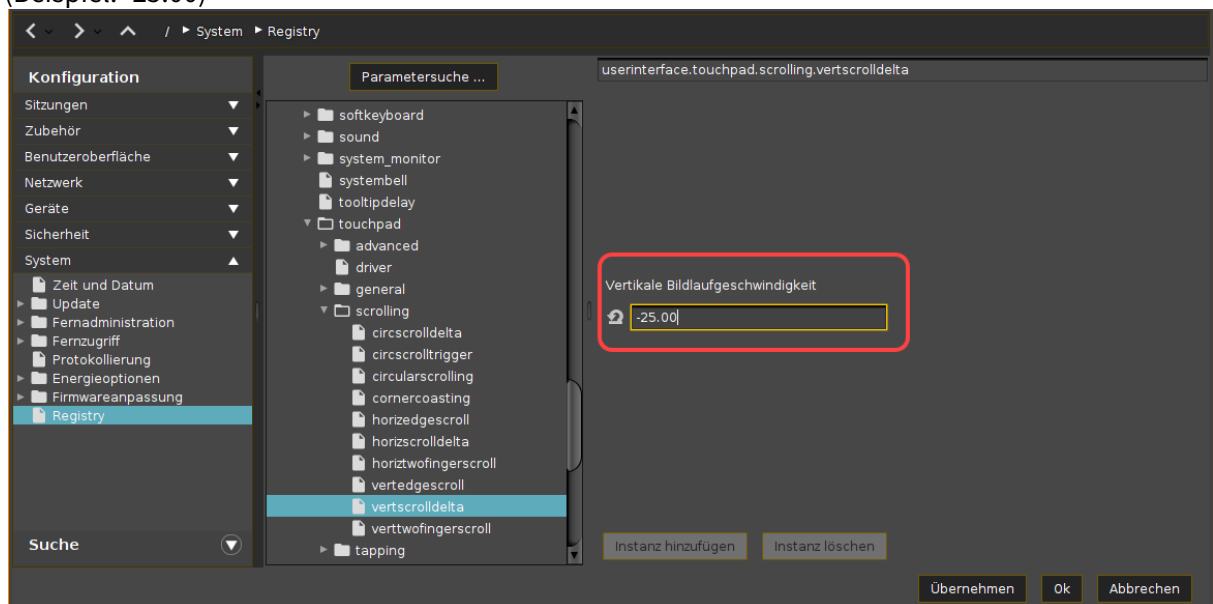
1. Öffnen Sie entweder lokal oder in der UMS die Gerätekonfiguration.
2. Gehen Sie auf **Benutzeroberfläche > Eingabe > Touchpad** und aktivieren Sie **Benutzerdefinierte Konfiguration**.



3. Bestimmen Sie unter **Scrolling** die **vertikale Bildlaufgeschwindigkeit** und, falls erforderlich und unterstützt, die **horizontale Bildlaufgeschwindigkeit**. (Standard: 25,00)



4. Gehen Sie auf **System > Registry > userinterface > touchpad > scrolling > vertscrolldelta** und/oder **horzscrolldelta**.
5. Um die umgekehrte Scrollrichtung zu aktivieren, ändern Sie den Wert auf einen negativen Wert. (Beispiel: -25.00)



Wenn Sie die normale Scrollrichtung wieder aktivieren möchten, ändern Sie den Wert einfach wieder auf den positiven Wert.


6. Speichern Sie die Einstellungen und starten Sie das Gerät neu.



## Einen seriellen Barcodescanner verbinden

### Barcodescanner über einen COM-Port verbinden

1. Bestimmen Sie, an welchem COM-Port des Geräts der Barcodeleser physikalisch angeschlossen ist.
2. Öffnen Sie das IGEL Setup und gehen Sie unter **System > Registry > Geräte > serial > inputattach** und aktivieren Sie den relevanten Schlüssel entsprechend dem verwendeten COM-Port:
  - COM1 ( `/dev/ttyS0` ): **devices.serial.inputattach.com0.enabled**
  - COM2 ( `/dev/ttyS1` ): **devices.serial.inputattach.com1.enabled**
  - COM3, COM4 ...: Fügen Sie eine neue Instanz hinzu, indem Sie auf **devices.serial.inputattach.com% > Instanz hinzufügen** gehen und definieren Sie den entsprechenden Port, z. B. `/dev/ttyS2` für COM3.
3. Wenn der Baud des Geräts von 9600 (Standard) abweicht, geben Sie den richtigen Baud unter **devices.serial.inputattach.com0.baud** ein.

 Mit den meisten Barcodelesegeräten kann man den Baud durch Scannen eines spezifischen Barcodes ändern.
4. Klicken Sie im Setup auf **Übernehmen** oder **Ok**, um die neuen Einstellungen zu übernehmen. Um sicherzustellen, dass die neuen Einstellungen wirksam sind, können Sie das Gerät neu starten.
5. Überprüfen Sie, ob der Barcodescanner funktioniert.


### Barcodescanner über USB verbinden

Wenn der Barcodescanner über USB verbunden ist, besteht die Herausforderung darin, das Gerät zu identifizieren, das ihm zugeordnet ist. Abhängig von Ihrem spezifischen Gerät und Ihrer Umgebung kann die Laufleistung variieren. Beginnen Sie mit der [einfachen Vorgehensweise](#) (see page 788). Wenn Sie Glück haben, wird es das tun. Wenn nicht, fahren Sie mit dem [erweiterten Verfahren](#) (see page 789) fort.

#### Einfache Vorgehensweise

1. Verbinden Sie den Barcodescanner mit einem USB-Port. Dies löst ein Ereignis aus, das protokolliert und von `dmesg` gemeldet wird.
2. Öffnen Sie ein Terminal auf Ihrem Endgerät. Weitere Informationen über das Geräteterminal finden Sie unter **Terminals**.
3. Um die richtige Gerätedatei zu finden, geben Sie `dmesg | grep tty` in das Terminal ein. Wenn Sie Glück haben, wird die relevante Gerätedatei aufgelistet. Ihr Name ist entweder `ttyUSB<NUM>` oder `ttyACM<NUM>`. Beispiel: `ttyUSB0`  
Wenn die relevante Gerätedatei nicht aufgelistet ist, versuchen Sie die erweiterte Vorgehensweise unten.

4. Öffnen Sie das IGEL Setup und gehen Sie unter **System > Registry > devices > serial > inputattach**.
5. Stellen Sie den Port **devices.serial.inputattach.com0.port** auf die gefundene Gerätedatei ein.  
Beispiel: Wenn die Gerätedatei `ttyUSB0` heißt, geben Sie `/dev/ttyUSB0` ein.
6. Aktivieren Sie **devices.serial.inputattach.com0.port**.
7. Wenn der Baud des Geräts von 9600 (Standard) abweicht, geben Sie den richtigen Baud unter **devices.serial.inputattach.com0.baud** ein.

 Mit den meisten Barcodelesegeräten kann man den Baud durch scannen eines spezifischen Barcodes ändern.

8. Klicken Sie **Übernehmen** oder **Ok**, um die neuen Einstellungen zu übernehmen. Um sicherzustellen, dass die neuen Einstellungen wirksam sind, können Sie das Endgerät neu starten.
9. Überprüfen Sie, ob der BarcodeScanner funktioniert.

### Erweiterte Vorgehensweise: Gerätedatei wurde auf Anhieb nicht gefunden.

Wenn die Gerätedatei nicht mit der einfachen Vorgehensweise gefunden werden konnte, versuchen Sie, den Gerätetreiber manuell zu laden. Da das explizite Laden des Treibers bei jedem Systemstart durchgeführt werden muss, muss ein eigener Befehl hinzugefügt werden.

1. Geben Sie im Terminal folgende Kommandos ein, einen nach dem anderen:


```
modprobe cdc-acm
```

```
dmesg | grep tty
```

Die relevante Gerätedatei wird aufgelistet. Ihr Name ist entweder `ttyUSB<NUM>`

oder `ttyACM<NUM>`. Beispiel: `ttyACM0`.

2. Öffnen Sie IGEL Setup und gehen Sie unter **System > Registry > devices > serial > inputattach**.
3. Stellen Sie den Port **devices.serial.inputattach.com0.port** auf die gefundene Gerätedatei ein.  
Beispiel: Wenn die Gerätedatei `ttyUSB0` ist, geben Sie `/dev/ttyACM0` ein.
4. Aktivieren Sie **devices.serial.inputattach.com0.enabled**.
5. Wenn der Baud des Geräts von 9600 (Standard) abweicht, geben Sie den richtigen Baud unter **devices.serial.inputattach.com0.baud** ein.

 Mit den meisten Barcodelesegeräten kann man den Baud durch scannen eines spezifischen Barcodes ändern.

6. Gehen Sie unter **System > Firmwareanpassung > Eigene Befehle > Basis** und geben Sie unter **Initialisierung** `modprobe cdc-acm` ein.
7. Klicken Sie **Übernehmen** oder **Ok**, um die neuen Einstellungen zu übernehmen. Um sicherzustellen, dass die neuen Einstellungen wirksam sind, können Sie das Gerät neu starten.
8. Überprüfen Sie, ob der BarcodeScanner funktioniert.

## DriveLock mit IGEL Geräten verwenden

### Thema

DriveLock ermöglicht es dem Systemadministrator, den Zugriff auf Wechseldatenträger innerhalb von Citrix- oder RDP-Sitzungen zu steuern. Dies ist für USB-Geräte möglich; ab IGEL OS Version 10.04.100 werden auch SATA-Geräte unterstützt.

### Problem

Wie kann man die DriveLock-Lösung in IGEL OS Geräte integrieren?

### Lösung

Nachdem Sie den Citrix- oder RDP-Server gemäß der Originaldokumentation konfiguriert haben, müssen Sie den virtuellen DriveLock-Kanal im Setup aktivieren. Sehen Sie die originale DriveLock Dokumentation.

#### DriveLock mit RDP verwenden:

1. Unter **Geräte > Speichergeräte > Hotplug-Speichergerät**, ändern Sie die Einstellungen wie folgt:
  - Deaktivieren Sie **dynamische Laufwerkzuordnung**
  - Stellen Sie die **Zahl der Laufwerke** auf 1 oder höher ein.
  - Aktivieren Sie **Eigener Laufwerksbuchstabe für Speicherlaufwerke**.
2. Unter **Sitzungen > RDP > RDP Global > Mapping > Laufwerkzuordnung**
  - Aktivieren Sie **Laufwerkzuordnung aktivieren**
3. Unter **Sitzungen > RDP > RDP Global > Mapping > Geräteunterstützung**
  - Aktivieren Sie **DriveLock Kanal**.

#### DriveLock mit Citrix verwenden:

1. Unter **Geräte > Speichergeräte > Hotplug-Speichergerät**, ändern Sie die Einstellungen wie folgt:
  - Deaktivieren Sie **dynamische Laufwerkzuordnung**
  - Stellen Sie die **Zahl der Laufwerke** auf 1 oder höher ein.
  - Aktivieren Sie **Eigener Laufwerksbuchstabe für Speicherlaufwerke**.
2. Unter **Sitzungen > Citrix > Citrix Global > Mapping > Laufwerkzuordnung**
  - Aktivieren Sie **Laufwerkzuordnung**.
3. Unter **Sitzungen > Citrix > Citrix Global > Mapping > Geräteunterstützung**
  - Aktivieren Sie **DriveLock Kanal**.

## Einschränkung der Montage von Hotplug-Speichergeräten auf IGEL Linux

### Ziel:


Sie möchten das Montieren von Hotplug-Speichergeräten einschränken

### Lösung:

Ab IGEL Linux Version 5.10.100 können Sie mit den folgenden Registrierungsschlüsseln das Montieren von Hotplug-Speichergeräten, abhängig von der Geräteklasse (Diskette, optisch, Festplatte, Flash, andere) deaktivieren.

- `devices.hotplug.enable_floppy`
- `devices.hotplug.enable_optical`
- `devices.hotplug.enable_harddisk`
- `devices.hotplug.enable_flash`
- `devices.hotplug.enable_other`

Diese sind alle vom Typ **bool**. Ihr Standardwert ist **true**. Wenn true, ist das Montieren von Volumen auf Disketten, optischen Medien, Festplatten, Flash-Speichergeräten und anderen Geräten entsprechend aktiviert.


 Auch wenn die obigen Einstellungen das Anbringen von Hotplug-Speichergeräten erlauben, können die folgenden Einstellungen diese dennoch einschränken:

- **Geräte > USB-Zugriffskontrolle**
- **Geräte > Speichergeräte > Hotplug-Speichergeräte**

Um das Montieren einer Geräteklasse Systemübergreifend zu deaktivieren:

1. Gehen Sie im Setup auf **System > Registry**.
2. In den **Parameter** Baum öffnen Sie **Devices > hotplug**.
3. Um das Montieren einer Geräteklasse zu verhindern, entfernen Sie das Häkchen bei **Hotplug [...]** **aktivieren** Parameter.

## When to Use USB Redirection

 Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.



## USB-Zugriffskontrolle konfigurieren

Sie können die Verwendung von USB-Geräten auf Ihrem Endgerät zulassen und verbieten. Spezifische Regeln für einzelne Geräteklassen sind möglich.

**!** Das Aktivieren der **USB-Zugriffskontrolle** und das Setzen der **Vorgaberegeln** auf **Verbieten** blockiert die Verwendung von USB-Geräten lokal und in der Sitzung und kann somit die Geräte deaktivieren, die die Benutzer benötigen. Aktivieren Sie daher die USB-Zugriffskontrolle nur, wenn Ihre Sicherheitsrichtlinie dies erfordert. Setzen Sie in diesem Fall die **Vorgaberegeln** auf **Verbieten** und konfigurieren Sie die **Erlauben**-Regeln für die erforderlichen USB-Geräte und USB-Geräteklassen. Es wird empfohlen, die Einstellungen für die **USB-Zugriffskontrolle** als letzten Schritt in der Gerätekonfiguration vorzunehmen. Bevor Sie die USB-Zugriffskontrolle aktivieren, überprüfen Sie, ob alle anderen Einstellungen für Drucker, Unified Communication, USB Redirection und Mapping-Einstellungen für USB-Geräte wie erwartet funktionieren. Beachten Sie, dass die USB-Zugriffskontrolle völlig getrennt von der USB-Umleitung für Remotesitzungen ist, siehe [When to Use USB Redirection](#) (see page 792). Beachten Sie auch, dass das Feature einen USB-Anschluss nicht physisch deaktiviert, d. h. die Spannungsversorgung wird weiterhin funktionieren.

## USB-Zugriffskontrolle aktivieren

1. Öffnen Sie das Setup und gehen Sie auf **Geräte > USB-Zugriffskontrolle**.
2. Aktivieren Sie die Option **Aktivieren**.
3. Wählen Sie die **Vorgaberegeln**. Die Vorgaberegeln legt fest, ob die Verwendung von USB-Geräten generell erlaubt oder verboten ist.
4. Erstellen Sie eine oder mehrere Regeln für Geräteklassen oder einzelne Geräte.

## Klassenregel erstellen

1. Um eine neue Regel zu erstellen, klicken Sie **+** im Bereich **Klassenregeln**.
2. Wählen Sie eine **Regel**. Die Regel gibt an, ob die Verwendung, der hier definierten Geräteklasse erlaubt oder verboten ist.
3. Unter **Klassen-ID** wählen Sie die Geräteklasse aus, für die die Regel gelten soll. Beispiel: **Audio, Drucker, Mass Storage**.
4. Unter **Name** geben Sie einen Namen für die Regel ein.
5. Klicken Sie **Weiter**.
6. Speichern Sie die Änderungen.  
Die Regel ist aktiv.

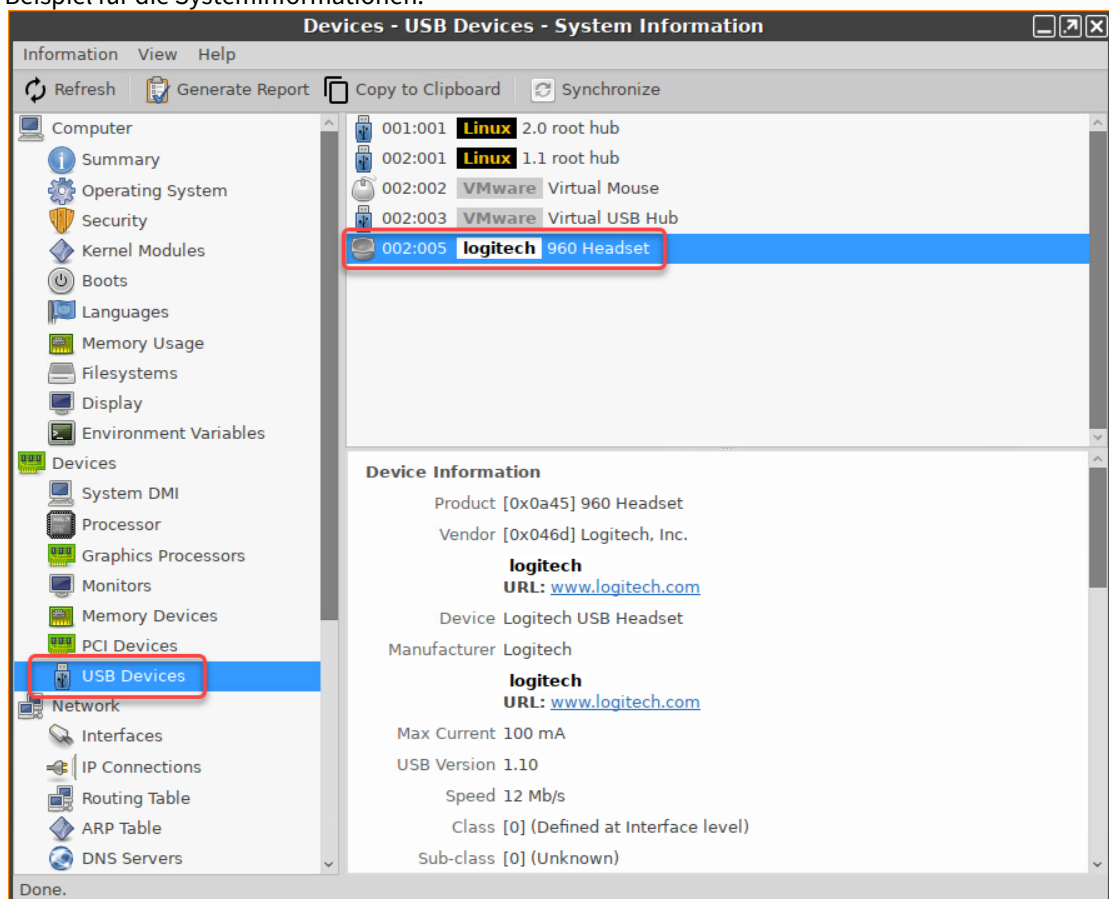
## Geräteregel erstellen

**i** Bei der Definition einer Regel muss mindestens eine der Eigenschaften, **Hersteller-ID** oder **Produkt-ID** oder **Uuid** angegeben werden.

1. Um eine neue Regel zu erstellen, klicken Sie **+** im **Klassenregeln** Bereich.
2. Wählen Sie eine **Regel**. Die Regel gibt an, ob die Verwendung, der hier definierten Geräteklasse erlaubt oder verboten ist.
3. Geben Sie die **Hersteller-ID** des Gerätes als hexadezimalen Wert an.
4. Geben Sie die **Produkt-ID** des Geräts als hexadezimalen Wert an.

### **i** Informationen zu USB-Geräten erhalten

Um die **Klassen-ID**, die **Unterklassen-ID**, die **Hersteller-ID** und die **Produkt-ID** des angeschlossenen USB-Geräts herauszufinden, können Sie die Funktion **Systeminformationen** verwenden. Weitere Informationen finden Sie unter Using "System Information" Function.  
Beispiel für die Systeminformationen:



Alternativ können Sie auch den Befehl `lsusb` (oder `lsusb | grep -i [Suchbegriff]`) im Terminal verwenden.

Beispiel für `lsusb` :

```
root@ITC005056930CAD:~# lsusb | grep -i logitech
Bus 002 Device 005: ID 046d:0a45 Logitech, Inc. 960 Headset
root@ITC005056930CAD:~#
```

5. Geben Sie die **Uuid** (Universal Unique Identifier) des Geräts an.
6. Geben Sie die **Zugriffsrechte** für das Gerät an.  
Mögliche Werte:
  - Globale Einstellung: Die Standardeinstellung für Hotplug-Speichergeräte wird angewendet; sehen Sie **Standardzugriffsrechte** unter **Geräte > Speichergeräte > Hotplug-Speichergerät**.
  - Nur Lesen
  - Lesen/Schreiben
7. Unter **Name**, geben Sie einen Namen für die Regel an.
8. Klicken Sie **Weiter**.
9. Speichern Sie die Änderungen.  
Die Regel ist aktiv.

### Beispiel

- Die festgelegte Regel verbietet dem Benutzer die Verwendung von USB-Geräten auf dem Gerät.
- Eine Klassenregel erlaubt die Verwendung von allen Eingabegeräten (HID = Human Interface Devices).
- Eine Geräteregele erlaubt die Verwendung von USB-Speichergeräten, mit der UUID 67FC-FDC6.
- Die Verwendung von allen anderen USB-Geräten, wie zum Beispiel Speichergeräte oder Drucker, ist verboten.

The screenshot shows the configuration interface for device rules. At the top, there are three settings: 'Aktivieren' (checked), 'Vorgaberegeln' (set to 'Verboten'), and 'Standardzugriffsrechte' (set to 'Lesen/Schreiben'). Below these are two tables: 'Klassenregeln' and 'Geräteregele'.

Regel	Klassen-ID	Name
Erlauben	HID (Human Interface Device)	Allow HID

Regel	Hersteller-ID	Produkt-ID	Uuid	Zugriffsrechte	Name
Erlauben			67FC-FDC6	Lesen/Schreiben	Storage Device

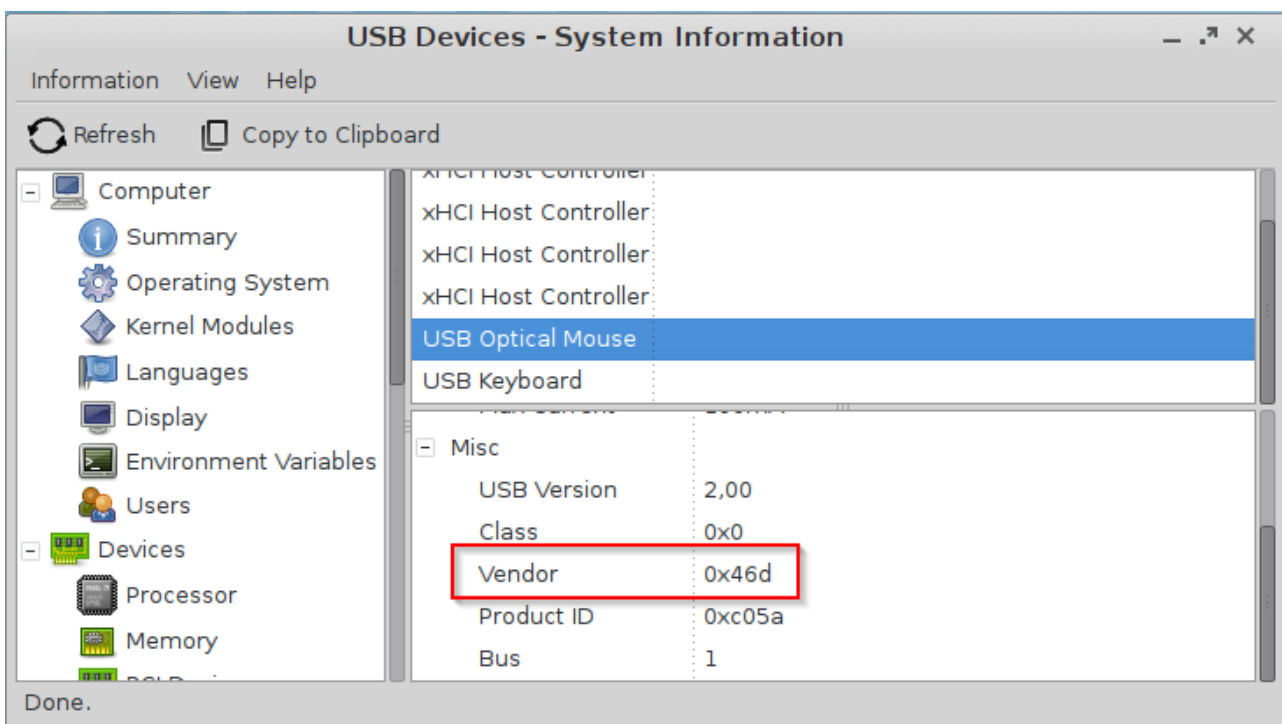
## Probleme mit USB-IDs in den USB-Geräteregeln

### Symptom

Die von Ihnen konfigurierten USB-Geräteregeln werden nicht wirksam.

### Problem

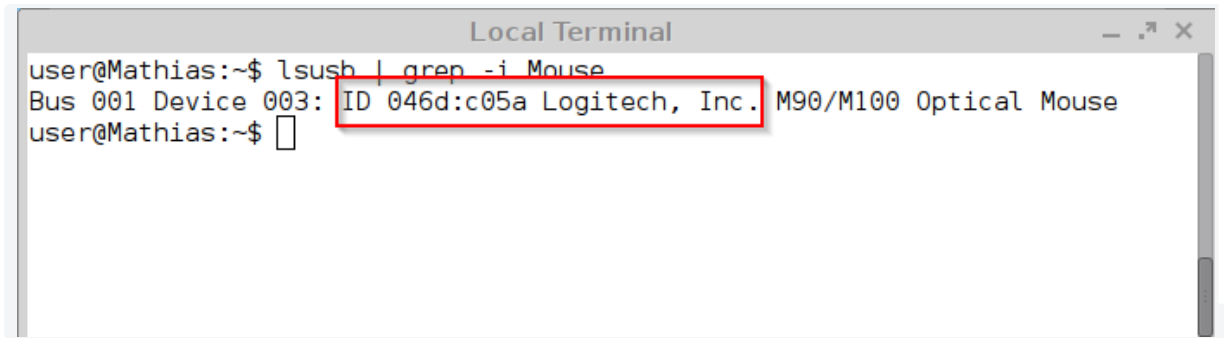
Das Tool **Systeminformationen** in IGEL OS bis zur Version 11.04.100 lässt führende Nullen bei USB-Hersteller-IDs und Produkt-IDs weg. Diese sind nur drei hexadezimale Ziffern lang dargestellt.



### Lösung

Wenn Sie dreistellige USB-IDs in den **Systeminformationen** sehen, verwenden Sie den Befehl `lsusb` :


1. Öffnen Sie **Lokales Terminal**.
2. Geben Sie den Befehl `lsusb` ein.
3. Suchen Sie nach dem betreffenden Gerät, möglicherweise mit `grep` , um in der `lsusb` -Ausgabe zu suchen: `lsusb | grep -i [search term]`




```
Local Terminal
user@Mathias:~$ lsusb | grep -i Mouse
Bus 001 Device 003: ID 046d:c05a Logitech, Inc. M90/M100 Optical Mouse
user@Mathias:~$
```

4. Verwenden Sie die vierstelligen IDs, die `lsusb` ausgibt.


## Fixing Touchpad Issues

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## How Do I Configure a Fujitsu PalmSecure Vein Scanner with IGEL OS?

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einsteilen um Ihr Verständnis.

## Virtual Background for Unified Communication Apps in IGEL OS

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.



## Drucker

- [So richten Sie auf IGEL OS einen lokalen Drucker für eine Citrix oder RDP Sitzung ein \(see page 802\)](#)
- [Druckerserver-Konfiguration \(see page 807\)](#)
- [Benutzerdefinierten CUPS-Treiber installieren \(see page 810\)](#)
- [Dynamic Selection of the Default Printer on IGEL OS \(see page 811\)](#)

## So richten Sie auf IGEL OS einen lokalen Drucker für eine Citrix oder RDP Sitzung ein

In diesem Artikel wird erklärt, wie man unter IGEL OS einen Standard-USB-Laser- oder Tintenstrahldrucker in eine Citrix- oder Remote Desktop (RDP)-Sitzung einbindet.

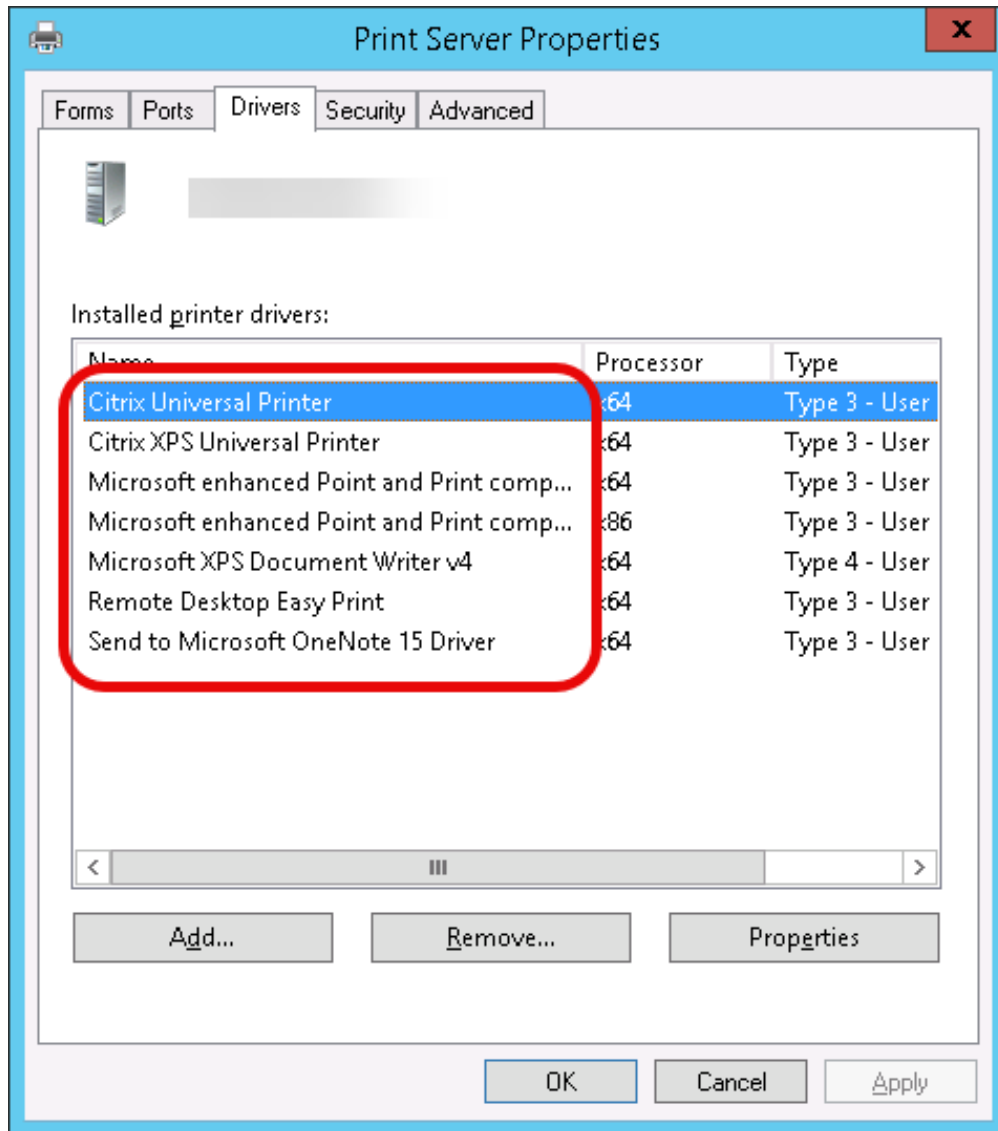
**i** Diese Methode funktioniert möglicherweise nicht mit Spezialdruckern (z. B. Etikettendruckern oder Thermodruckern). Wenn dies bei Ihrem Drucker nicht funktioniert, müssen Sie möglicherweise eine USB-Umleitung verwenden.

### Voraussetzungen

- Citrix: Installieren Sie den HP Color LaserJet 2800 Series PS-Treiber auf der Serverseite, um den lokalen Drucker auf Citrix-Sitzungen umzuleiten; siehe <https://support.citrix.com/article/CTX140208>.

### Drucker für Raw Redirection konfigurieren

1. Gehen Sie auf **Geräte > Drucker > CUPS > Drucker**.
2. Erstellen Sie einen neuen Drucker und vergeben Sie einen **Druckernamen**.
3. Wählen Sie den **Druckeranschluss** für Ihren Drucker.
4. Setzen Sie **Hersteller** auf **Generic**.
5. Setzen Sie **Druckernamen** auf **Raw Queue**.
6. Wechseln Sie zum Tab **Mapping in Sitzungen**.
7. Aktivieren Sie **Drucker in ICA-Sitzungen mappen** (für Citrix Sitzungen) or **Drucker in RDP-Sitzungen mappen**.
8. Aktivieren Sie **Benutzerdefinierten Windows Treibernamen verwenden**.
9. Geben Sie im Feld **Drucktreiber** einen der folgenden Treibernamen ein:
  - Wenn Sie den universellen Druckertreiber von Citrix verwenden wollen, geben Sie "Citrix Universal Printer" ein.
  - Wenn Sie einen anderen Druckertreiber verwenden möchten, öffnen Sie Ihr entferntes Windows-System und ermitteln Sie den genauen Namen des Treibers:



- Überprüfen Sie die Einstellungen in den Tabs **Allgemein** und **Mapping in Sitzungen** und klicken Sie dann Weiter.

**Hinzufügen** ✕

Druckername MeinDrucker

Allgemein Mapping in Sitzungen

Druckeranschluss USB-Schnittstelle

USB-Gerät 1. USB-Drucker

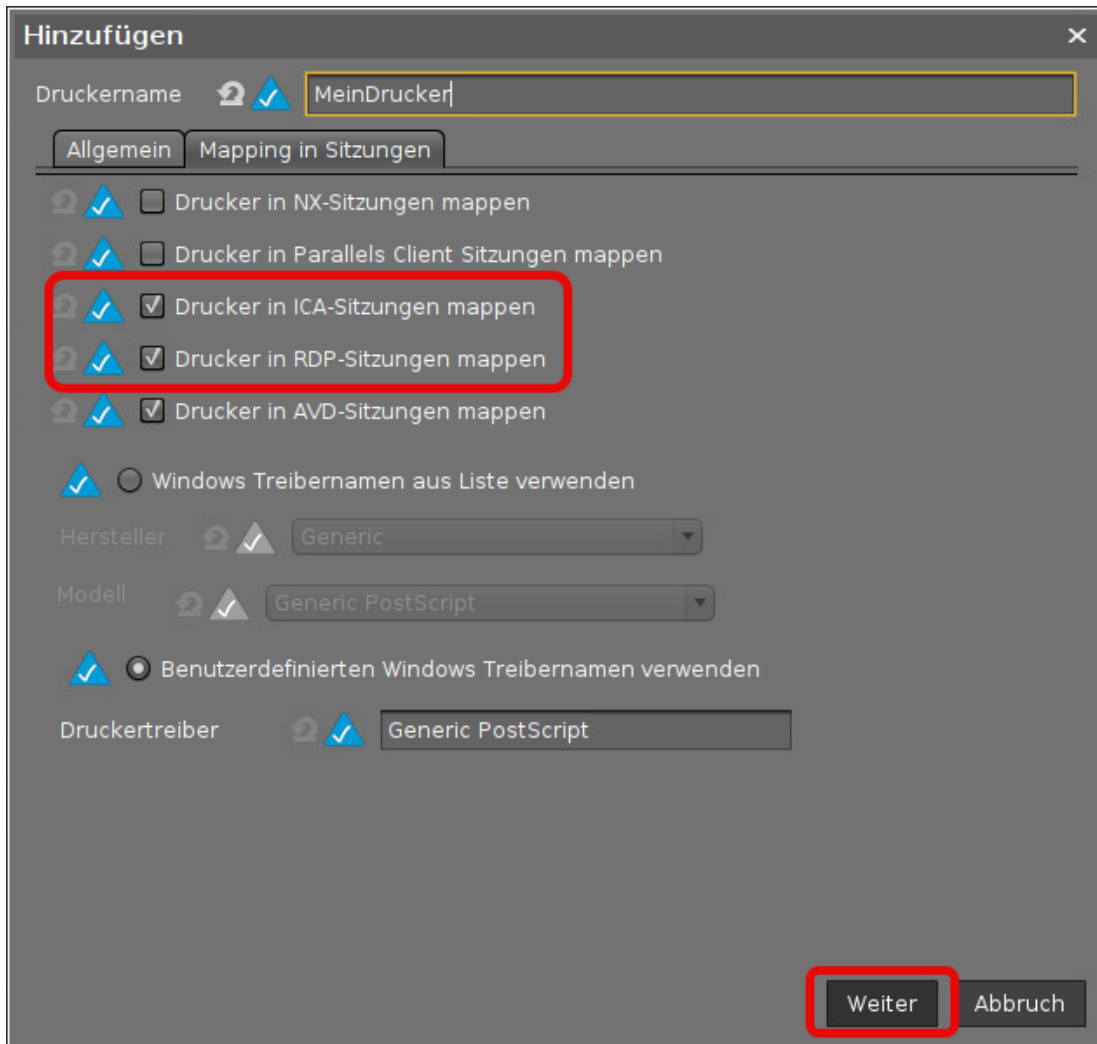
Hersteller Generic

Druckernamen Raw Queue

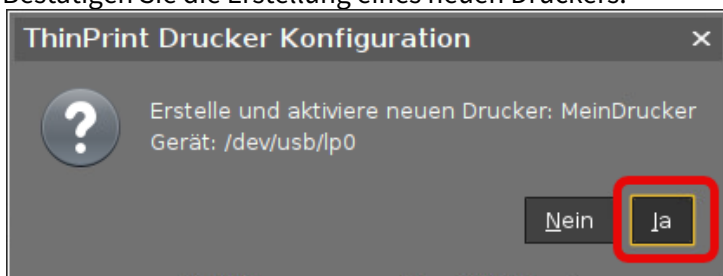
Standardpapiergröße Systemeinstellung

Drucker freigeben

Weiter Abbruch



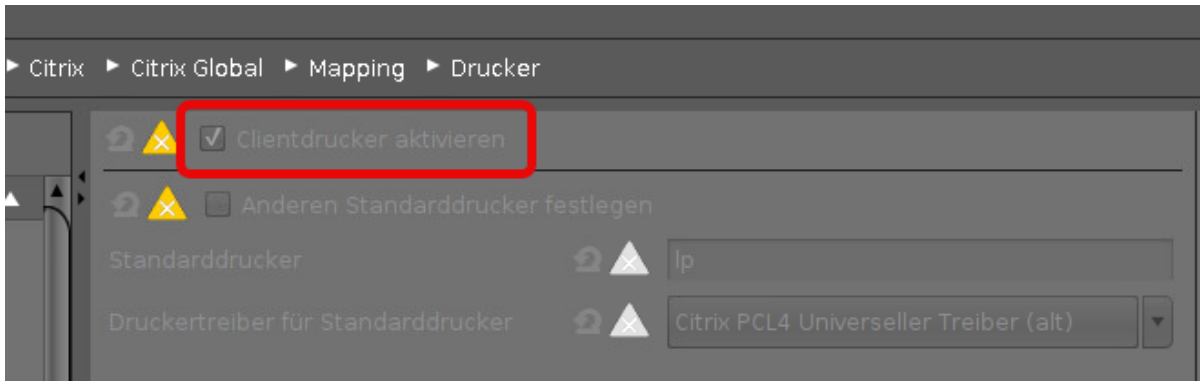
11. Bestätigen Sie die Erstellung eines neuen Druckers.



## Sitzung auf dem Client konfigurieren

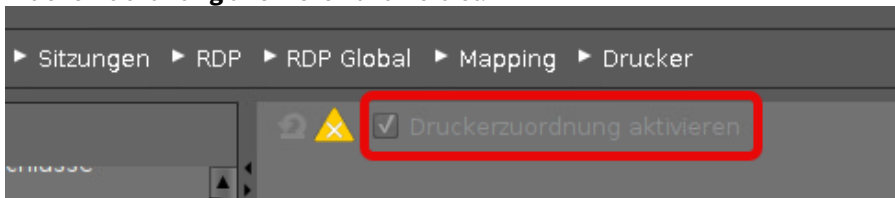
### Citrix

► Gehen Sie auf **Sitzungen > Citrix > Citrix Global > Mapping > Drucker** und stellen Sie sicher, dass **Clientdrucker aktivieren** aktiviert ist.



### RDP

► Gehen Sie auf **Sitzungen > RDP > RDP Global > Mapping > Drucker** und stellen Sie sicher, dass **Druckerzuordnung aktivieren** aktiviert ist.



## Druckertreiber serverseitig installieren (wenn nicht bereits vorhanden)

Der folgende Schritt ist nur erforderlich, wenn der Drucker nicht bereits auf dem Server ist.

► Starten Sie die ICA oder RDP Sitzung als Administrator und installieren Sie den Druckertreiber mit dem umgeleiteten Port "TS00x/ClientPort".

## Verwandte Informationen

- Drucker - CUPS-Drucker in IGEL OS konfigurieren, Abschnitt "Drucker in ICA-Sitzungen mappen"
- Drucker - CUPS-Drucker in IGEL OS konfigurieren, Abschnitt "Drucker in RDP-Sitzungen mappen"

## Druckerserver-Konfiguration

### Voraussetzungen

- IGEL OS Version 10 oder neuer
- Drucker mit integriertem PCL/PS Controller

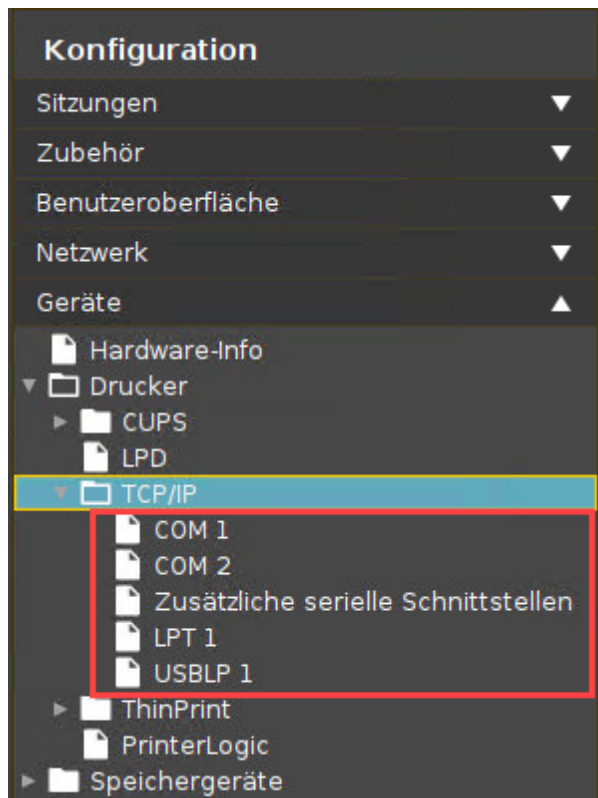
### Empfehlung

Weisen Sie dem IGEL Gerät eine feste IP-Adresse zu oder reservieren Sie sie über DHCP.

### Anleitung

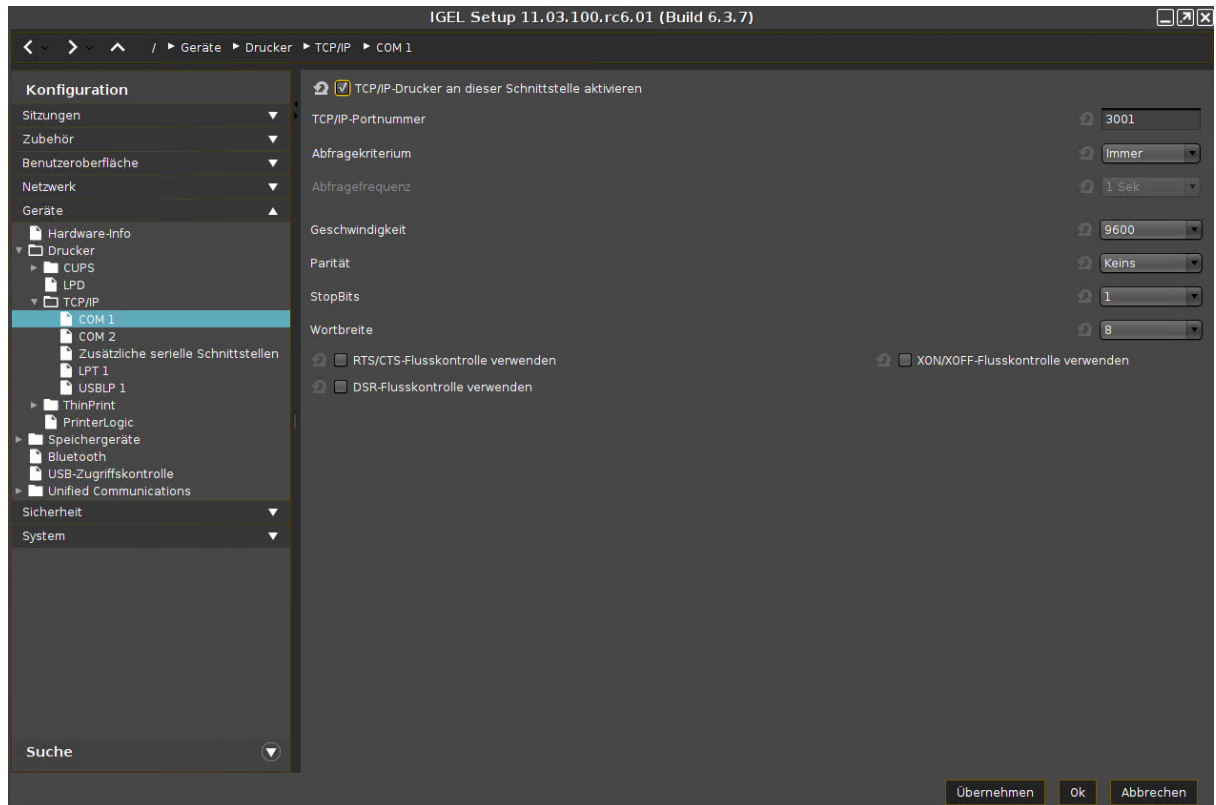
Um das IGEL Gerät als Druckerserver für lokal angeschlossene Drucker zu verwenden, führen Sie die folgenden Schritte aus:

1. Gehen Sie im IGEL Setup unter **Geräte > Drucker > TCP/IP**.
2. Wählen Sie den Port aus, an den der Drucker angeschlossen ist.
  - COM 1
  - COM 2
  - Zusätzliche serielle Schnittstellen
  - LPT 1
  - USBLP 1



3. Aktivieren Sie **TCP/IP-Drucker an dieser Schnittstelle aktivieren**.  
Geben Sie die **TCP/IP-Portnummer** ein, an der der Druckerserverdienst lauscht. (Standard für Windows: 9100)  
**Abfragekriterium** und **Abfragefrequenz** müssen nur angepasst werden, wenn es die Umgebung erfordert.
4. Klicken Sie **Übernehmen** oder **Ok**, um die Einstellungen zu speichern.





Der Drucker kann wie ein normaler Netzwerkdrucker installiert und von anderen Systemen verwendet werden.

## Benutzerdefinierten CUPS-Treiber installieren

### Voraussetzung

IGEL Linux v5 und höher.

### Problem

Ihr Drucker ist nicht in der CUPS-Standardkonfiguration enthalten.

### Lösung


Sie können einen benutzerdefinierten Treiber von Ihrem Hersteller installieren.


#### Die PPD-Treiber-Datei auf das Gerät kopieren

► Kopieren Sie die Treiberdatei (PPD-Datei) mit Hilfe des UMS-Dateiübertragungsmechanismus in den Ordner `/wfs`, siehe Dateien.


#### Einen neuen CUPS-Treiber hinzufügen

Nachdem Sie nun die Treiberdatei auf das Gerät kopiert haben, müssen Sie einen neuen Drucker hinzufügen und die PPD-Datei als Treiberdefinition festlegen. Gehen Sie dazu wie folgt vor:

 Eine detaillierte Beschreibung der CUPS-Konfigurationsoptionen finden Sie unter CUPS.

1. Gehen Sie im Setup unter **Geräte > Drucker > CUPS > Drucker**.
2. Klicken Sie , um zum Dialogfeld **Hinzufügen** zu gelangen.
3. Definieren Sie die folgenden Einstellungen:
  - **Druckername:** Name des Druckers.
  - **Drucker Anschluss:** Anschluss, an den der Drucker angeschlossen ist. Je nachdem, welchen Typ Sie wählen, müssen Sie zusätzliche Informationen angeben, z. B. Server und Port bei **TCP-Druckerport**.
  - **Hersteller:** Wählen Sie **Benutzerdefiniert**. Das Feld **Treiberdefinition** wird angezeigt.
  - **Treiberdefinition:** Geben Sie den kompletten Pfad zur PPD-Datei ein.
4. Klicken Sie **Ok**, um die Einstellungen zu speichern.
5. Starten Sie Ihr Gerät neu.

## Dynamic Selection of the Default Printer on IGEL OS

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## UD Pocket

- [UD Pocket von IGEL OS auf einem Dell WYSE ZX0D \(aka 7010\) Gerät ausführen \(see page 813\)](#)
- [UD Pocket auf Acer Chromebook C910 ausführen \(see page 814\)](#)
- [UD Pocket Seems to Break Microsoft Surface \(see page 816\)](#)
- [Vom UD Pocket auf Mac mini, MacBook Air 2018, MacBook Pro booten \(see page 818\)](#)
- [Wie kann ich meinen IGEL UD Pocket neu flashen? \(see page 819\)](#)

## UD Pocket von IGEL OS auf einem Dell WYSE ZX0D (aka 7010) Gerät ausführen

Hier erfahren Sie, welche Einstellungen Sie am Dell WYSE ZX0D (aka 7010) vornehmen müssen, um das Gerät mit einem UD Pocket starten zu können.

1. Starten Sie das Dell Gerät
2. Gehen Sie im BIOS auf die Registrierkarte **Erweitert**.
3. Aktivieren Sie **Mit USB starten**.
4. Ändern Sie die Startprioritäten, um die **USB Festplatte** zum Standard zu machen, indem Sie sie nach oben verschieben.
5. Sichern Sie die Einstellungen
6. Schließen Sie den UD Pocket an

Siehe Video:




Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=C0NWdjVE1RI>




## UD Pocket auf Acer Chromebook C910 ausführen

In diesem How-To lernen Sie, wie Sie den UD Pocket auf einem Acer Chromebook C910 ausführen. Dies erfordert die Installation einer BIOS-Erweiterung, die es dem Gerät ermöglicht, in ein alternatives Betriebssystem zu starten.

 Die hier beschriebenen Verfahren wurden mit dem Acer Chromebook C910 getestet; die Verfahren können je nach Chromebook-Typ unterschiedlich sein.

Weitere Informationen finden Sie unter [MrChromebox.tech](https://mrchromebox.tech)<sup>77</sup>.

### Das Gerät zum Starten von UD Pocket aktivieren

1. Stellen Sie sicher, dass eine WiFi Verbindung besteht; dies ist für das Herunterladen der SeaBios-Erweiterung notwendig.
2. Starten Sie in den Recovery Mode durch gleichzeitiges drücken von [ESC] +  (aktualisieren) +  (Power).  
Der Recovery Mode Bildschirm wird angezeigt, der angibt, dass das Betriebssystem defekt ist.
3. Drücken Sie [Ctrl] + [D] um in den Entwicklermodus zu gelangen.  
Der Entwicklermodus Bildschirm wird angezeigt, der bestätigt, dass die Betriebssystemverifizierung deaktiviert ist.
4. Öffnen Sie eine root-fähige Shell durch drücken von [Strg] + [Alt] +  (F2).
5. Melden Sie sich als `chronos` an; es ist kein Passwort erforderlich, es sei denn, es wurde eines festgelegt.
6. Wechseln Sie zu /tmp: `cd /tmp`.
7. Laden Sie das Utility-Skript für die ChromeOS Firmware herunter: `curl -LO https://mrchromebox.tech/firmware-util.sh`
8. Starten Sie das Skript mit root-Rechten: `sudo bash firmware-util.sh`
9. Geben Sie `1` ein um die erste Position zu wählen.
10. Geben Sie zur Bestätigung `y` ein.  
Die RW\_Legacy Firmware wird auf Ihr Gerät heruntergeladen.
11. Wenn der Download vollständig ist, drücken Sie [Enter].
12. Geben Sie `r` ein um den Neustart durchzuführen.  
Das Gerät startet neu in den Entwicklermodus.
13. Um vom UD Pocket zu starten, drücken Sie [Strg]+ [L].


---


<sup>77</sup> <https://mrchromebox.tech/>

### Von UD Pocket aus starten

1. Stellen Sie sicher, dass sich das Gerät im Entwicklermodus befindet. Dies sollte der Fall sein, wenn das Gerät gemäß den oben beschriebenen Verfahren konfiguriert wurde und seitdem keine Änderungen vorgenommen wurden, die den Entwicklermodus beeinflusst haben.
2. Drücken Sie [Strg] + [L] um vom UD Pocket aus zu starten.

## UD Pocket Seems to Break Microsoft Surface

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

 Please note that this device is not officially supported. Therefore, we can not offer any guarantee or support for the procedures described in this article.

### Tested Environment

The following information describes the exact environment on which the issue and the troubleshooting method have been tested. However, the method will probably work on similar versions.

- Microsoft Surface Book 1
- Windows 10 build 1903 4/25/2019 18362.267
- IGEL UD Pocket with IGEL OS 11.02.100

### Issue

After having booted successfully into UD Pocket once, the Microsoft Surface notebook is not able to boot into Windows anymore.

### Solution

With the following procedures, you can set your Microsoft Surface to boot from USB storage permanently or, alternatively, on-demand.

For detailed information, see [How do I use the BIOS/UEFI?](#)<sup>78</sup> by Microsoft.

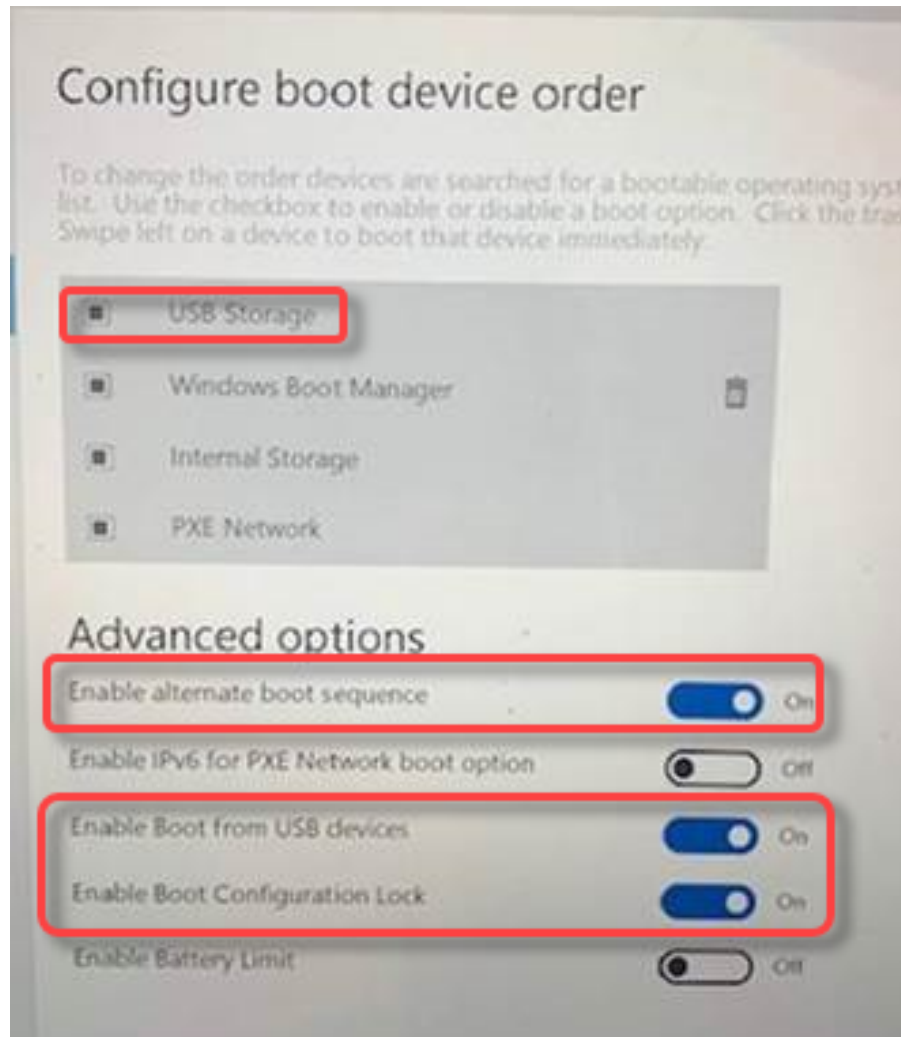
#### Enabling Boot from USB Storage Permanently

1. Ensure that your Microsoft Surface has shut down.
2. Press and hold down the volume + (up) button and at the same time, power up the Microsoft Surface.
3. When the Surface logo appears, release the volume + (up) button.  
The UEFI menu is displayed.
4. Under **Configure boot device order**, move **USB Storage** to the top using drag & drop.
5. Under **Advanced options**, change the settings as follows:
  - **Enable alternate boot sequence: On**
  - **Enable Boot from USB devices: On**
  - **Enable Boot Configuration Lock: On**Your UEFI settings should look like this:

---

<sup>78</sup> <https://support.microsoft.com/en-ae/help/4023532/surface-how-do-i-use-the-bios-uefi>





6. Exit the UEFI settings.
7. Insert the UD Pocket into the USB port of your Microsoft Surface.
8. Reboot your Microsoft Surface.  
Your Microsoft Surface boots from your UD Pocket.

### Booting from USB Storage On-Demand

1. Ensure that your Microsoft Surface has shut down.
2. Insert the UD Pocket into the USB port of your Microsoft Surface.
3. Press and hold down the volume + (up) button and at the same time, power up the Microsoft Surface.
4. When spinning dots appear beneath the Surface logo, release the volume + (up) button.  
Your Microsoft Surface boots from your UD Pocket.

## Vom UD Pocket auf Mac mini, MacBook Air 2018, MacBook Pro booten

### Lösung beruht auf Erfahrungen im Feld

Dieser Artikel stellt eine Lösung bereit, die nicht durch die IGEL Forschungs- und Entwicklungsabteilung geprüft wurde. Daher kann IGEL keinen offiziellen Support leisten. Soweit durchführbar, testen Sie die Lösung, bevor Sie diese in einer Produktivumgebung zum Einsatz bringen.

## Umgebung

- Mac-Geräte mit Apple T2 Security Chip, z.B. Mac mini, MacBook Pro, MacBook Air 2018, iMac Pro

## Problem

Der mit dem Apple T2 Security Chip implementierte Secure Boot erlaubt es nicht, Linux auf den oben genannten Geräten zu booten. Details finden Sie in der deutschsprachigen Übersicht <https://www.computerbase.de/2018-11/apple-t2-linux-installation-umgehung/>. Daher sind einige Konfigurationsänderungen auf diesen Geräten erforderlich, um vom UD Pocket booten zu können.

## Lösung

Es ist möglich, die Secure-Boot-Option über das Wiederherstellungsmenü zu deaktivieren. Gehen Sie dazu wie folgt vor:

1. Um das Wiederherstellungsmenü von macOS zu öffnen, halten Sie während des Bootvorgangs die Befehlstaste [⌘] + [R] gedrückt, sobald das Apple-Logo erscheint.
2. Unter **Dienstprogramme** wählen Sie **Startsicherheitsdienstprogramm**.
3. Verwenden Sie ein Administratorkonto, um die Secure-Boot-Option unter **Sicheres Starten > Ohne Sicherheit** zu deaktivieren.

Weitere Informationen über das Startsicherheitsdienstprogramm auf Mac-Geräten finden Sie unter <https://support.apple.com/de-de/HT208198>.

## Wie kann ich meinen IGEL UD Pocket neu flashen?

Aufgrund einer Fehlkonfiguration, eines fehlerhaft durchgeführten Updates oder aus einem anderen Grund kann es erforderlich sein, ein Re-Imaging des IGEL UD Pockets durchzuführen. Das Verfahren ist im Allgemeinen dasselbe wie bei der Installation des IGEL OS Creator (OSC). Der Unterschied besteht darin, dass Sie während der Installation Ihren UD Pocket als Zielgerät auswählen müssen, und nicht Ihren PC.

---

### Voraussetzungen

- PC mit 2 freien USB-Anschlüssen
- 1 USB-Stick mit 4 GB oder mehr ohne wichtige Daten (wird überschrieben)
- IGEL UD Pocket

### Das neue Image auf IGEL UD Pocket installieren

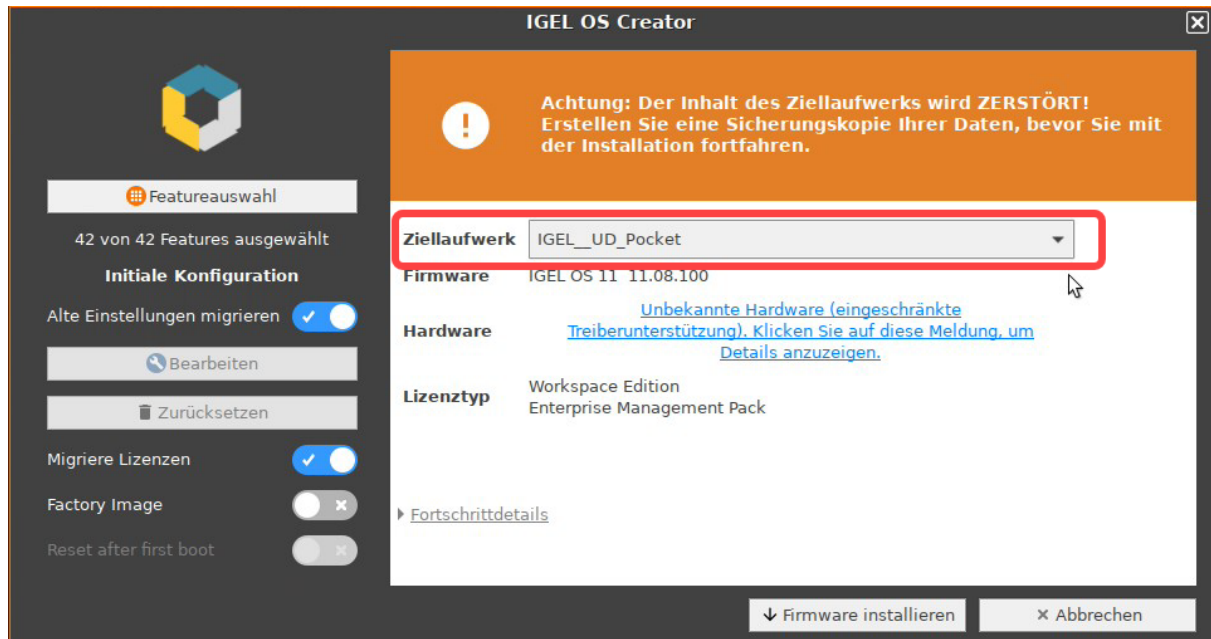
1. Zunächst müssen Sie einen IGEL OS Creator-Stick erstellen. Die Anleitung dazu finden Sie unter:
  - USB-Installationsmedium erzeugen (Windows)
  - USB-Installationsmedium erzeugen (Linux)
2. Falls nicht bereits aktiviert, aktivieren Sie das Booten von USB-Speichergeräten auf Ihrem PC, siehe Booteinstellungen.
3. Schließen Sie den erstellten IGEL OS Creator-Stick an den PC an.
4. Schließen Sie den IGEL UD Pocket an den PC an.
5. Schalten Sie den PC ein und stellen Sie sicher, dass Sie vom IGEL OS Creator-Stick booten.

6. Wählen Sie im Bootmenü die Option **Standard Installation + Recovery** aus.




7. Wählen Sie die Sprache für den Installationsvorgang aus.
8. Wählen Sie unter **Ziellaufwerk** Ihren UD Pocket aus.

⚠ Stellen Sie sicher, dass Sie **das richtige Zielgerät auswählen! Andernfalls werden die Daten auf Ihrem PC gelöscht!**  
Bei der Installation von IGEL OS über OSC werden alle Daten auf dem unter **Ziellaufwerk** ausgewählten Gerät zerstört. Achten Sie deswegen darauf, dass Sie keine Festplatte Ihres PCs versehentlich auswählen!

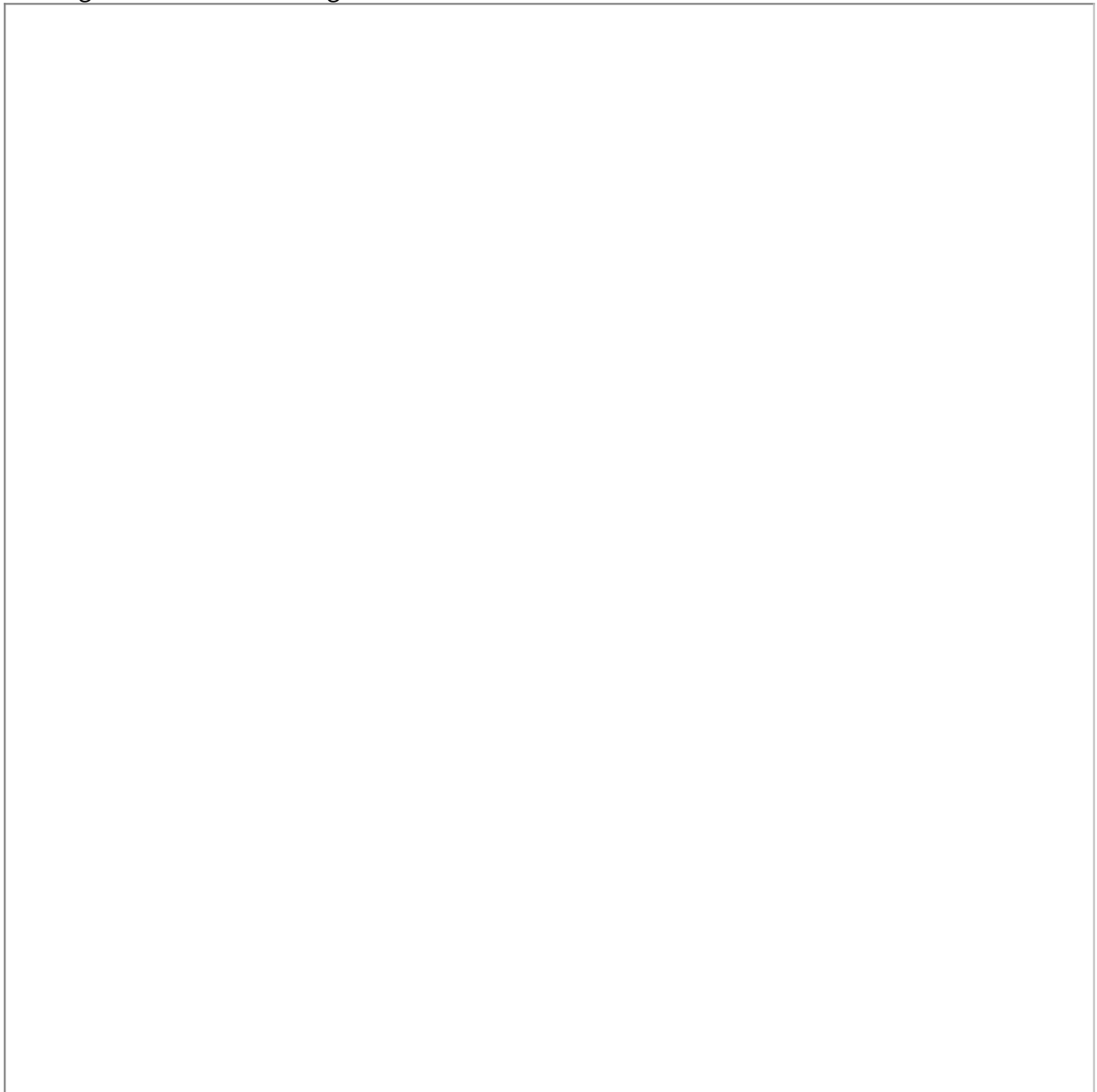


9. Wenn Ihr UD Pocket funktionsfähig ist und keine Fehler aufweist, lassen Sie die Option **Alte Einstellungen migrieren** aktiviert, um die vorherigen Einstellungen zu migrieren.

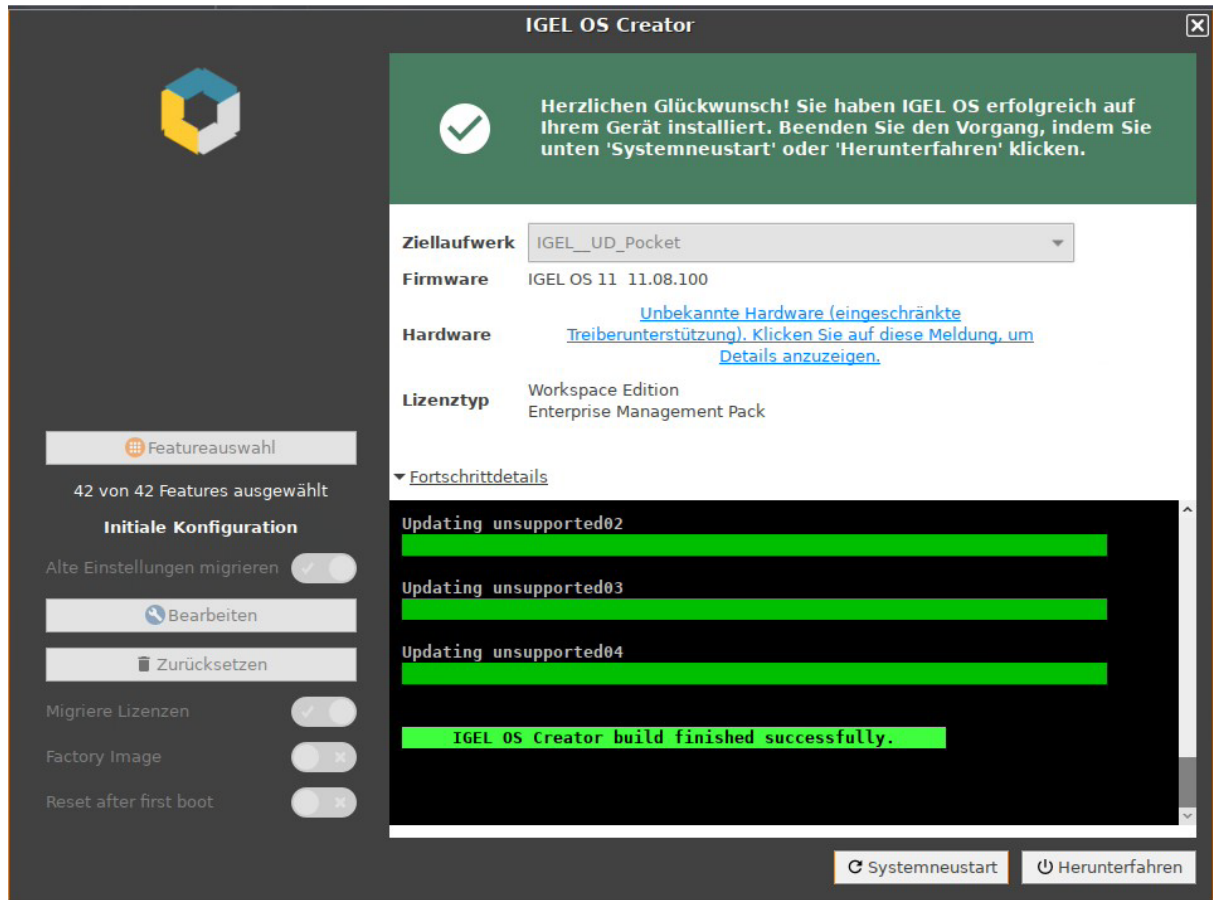
 Deaktivieren Sie die Option **Alte Einstellungen migrieren**, wenn Ihr UD Pocket Konfigurationsprobleme hat oder nicht mehr bootfähig ist.

10. Wenn Sie die vorhandenen Lizenzen weiterhin verwenden möchten, stellen Sie sicher, dass **Migriere Lizenzen** aktiviert ist.
11. Optionale Einstellungen:
- **Legacy-Installation erzwingen** (nur verfügbar, wenn der PC im UEFI-Modus gebootet hat)
  - **MS-DOS-Partitionierung erzwingen** (nur verfügbar, wenn der PC im UEFI-Modus gebootet hat)
  - **Featureauswahl**
  - **Bearbeiten / Zurücksetzen**
- Einzelheiten zu diesen Optionen finden Sie unter Installationsvorgang.
12. Klicken Sie auf **Firmware installieren**.  
Das Installationsprogramm richtet IGEL OS 11 auf dem UD Pocket ein.
13. Akzeptieren Sie die EULA, indem Sie auf **Ich stimme zu** klicken.

14. Bestätigen Sie den Warndialog.



15. Wenn Sie die Meldung **IGEL OS Creator build finished successfully** sehen, ist die Installation abgeschlossen.



16. Klicken Sie am unteren Rand des Installationsfensters auf **Systemneustart**.
17. Entfernen Sie den IGEL OS Creator-Stick.
18. Schließen Sie das Meldungsfenster.  
Das System fährt herunter und bootet anschließend IGEL OS 11 von Ihrem neu eingerichteten UD Pocket.

## Sonstiges

- [Geräteprotokolldateien an den IGEL Support senden \(see page 825\)](#)
- [Lokale Konfiguration des IGEL OS Geräts exportieren \(see page 833\)](#)
- [Welche Unified Communication-Lösungen werden von IGEL OS unterstützt? \(see page 836\)](#)
- [Passthrough-Authentifizierung \(see page 838\)](#)
- [Hardware-Videobeschleunigung auf IGEL OS \(see page 853\)](#)
- [Shell-Befehle vor Sitzungsstart und nach Sitzungsende ausführen \(see page 856\)](#)
- [Sitzungen im Setup oder in der UMS kopieren \(see page 857\)](#)
- [Verwendung von RAM bei IZ1 und UD2-MM \(see page 858\)](#)
- [Symantec Ghost zur Bereitstellung von IGEL OS verwenden \(see page 859\)](#)
- [Das Starten der UMS-Konsole führt zum Absturz der NX-Sitzung \(see page 861\)](#)
- [IGEL Setup im Appliance-Modus aufrufen \(see page 862\)](#)
- [Eine Anwendung wird beendet mit der Nachricht "Speicherstand niedrig! Prozess ... wird beendet" \(see page 863\)](#)
- [Ein Anwendungsfenster kann nicht verschoben werden \(see page 864\)](#)
- [IGEL UMD aktualisieren: Fehler "Nicht kompatibel mit System 5" \(see page 866\)](#)
- [IGEL Endpoint Partners: Ensuring Image Integrity with a Checksum \(see page 867\)](#)
- [Wird meine Sitzung geschlossen, wenn mein IGEL OS Endgerät in den Suspend-Modus wechselt? \(see page 868\)](#)
- [IGEL OS - Integrationen von Drittherstellerprodukten \(see page 870\)](#)



## Geräteprotokolldateien an den IGEL Support senden

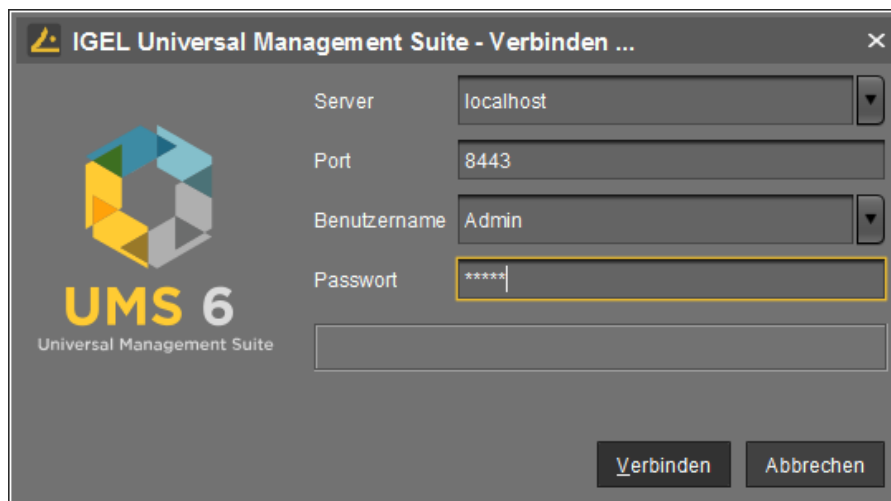
Wenn das IGEL Support Team Sie auffordert, die Protokolldateien Ihres Geräts anzugeben, befolgen Sie die folgenden Anweisungen.

Es gibt zwei Möglichkeiten, die Protokolldateien an das Support-Team zu senden:

- [Mit UMS](#) (see page 825)
- [Ohne UMS](#) (see page 829)

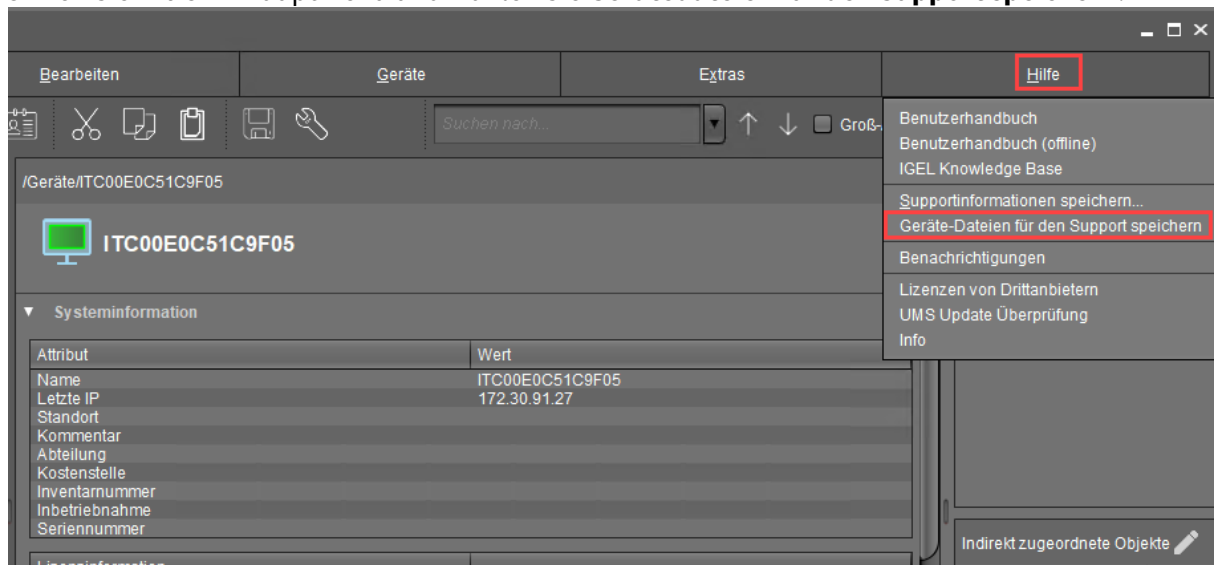
### Mit UMS

1. Starten Sie die UMS Konsole und geben Sie Ihren **Benutzername** und **Passwort** ein.



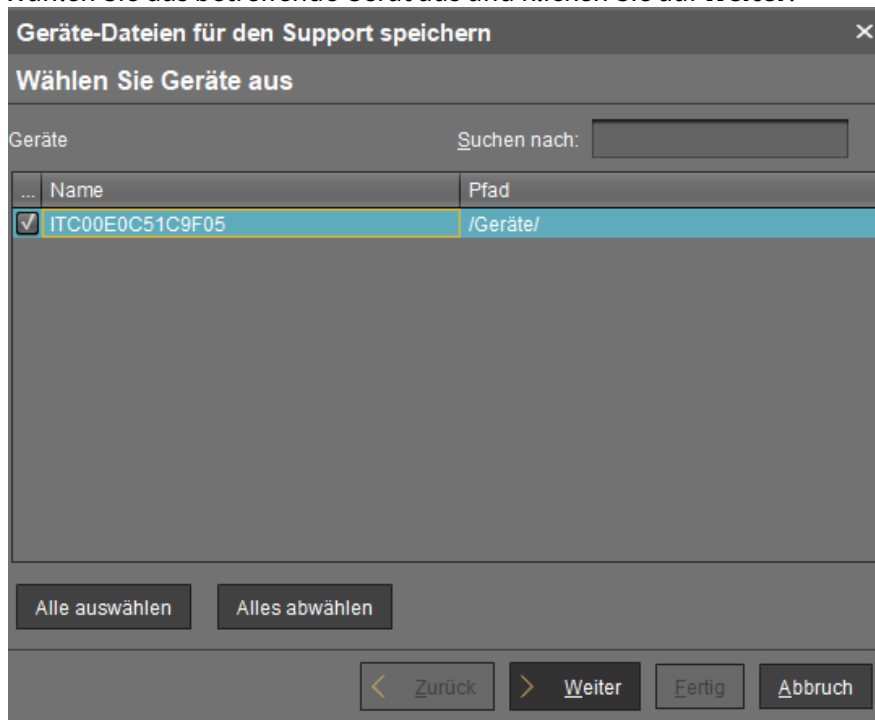
2. Klicken Sie **Verbinden**.  
Das UMS Konsolenfenster öffnet sich.

- Öffnen Sie **Hilfe** im Hauptmenü und wählen Sie **Geräte-dateien für den Support speichern**.



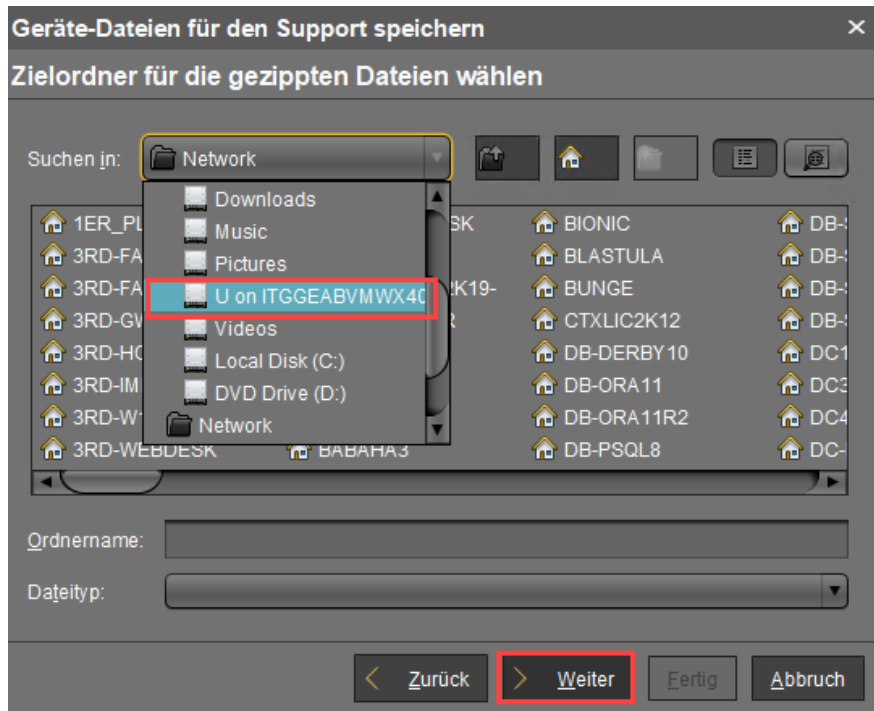
Der Dialog **Geräte-dateien für den Support speichern** öffnet sich.

- Wählen Sie das betreffende Gerät aus und klicken Sie auf **Weiter**.

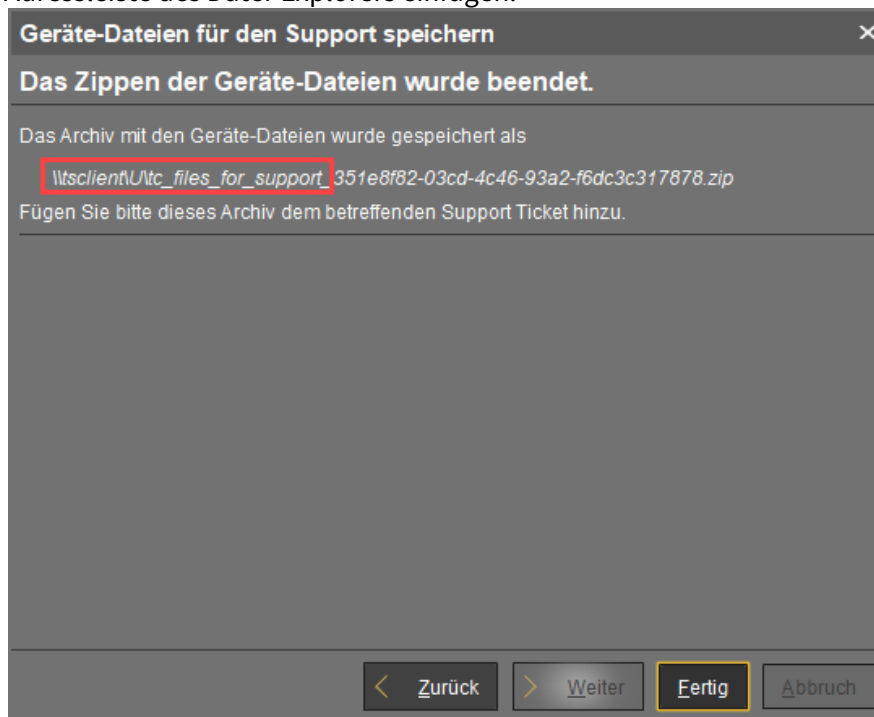


Der Dialog **Zielordner für die gezippten Dateien wählen** öffnet sich.

- Wählen Sie ein Verzeichnis aus, das zum Speichern der gezippten Protokolldateien geeignet ist, und klicken Sie auf **Weiter**.

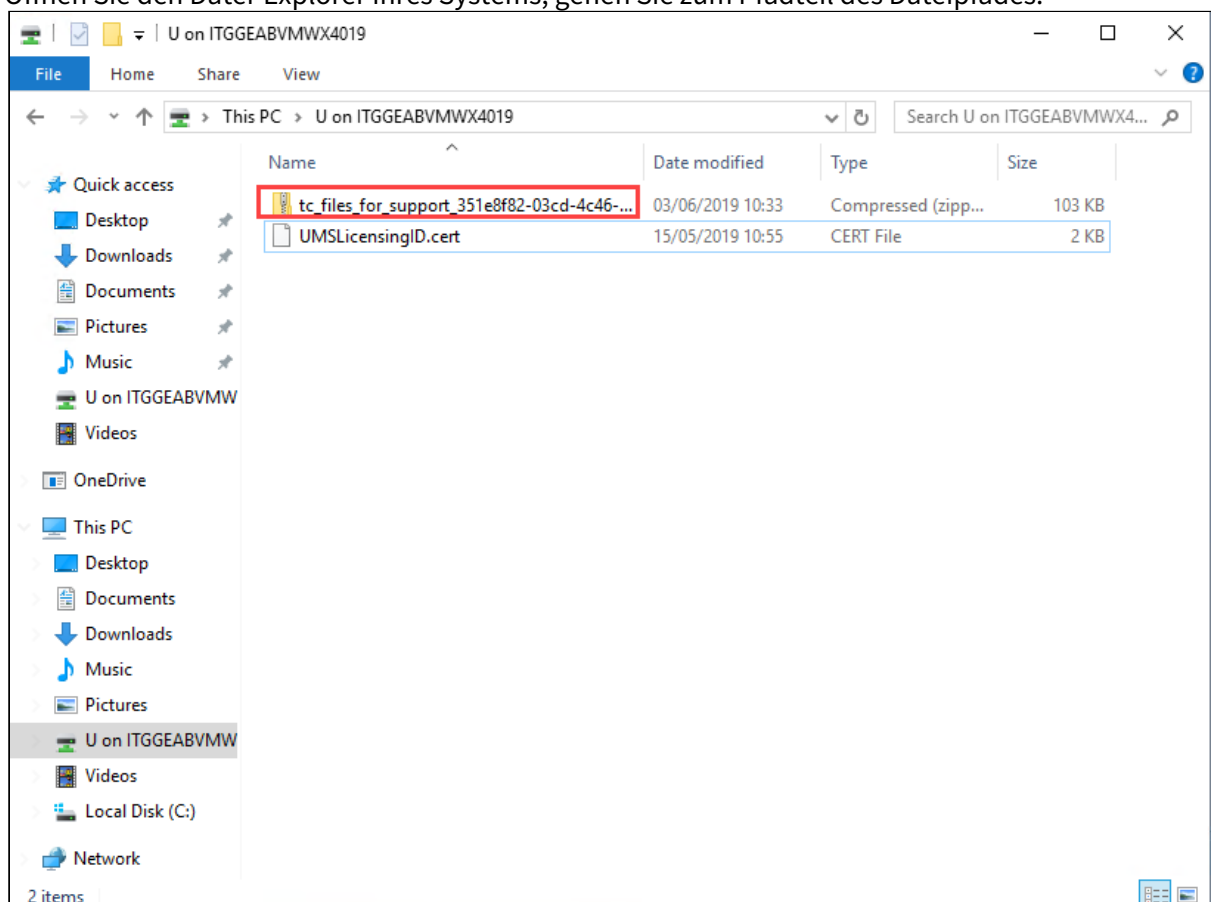


Ein Bestätigungsdialog zeigt den Pfad und Dateinamen, unter dem die Protokolldateien gespeichert sind. Je nach Ihrem System können Sie den Pfad mit [Strg] +[C] kopieren und in die Adressleiste des Datei-Explorers einfügen.



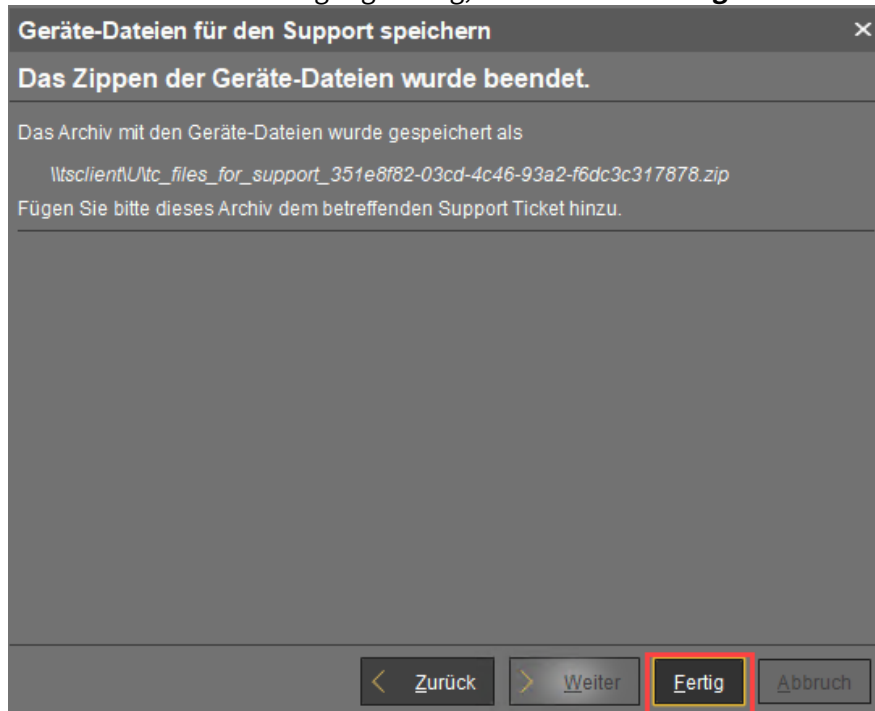
- i** Je nach Ihrem Netzwerk, Ihrer Hardware und Größe der Protokolldateien kann das Sammeln und Hochladen der Dateien bis zu einigen Minuten dauern.  
Falls der Vorgang fehlschlägt, versuchen Sie das Folgende:
- Wenn Sie UMS 6.10.110 oder höher verwenden: Gehen Sie auf **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** und ändern Sie den Parameter **Timeout für das Hochladen der Gerätedateien für den Support (Sekunden)** auf einen höheren Wert. Der Höchstwert ist 9000 Sekunden.
  - Prüfen Sie, ob Port 8443 für TCP-Verbindungen geöffnet ist.
  - Sollte alles fehlschlagen, versuchen Sie die unter [Ohne UMS \(see page 829\)](#) beschriebene Methode.

6. Öffnen Sie den Datei-Explorer Ihres Systems, gehen Sie zum Pfadteil des Dateipfades.



7. Senden Sie die ZIP-Datei an das IGEL Support Team.

- Schließen Sie den Bestätigungsdialog, indem Sie auf **Fertig** stellen klicken.



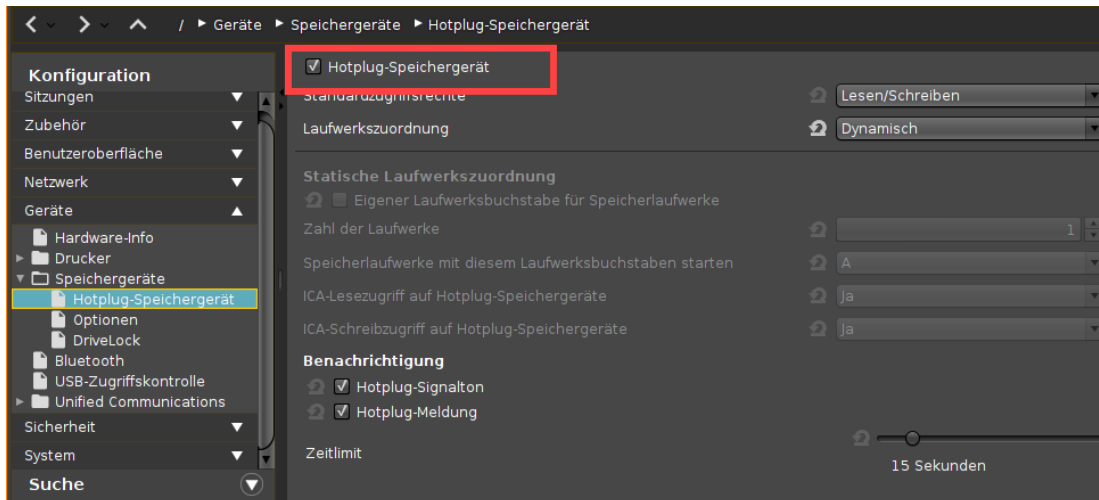
**i** Bei der obigen Vorgehensweise werden nur die Protokolle gesammelt, die seit dem letzten Systemstart geschrieben wurden. Um dauerhafte Protokolle zu ermöglichen, können Sie eine dedizierte Partition für Debug-Protokolle konfigurieren. Weitere Informationen, auch zum Hinzufügen weiterer Protokolle, finden Sie unter [Erweitertes Logging mit Syslog, Tcpdump und Netlog](#) (see page 420).


## Ohne UMS

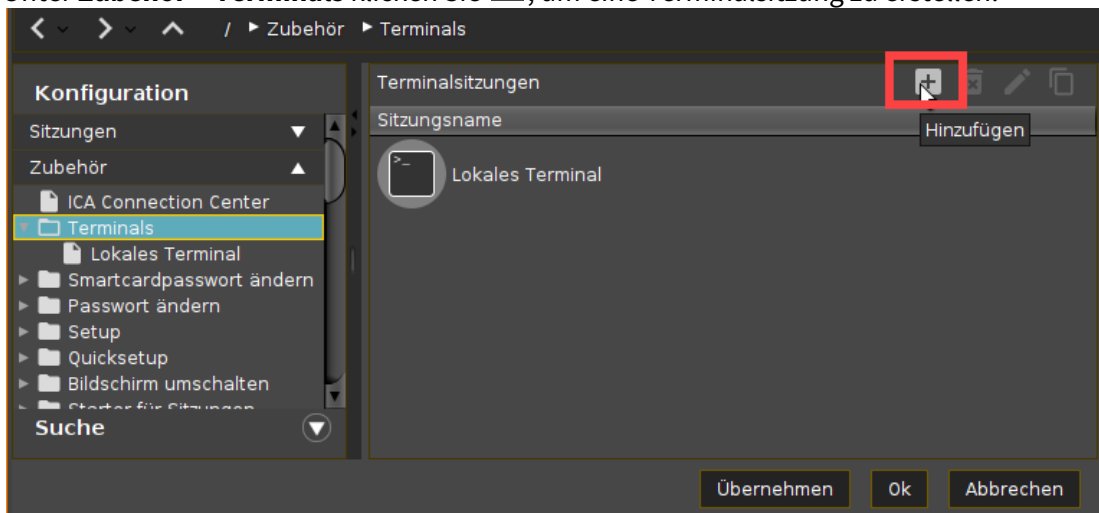
Wenn die UMS nicht erreichbar ist oder ein Problem mit der Netzwerkverbindung besteht, können Sie trotzdem Systemprotokolle von einem Gerät extrahieren und an das Support-Team senden. Sie benötigen einen USB-Stick, der idealerweise im NTFS-Format formatiert ist, um die Protokolle zu übertragen.

### Das Gerät einrichten

- Gehen Sie im IGEL Setup auf **Geräte > Speichergeräte > Hotplug-Speichergerät** und aktivieren Sie **Hotplug-Speichergerät**.

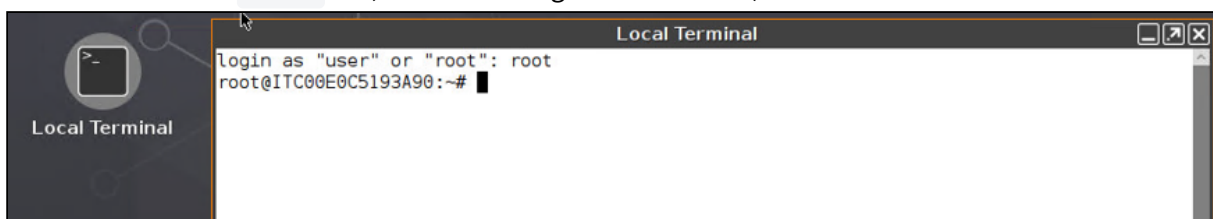


2. Unter **Zubehör > Terminals** klicken Sie , um eine Terminalsitzung zu erstellen.



### USB-Stick identifizieren

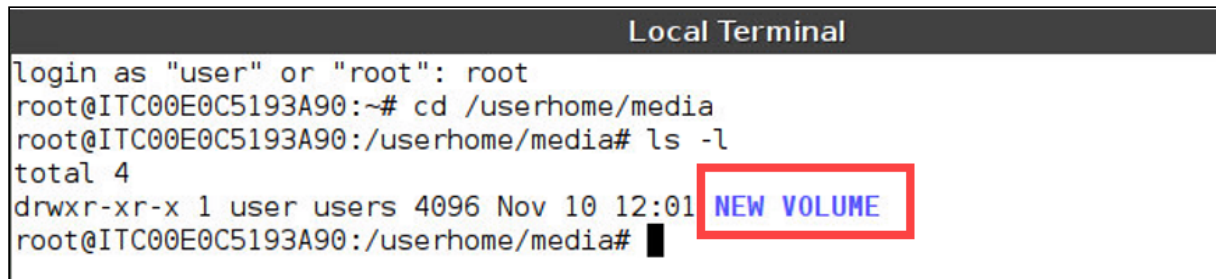
1. Stecken Sie den USB-Stick in das IGEL OS Gerät und starten Sie die Terminalsitzung.
2. Melden Sie sich als `root` an (standardmäßig ohne Passwort).



- Geben Sie die folgenden Befehle ein:

```
cd /userhome/media
ls -l
```

- Notieren Sie den Namen des USB-Sticks:



```
Local Terminal
login as "user" or "root": root
root@ITC00E0C5193A90:~# cd /userhome/media
root@ITC00E0C5193A90:/userhome/media# ls -l
total 4
drwxr-xr-x 1 user users 4096 Nov 10 12:01 NEW VOLUME
root@ITC00E0C5193A90:/userhome/media#
```

## Protokolldatei erstellen


- Führen Sie im Terminal den Befehl `cd /userhome/media/[Name Ihres USB-Sticks]` aus.

**i** Nach `/media/` können Sie die Tab-Taste zur automatischen Ausfüllung drücken.  
**WICHTIG:** Wenn der Gerätenamen Leerzeichen enthält, verwenden Sie Anführungszeichen `"`.  
 Beispiel: `cd /userhome/media/"NEW VOLUME"`  
 Wenn der Gerätenamen keine Leerzeichen enthält, sind keine Anführungszeichen erforderlich.

- Führen Sie den Befehl `/config/bin/create_support_information` aus.  
 Dadurch wird die Datei `tclogs.zip` im Ordner `/tmp` erstellt.

- Kopieren Sie `tclogs.zip` mit folgendem Befehl auf Ihren USB-Stick. Der Punkt am Ende bedeutet den aktuellen Ordner:

```
cp /tmp/tclogs.zip .
```



```
Local Terminal
login as "user" or "root": root
root@ITC00E0C520986A:~# cd /userhome/media/"NEW VOLUME"
root@ITC00E0C520986A:/userhome/media/NEW VOLUME# /config/bin/create_support_information
XDG_RUNTIME_DIR (/run/user/777) is not owned by us (uid 0), but by uid 777! (This could e.g. happen if you try to connect to a non-root PulseAudio as a root user, over the native protocol. Don't do that.)
vmware-view-log-collector: No log found in /tmp/vmware-user.
chown: cannot access '/var/log/vmware-view/horizon-2023-04-26+17_50_58+02.tar.gz': No such file or directory
zip warning: No such device or address
zip warning: No such device or address
root@ITC00E0C520986A:/userhome/media/NEW VOLUME# cp /tmp/tclogs.zip .
root@ITC00E0C520986A:/userhome/media/NEW VOLUME# ls -la tclogs.zip
-rw-r--r-- 1 user users 892540 Apr 26 17:51 tclogs.zip
root@ITC00E0C520986A:/userhome/media/NEW VOLUME#
```

4. Entfernen Sie den USB-Stick sicher aus dem IGEL OS Gerät.  
Diese Protokolldatei können Sie nun selbst untersuchen oder an den IGEL Support zur Analyse senden.



## Lokale Konfiguration des IGEL OS Geräts exportieren

Wenn Sie die aktuelle lokale Konfiguration des Geräts auslesen müssen (z. B. während eines speziellen Supportfalls), können Sie die zwei lokalen Dateien `setup.ini` und `group.ini` kopieren, egal ob lokal oder via IGEL Universal Management Suite (UMS).

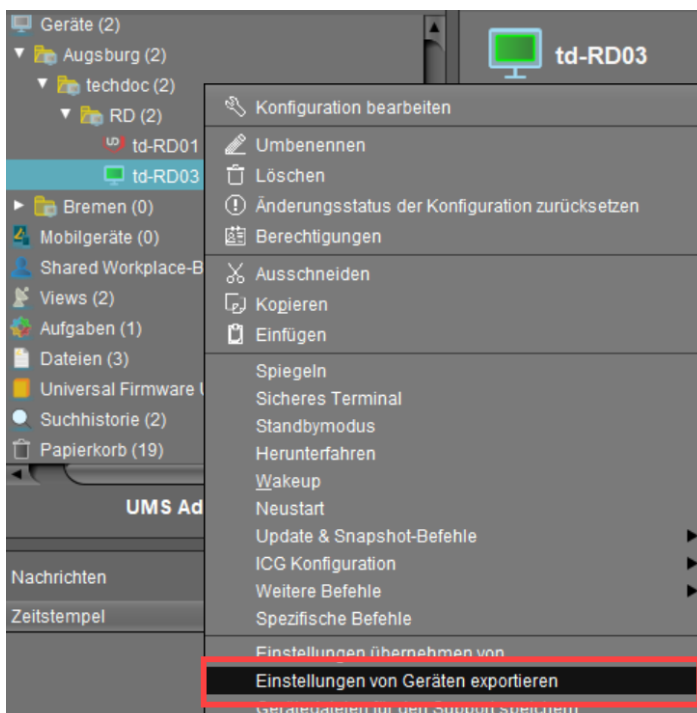
### Option 1: Über UMS Konsole > Hilfe > Gerätedateien für den Support speichern

Sie können die Dateien `setup.ini` und `group.ini` zusammen mit den Geräteprotokolldateien versenden, siehe den Abschnitt "Mit UMS" unter [Geräteprotokolldateien an den IGEL Support senden](#) (see page 825).

### Option 2: Über UMS Konsole > [Kontextmenü des Geräts] > Einstellungen von Geräten exportieren

Alternativ können Sie die effektiven Einstellungen, die auf das Gerät wirken (d. h. das Zusammenspiel von lokalen Einstellungen und allen Profilen), als XML-Datei exportieren: **UMS Konsole > [Kontextmenü des Geräts] > Einstellungen von Geräten exportieren.**

Der IGEL Support kann diese Datei als Profil in die UMS importieren und die effektiven Einstellungen direkt in der UMS Konsole einsehen.




### Option 3: Über UMS Konsole > [Kontextmenü des Geräts] > Weitere Befehle > Gerätedatei->UMS

Die Dateien `setup.ini` und `group.ini` können Sie vom Gerät an die UMS auch über **UMS Konsole > [Kontextmenü des Geräts] > Weitere Befehle > Gerätedatei->UMS** übertragen, siehe Datei auf den IGEL UMS Server übertragen.

### Option 4: Über das Kopieren auf ein USB-Speichergerät

Die Dateien können Sie auch lokal auf einem FAT32-formatierten USB-Stick speichern:

1. Gehen Sie im IGEL Setup auf **Geräte > Speichergeräte > Hotplug-Speichergerät** und aktivieren Sie **Hotplug-Speichergerät**.  
Wenn Sie die statische Laufwerkszuordnung verwenden, stellen Sie sicher, dass die **Zahl der Laufwerke** größer als Null ist. Siehe Hotplug-Speichergerät.
2. Erstellen Sie eine Terminalsitzung unter **Zubehör > Terminals**.
3. Schließen Sie den USB-Stick an.
4. Starten Sie die Terminalsitzung und melden Sie sich als `root` an.

 Um den Namen des USB-Sticks herauszufinden, können Sie die folgenden Befehle verwenden:

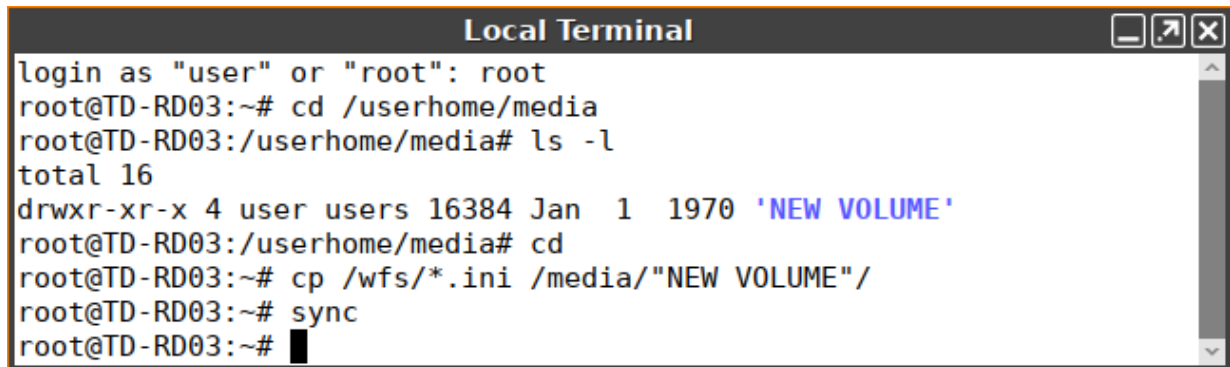
```
cd /userhome/media
```

```
ls -l
```

Wenn der Gerätenamen Leerzeichen enthält, müssen Sie ihn später in Anführungszeichen "" einschließen.

Wenn der Gerätenamen keine Leerzeichen enthält, sind keine Anführungszeichen erforderlich.

5. Tippen Sie `cp /wfs/*.ini /media/[Name des USB-Speichergeräts]/` ein und drücken Sie [Return], um alle `.ini`-Dateien, inkl. `setup.ini` und `group.ini`, von Ihrem Gerät auf den USB-Stick zu kopieren.
6. Geben Sie `sync` ein und drücken Sie [Return]. Warten Sie einige Sekunden, bevor Sie den USB-Stick sicher aus dem Endgerät entfernen.



```
Local Terminal
login as "user" or "root": root
root@TD-RD03:~# cd /userhome/media
root@TD-RD03:/userhome/media# ls -l
total 16
drwxr-xr-x 4 user users 16384 Jan  1  1970 'NEW VOLUME'
root@TD-RD03:/userhome/media# cd
root@TD-RD03:~# cp /wfs/*.ini /media/"NEW VOLUME"/
root@TD-RD03:~# sync
root@TD-RD03:~# █
```

## Welche Unified Communication-Lösungen werden von IGEL OS unterstützt?

Dieser Artikel gibt einen Überblick über die Software- und Hardwarelösungen im Bereich Unified Communications, die von IGEL OS unterstützt werden.

### Die von IGEL OS unterstützte Unified Communication-Hardware

- Jabra Handsets / Headsets
- Plantronics Headsets
- EPOS / Sennheiser

### Virtual Desktop-Optimierungen in IGEL OS

Die Virtual Desktop-Optimierungen rüsten das Endgerät mit einer Media Engine aus und leiten die Audio- und Videoströme so um, dass sie direkt zwischen den Endgeräten ausgetauscht werden. Dies äußert sich in einer besseren Performanz und einer niedrigeren Serverauslastung.

### Virtual Desktop-Optimierungen für Citrix Sitzungen

IGEL OS unterstützt die folgenden Virtual Desktop-Optimierungen für Citrix Sitzungen:

- Skype for Business
- Cisco Jabber (JVDI Client)
- Cisco Webex Meetings VDI und Cisco Webex VDI
- Microsoft Teams Optimierung
- Zoom VDI Media Plugin

Zur Konfiguration siehe Unified Communications-Einstellungen für Citrix Sitzungen in IGEL OS.

### Virtual Desktop-Optimierungen für Horizon Sitzungen

IGEL OS unterstützt die folgenden Virtual Desktop-Optimierungen für VMware Horizon Sitzungen:

- Skype for Business
- Cisco Jabber (JVDI)
- Cisco Webex Meetings VDI und Cisco Webex VDI
- Microsoft Teams Optimierung
- Zoom VDI Media Plugin

Zur Konfiguration siehe Unified Communications-Einstellungen für VMware Horizon Sitzungen in IGEL OS.

### Lokale Installation auf dem Endgerät mit einer Custom Partition

Im Gegensatz zu den Virtual Desktop-Optimierungen, wo die Unified Communication-Anwendungen auf dem VDI-Server installiert sind, sieht dieser Ansatz die Installation der Anwendungen auf dem Endgerät vor.

Um selber eine Custom Partition zu erstellen, siehe das [Custom Partition Tutorial \(see page 589\)](#).

Sie können jede der folgenden Custom Partitions erhalten; fragen Sie einfach Ihren Ansprechpartner bei IGEL:

- Microsoft Teams (siehe auch [Microsoft Teams as a Custom Partition \(see page 613\)](#))
- Zoom (siehe auch [Zoom as a Custom Partition \(see page 603\)](#))
- TeamViewer

## Passthrough-Authentifizierung

Passthrough-Authentifizierung ist eine komfortable Single-Sign-On-Methode. Durch diese Funktion muss sich ein Benutzer nur ein einziges Mal einloggen und erhält dann Zugriff auf alle Sitzungen, ohne sich bei jeder einzelnen nochmals einloggen zu müssen.

In diesem Dokument werden die Grundeinstellungen einer Passthrough-Authentifizierung beschrieben sowie erläutert, wie Sie Passthrough-Authentifizierung für die jeweiligen Sitzungen aktivieren.

- [Überblick](#) (see page 839)
- [Grundkonfiguration](#) (see page 841)
- [Sitzungskonfiguration](#) (see page 848)

### IGEL Tech Video



Sorry, the widget is not supported in this export.  
But you can reach it using the following URL:

<https://www.youtube.com/watch?v=JxGOEGAb3LI>

## Überblick

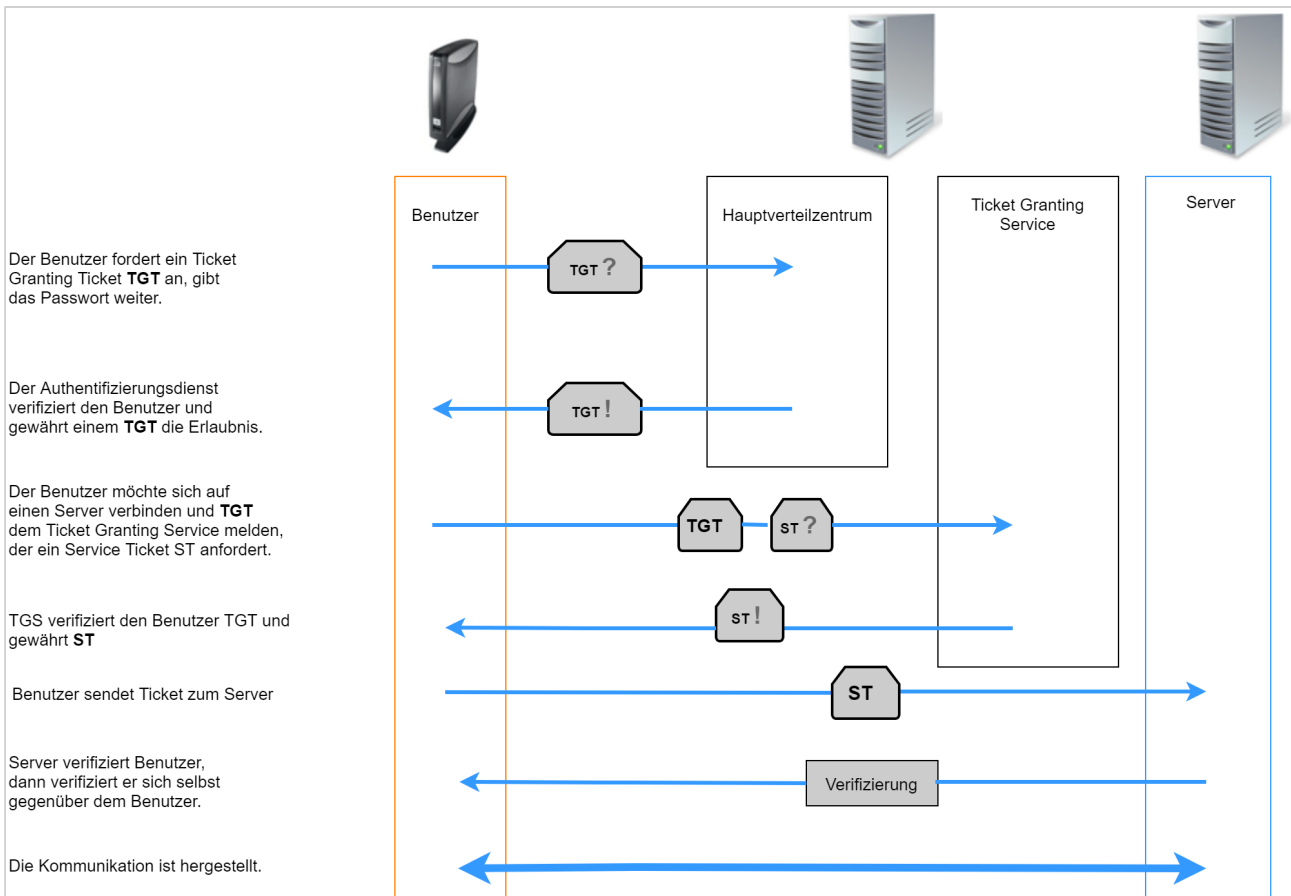
Die folgenden zwei Single-Sign-On-Methoden stehen zur Verfügung:

Kerberos Passthrough	Sofern ein Client Kerberos unterstützt, wird eine echte Kerberos-Authentifizierung verwendet.
Passthrough	Die bei der lokalen Anmeldung eingegebenen Zugangsdaten (Benutzername und Passwort) werden in einem Cache gespeichert und auf diese Weise bei der Authentifizierung bereitgestellt.  Eine erneute Eingabe der Zugangsdaten ist erforderlich, wenn in einer Sitzung auf Netzwerkressourcen zugegriffen werden soll.

Kerberos ist ein Authentifizierungsdienst. Der Dienst arbeitet mit den Entitätstypen "Benutzer", "Dienst" und "Computer", die als **Principals** bezeichnet werden. Principals gehören einem **Realm** an, dabei handelt es sich um eine Administrationseinheit. Im Realm hat jeder Principal einen eindeutigen **Principal Name**. Der das Authentifizierungssystem bereitstellende Dienst heißt **Key Distribution Center**.

Beispiel: Microsoft Windows-Domänen bilden ein Realm. Der Domänenname, z. B. EXAMPLE.COM, ist der Realm Name. Ein Principal wäre z. B. user@EXAMPLE.COM. Die Domänencontroller haben die Rolle von Key Distribution Centers.

Wenn sich ein Benutzer einloggt, dann bezieht er ein Ticket Granting Ticket vom Key Distribution Center. Das Ticket verfällt nach einer gewissen Zeit (normalerweise nach 1 Tag). Wenn der Benutzer nun z. B. eine ICA-Sitzung startet, dann kann der Client mithilfe des Ticket Granting Ticket ein sogenanntes Service Ticket vom Key Distribution Center beziehen. Mit dem Service Ticket wird die Authentifizierung gegen den ICA-Server erreicht.



Um die Passthrough-Authentifizierung zu aktivieren, müssen Sie bestimmte Einstellungen vornehmen:

1. [Grundkonfiguration](#) (see page 841)
2. [Sitzungskonfiguration](#) (see page 848)



## Grundkonfiguration

Damit Sie Passthrough-Authentifizierung aktivieren können, muss die Konfiguration Ihres Clients bestimmte Anforderungen erfüllen.

- [Stellen Sie auf allen beteiligten Clients und Hosts die Zeit richtig ein.](#) (see page 842)
- [Konfigurieren Sie die Domäne.](#) (see page 843)
- [Aktivieren Sie die Anmeldung an Active-Directory-Domäne.](#) (see page 845)

 Wenn die Anmeldemethode **Smartcard** verwendet wird, [sind zusätzliche Einstellungen erforderlich](#) (see page 846).

## Zeit

Auf allen beteiligten Clients und Hosts muss eine korrekte Uhrzeit eingestellt sein.

Als Best-Practice-Lösung wird empfohlen, die Uhrzeit über einen NTP-Server zu beziehen.


So konfigurieren Sie einen NTP-Server:

1. Gehen Sie in IGEL Setup zu **System > Zeit und Datum**.
2. Aktivieren Sie **NTP-Zeitserver verwenden**.
3. Geben Sie einen **NTP-Zeitserver** an.

## Domänen/Realms

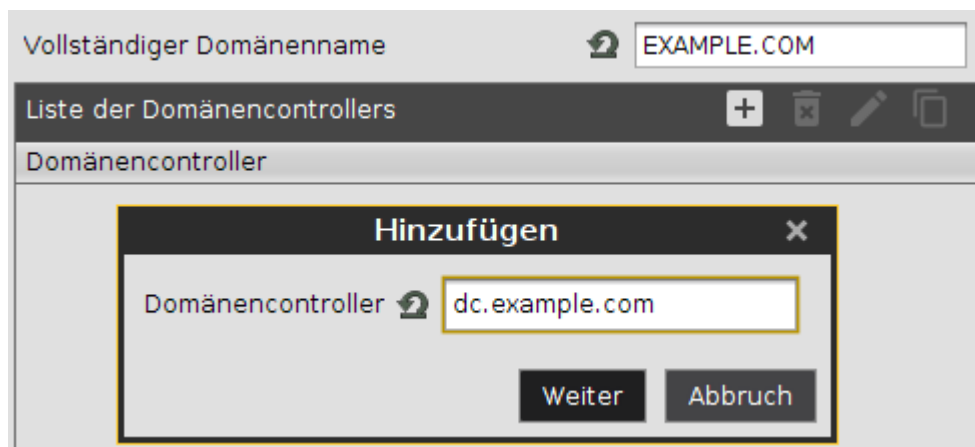
So konfigurieren Sie eine oder mehrere Domänen:

1. Gehen Sie in IGEL Setup zu **Sicherheit > Active Directory/Kerberos**.
2. Aktivieren Sie das Kontrollkästchen **Aktivieren**.
3. Geben Sie im Feld **Standarddomäne (vollständiger Domänenname)** den FQDN (fully qualified domain name) ein, z. B. `EXAMPLE.COM` (Großbuchstaben).
4. Aktivieren Sie **DNS-Suche nach Domänencontroller**.
5. Aktivieren Sie **DNS-Suche nach Domäne**.

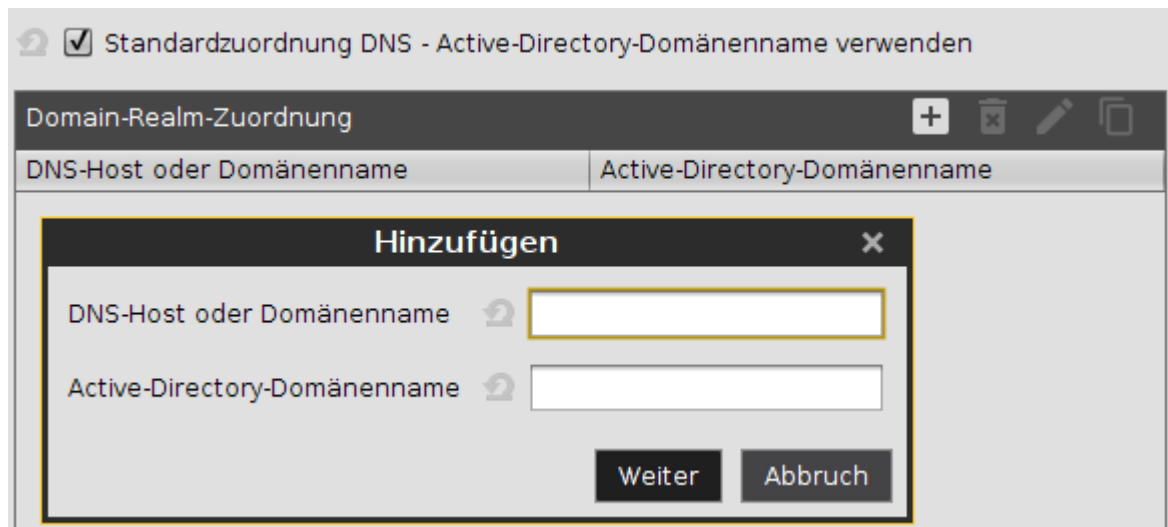
 Diese Einstellungen sind hinreichend, wenn der DNS-Server Active Directory automatisch erkennt.

Ansonsten können Sie bis zu 4 Domänen/Realms konfigurieren:

1. Gehen Sie im IGEL Setup unter **Sicherheit > Active Directory/Kerberos > Domain 1...4**.
2. Geben Sie unter **Vollständiger Domänenname** den FQDN ein, z. B. `EXAMPLE.COM` (Großbuchstaben).
3. Geben Sie in der **Liste der Domänencontroller** mindestens einen Windows-Domänencontroller (Kerberos Key Distribution Center) an.  
Es kann ein DNS-Name oder eine IP-Adresse sein.



4. Klicken Sie auf **Sicherheit > Active Directory/Kerberos > Domain-Realm-Zuordnung**, um die Zuordnung zwischen Active Directory-Domännennamen und DNS-Namen zu definieren.
5. Aktivieren Sie **Standardzuordnung DNS - Active-Directory-Domänenname verwenden**.



- ⓘ Wenn beide Namen übereinstimmen, d. h. wenn ein Host in der Domäne `EXAMPLE.COM` den DNS-Namen `host.example.com` hat, muss hier nichts getan werden und die Standardeinstellung ist ausreichend. Andernfalls muss ein entsprechender Eintrag in der Liste **Domain-Realm-Zuordnung** erstellt werden.


## Anmeldung

1. Gehen Sie in IGEL Setup auf **Sicherheit > Anmeldung > Active Directory/Kerberos**.
2. Aktivieren **Anmeldung an Active-Directory-Domäne**.
3. Wählen Sie eine der **Anmeldemethoden**:
  - **Explizit**: Dem Benutzer wird eine Anmeldedialog angezeigt.
  - **Letzten Benutzer bei der Anmeldung anzeigen**: Der Anmeldedialog wird mit dem zuletzt verwendeten Benutzernamen vorausgefüllt. Diese Option kann für eine komfortablere Anmeldung verwendet werden, wenn die Option **Explizit** aktiviert ist.
  - **Smartcard**: Die Anmeldung erfolgt mit einer Smartcard und der dazugehörigen PIN.
4. Unterhalb von **Verknüpfung zum Abmelden** können Sie festlegen, wo die Schaltfläche zum Abmelden erscheint.


## Smartcard

Für die Verwendung der Anmeldemethode **Smartcard** sind weitere Einstellungen erforderlich:

1. Gehen Sie in IGEL Setup zu **Sicherheit > Anmeldung > Active Directory/Kerberos**.
2. Aktivieren Sie bei **Anmeldemethoden** die Option **Smartcard**.
3. Legen Sie eine **Aktion bei Entfernen der Smartcard** fest:
  - **Abmelden**: Die Verbindung zu einer laufenden Sitzung wird beendet, alle benutzerbezogenen Daten werden vom Gerät gelöscht und das Gerät für eine neue Benutzeranmeldung vorbereitet.
  - **Gerät sperren**: Sperrt den Bildschirm bei einer laufenden Sitzung. Nur der aktuell angemeldete Benutzer kann den Bildschirm mit seiner Smartcard und PIN wieder entsperren. Damit die Einstellung wirksam wird, müssen Sie außerdem unter **Benutzeroberfläche > Bildschirmsperre/-schoner > Optionen** im Bereich **Passwort für Bildschirmsperre** die Option **Benutzerpassword** aktivieren.
4. Gehen Sie zu **Sicherheit > Smartcard > Middleware** und wählen Sie ein PKCS#11-Modul aus.

 Die Smartcards für diesen Login müssen von einem PKCS#11-Modul unterstützt werden, dass auf die Zertifikate auf der Smartcard zugreifen kann.

Bei einer Kerberos-Anmeldung per Smartcard werden Zertifikate verwendet. Darum muss das Root-Zertifikat des Zertifikats, das vom Key Distribution Center verwendet wird (Domänencontroller), auf dem Gerät vorhanden sein. Das Root-Zertifikat muss entweder von einer öffentlichen Certificate Authority stammen oder auf das Gerät übertragen werden, siehe [Vertrauenswürdige Stammzertifikate in IGEL OS einspielen](#) (see page 523).

 Wenn Sie eine Smartcard-Anmeldung in Verbindung mit einem auf Windows 2000 oder Windows Server 2003 basierenden Domänencontroller verwenden, muss in der Registry der Parameter `auth.krb5.realms.pkinit.pkinit_win2k` aktiviert sein. Dadurch wird eine frühere Protokollversion von PKINIT `preauthentication` verwendet.

## Kerberos-Ports

In Linux-Umgebungen werden von Kerberos folgenden Ports genutzt:

	UDP-Port	TCP-Port
Ticketbezug, inklusive des initialen TGT	88	88
Passwort von UNIX/Linux ändern		749

## Sitzungskonfiguration

Für eine Single-Sign-On-Anmeldung an Sitzungen stehen zwei Methoden zur Verfügung:

- Kerberos Passthrough: Bei Clients, die Kerberos unterstützen, wird eine echte Kerberos-Authentifizierung verwendet.
- Passthrough: Verwendet für die Authentifizierung den Benutzernamen und das Passwort des lokalen Logins. Die Zugangsdaten werden dazu in einem Cache gespeichert.

 Derzeit ist die echte Kerberos-Authentifizierung nur für Citrix-Sitzungen verfügbar.

So konfigurieren Sie die Passthrough-Authentifizierung für die folgenden Sitzungen:

- [Citrix StoreFront/Web Interface](#) (see page 849)
- [RDP](#) (see page 850)
- [Horizon Client](#) (see page 851)
- [Parallels Client](#) (see page 852)



## Citrix StoreFront/Web Interface

1. Gehen Sie unter **Sitzungen > Citrix > Citrix Global > StoreFront-Anmeldung**.
2. Wählen Sie den **Authentifizierungstyp**:
  - **Passwort-Authentifizierung**: Um Passthrough zu aktivieren, muss diese Option ausgewählt werden und **Passthrough-Authentifizierung verwenden** muss aktiviert werden.
  - **Kerberos Passthrough-Authentifizierung**
  - **Smartcard-Authentifizierung (nur StoreFront, nicht Web Interface)**: Die Authentifizierung über Smartcard funktioniert nur mit StoreFront, nicht mit der Web Interface.
  - **Citrix Authentifizierungsmechanismus (statt IGEL), ohne Smartcard**
  - **Citrix Authentifizierungsmechanismus (statt IGEL), mit Smartcard**

Siehe auch StoreFront-Anmeldung.

## RDP

Für RDP-Sitzungen wird die Weitergabe unterstützt. Kerberos Passthrough wird noch nicht unterstützt.

1. Gehen Sie unter **Sitzungen > RDP > RDP-Sitzungen > [Sitzungsname] > Anmeldung**.
2. Aktivieren Sie **Passthrough-Authentifizierung verwenden**.

## Horizon Client

Für Horizon Client-Sitzungen wird die Weitergabe unterstützt. Kerberos Passthrough wird noch nicht unterstützt.

1. Gehen Sie unter **Sitzungen > Horizon Client > Horizon Client-Sitzungen > [Sitzungsname] > Verbindungseinstellungen**
2. Aktivieren Sie **Passthrough-Authentifizierung verwenden**.

## Parallels Client

Für Parallels Client-Sitzungen wird Passthrough unterstützt. Kerberos Passthrough wird noch nicht unterstützt.

1. Gehen Sie unter **Sitzungen > Parallels Client > Parallels Client Sitzungen > [Sitzungsname] > Verbindung**.
2. Aktivieren Sie **Verwende Systemanmeldedaten**, um die Passthrough-Authentifizierung zu verwenden.

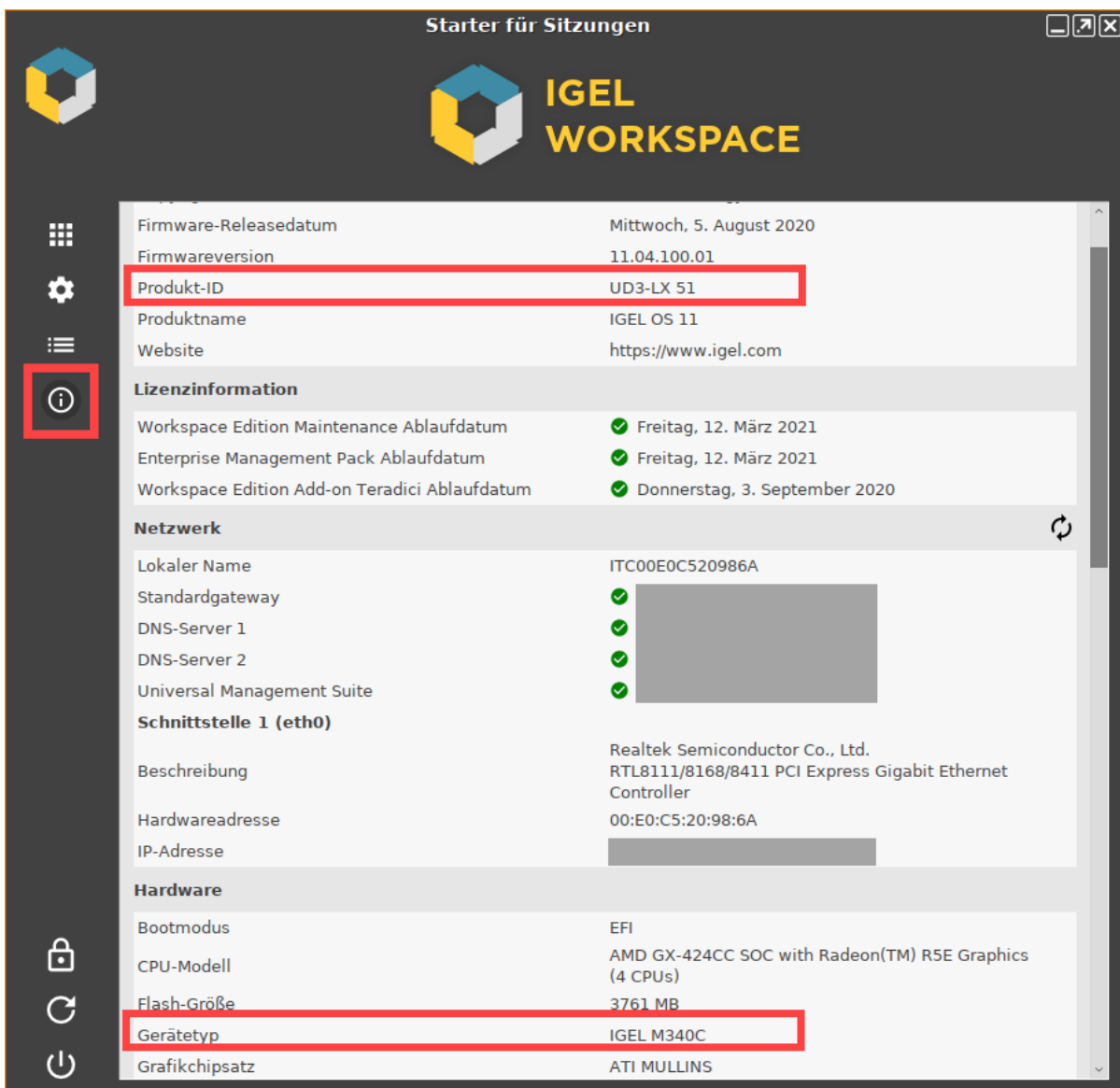
## Hardware-Videobeschleunigung auf IGEL OS

### Frage

Bietet meine Hardware mit IGEL OS eine Videobeschleunigung an?

### Antwort

Öffnen Sie **Starter für Sitzungen > Informationen**, um Ihre Produkt-ID und Ihren Gerätetyp nachzuschlagen:



The screenshot shows the 'Starter für Sitzungen' window in IGEL Workspace. The interface is dark-themed with a sidebar on the left containing icons for home, settings, and information. The main content area displays system information in a light-colored panel. The 'Produkt-ID' field is highlighted with a red box, showing 'UD3-LX 51'. The 'Gerätetyp' field is also highlighted with a red box, showing 'IGEL M340C'. Other visible information includes the firmware release date (August 5, 2020), license expiration dates, network settings, and hardware details like the CPU model (AMD GX-424CC) and graphics (ATI MULLINS).

Starter für Sitzungen	
Firmware-Releasedatum	Mittwoch, 5. August 2020
Firmwareversion	11.04.100.01
<b>Produkt-ID</b>	<b>UD3-LX 51</b>
Produktname	IGEL OS 11
Website	https://www.igel.com
<b>Lizenzinformation</b>	
Workspace Edition Maintenance Ablaufdatum	✔ Freitag, 12. März 2021
Enterprise Management Pack Ablaufdatum	✔ Freitag, 12. März 2021
Workspace Edition Add-on Teradici Ablaufdatum	✔ Donnerstag, 3. September 2020
<b>Netzwerk</b>	
Lokaler Name	ITC00E0C520986A
Standardgateway	✔ [Redacted]
DNS-Server 1	✔ [Redacted]
DNS-Server 2	✔ [Redacted]
Universal Management Suite	✔ [Redacted]
<b>Schnittstelle 1 (eth0)</b>	
Beschreibung	Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller
Hardwareadresse	00:E0:C5:20:98:6A
IP-Adresse	[Redacted]
<b>Hardware</b>	
Bootmodus	EFI
CPU-Modell	AMD GX-424CC SOC with Radeon(TM) R5E Graphics (4 CPUs)
Flash-Größe	3761 MB
<b>Gerätetyp</b>	<b>IGEL M340C</b>
Grafikchipsatz	ATI MULLINS

In Version 5.07.100 und neuer sowie in Version 10.01.100 und neuer bietet IGEL OS die Hardware-Videobeschleunigung für folgende Bereiche:

- Media Player
- Citrix Multimedia Redirection
- RDP Multimedia Redirection (TSMF and EVOR)
- VMware Horizon Multimedia Redirection


auf ausgewählten Geräten an. Dies erlaubt die Wiedergabe von HD-Video mit einer maximalen CPU-Auslastung von 20%.

**i** Für diese Funktion wird das Multimedia Codec Pack benötigt, falls Ihre Version von IGEL OS niedriger als 11.01.100 ist.

Hardware-Videobeschleunigung wird von den folgenden IGEL Geräten unterstützt:

Produkt-ID	Gerätetyp	Chipsatz	IGEL Linux >=			
			v5.07.100	v5.09.100	IGEL OS 10	IGEL OS 11
IZ2-HDX/RFX/ HORIZON 40* (see page 855)	IGEL D220	Intel Bay Trail	✓	✓	✓	✓* (see page 855)
IZ3-HDX/RFX/ HORIZON 41, 42	IGEL M330C	VIA VX900	✓			
IZ3-HDX/RFX/ HORIZON 50* (see page 855)	IGEL M340C	ATI Mullins		✓	✓	✓* (see page 855)
IZ3-HDX/RFX/ HORIZON 51* (see page 855)	IGEL M340C	ATI Mullins			✓	✓* (see page 855)
UD2-LX 40	IGEL D220	Intel Bay Trail	✓	✓	✓	✓
UD2-LX 50, 51	IGEL M250C	Intel HD Graphics				✓
UD3-LX 40	IGEL M320C	VIA VX900	✓	✓		
UD3-LX 41, 42	IGEL M330C	VIA VX900	✓	✓		
UD3-LX 50	IGEL M340C	ATI Mullins		✓	✓	✓
UD3-LX 51	IGEL M340C	ATI Mullins			✓	✓

Produkt-ID	Gerätetyp	Chipsatz	IGEL Linux >= v5.07.100	IGEL Linux >= v5.09.100	IGEL OS 10	IGEL OS 11
UD3-LX 60	IGEL M350C	AMD Radeon Vega 3 Graphics				✓
UD5-LX 40	IGEL H820C	Intel Sandy Bridge	✓	✓	✓	
UD5-LX 50	IGEL H830C (Dualcore CPU Model)	Intel Bay Trail	✓	✓	✓	✓
UD6-LX 51	IGEL H830C (Quadcore CPU Model)	Intel Bay Trail	✓	✓	✓	✓
UD7-LX 10	IGEL H850C	AMD Radeon Graphics			✓	✓
UD7-LX 11	IGEL H850C	AMD Radeon Graphics				✓
UD7-LX 20	IGEL H860C	AMD Radeon Vega 8 Graphics				✓
UD9-LX 40, UD9-LX 41 Touch	IGEL UD9 BT	Intel Bay Trail		✓	✓	✓
UD10-LX	IGEL UD10 TC236	VIA VX900	✓	✓		

 Auf Hardware von Drittanbietern mit UDC3, IGEL OS Creator (OSC) und UD Pocket hängt die Hardwarebeschleunigung vom Grafik-Chipsatz des Geräts ab.

## Codecs

Die folgenden Codecs werden unterstützt:

- MPEG-2 (simples und Hauptprofile)
- H.264 (Basis-, Haupt- und Spitzenprofile)
- WVC1/WMV3 (simples, Haupt- und Fortgeschrittenes Profil)
- MPEG-4 (DivX/Xvid): nur auf VIA VX900 und ATI Mullins

\* Für ein Upgrade Ihres IZ-Geräts auf IGEL OS 11 wenden Sie sich bitte an Ihren IGEL Vertriebsrepräsentanten. Siehe auch <https://www.igel.de/tradeup/> und Der IGEL OS 11 Migrationsplan.

## Shell-Befehle vor Sitzungsstart und nach Sitzungsende ausführen

In diesem How-to erfahren Sie, wie Sie Sitzungen so konfigurieren, dass vor Sitzungsstart und nach Sitzungsende ein benutzerdefinierter Shell-Befehl ausgeführt wird.

Diese Funktion steht für folgende Sitzungsarten zur Verfügung:

- Citrix/ICA
- RDP
- VNC Viewer

### Schritte

Shell-Befehle können nur über die Registry festgelegt werden.

1. Gehen Sie in IGEL Setup zu **System > Registry**.
2. Verwenden Sie die Suchfunktion **Parametersuche...** oder navigieren Sie manuell zu folgenden Registry-Keys:

Für VNC Viewer:

```
sessions.vncviewer*.init_action  
sessions.vncviewer*.final_action
```

Für RDP:


```
sessions.winconnect*.init_action  
sessions.winconnect*.final_action
```


Für Citrix/ICA:

```
sessions.ica*.init_action  
sessions.ica*.final_action
```

(Das Asterisk-Symbol \* steht für die jeweilige Nummer der Sitzung, z. B. 0, 1, 2, 3, ...).

`_init_action` wird vor dem Start der Sitzung ausgeführt. `final_action` wird nach Beendigung der Sitzung ausgeführt. Geben Sie jeweils als Parameterwert einen Shell-Befehl, den Pfad zu einem eigenen Skript oder zu einer ausführbaren Datei ein.

 Registry-Keys von neu angelegten Sitzungen stehen erst nach dem Neustart von IGEL Setup zur Verfügung.

 Die Sitzung startet erst dann, wenn die Ausführung des für `_init_action` festgelegten Befehls abgeschlossen ist. Wenn Sie den Befehl dagegen im Hintergrund ausführen möchten, können Sie dies erreichen, indem Sie dem Befehl ein `' & '` anhängen.




## Sitzungen im Setup oder in der UMS kopieren

In manchen Situationen möchte man eine Sitzung erstellen, die sich nur in wenigen Details von der anderen unterscheidet. IGEL Linux Version 5.10.100 oder neuer und UMS Version 5.02.100 oder neuer lassen Sie die komplette Sitzung kopieren. Nach dem Kopieren der Sitzung können Sie die gewünschten Einstellungen einfach anpassen.

Das Kopieren ist im Abschnitt **Sitzungen** von IGEL Setup (und gelegentlich auch in einigen anderen Abschnitten) sowie in der Funktion **Konfiguration bearbeiten** in der UMS verfügbar.

Um eine Mappe zu kopieren, gehen Sie wie folgt vor:

1. Öffnen Sie im Setup den Menüpfad **Sitzungen > [Sitzungstyp] > [Sitzungstyp] Sitzung**.  
Beispiel: **Sitzungen > RDP > RDP-Sitzungen**  
Die bereits vorhandene Sitzungen werden angezeigt
2. Markieren Sie die Mappe, die Sie kopieren möchten
3. Klicken Sie .  
Eine Kopie der Mappe wird im gleichen Ordner erstellt.


## Verwendung von RAM bei IZ1 und UD2-MM

Wie wird RAM von Prozessen in UD2-MM und IZ1 (auch bekannt als ARM- oder SoC-Geräte) genutzt?

Insgesamt 1024 MB Hauptspeicher werden wie folgt aufgeteilt:

- ~128 MB werden für Grafiken verwendet
- ~362 MB werden für interne Prozesse wie die Kommunikation zwischen DSP und ARM-Prozessor verwendet
- ~534 MB ist für Benutzerprozesse verfügbar

## Symantec Ghost zur Bereitstellung von IGEL OS verwenden

 Dieser Inhalt stammt aus Erfahrungen im Feld und wurde nicht von der Entwicklungsabteilung geprüft!

### Diskussionsthema/Problem

Symantec Ghost zur Bereitstellung von IGEL OS verwenden

### Firmware Version

IGEL OS10 und OS11 (11.02.100)

### UMS Version

6.01

### Beschreibung

Dies ist anstelle von SCCM und unserer Deployment-Appliance.

### Lösung

Wir implementieren und erfassen unsere IGEL-Basisinstallation auf/von einer virtuellen Maschine mit:

#### **vSphere Client 6.0, Version 11 VM:**

- 8 GB RAM
- 4 CPUs (1 Steckdose, 4-adrig)
- Video: 1 Bildschirm, 4 MB Speicher
- SCSI Controller Typ: LSI Logic SAS
- CD/DVD Drive 1: IGEL\_UDC\_10.05.500.ISO
- CD/DVD Drive 2: Symantec WinPE
- HDD: SCSI, Thick Provision Lazy Zeroed, 20 GB
- Netzwerk Adapter: VMXNET 3
- Boot Optionen/Firmware: EFI

#### **Booten Sie auf CD/DVD-Laufwerk 1 und navigieren Sie durch die UDC-Installationsoptionen:**

- UDC Installation
- Sprache: Englisch
- EULA: Ich stimme zu
- Legacy-Installation erzwingen: Nicht ausgewählt
- MS-DOS-Partitionierung während der Installation erzwingen: Ausgewählt
- Alte Einstellungen migrieren: Nicht ausgewählt
- Firmware installieren

- Herunterfahren (KEIN Neustart)


#### Booten Sie auf CD/DVD-Laufwerk 2:

- Boot nach WinPE
- Erfassen Sie HDD-Bilder mit dem Ghost-Befehl: `ghost64.exe -sure -clone,mode=create,src=1,dst=s:\igel\igel 10.05.500-YYYYMMDD_HHMMSS-0.gho -ial -ibg -nolilo`
  - `-ial` = Erzwingt eine Story-by-Sector-Kopie von Linux-Partitionen. Andere Partitionen werden normal kopiert.
  - `-ibg` = Ignoriere Ghost Boot Partition.
  - `-nolilo` = Versucht nicht, den LILO- oder GRUB-Bootloader nach einem Klon zu patchen. Wenn Sie den Schalter -NOLILO verwenden, können Sie Ihren Computer nach einem Klon von einem Speichermedium neu starten und dann `/sbin/lilo` oder das GRUB-Installationskript als root-Benutzer ausführen, um den Bootloader neu zu installieren

#### Zur Bereitstellung auf einem physischen Client:

- Boot nach WinPE
- Diskpart ausführen:
  - Wählen Sie Disk 0
  - bereinigen
  - Beenden
- Erfassen Sie HDD-Bilder mit dem Ghost-Befehl: `ghost64.exe -sure -clone,mode=restore,dst=1,src=s:\igel\igel 10.05.500-20190510_185741-0.gho -ial -ibg -nolilo`
  - `-ial` = Erzwingt eine Story-by-Sector-Kopie von Linux-Partitionen. Andere Partitionen werden normal kopiert
  - `-ibg` = Ignoriere Ghost Boot Partition.
  - `-nolilo` = Versucht nicht, den LILO- oder GRUB-Bootloader nach einem Klon zu patchen. Wenn Sie den Schalter -NOLILO verwenden, können Sie Ihren Computer nach einem Klon von einem Speichermedium neu starten und dann `/sbin/lilo` oder das GRUB-Installationskript als root-Benutzer ausführen, um den Bootloader neu zu installieren
  - `-szee` = Zwing Norton Ghost, die Größen aller Zielpartitionen gleich wie in der Quellpartition zu halten (keine Größenänderung).

Wir führen keine Bildvorbereitung durch, außer dem Befehl `diskpart clean`.

 Dieser Inhalt stammt aus Erfahrungen im Feld und wurde nicht von der Entwicklungsabteilung geprüft!

## Das Starten der UMS-Konsole führt zum Absturz der NX-Sitzung

### Problem

Wenn Sie mit einem Ubuntu-Host über NX verbunden sind, verursacht das Starten der UMS-Konsole auf dem Ubuntu-Host den Absturz der NX-Sitzung.

### Lösung

1. Werden Sie **Root** auf dem Ubuntu-Host.
2. Öffnen Sie die Konfigurationsdatei `/opt/IGEL/RemoteManager/rmclient/RemoteManager.bin.config` in einem Texteditor.
3. Fügen Sie in die Datei die Zeile `vmparam -Dsun.java2d.xrender=false` hinzu.
4. Speichern Sie die Datei.
5. Werden Sie ein regulärer Benutzer.
6. Starten Sie die UMS-Konsole.

## IGEL Setup im Appliance-Modus aufrufen

### Symptom

Im Appliance-Modus ist IGEL Setup nicht direkt zugänglich.

### Problem

Im Appliance-Modus sind alle anderen lokalen Anwendungen versteckt; der Hotkey des Systems [Strg+Alt+s] funktioniert auch nicht.

### Lösung

Um IGEL Setup im Appliance-Modus zu starten, drücken Sie den Hotkey [Strg+Alt+F2].

Eine Anwendung wird beendet mit der Nachricht "Speicherstand niedrig! Prozess ... wird beendet"

## Symptom

Eine lokale Anwendung oder Sitzung wird beendet, und eine Nachricht wird angezeigt, die **Speicherstand niedrig! Prozess [...] wird beendet** lautet.

Beispiel:



## Umgebung

- IGEL OS 11.04 oder höher

## Problem

Das System hat zu wenig freien Arbeitsspeicher. Als Gegenmaßnahme hat das System die Anwendung beendet.

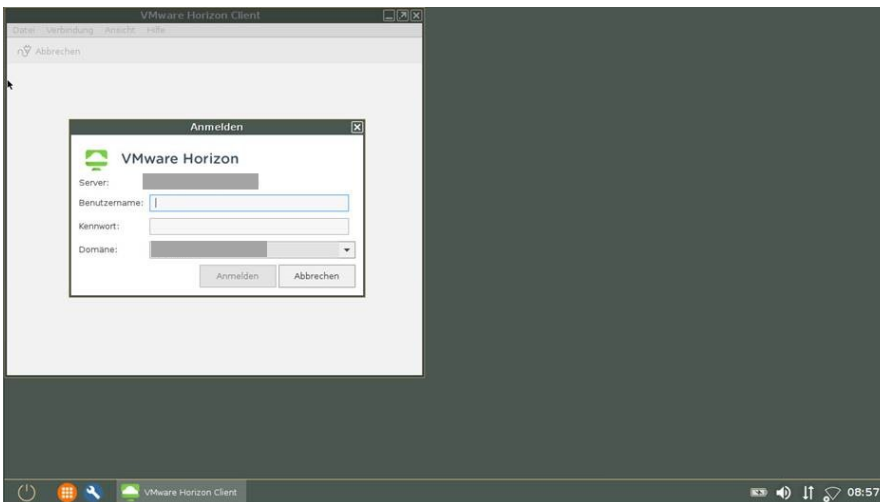
## Lösung

- ▶ Schließen Sie andere Anwendungen, die nicht benötigt werden, und starten Sie die Anwendung neu.
- ▶ Wenn die beendete Anwendung Chromium oder Firefox ist, starten Sie diese neu und versuchen Sie, weniger offene Tabs zu verwenden.
- ▶ Wenn das Problem oft auftritt, ziehen Sie eine Speichererweiterung für die Geräte in Erwägung.

## Ein Anwendungsfenster kann nicht verschoben werden

### Symptom

Einige Anwendungsfenster, z.B. VMware Horizon Fenster, werden beim Start in der linken oberen Ecke platziert, anstatt mittig angezeigt zu werden. Bei rahmenlosen Anwendungen kann das Fenster in diesem Fall nicht verschoben werden und verdeckt möglicherweise Symbole.



### Problem

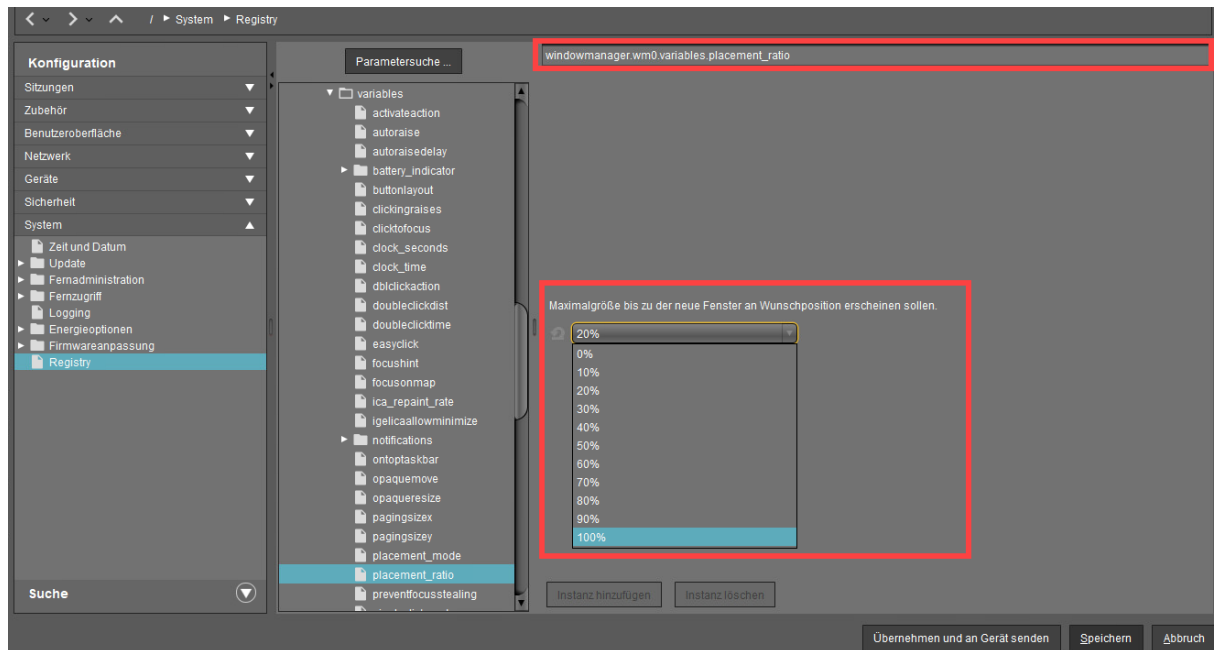
Entweder ist der Bildschirm zu klein oder die gewählte Auflösung ist zu niedrig.

### Lösung

1. Gehen Sie auf **System > Registry**.
2. Suchen Sie nach dem Registry Key `windowmanager.wm0.variables.placement_ratio`.
3. Geben Sie unter **Maximalgröße bis zu der neue Fenster an Wunschposition erscheinen sollen** einen höheren Prozentwert ein. Diese Angabe bezieht sich auf die Gesamtarbeitsfläche.

**i** Die Wunschposition wird mit dem Registry Key `windowmanager.wm0.variables.placement_mode` festgelegt.





## Beispiel

Sitzung: VMware Horizon Client

Bildschirmauflösung: 1366x768

Wert für **Maximalgröße bis zu der neue Fenster an Wunschposition erscheinen sollen**: mindestens 40%

## IGEL UMD aktualisieren: Fehler "Nicht kompatibel mit System 5"

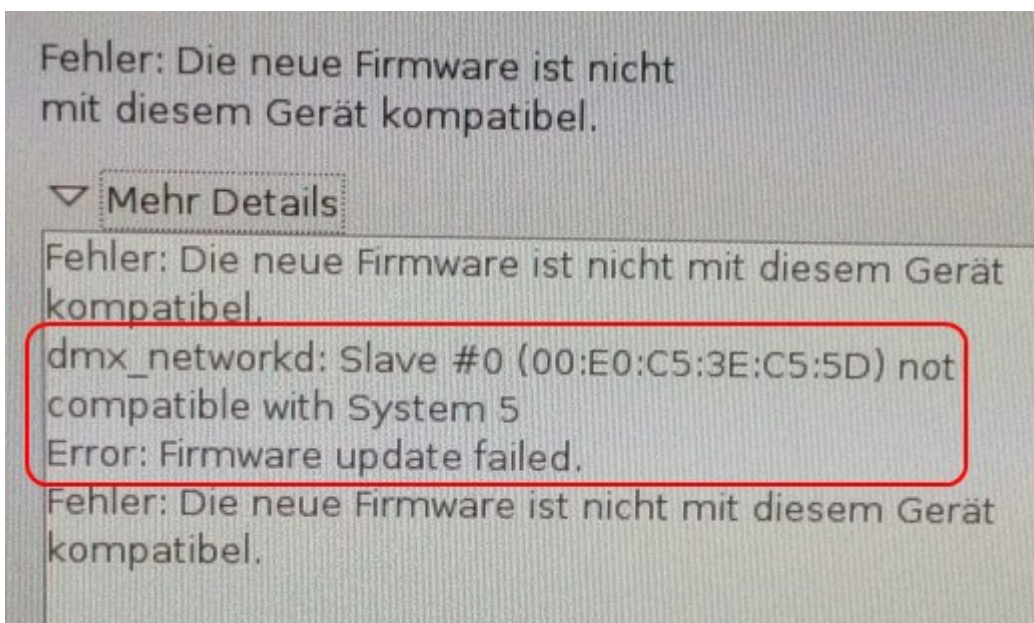
### Symptom

Universal Multi Display Firmware (IGEL UMD) kann nicht auf Version 4.13.100 aktualisiert werden.

Fehlermeldung:

```
Firmware not compatible.
```


```
dmx_networkd: Slave #0 (MAC) not compatible with System5
```



### Lösung

Datei `/tmp/NOT_SYS_5_COMPATIBLE` aus dem UMD-Master-Client löschen und ohne Neustart erneut aktualisieren.

## IGEL Endpoint Partners: Ensuring Image Integrity with a Checksum

 Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

## Wird meine Sitzung geschlossen, wenn mein IGEL OS Endgerät in den Suspend-Modus wechselt?

In diesem Artikel erfahren Sie, wie Sie Ihr IGEL OS-Gerät so konfigurieren, dass Ihre Sitzung nicht unterbrochen wird, wenn das Gerät in den Suspend-Modus geht.

### Sitzungsunterbrechung bei Suspend

Wenn ein IGEL OS Endgerät in den Suspend-Modus (S3) wechselt, werden Remote-Sitzungen, wie z. B. Citrix, Microsoft Windows RDP oder VMware Horizon, getrennt.

### IGEL Umgebung

- Endgerät mit IGEL OS 11
- Remote-Sitzung, z. B. Citrix, Microsoft Windows RDP oder VMware Horizon

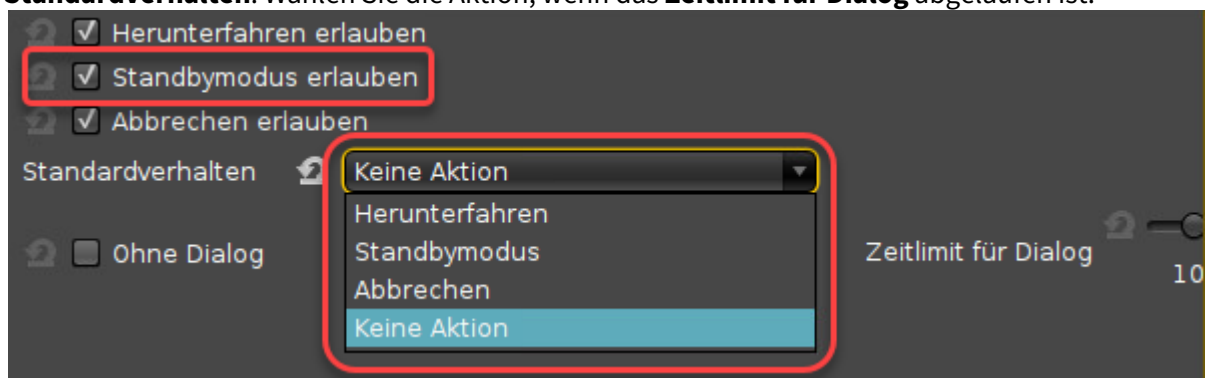
### Mögliche Probleme vermeiden

Moderne serverbasierte oder cloudbasierte Systeme verfügen über serverseitige Funktionen zur Wiederaufnahme von Remote-Sitzungen. Lesen Sie die entsprechende Dokumentation für Ihr System.

### Suspend-Modus konfigurieren

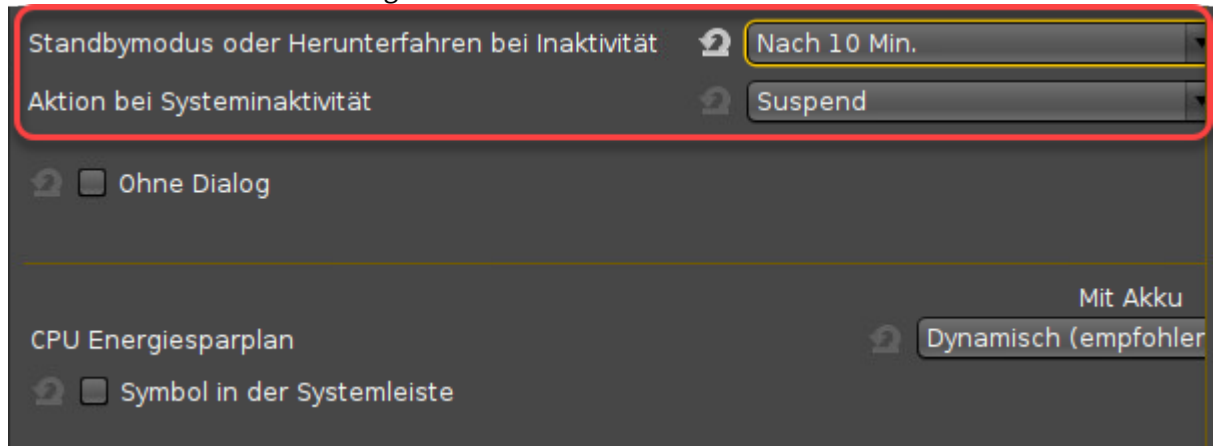
► Um den Suspend-Modus zuzulassen oder zu verbieten, gehen Sie zu **System > Energieoptionen > Herunterfahren** und stellen Sie die folgenden Parameter gemäß Ihren Anforderungen ein:

- **Standbymodus erlauben**
- **Standardverhalten:** Wählen Sie die Aktion, wenn das **Zeitlimit für Dialog** abgelaufen ist.



► Um das Anhalten oder Herunterfahren bei Inaktivität zu konfigurieren, gehen Sie zu **System > Energieoptionen > System** und stellen Sie die folgenden Parameter gemäß Ihren Anforderungen ein:

- **Standbymodus oder Herunterfahren:** Legen Sie den Timeout fest, nach der das System herunterfährt oder in den Suspend-Modus wechselt.
- **Aktion bei Systeminaktivität:** Legen Sie fest, ob das System nach dem Timeout in den Suspend-Modus wechseln oder heruntergefahren werden soll.



## IGEL OS - Integrationen von Drittherstellerprodukten

**i Rolling Release Info: OS 11.07.110**

Die hier angegebenen Informationen gelten für IGEL OS 11.07.110 und höher.

Die folgende Tabelle zeigt die in IGEL OS enthaltenen Funktionen von Drittanbietern, die derzeit mit den aufgeführten VDI-Verbindungen unterstützt werden.

Feature	IGEL OS AVD / W365	IGEL OS Citrix	IGEL OS VMwar e	IGEL OS RDP	Kommentare
Cisco JVDI Client	no	yes	yes	no	
Cisco WebEx Meetings VDI	no	yes	yes	no	
Cisco WebEx VDI	no	yes	yes	no	
Zoom VDI Media Plugin	yes	yes	yes	no	
Microsoft Teams Optimierung	yes	yes	yes	no	
Fabulatech USB Redirection	yes	yes	yes	yes	
Fabulatech Camera Redirection	yes	yes	no	no	
Fabulatech Scanner Redirection	yes	yes	yes	yes	
deviceTRUST	yes*	yes	yes*	no	* In Kürze verfügbar
DriveLock	no	yes	no	yes	
Diktamen	no	yes	partially*	yes	* Diktierfunktion wird unterstützt. es wird jedoch kein virtueller Kanal initiiert
Grundig dictation	no	yes	partially*	yes	* Diktierfunktion wird unterstützt. es wird jedoch kein virtueller Kanal initiiert

Feature	IGEL OS AVD / W365	IGEL OS Citrix	IGEL OS VMware	IGEL OS RDP	Kommentare
Nuance dictation	no	yes	partially *	no	* Diktierfunktion wird unterstützt. es wird jedoch kein virtueller Kanal initiiert
Olympus dictation	no	yes	partially *	yes	* Diktierfunktion wird unterstützt. es wird jedoch kein virtueller Kanal initiiert
Philips dictation	no	yes	partially *	yes	* Diktierfunktion wird unterstützt. es wird jedoch kein virtueller Kanal initiiert
SpeechWrite	no	yes	partially *	no	* Diktierfunktion wird unterstützt. es wird jedoch kein virtueller Kanal initiiert
Signotec signature	no	yes	yes*	yes	* Unter Verwendung der VMware HID Optimierung
StepOver signature	no	yes	yes*	yes	* Unter Verwendung der VMware HID Optimierung
Kofax signature (Wacom)	no	yes	yes*	yes	* Unter Verwendung der VMware HID Optimierung
Lakeside SysTrack	yes	yes	yes	yes	Unter Verwendung von clientseitigen virtuellen Kanälen
PrinterLogic	no	yes	no	yes	
ThinPrint	yes*	yes	yes	yes	* Unter Verwendung von ezeep für Azure
Tricerat	yes*	no	no	no	* Unter Verwendung der Tricerat Custom Partition für IGEL