

6

Working Paper
2023

KonsortSWD



Konsortium für die
Sozial-, Verhaltens-, Bildungs- und
Wirtschaftswissenschaften

Implementierung eines Gastwissenschafts- arbeitsplatzes im RDCnet

Technische Anleitung zur
Konfiguration eines Thin Clients

Jan Goebel, Neil Murray,
Kenny Pedrique, Ingo Sieber



September 2023

www.konsortswd.de

Implementierung eines Gastwissenschaftsarbetsplatzes im RDCnet

Technische Anleitung zur Konfiguration eines Thin Clients

Jan Goebel¹, Neil Murray¹, Kenny Pedrique¹, Ingo Sieber¹

September 2023

¹ SOEP am DIW Berlin

Abstract

Im Rahmen des RDCnet stellt jedes teilnehmende Forschungsdatenzentrum (FDZ) einen Gastwissenschaftsarbetsplatz (GWAP) zur Verfügung, über den Nutzende auf die Forschungsdaten anderer teilnehmender FDZ zugreifen können. Um die im multilateralen Kooperationsvertrag definierten technischen und organisatorischen Maßnahmen für den GWAP umzusetzen, empfiehlt es sich, restriktiv konfigurierte Thin Clients als Endgeräte zu verwenden. In diesem Dokument wird anhand eines Thin Clients der Marke "IGEL" konkret aufgezeigt, wie das Gerät, unter Berücksichtigung der technischen und organisatorischen Maßnahmen, für das RDCnet eingerichtet und konfiguriert werden kann.

Keywords: Forschungsdateninfrastruktur, Remote Access, Gastwissenschaftsarbetsplatz, Forschungsdatenzugang, Sensible Forschungsdaten

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
1. Einleitung und technisches Konzept des RDCnet	4
2. Anforderung als Datenempfänger: Bereitstellung eines GWAP	6
3. Ressourcen und Kosten.....	8
4. Registrieren einer IGEL Lizenz.....	10
4.1. Registrierung IGEL License Portal.....	10
4.2. Registrierung einer IGEL Lizenz.....	11
5. Installation und Konfiguration der UMS	12
5.1. Download und Systemvoraussetzungen	12
5.2. Installation der UMS	13
5.3. Konfiguration der UMS.....	15
5.3.1. Netzwerkkonfiguration.....	15
5.3.2. UMS Lizenz-ID.....	16
5.3.3. Backup	17
5.3.4. Datasource	18
5.4. Hinzufügen eines IGEL OS Gerät (Thin-Client)	19
5.4.1. Geräte Lizenz der UMS hinzufügen	19
5.4.2. IGEL OS Gerät suchen	20
5.4.3. IGEL OS Gerät registrieren.....	21
5.4.4. Thin Client Vorschau.....	22
6. Sicherheitskonfiguration des Thin Client.....	23
6.1. Vorbereitung	23
6.2. Deaktivierung von Peripheriegeräten	24
6.3. Deaktivierung von Druckern.....	25
6.4. Deaktivierung von Bildschirmaufnahmen	26
6.5. Deaktivierung von Fernzugriffen auf das Terminal.....	26
6.6. Deaktivierung von Hotplug-Speichergeräten.....	27
6.7. Fertigstellung.....	27
7. VMware Horizon Client	29
7.1. Konfiguration VMware Horizon Client.....	30
7.1.1. Globale Horizon Client Konfigurationen.....	33

7.1.2.	Konfiguration Horizon Client Sitzungen	36
7.2.	Profil einem IGEL-Gerät hinzufügen	38
7.3.	Prüfung	40
8.	Zusammenfassung	41
	Literaturverzeichnis	42

1. Einleitung und technisches Konzept des RDCnet

Das RDCnet dient dazu, bestehende Gastwissenschaftsarbeitsplätze (GWAP) der teilnehmenden Forschungsdatenzentren (FDZ) in einem Netzwerk von gesicherten Datenzugangsstellen zu vereinen. Dadurch können Forschende auf sensitive Daten (z.B. nur formal anonymisierte) der teilnehmenden FDZ zugreifen, unabhängig davon, an welchem GWAP sie arbeiten. Durch den erleichterten Zugang kann die Anzahl der Datennutzenden erhöht werden, wobei die Kontrolle über den letztendlichen Zugriff auf Datensätze weiterhin den Datenanbietern obliegt, um somit auch individuelle Standards der Datensicherheit gewährleisten zu können.

Neben den vertraglichen Richtlinien (siehe Murray & Goebel, 2022) ist die Festlegung von technischen Standards eine wichtige Grundlage für die Schaffung eines kompatiblen und realisierbaren Netzwerks. Die technische Umsetzung baut auf dem Konzept des "FDZ-im-FDZ" (Bender & Heinig, 2011) auf und erweitert es für multilaterale Kooperationen. Jedes FDZ stellt dabei einen GWAP in Form eines Thin-Clients innerhalb eines Datensicherheitsraums zur Verfügung. Von diesem GWAP aus besteht die Möglichkeit, über "Secure Remote Access"¹ auf virtuelle Desktops anderer FDZ zuzugreifen, um die bereitgestellten Forschungsdaten zu bearbeiten. Dabei befinden sich die Forschungsdaten stets auf den Servern des datengebenden FDZ und verlassen diese zu keinem Zeitpunkt physisch. Jedes teilnehmende FDZ übernimmt im RDCnet also zwei Rollen: Zum einen die Rolle des Datenempfängers (Bereitstellung eines GWAP, um in einer sicheren Umgebung auf die Daten anderer FDZ zuzugreifen) und zum anderen die Rolle des Datengebers (Bereitstellung virtueller Desktops, auf denen die eigenen Forschungsdaten von den GWAP der teilnehmenden FDZ per Secure Remote Access analysiert werden können).

Ein solches Netzwerk von sicheren Datenzugangsstellen kann durch den Einsatz einer "Virtuellen Desktop-Infrastruktur" (VDI) realisiert werden. Dabei werden den Nutzenden virtuelle Desktops zur Verfügung gestellt, die jedoch nicht lokal an den GWAP, sondern auf den Servern der datengebenden FDZ gehostet werden. Über den Secure Remote Access wird den Nutzenden lediglich eine visuelle Kopie des Desktops an ihren GWAP angezeigt, der sich tatsächlich auf den Servern der datengebenden FDZ befindet. Die Daten, die durch den Thin Client übertragen werden, beschränken sich auf ein Abbild des Desktops sowie Tastatur- und Mausbewegungen. Dadurch wird zweierlei sichergestellt, (a) dass die Daten weiterhin nur in kontrollierten Umgebungen analysiert werden können und (b) die datengebenden FDZ zu jedem Zeitpunkt die volle Kontrolle über den Zugriff auf die Daten behalten.

Dieses Dokument hat den Zweck, die technischen Anforderungen und Kriterien in der Rolle des Datenempfängers zu definieren. Es beinhaltet eine Beschreibung und konkrete technische

¹ Secure Remote Access wird als gesicherter Fernzugriff definiert. Dies bedeutet, dass der Fernzugriff nur von dedizierten Zugangsstellen erfolgen kann.

Anleitung, wie ein Thin Client unter Berücksichtigung der vertraglich festgelegten technischen und organisatorischen Maßnahmen (siehe Murray & Goebel, 2022) als GWAP für das RDCnet konfiguriert und umgesetzt werden kann.

Da die in diesem Dokument gegebenen Anleitungen und Konfigurationsschritte von der Versionierung verschiedener Software abhängig sind, kann es sein, dass einzelne Passagen über die Zeit überarbeitet und aktualisiert werden müssen. In einem solchen Fall erscheint dieses Dokument als neue Version auf Zenodo. Änderungen der Versionierung werden in den Zenodo-Metadaten gekennzeichnet.

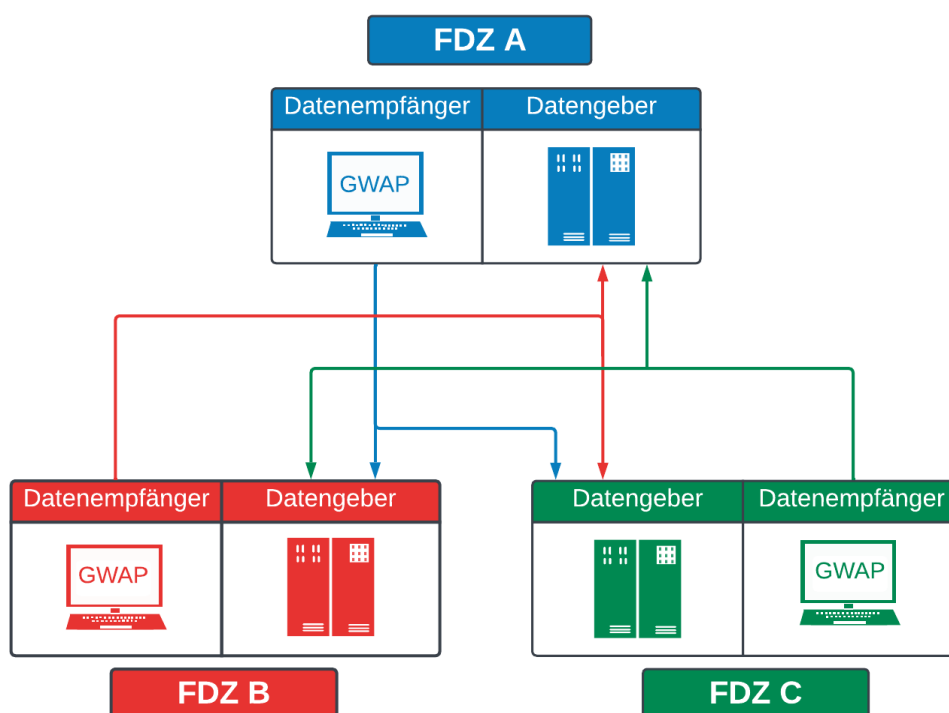


Abbildung 1: Netzwerkstruktur und Rollen im RDCnet. Pfeile stellen den sicheren Fernzugriff dar.
Quelle: Eigene Darstellung

2. Anforderung als Datenempfänger: Bereitstellung eines GWAP

Auf einer technischen Ebene benötigt jedes teilnehmende FDZ zum einen eine VDI, die den Secure Remote-Access von den anderen FDZ aus ermöglicht, und zum anderen ein eigenes Endgerät für den GWAP, mit dem eine Verbindung zu den virtuellen Desktops der anderen FDZ aufgebaut werden kann. Grundsätzlich steht es jedem teilnehmenden FDZ frei, einen beliebigen Computer als Endgerät zu nutzen, sofern die technischen und organisatorischen Maßnahmen erfüllt sind. Dennoch hat sich gezeigt, dass die Verwendung eines sogenannten Thin Client (siehe Kasten für Definition) als Endgerät besonders geeignet ist, wenn man die Konfiguration von Remote-Access Software und die Einhaltung der Sicherheitskriterien berücksichtigt. Thin Clients bieten also einige Merkmale, die sich optimal für den Anwendungsfall im RDCnet eignen:

1. Remote Access: Thin Clients sind speziell dafür konzipiert, eine Verbindung zu Servern mittels Remote Access Software herzustellen. Die Konfiguration solcher Verbindungen ist in der Regel intuitiv und kann zentralisiert erfolgen.
2. Keine lokale Speicherung: Thin Clients verfügen in der Regel nicht über interne Speicherkapazitäten. Dadurch ist es nicht möglich, Daten lokal auf dem Gerät zu speichern. Dies gewährleistet eine bessere Datensicherheit und schützt vor unbefugter Weitergabe von Daten und Informationen.
3. Sicherheitsoptionen: Thin Clients bieten Sicherheitsoptionen, die sich für sensible Umgebungen wie das RDCnet eignen. In der Administrationsoberfläche können beispielsweise Funktionen wie das Verhindern von Bildschirmaufnahmen, die Deaktivierung von Peripheriegeräten oder der eingeschränkte Zugriff auf das interne Netzwerk mit wenigen Klicks aktiviert werden.
4. Betriebssystem: Ein weiterer Vorteil ist, dass Thin Clients mit einem "Thin-OS" ausgestattet sind. Im Vergleich zu einem gängigen Betriebssystem, müssen nicht umständlich alle unerwünschten Eigenschaften abgeschaltet und Standard-einstellungen eruiert und umgestellt werden. Dies minimiert den Aufwand für die Ersteinrichtung als auch die kontinuierliche Wartung der Zugangsgeräte.

Zusammenfassend lässt sich festhalten, dass die Verwendung von Thin Clients als GWAP innerhalb des RDCnet eine kosteneffiziente und zeitsparende Möglichkeit bietet, die erforderlichen technischen und organisatorischen Maßnahmen umzusetzen.

Im vorliegenden Dokument wird eine umfassende Anleitung zur Konfiguration eines Thin Clients der Marke "IGEL" bereitgestellt, um die Sicherheitskriterien gemäß der multilateralen Kooperationsvereinbarung des RDCnet zu erfüllen und den Thin Client als GWAP nutzen zu können. Das Dokument bietet insbesondere denjenigen FDZ eine Hilfestellung, die noch

keinen GWAP implementiert haben und soll die Einstiegshürde senken, einen solchen Arbeitsplatz umzusetzen.

Das Dokument ist wie folgt strukturiert: Zunächst werden allgemeine Informationen zum Modell des Thin Clients dargelegt, einschließlich der Hardware- und Lizenzkosten. Anschließend wird erläutert, wie eine IGEL-Lizenz registriert wird. Im nächsten Kapitel wird die Installation und Konfiguration der zentralen Administrationsoberfläche (UMS) erläutert und es wird das Vorgehen zum Hinzufügen von IGEL Thin Clients innerhalb der UMS beschrieben. Das darauffolgende Kapitel zeigt, wie die Sicherheitskonfiguration des Thin Clients durchgeführt werden sollte, um die technischen und organisatorischen Anforderungen zu erfüllen. Schließlich wird im letzten Kapitel erläutert, wie der VMware Horizon Client auf dem Thin Client installiert wird und wie Verbindungen zu anderen FDZ vordefiniert und hergestellt werden.

Was sind Thin Clients?

Ein Thin Client ist ein Endgerät, das insbesondere in Computernetzwerken verwendet wird. Im Gegensatz zu herkömmlichen PCs ist ein Thin Client weniger leistungsfähig und hat eine geringere Speicherkapazität. Er dient hauptsächlich als Zugriffspunkt auf Anwendungen und Daten, die auf einem zentralen Server gespeichert sind. Der Thin Client fungiert also als eine Art Terminal, das über eine Netzwerkverbindung mit dem Server kommuniziert und die Berechnungen und Verarbeitungsaufgaben auf dem Server ausführt. Dabei wird das Betriebssystem und die Anwendungssoftware auf dem Server ausgeführt, während der Thin Client lediglich die Benutzeroberfläche darstellt und die Eingaben und Ausgaben verarbeitet. Thin Clients haben den Vorteil, dass sie kostengünstiger, energieeffizienter und leichter zu verwalten sind als traditionelle Computer. Sie eignen sich also besonders gut für Umgebungen, in denen eine zentrale Steuerung, Datensicherheit und ein einfacher Zugriff auf gemeinsam genutzte Ressourcen erforderlich sind.

Hinweis: Dies ist keine offizielle Dokumentation des Herstellers IGEL, sondern eine eigene Zusammenfassung der relevanten Schritte und Konfigurationen, die notwendig sind, um einen IGEL Thin Client für das RDCnet einzurichten. Sollten Schritte in dieser Anleitung zusätzliches Hintergrundwissen erfordern, empfehlen wir, den offiziellen "Getting-started-Guide" von IGEL (<https://www.igelcommunity.com/igel-getting-started-guide>) oder die IGEL Knowledge Base (<https://kb.igel.com/>) zu konsultieren. Diese Quellen bilden auch die Grundlage für diese Anleitung.

3. Ressourcen und Kosten

Die vorliegende Dokumentation beschreibt die Verwendung eines IGEL Thin Clients (Modell: UD3 M350C-LX) in Verbindung mit der aktuellen Version des IGEL OS (Betriebssystem des Thin Client). Grundsätzlich werden für die Nutzung des Thin Clients folgende Komponenten benötigt:

1. IGEL Thin Client (Gerät):



IGEL UD3-LX M350c 4/8 GB OS11 SCR (HD05B0101F00000)

★★★★★ (0)

Hersteller-Nr.: HD05B0101F00000
Bechtle-Nr.: 4461123

- Prozessormodell: AMD Ryzen Embedded R1505G, 2,40 GHz
- Arbeitsspeicher: 4 GB
- Betriebssystem: IGEL Universal Desktop (Linux)
- Grafikkarte: AMD Radeon Vega 3 Graphics
- Herstellergarantie: 2 Jahre Bring-In, bei Registrierung 5 Jahre Bring-In (Details siehe Hersteller-Web-Site)

Mehr Produkte zu IGEL UD3 M350c Thin Clients

Modellvariante ändern

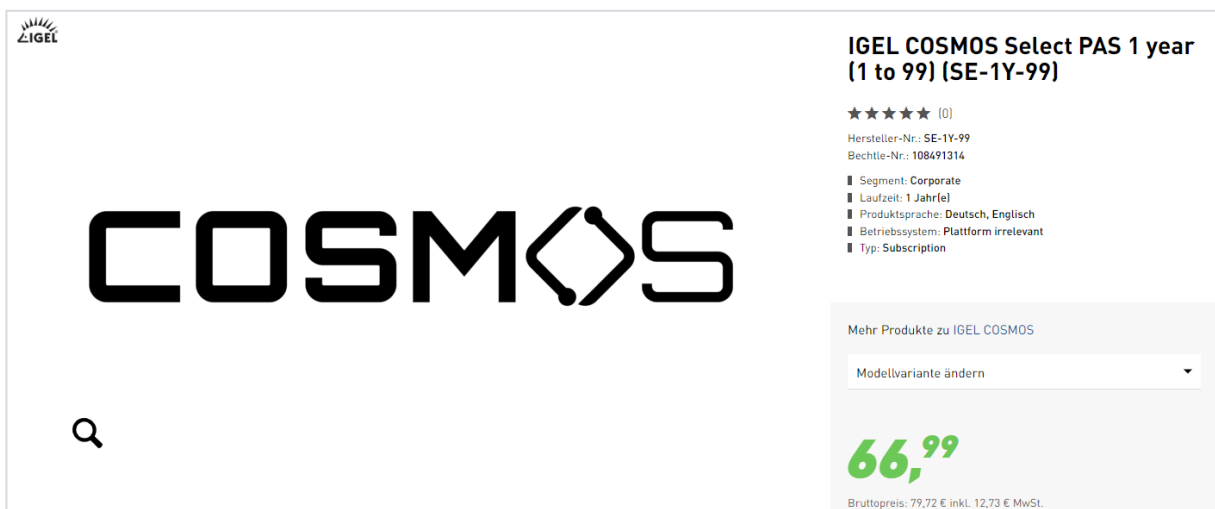
481,99

Bruttopreis: 573,57 € inkl. 91,58 € MwSt.

Abbildung 2: Referenzangebot eines IGEL UD3

Quelle: <https://www.bechtle.com/shop/igel-ud3-lx-m350c-4-8-gb-os11-scr--4461123--p>, 16.05.2023

2. IGEL OS 11 (Betriebssystem des Thin Client- Bestandteil des IGEL „COSMOS“ Lizenzpakets)



IGEL COSMOS Select PAS 1 year (1 to 99) (SE-1Y-99)

★★★★★ (0)

Hersteller-Nr.: SE-1Y-99
Bechtle-Nr.: 108491314

- Segment: Corporate
- Laufzeit: 1 Jahr(e)
- Produktsprache: Deutsch, Englisch
- Betriebssystem: Plattform irrelevant
- Typ: Subscription

Mehr Produkte zu IGEL COSMOS

Modellvariante ändern

66,99

Bruttopreis: 79,72 € inkl. 12,73 € MwSt.

Abbildung 3: Referenzangebot IGEL COSMOS Lizenz (1 Jahr)

Quelle: <https://www.bechtle.com/shop/igel-cosmos-select-pas-1-year-1-to-99--108491314--p>, 16.05.2023

4. Registrieren einer IGEL Lizenz

4.1. Registrierung IGEL License Portal

Der erste Schritt nach dem Erwerb eines IGEL Thin-Clients und des entsprechenden Lizenzpakets besteht darin, die Lizenz im IGEL License Portal (ILP) zu registrieren. Das ILP ist ein cloudbasiertes Portal zur Verwaltung aller IGEL-Lizenzen. Bevor jedoch eine IGEL-Lizenz registriert werden kann, ist es erforderlich, ein Konto für das ILP zu erstellen.

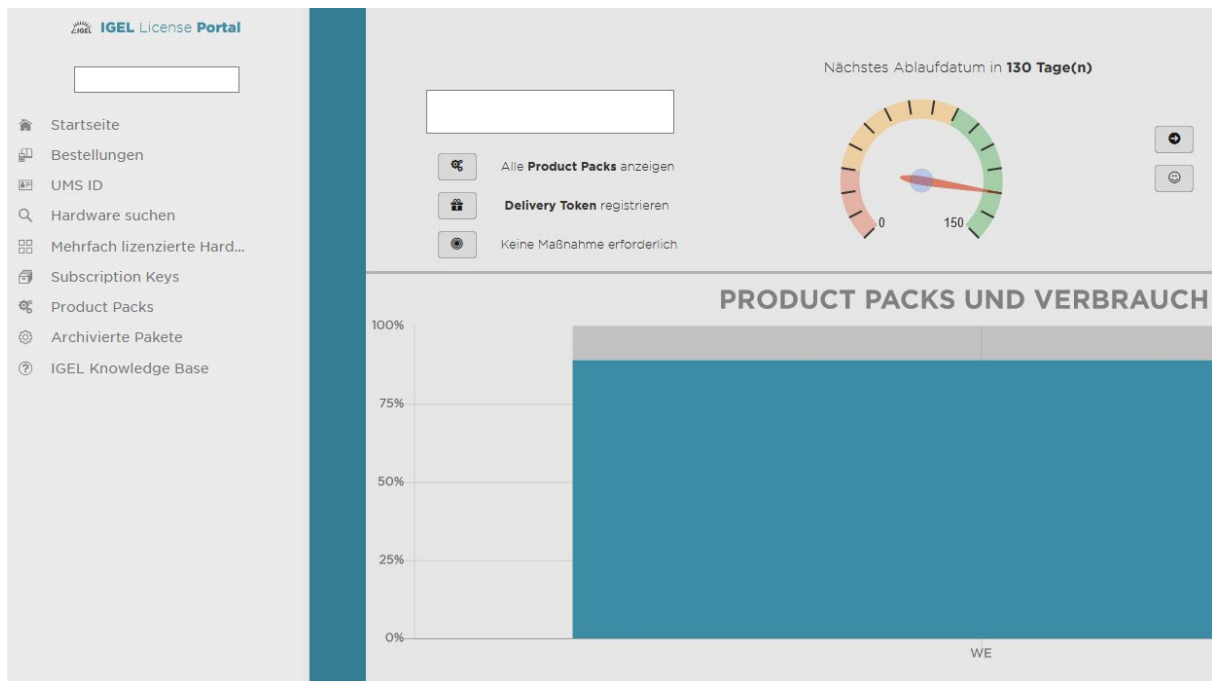


Abbildung 5: IGEL License Portal

Quelle: Eigene Darstellung

Gehen Sie hierfür wie folgt vor:

1. Gehen Sie auf activation.igel.com und klicken auf „Registrieren“.
2. Füllen Sie alle Felder aus und klicken auf „Weiter“.
3. Füllen Sie die Felder auf der Seite „Firmendetails“ aus. Geben Sie einen IGEL Subscription Key (Seriennummer der Subscription) an, z. B. "WE-12345-C". Ein Subscription Key ist für den Abgleich ausreichend. Alternativ können Sie auch den Delivery Token angeben, z. B. "ITUS-DN-123456". Wenn Sie fertig sind, klicken Sie auf „Weiter“.
4. Bestätigen Sie die Datenschutzbestimmungen, lösen Sie das Captcha und klicken Sie „Weiter“.
5. Wenn Sie sicher sind, dass Ihre Daten korrekt sind, klicken Sie innerhalb des Bestätigungsdialogs auf „Ja“ und dann im Hauptfenster auf „Fertigstellen“. Die Anfrage wird nun an das IGEL Support Team gesendet. War die Registrierung erfolgreich, erhalten Sie eine E-Mail vom IGEL Support Team, mit der Sie sich im IGEL License Portal anmelden können.

(IGEL Knowledge Base [1]: Die in diesem Kapitel vorliegenden Informationen sind am 17.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/gettingstarted/de/igel-license-portal-ilp-51194193.html> nachgelesen werden)

4.2. Registrierung einer IGEL Lizenz

Dieses Kapitel betrifft ausschließlich Lizenzen, die vor September 2021 erworben wurden. Ab September 2021 sind die Lizenzen sofort einsatzbereit und erfordern keine Delivery Tokens². In diesem Fall kann Kapitel 4.2 übersprungen werden.

Für die erfolgreiche Registrierung einer IGEL Lizenz müssen nun folgende Dinge vorhanden sein:

- ✓ Ein bestätigtes Benutzerkonto und ein Kennwort für den Zugriff auf das IGEL-Lizenzportal (siehe dazu Kapitel 3.1).
- ✓ Eine gültige IGEL-Lizenz, die Sie zuvor erworben haben (IGEL Workspace Edition oder IGEL Enterprise Management Pack).
- ✓ Die ID des Thin Client-Geräts, das Sie registrieren möchten (Diese findet sich beispielsweise auf dem Gerätelabel auf der Rückseite des Geräts).

Mit diesen Informationen kann nun die Registrierung des Geräts innerhalb des ILP erfolgen. Gehen Sie dabei wie folgt vor:

1. Rufen Sie das IGEL-Lizenzportal über Ihren Webbrowser auf: activation.igel.com.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf "Login".
3. Drücken Sie das Benutzersymbol oben links auf dem Bildschirm.
4. Klicken Sie auf die Schaltfläche "Delivery Token registrieren" auf dem Bildschirm.
5. Geben Sie die Delivery Token des Thin Client-Gerätes ein, das Sie registrieren möchten, und klicken Sie auf "Weiter".
6. Wählen Sie den von Ihnen erworbenen Lizenztyp (IGEL Workspace Edition oder IGEL Enterprise Management Pack) und klicken Sie auf "Weiter".
7. Überprüfen Sie die Lizenzdetails und klicken Sie auf "Fertig stellen", um die Registrierung abzuschließen.

(IGEL Knowledge Base [1]: Die in diesem Kapitel vorliegenden Informationen sind am 17.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/gettingstarted/de/igel-license-portal-ilp-51194193.html> nachgelesen werden)

² Ein Delivery Token ist ein Code, den Sie von Ihrem IGEL-Händler erhalten, nachdem Sie Lizenzen für ein IGEL-Produkt erworben haben. Ein Beispiel für ein Delivery Token lautet: DLV-32LEW. Sie erhalten das Delivery Token entweder per E-Mail oder es ist auf dem Lieferschein eines Geräts vermerkt. Sie können beispielsweise auf Ihrem IGEL Universal Desktop Paket nachsehen. Um Ihre Lizenzen zu erhalten, registrieren Sie Ihr Delivery Token im IGEL Lizenz-Portal. Nach der Registrierung Ihres Delivery Tokens erhalten Sie Zugriff auf die erworbenen Lizenzen. Diese Lizenzen sind in Produkt-Paketen organisiert. Weitere Informationen finden Sie in der IGEL Knowledge Base unter folgendem Link: [1]: <https://kb.igel.com/gettingstarted/de/igel-license-portal-ilp-51194193.html> (Stand: 14.06.2023).

5. Installation und Konfiguration der UMS

Die IGEL Universal Management Suite (UMS) ist eine Softwarelösung zur zentralen Verwaltung von IGEL Thin Clients. Mit der UMS können Administratoren Firmware-Updates durchführen, Konfigurationen verwalten, Sicherheitseinstellungen implementieren und Softwareanwendungen bereitstellen. Die Oberfläche ermöglicht die Verwaltung von Gerätegruppen, die Festlegung von Richtlinien und individuelle Einstellungen. Die UMS bietet zudem erweiterte Funktionen wie Energiesparmanagement, Remote-Desktop-Sitzungen und Fernüberwachung.

5.1. Download und Systemvoraussetzungen

Die aktuelle Version der UMS kann unter <https://www.igel.com/software-downloads/workspace-edition/> heruntergeladen werden und ist unter anderem für Windows und Linux Systeme verfügbar. Für den Download müssen zuerst die Benutzerinformationen (Name, Unternehmensname und E-Mail), welche bei der Registrierung des ILP verwendet wurden, angegeben werden. In der folgenden Beschreibung wird die **UMS Version 12.1.110³** verwendet, wobei empfohlen wird stets die aktuelle Version zu nutzen.

Die Systemvoraussetzungen der UMS lauten dabei wie folgt:

- Betriebssystem:
 - Linux-Distributionen wie Ubuntu 20.04, CentOS 7/8, Red Hat Enterprise Linux 7/8 oder SUSE Linux Enterprise Desktop/Server 15 SP2/SP3.
 - Windows: Windows 10 oder höher, Windows Server 2012 R2 oder höher, Windows 7 oder höher, Windows Server 2008 R2 oder höher
- Prozessor: Ein 64-Bit-Prozessor mit mindestens 4 Kernen wird empfohlen.
- Arbeitsspeicher (RAM): Mindestens 8 GB RAM sind erforderlich, aber 16 GB oder mehr werden empfohlen.
- Festplattenspeicher: Mindestens 5 GB freier Speicherplatz auf der Festplatte wird empfohlen.
- Java Runtime Environment (JRE): Version 11 von Oracle JRE oder OpenJDK 11 wird benötigt.
- Netzwerk: Ein Netzwerk mit einer Bandbreite von mindestens 1 Gbit/s wird empfohlen, um eine reibungslose Verwaltung von Geräten zu gewährleisten.

(IGEL Knowledge Base [2]: Die in diesem Kapitel vorliegenden Informationen sind am 17.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/endpointmgmt-6.04/en/installation-requirements-26035258.html> nachgelesen werden)

³ Screenshots sind teilweise in älteren Versionen erstellt worden und können sich visuell von der neusten UMS Version unterscheiden. Die Konfigurationsschritte können jedoch analog umgesetzt werden.

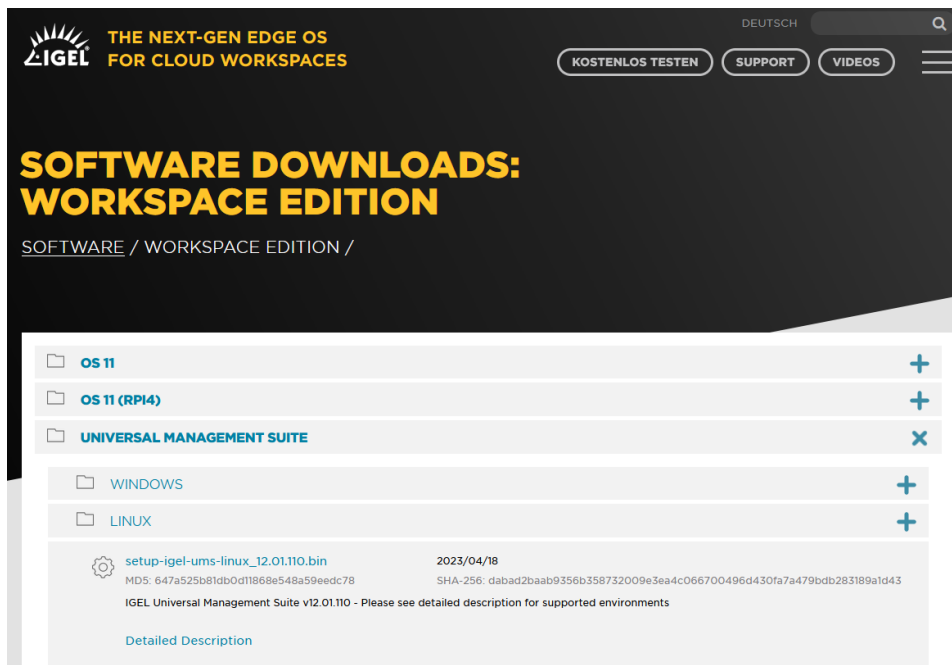


Abbildung 6: Download UMS.

Quelle: <https://www.igel.de/software-downloads/workspace-edition/> zugegriffen am 23.05.2023

5.2. Installation der UMS

Die Installation umfasst zwei Programme, die für weitere Konfigurationen relevant sind: der **UMS Administrator** und die **UMS Konsole**. Mit dem UMS Administrator werden globale Konfigurationen wie Netzwerkeinstellungen, Datenquellen oder Lizenzen für die UMS vorgenommen. Die UMS Konsole hingegen ist die Anwendung, mit der Thin Clients eingerichtet, konfiguriert und verwaltet werden können. Führen Sie für die Installation der beiden Programme folgende Schritte aus:

1. Führen Sie die entsprechende Installationsdatei unter Windows oder Linux aus und wählen Sie im ersten Schritt aus, in welchem Ordner die UMS installiert werden soll.
2. Wählen Sie folgenden Komponenten zur Installation aus: UMS Standardinstallation mit integrierter Datenbank -> UMS Standardserver -> Mit UMS Web App, Mit UMS Konsole, Mit integrierter Datenbank (siehe Abb. 6).

Komponenten auswählen
Welche Komponenten sollen installiert werden?

Wählen Sie die Komponenten aus, die Sie installieren möchten. Klicken Sie auf "Weiter", wenn sie bereit sind fortzufahren.

UMS Standardinstallation mit integrierter Datenbank

<input checked="" type="radio"/> UMS Standardserver (stand-alone)	1.148,3 MB
<input checked="" type="checkbox"/> Mit UMS Web App	416,5 MB
<input checked="" type="checkbox"/> Mit UMS Konsole	170,4 MB
<input checked="" type="checkbox"/> Mit integrierter Datenbank	20,1 MB
<input type="radio"/> Distributed UMS	541,6 MB
<input type="checkbox"/> Mit UMS Web App	416,5 MB
<input type="checkbox"/> Mit UMS Konsole	170,4 MB
<input type="radio"/> UMS High Availability Netzwerk	
<input type="checkbox"/> UMS Server	616,4 MB
<input type="checkbox"/> Mit UMS Konsole	170,4 MB
<input type="checkbox"/> Mit UMS Web App	416,5 MB
<input type="checkbox"/> UMS Load Balancer	215,4 MB
<input type="radio"/> Nur UMS Konsole	170,4 MB

Die aktuelle Auswahl erfordert min. 1.267,5 MB Speicherplatz.

Abbildung 7: Komponenten UMS Installation
Quelle: Eigene Darstellung

3. Nun muss angegeben werden in welchem Ordner das UMS Datenverzeichnis angelegt werden soll (notwendig für Benutzerdateien, Firmwareupdates...).
4. Definieren Sie einen Benutzernamen und Passwort für die Datenbankverbindung:

Benutzerangaben für die Datenbankverbindung
Geben Sie hier Ihren Benutzernamen und Ihr Passwort für die Datenbankverbindung ein

Geben Sie hier Ihren Benutzernamen und Ihr Passwort ein und klicken Sie 'Weiter'.

Benutzername

Passwort

Passwort wiederholen

Abbildung 8: Benutzerdaten festlegen
Quelle: Eigene Darstellung

Nach erfolgreicher Eingabe der Nutzerdaten sollte die Installation der UMS fertiggestellt sein.

5.3. Konfiguration der UMS

Um die UMS nach der Installation erfolgreich einzurichten, sind einige grundlegende Konfigurationen erforderlich, die im Folgenden beschrieben werden.

Öffnen Sie hierfür zuerst das „RMAAdmin“ Programm:

Unter Windows: Der Standardpfad zum UMS Administrator unter Windows: C:\Program Files (x86)\IGEL\RemoteManager\rmadmin\RMAAdmin.exe

Unter Linux: Lässt sich der UMS Administrator unter Linux nicht per Menü- oder Desktopverknüpfung starten, können Sie die Anwendung auf der Kommandozeile als root mit folgendem Befehl starten:

[IGEL-Installationsverzeichnis]/RemoteManager/RMAAdmin.sh (wenn das standardmäßige Installationsverzeichnis verwendet wird: /opt/IGEL/RemoteManager/RMAAdmin.sh).

5.3.1. Netzwerkkonfiguration

Im Abschnitt „Einstellungen > Ports“ ist es erforderlich, die Konfiguration der Ports vorzunehmen, über die der Zugriff auf den UMS-Server ermöglicht wird. Zudem muss festgelegt werden, ob die Verbindungen zum Server mittels SSL-Zertifikate eingeschränkt werden sollen.

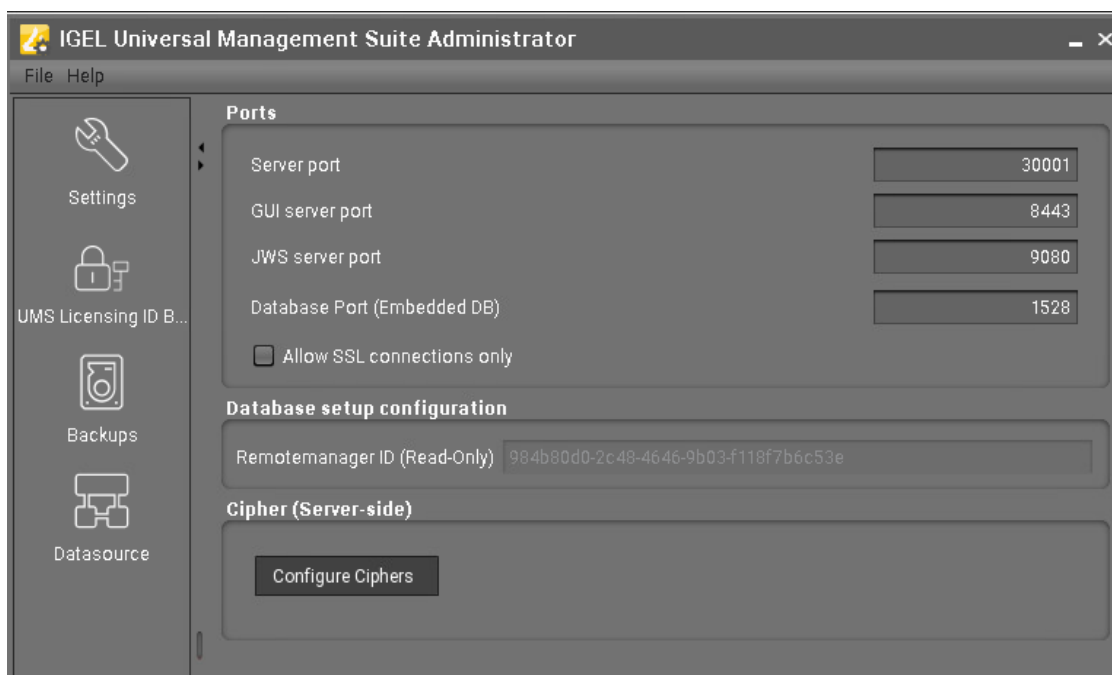


Abbildung 9: Konfiguration der Netzwerk-Ports.

Quelle: Eigene Darstellung

Folgende Ports werden verwendet (siehe Abb. 8):

- Server Port: der Port, über den der UMS-Server mit anderen Geräten oder Komponenten in Ihrem Netzwerk kommuniziert. Der Server Port wird verwendet, um

eingehende Verbindungen von IGEL Thin Clients, UMS-Administratoren oder anderen externen Systemen entgegenzunehmen. Standardmäßig ist der Server Port in der IGEL UMS auf Port 30001 eingestellt.

- GUI Server Port: Es handelt sich um den Port, der für die Kommunikation zwischen der UMS-Verwaltungskonsole und dem UMS-Server verwendet wird. Standardmäßig ist der GUI Server Port in der IGEL UMS auf Port 8443 eingestellt.
- JWS Server Port: Der Port, über den der Java Web Start (JWS) Server in der UMS kommuniziert. Der JWS Server ist für die Bereitstellung von Anwendungen und Updates auf den IGEL Thin Clients über das Netzwerk verantwortlich. Standardmäßig ist der JWS Server Port in der IGEL UMS auf Port 9080 eingestellt.
- Database Port (Embedded DB): Der Port, über den die UMS-Datenbank mit der UMS-Anwendung kommuniziert. Dieser Port ermöglicht den Datenaustausch und die Speicherung von Konfigurationsinformationen, Benutzerdaten, Geräteinformationen und anderen relevanten Daten. Standardmäßig ist der Database Port in der IGEL UMS auf Port 1528 eingestellt.

Die Server Ports können jedoch je nach Konfiguration der UMS geändert werden. Es kann erforderlich sein, den Port anzupassen, um mögliche Konflikte zu vermeiden oder die Sicherheitsrichtlinien Ihres Netzwerks zu erfüllen.

(IGEL Knowledge Base [3]: Die in diesem Kapitel vorliegenden Informationen sind am 17.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/endpointmgmt-5.09/de/igel-ums-kommunikationsports-22459132.html> nachgelesen werden)

5.3.2. UMS Lizenz-ID

Die richtige Konfiguration der UMS-Lizenz-ID ist entscheidend, um eine reibungslose automatische Lizenzbereitstellung in der UMS zu gewährleisten.

Der Abschnitt UMS-Lizenz-ID bietet die Möglichkeit, die Haupt-ID und die lokale ID zu konfigurieren. Zunächst sollten Sie sicherstellen, dass Sie über gültige Lizenzschlüssel verfügen. Die Haupt-ID repräsentiert die allgemeine Lizenz, die für die UMS-Bereitstellung verwendet wird, während die lokale ID spezifisch den UMS-Server anspricht. Durch die Konfiguration dieser IDs ermöglichen Sie die automatische Lizenzierung ohne die Notwendigkeit, für jeden einzelnen Lizenzkauf ein ALD-Token (Automatic License Deployment ⁴) zu verwenden.

⁴ Die korrekte Konfiguration der UMS-Lizenz-ID und die Nutzung des Automatic License Deployment (ALD) bietet mehrere Vorteile. ALD ermöglicht die automatische Bereitstellung von Lizenzen, ohne dass für jeden Lizenzkauf ein ALD-Token erforderlich ist. Dies spart Zeit und Aufwand bei der Verwaltung von Lizenzen und vereinfacht den Lizenzierungsprozess. Die UMS-Lizenz-ID wird im IGEL Lizenz-Portal registriert, um die automatische Lizenzierung zu aktivieren.

Zusätzlich zur Konfiguration der IDs müssen Sie das Verzeichnis festlegen, in dem das Backup dieser ID erstellt wird. Ein regelmäßiges Backup der UMS-Lizenz-ID ist äußerst wichtig, um mögliche Datenverluste zu vermeiden. Stellen Sie sicher, dass das Backup-Verzeichnis innerhalb eines sicheren Ordners gespeichert wird und regelmäßige Sicherungen durchgeführt werden.

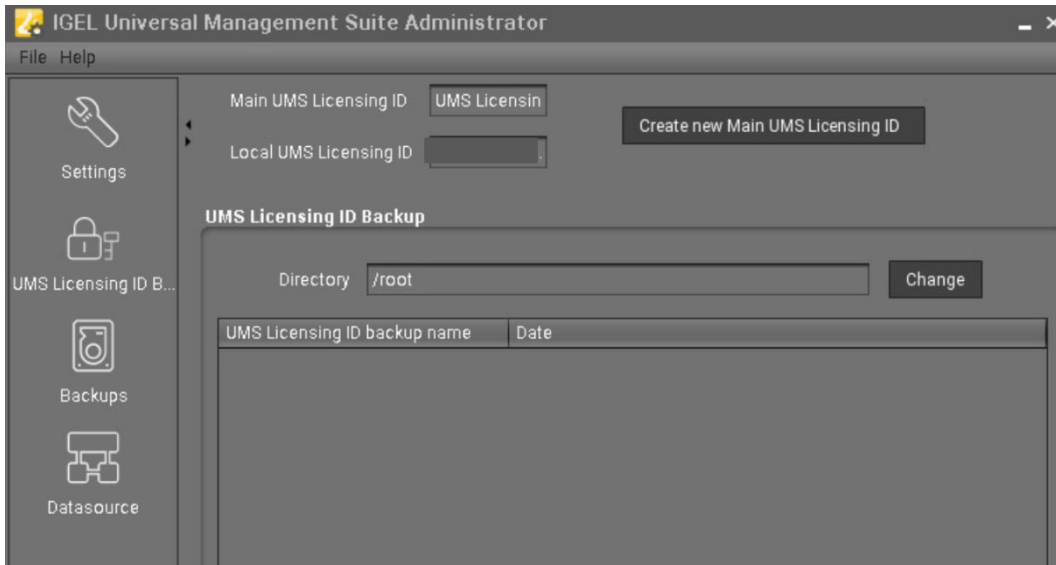


Abbildung 10: UMS Lizenz konfigurieren
Quelle: Eigene Darstellung

Um die UMS-Lizenz-ID erfolgreich zu nutzen, müssen Sie sie im IGEL Lizenz-Portal registrieren. Loggen Sie sich in das Portal ein und folgen Sie den Anweisungen zur Registrierung Ihrer Lizenz-ID.

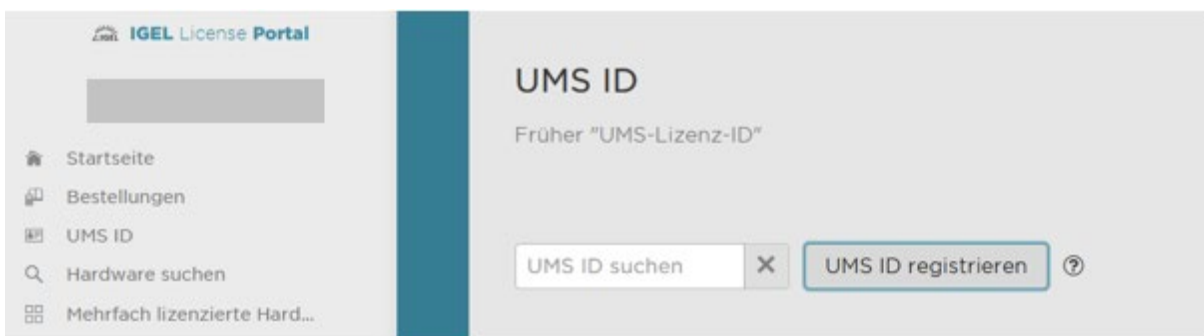


Abbildung 11: Registrierung UMS ID innerhalb des ILP
Quelle: Eigene Darstellung

5.3.3. Backup

Die UMS bietet die Möglichkeit, Backups Ihrer UMS-Konfiguration und Daten zu erstellen, um sicherzustellen, dass im Falle eines Systemausfalls oder Datenverlusts eine Wiederherstellungsoption besteht. Hierfür sind folgende Schritte notwendig:

1. Legen Sie den Speicherort und das Format der Backups fest. Dabei besteht die Möglichkeit, das Backup lokal auf dem UMS-Server oder auf einem externen Medium zu speichern. Wählen Sie den gewünschten Speicherort entsprechend aus.
2. Legen Sie fest, wie oft Backups automatisch erstellt werden sollen. Sie können beispielsweise tägliche, wöchentliche oder monatliche Backups definieren.
3. Geben Sie an, wie viele Backups gespeichert werden sollen. Sie können ebenso festlegen, dass nur eine bestimmte Anzahl von Backups gespeichert wird, um den Speicherplatz zu optimieren.



Abbildung 12: Konfiguration des Backups
Quelle: Eigene Darstellung

5.3.4. Datasource

Die Konfiguration der Datenquelle (Datasource) bezieht sich auf die Einrichtung der Verbindung zur Datenbank, die von der UMS für die Speicherung von Konfigurationsdaten, Benutzerinformationen und anderen relevanten Informationen verwendet wird. Um die Datenquelle zu konfigurieren, sind folgende Schritte notwendig:

1. Gehen Sie auf den Abschnitt „Datasource“ und klicken Sie auf „Add“.
2. DB-Type: Wählen Sie den entsprechenden Datenbanktyp aus, den Sie für die UMS verwenden. Dies kann beispielsweise PostgreSQL, Microsoft SQL Server oder ein anderer Datenbanktyp sein.
3. Host: Geben Sie den Hostnamen oder die IP-Adresse des Datenbankservers an, auf dem Ihre UMS-Datenbank gehostet wird.
4. Port: Geben Sie den Port an über den die Datenbank kommuniziert.
5. User: Geben Sie den Namen des Benutzers an, der auf die UMS-Datenbank zugreift.
6. Database / SID: Geben Sie den Namen der UMS-Datenbank ein.
7. Instance: Notwendig bei der Nutzung von SQL Server Cluster oder Oracle RAC.

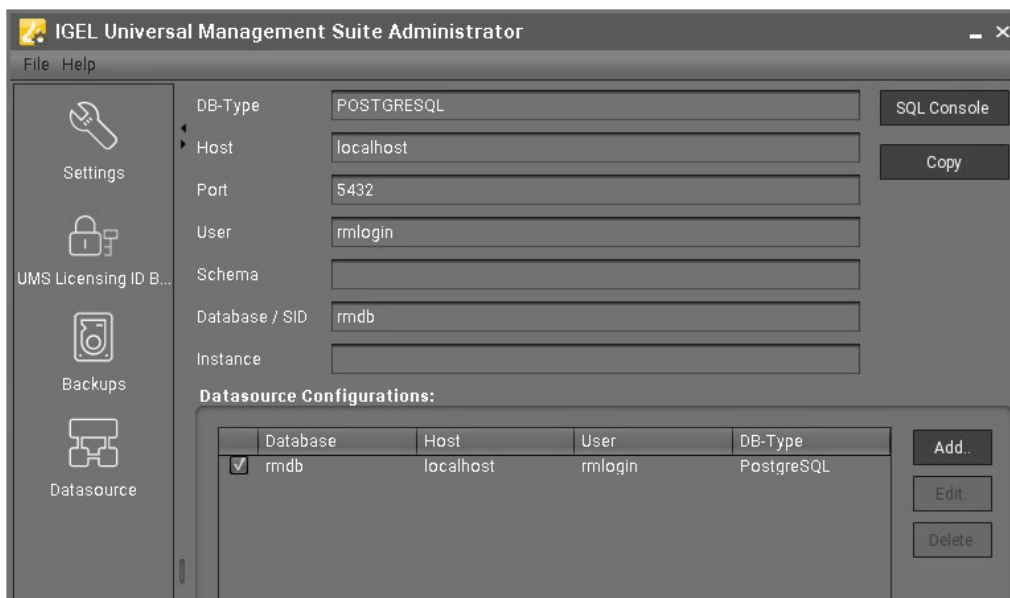


Abbildung 13: Festlegung der Datenquellen
Quelle: Eigene Darstellung

5.4. Hinzufügen eines IGEL OS Gerät (Thin-Client)

Nachdem alle notwendigen Konfigurationen innerhalb des UMS-Administrator (RMAdmin) vorgenommen wurden, kann im nächsten Schritt das Endgerät, d.h. der IGEL Thin Client, dem System hinzugefügt werden. Hierfür wird die zweite installierte Software: die **UMS-Konsole** verwendet.

5.4.1. Geräte Lizenz der UMS hinzufügen

In diesem Kapitel wird beschrieben, wie eine IGEL Gerätelizenz (die in Kapitel 4.2 innerhalb des Lizenzportals registriert und mit einem Gerät verknüpft wurde) auf die UMS übertragen wird. Gehen Sie dabei wie folgt vor:

1. Öffnen Sie die UMS-Konsole.
2. Melden Sie sich an: Verwenden Sie Ihre Administrator-Anmeldeinformationen, um sich bei der UMS-Konsole anzumelden.
3. Navigieren Sie zu "Lizenzmanagement": Suchen Sie in der UMS-Konsole nach der Option "Lizenzmanagement" oder "License Management". Normalerweise finden Sie dies im Hauptmenü oder in einem separaten Abschnitt.
4. Lizenz hinzufügen: Klicken Sie auf die Option "Lizenz hinzufügen" oder "Add License", um den Lizenzmanager zu öffnen.
5. Lizenzdaten eingeben: Geben Sie die erforderlichen Lizenzdaten ein, die normalerweise aus einem Lizenzschlüssel oder einer Datei bestehen. Diese Informationen erhalten Sie normalerweise beim Kauf Ihrer Thin Client Lizenz.
6. Bestätigen Sie die Lizenz: Nachdem Sie die Lizenzdaten eingegeben haben, überprüfen Sie die Informationen und bestätigen Sie die Hinzufügung der Lizenz.

(IGEL Knowledge Base [4]: Die in diesem Kapitel vorliegenden Informationen sind am 17.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/endpointmgmt/en/registering-thin-clients-on-the-ums-server-22459660.html> nachgelesen werden).

5.4.2. IGEL OS Gerät suchen

Zuerst muss ein Gerät im Netzwerk gefunden werden, um es der UMS hinzuzufügen. Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind, bevor Sie nach einem Gerät suchen:

1. Die Geräte sind eingeschaltet und funktionsfähig.
2. Geräte sind mit dem Netzwerk verbunden.
3. Die Firmware der Geräte unterstützt die UMS. Das ist bei folgenden Geräten der Fall:
 - IGEL Geräten mit Original-Firmware
 - Geräte, die mit IGEL OS Creator (OSC) konvertiert wurden
 - Geräte, auf denen IGEL OS über einen UD Pocket gebootet wurde
 - Geräte, auf denen IGEL OS mittels IGEL Universal Desktop Converter 2/3 (UDC2/UDC3) installiert wurde
 - Geräte, auf denen der UMA (Universal Management Agent) läuft

Sind diese Voraussetzungen erfüllt, können Sie nach einem Gerät suchen, indem Sie folgenden Schritte ausführen:

1. Klicken Sie im oberen Reiter auf das Symbol , um das Fenster zur Suche eines Geräts zu öffnen

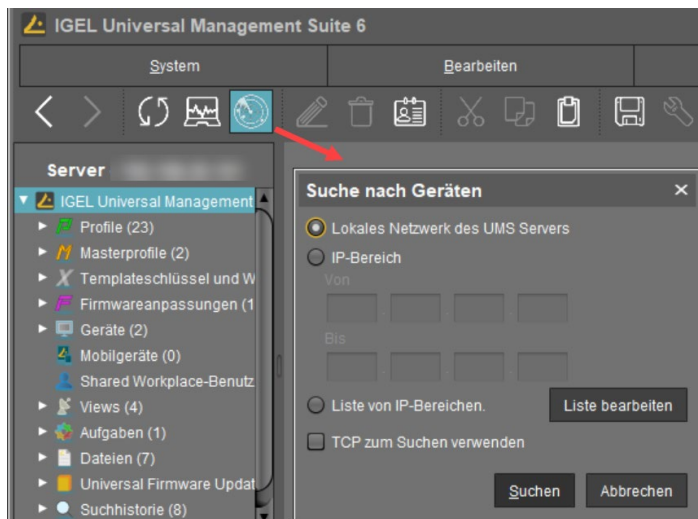


Abbildung 14: Suche eines IGEL Geräts

Quelle: <https://kb.igel.com/endpointmgmt-6.10/de/netzwerk-nach-geraeten-scannen-und-geraete-an-der-igel-ums-registrieren-57321103.html>, 14.06.2023

2. Legen Sie den Suchbereich fest. Hierbei haben Sie verschiedene Auswahlmöglichkeiten:

- Lokales Netzwerk des UMS Servers: Der UMS Server sendet eine Broadcast-Nachricht in das Netzwerk (*Bei mehreren Netzwerkschnittstellen ist zu beachten, dass die Broadcast-Nachricht nur über die erste Netzwerkschnittstelle gesendet wird. Bei Windows ist dies das erste Element in der Liste der Netzwerkverbindungen*).
- IP-Bereich: Der UMS Server kontaktiert jedes Gerät im angegebenen Bereich.
- Liste von IP-Bereichen: Unter „Liste bearbeiten“ können Sie die IP-Bereiche festlegen, in denen die UMS nach Geräten suchen soll.
- TCP zum Suchen verwenden: Wenn die Option aktiviert ist, erfolgt die Kommunikation mit den Geräten über TCP. Wenn die Option deaktiviert ist, wird UDP verwendet (*Wenn TCP zum Suchen verwendet wird, dauert der Suchvorgang länger; die Suchergebnisse können jedoch zuverlässiger sein*).

3. Klicken Sie nun auf „Suchen“. Im Fenster Gefundene Geräte werden die Suchergebnisse angezeigt. Die Geräte können nun registriert werden.

(IGEL Knowledge Base [5]: Die in diesem Kapitel vorliegenden Informationen sind am 23.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/endpointmgmt-6.05/de/netzwerk-nach-geraeten-scannen-und-geraete-an-der-igel-ums-registrieren-31599388.html> nachgelesen werden)

5.4.3. IGEL OS Gerät registrieren

1. Sobald Ihnen der entsprechenden Thin Client in den Suchergebnissen angezeigt wird, können Sie das neue Geräte registrieren.

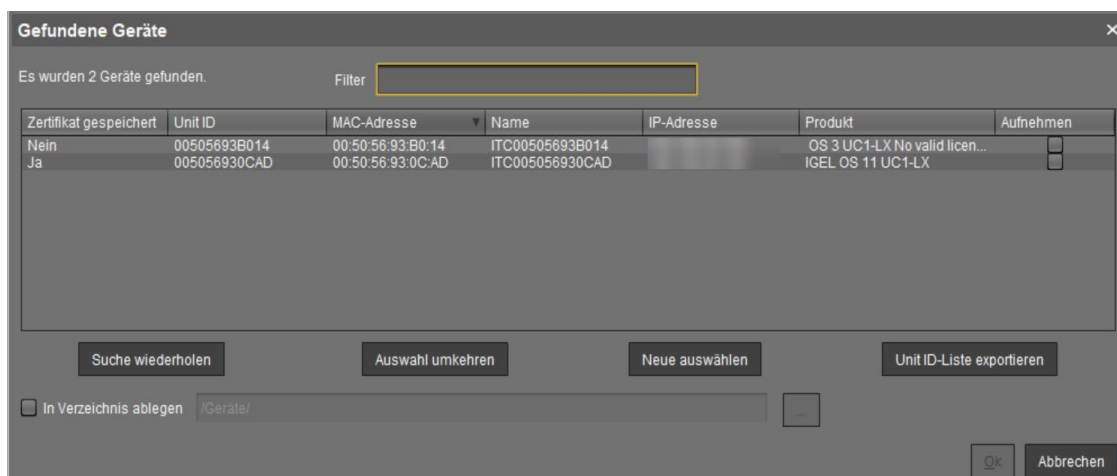


Abbildung 15: Gefundene IGEL OS Geräte in der UMS

Quelle: <https://kb.igel.com/endpointmgmt-6.10/de/netzwerk-nach-geraeten-scannen-und-geraete-an-der-igel-ums-registrieren-57321103.html>, 14.06.2023

2. Wählen Sie die Geräte aus, die registriert werden sollen. Sie haben folgende Möglichkeiten:

- Manuelle Auswahl: Markieren Sie in der Spalte Aufnehmen die zu registrierenden Geräte.
- Auswahl aller noch nicht registrierten Geräte: Klicken Sie auf Neue auswählen. Damit werden alle Geräte markiert, die noch kein Serverzertifikat von der UMS erhalten haben.

3. Bestätigen Sie die Auswahl und klicken sie auf „OK“. Die Geräte werden nun in der UMS Datenbank registriert (*Bei der Registrierung wird das Serverzertifikat der UMS auf dem Gerät gespeichert. Der weitere Zugriff auf das Gerät wird nach diesem Zertifikat validiert. Nur der Eigentümer des Zertifikats kann das Gerät verwalten*).

(IGEL Knowledge Base [5]: Die in diesem Kapitel vorliegenden Informationen sind am 23.05.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/endpointmgmt-6.05/de/netzwerk-nach-geraeten-scannen-und-geraete-an-der-igel-ums-registrieren-31599388.html> nachgelesen werden)

5.4.4. Thin Client Vorschau

Wenn alle vorangegangenen Konfigurationsschritte durchgeführt wurden und das Gerät innerhalb der UMS registriert wurde, kann der Thin Client nun gestartet werden. Da noch keine Software oder Applikationen für die Anwender konfiguriert wurden, erscheint vorerst ein leerer Desktop.

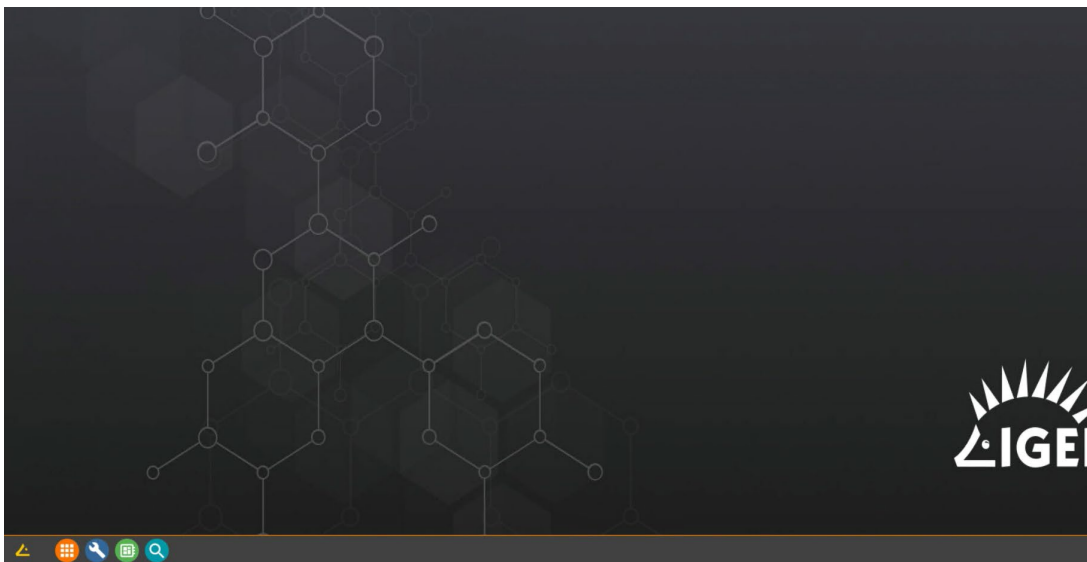


Abbildung 16: Desktop des Thin Client nach ersten Konfigurationsschritten

Quelle: Eigene Darstellung

6. Sicherheitskonfiguration des Thin Client

Die Nutzung von Thin Clients als GWAP bietet einen entscheidenden Vorteil durch die strikte Begrenzung der verfügbaren Software und Applikationen. Standardmäßig können Nutzende den Thin Client nicht zur externen Kommunikation nutzen, da Funktionen wie der Webbrowser, E-Mails oder die Kommandozeile nicht zugänglich sind. In Kombination mit zusätzlichen Sicherheitsmerkmalen wie eingeschränkten Peripheriegeräten und der Restriktion, Inhalte zu übertragen, zu speichern oder zu kopieren, bildet der Thin Client eine sichere Einheit. Mit den hier beschriebenen Konfigurationen besteht die einzige Verwendung der Thin Clients für Nutzende darin, Remote Access Software wie den VMware Client auszuführen, um eine Verbindung zu den Desktops der datengebenden Institute herzustellen.

Im folgenden Abschnitt werden die erforderlichen Sicherheitskonfigurationen beschrieben, die zur Umsetzung der technischen und organisatorischen Maßnahmen gemäß dem multilateralen Kooperationsvertrag des RDCnet notwendig sind.

6.1. Vorbereitung

Innerhalb der IGEL UMS können **Profile** verwendet werden. Das bedeutet, dass alle erforderlichen Konfigurationen zuerst in einem spezifischen Profil vorgenommen werden können, und diese Profilkonfigurationen dann mit jedem der gewünschten Thin-Client-Geräte verknüpft werden können.

Hierfür muss zuerst ein neues Profil erstellt werden. Klicken Sie dazu im linken Reiter auf „Profile“ und dann auf „Neues Profil“.

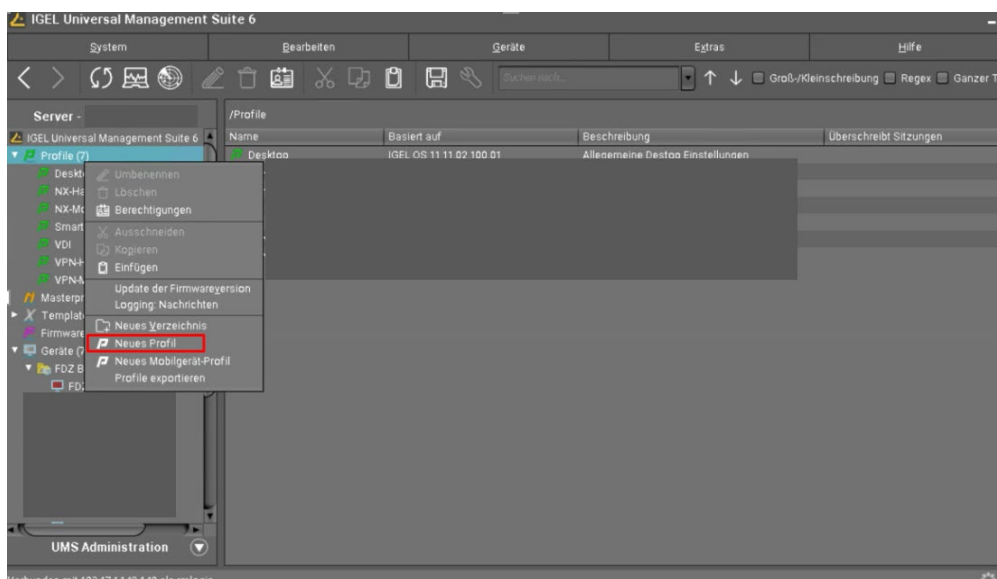


Abbildung 17: Neues Profil für Sicherheitskonfigurationen

Quelle: Eigene Darstellung

Geben Sie nun einen Profilnamen und eine Beschreibung für das Profil ein.

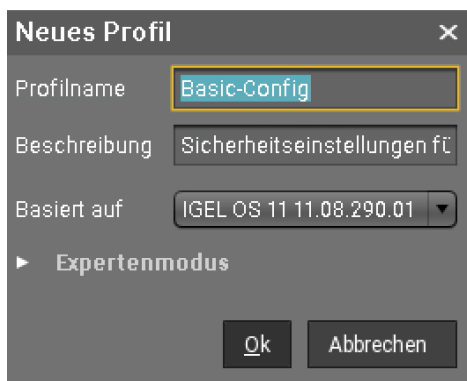


Abbildung 19: Profilbenennung
Quelle: Eigene Darstellung

Führen Sie nun für das erstellte Profil die folgenden Konfigurationsschritte durch und speichern Sie die Konfiguration, nachdem Sie alle Änderungen vorgenommen haben.

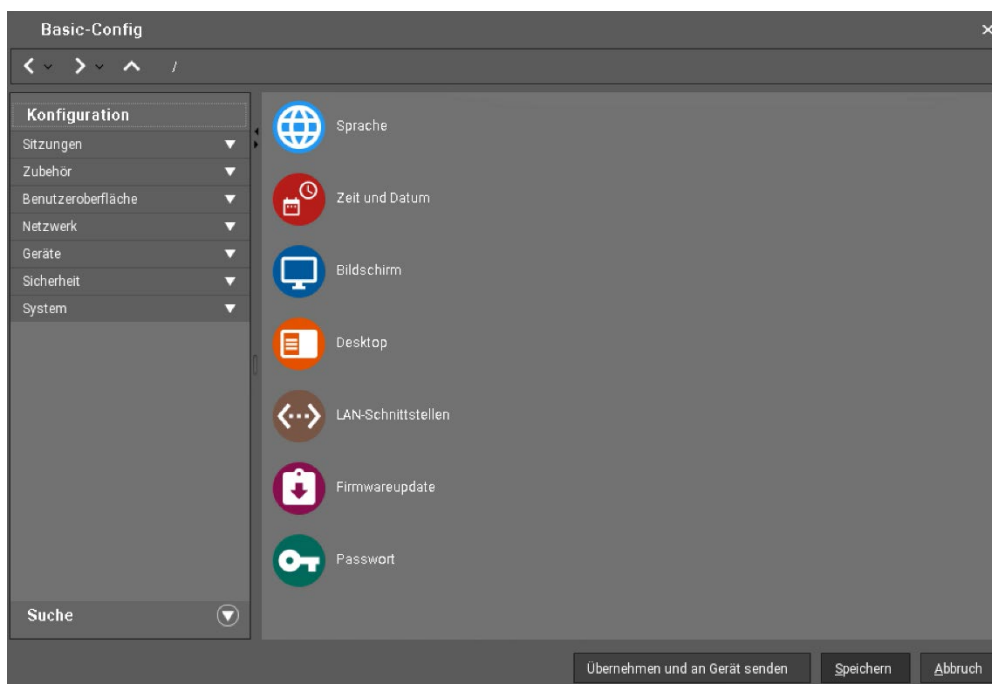


Abbildung 18: Konfigurationsmöglichkeiten des Profils
Quelle: Eigene Darstellung

6.2. Deaktivierung von Peripheriegeräten

1. Gehen Sie auf **Geräte > USB- Zugriffskontrolle**
2. Entfernen Sie den Haken bei „Aktivieren“, um die Nutzung von USB-Peripheriegeräten zu verbieten (siehe Abb. 19).

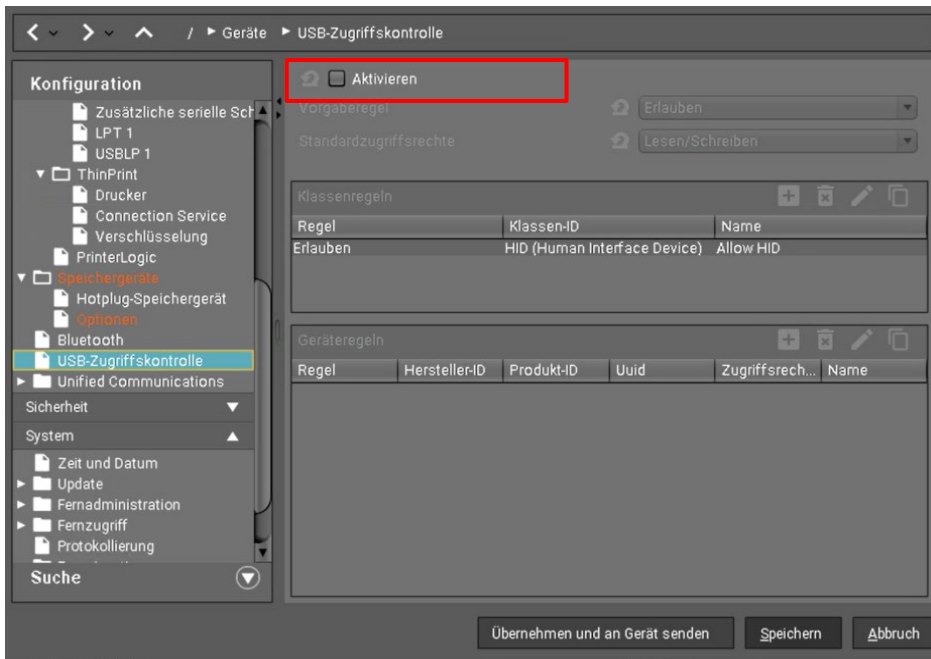


Abbildung 20: USB-Speichergeräte deaktivieren
Quelle: Eigene Darstellung

6.3. Deaktivierung von Druckern

1. Gehen Sie auf **Geräte > Drucker > LDP**
2. Deaktivieren Sie die Option „LPD-Druckserver aktivieren“ (siehe Abb. 20).

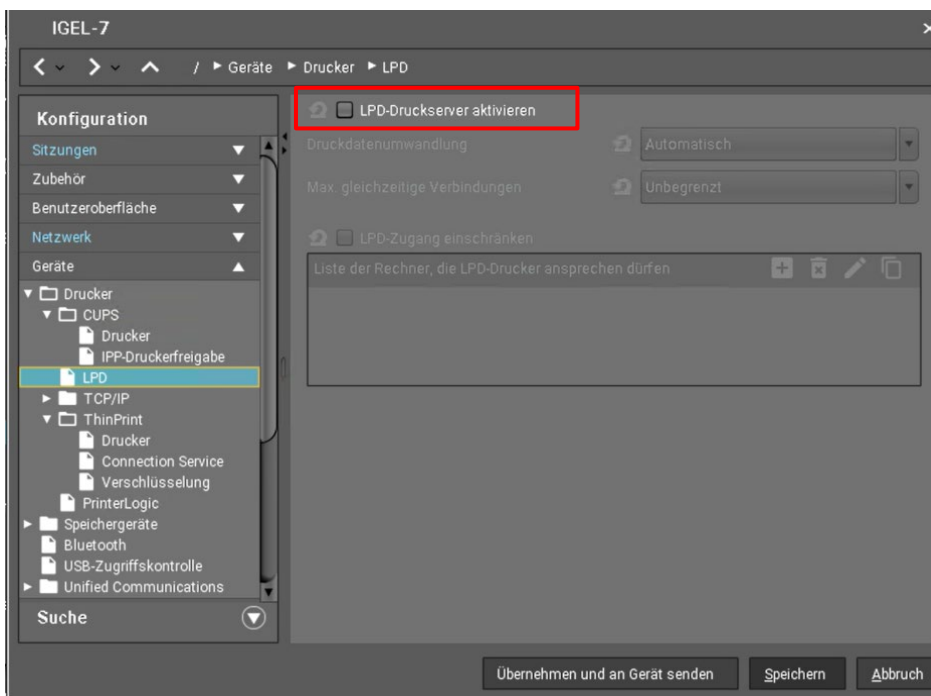


Abbildung 21: Drucker deaktivieren
Quelle: Eigene Darstellung

6.4. Deaktivierung von Bildschirmaufnahmen

1. Gehen Sie auf **Zubehör > Bildschirmfoto**
2. Deaktivieren Sie alle Optionen unter "Startmöglichkeiten der Sitzung" (siehe Abb. 21)

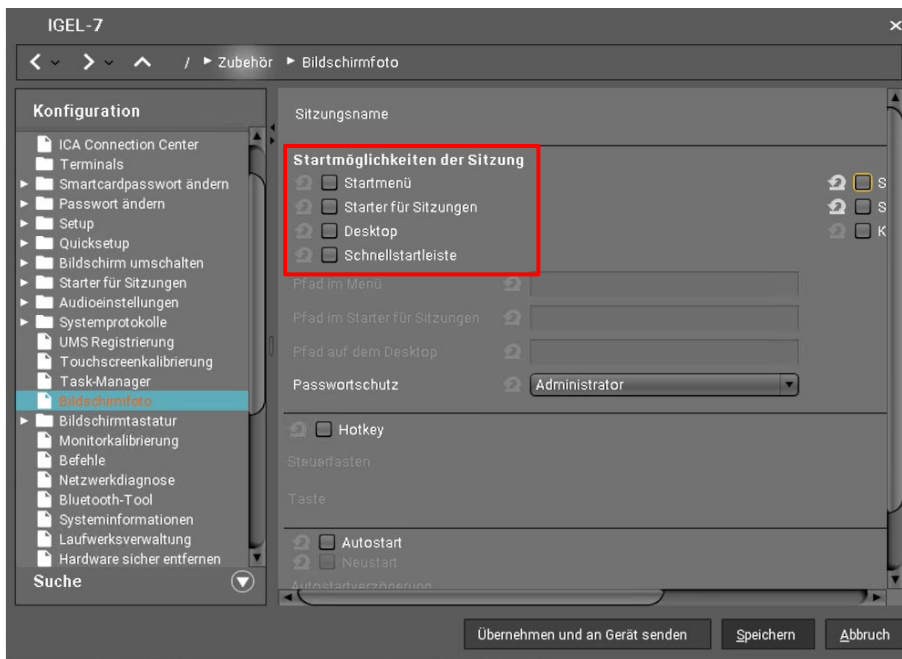


Abbildung 22: Deaktivierung von Bildschirmaufnahmen
Quelle: Eigene Darstellung

6.5. Deaktivierung von Fernzugriffen auf das Terminal

1. Gehen Sie auf **System > Fernzugriff > Sicheres Terminal**
2. Deaktivieren Sie die Option "Sicheres Terminal", damit das Terminal nicht durch andere Personen im Netzwerk unerlaubt verwendet werden kann (siehe Abb. 22).

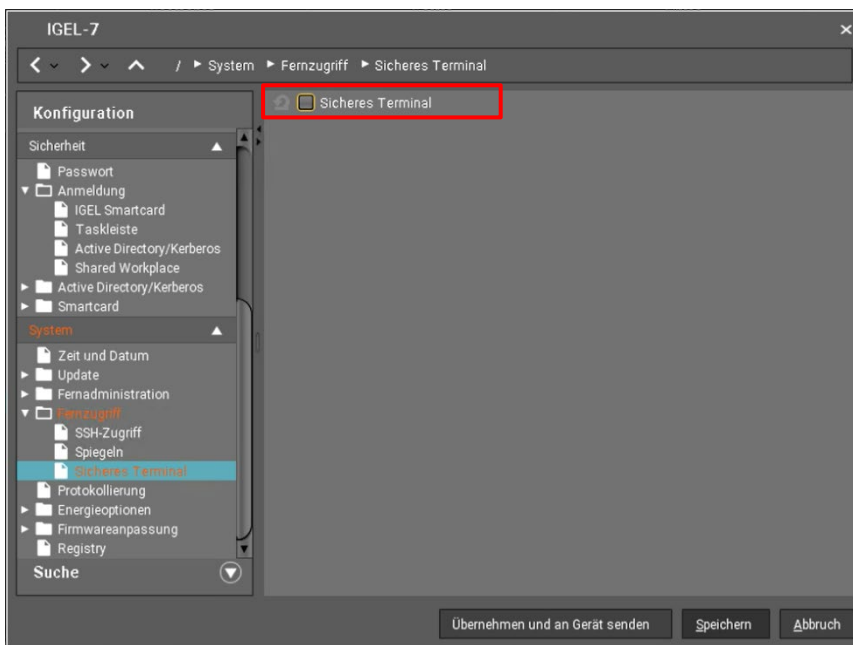


Abbildung 23: Deaktivierung von Fernzugriffen
Quelle: Eigene Darstellung

6.6. Deaktivierung von Hotplug-Speichergeräten

1. Gehen Sie auf **Geräte > Speichergeräte > Hotplug-Speichergerät**
2. Deaktivieren Sie die Option "Hotplug-Speichergerät" (siehe Abb. 23)

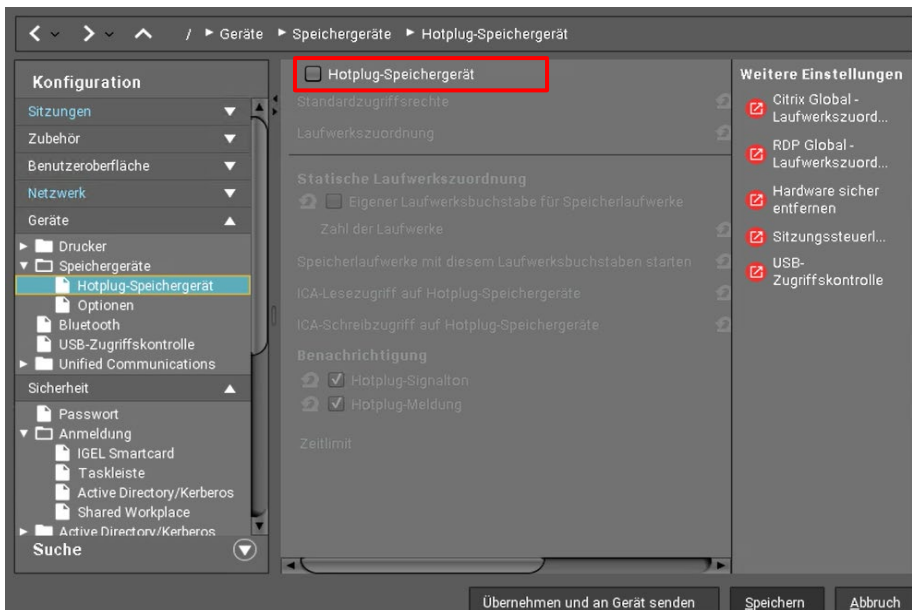


Abbildung 24: Deaktivierung von Hotplug-Speichergeräten

Quelle: Eigene Darstellung

6.7. Fertigstellung

Nachdem alle Konfigurationen umgesetzt wurden, klicken Sie auf "Speichern".

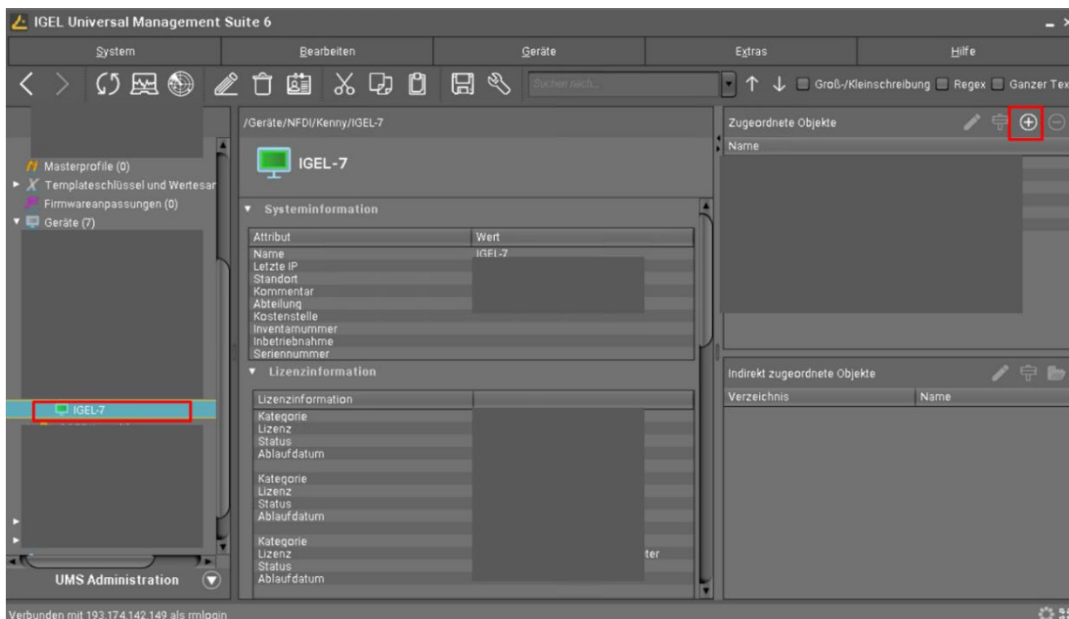


Abbildung 25: Profile verknüpfen

Quelle: Eigene Darstellung

Nun muss das erstellte Profil mit einem Thin Client verknüpft werden. Dazu wählen Sie im linken Reiter den gewünschten Thin Client aus und klicken in der oberen rechten Ecke auf das "+"-Symbol (siehe Abb. 24).

Als nächstes müssen Sie das konfigurierte Profil auswählen und auf den Pfeil > klicken, um es dem Thin Client zuzuweisen. Überprüfen Sie, ob das richtige Profil in das rechte Menü verschoben wurde, und klicken Sie dann auf OK.

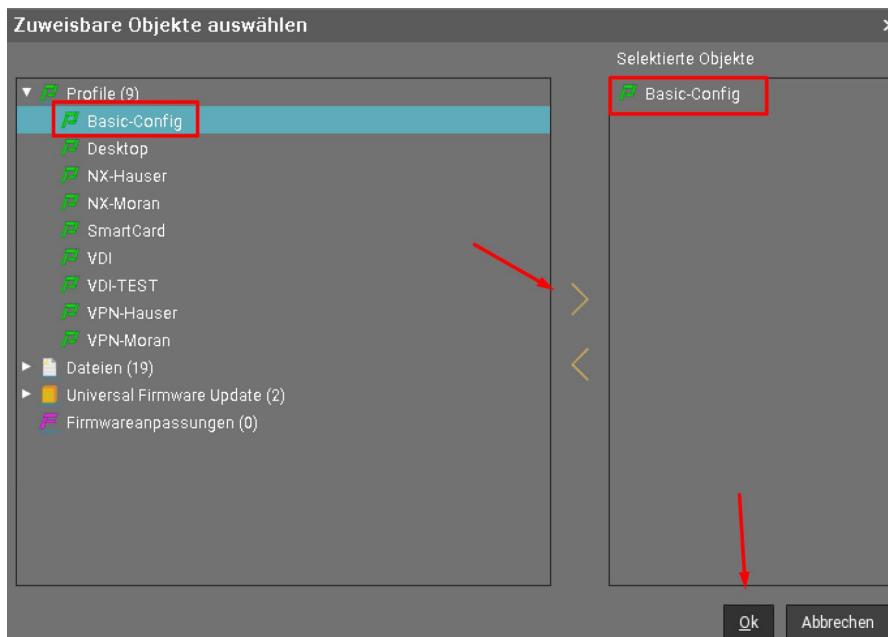


Abbildung 26: Profil auswählen und übertragen

Quelle: Eigene Darstellung

Es empfiehlt sich nun, manuell zu überprüfen, ob die entsprechenden Konfigurationen am Thin Client wirksam sind. Dies kann beispielsweise durch Tests von USB-Speichergeräten, Durchführung von Screenshots oder Ansicht der Druckmöglichkeiten geschehen.

Mit der Umsetzung der Konfigurationsschritte in diesem Kapitel wurde der Thin Client erfolgreich für die Nutzung vorbereitet und ist nun grundsätzlich einsatzbereit. Allerdings verfügt der Thin Client noch über keine Applikation, die den Remote Access ermöglicht.

Im kommenden Kapitel widmen wir uns deshalb der Installation und Konfiguration des VMware Clients, der es den Nutzenden ermöglicht, eine Verbindung zu den Desktops der datengebenden FDZ herzustellen.

7. VMware Horizon Client

Um den konfigurierten Thin Client für das RDCnet nutzen zu können, ist in einem letzten Schritt die Installation und Konfiguration des VMware Clients erforderlich. Dadurch wird der Remotezugriff auf die Server der teilnehmenden datengebenden FDZ ermöglicht. Das Ziel besteht darin, für jedes teilnehmende FDZ eine vorkonfigurierte "Sitzung" zu erstellen, die als Symbol auf dem Desktop angezeigt wird. Für jede Sitzung werden relevante Parameter vordefiniert z.B. die Adresse des Connection Servers und die Domäne.

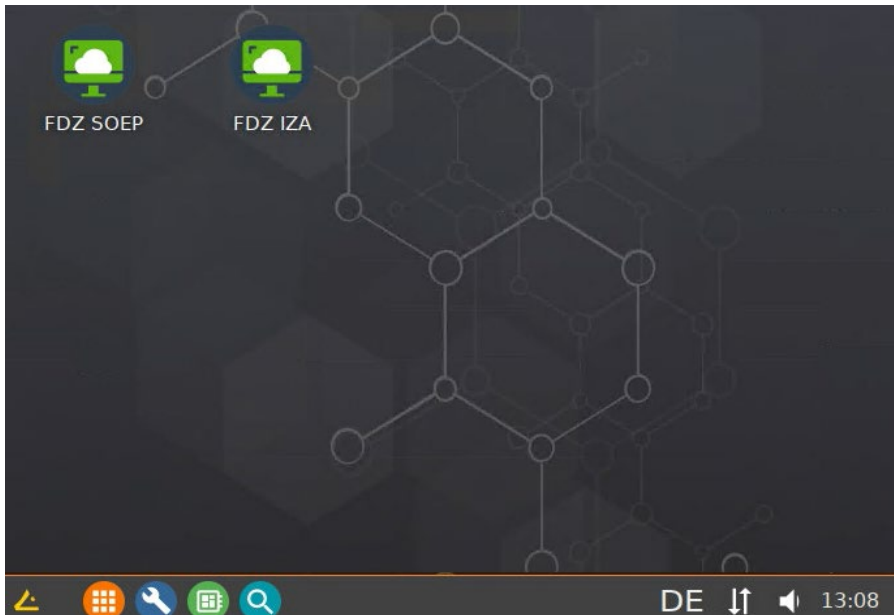


Abbildung 22: IGEL-Desktop mit vordefinierten VMware Horizon Sitzungen

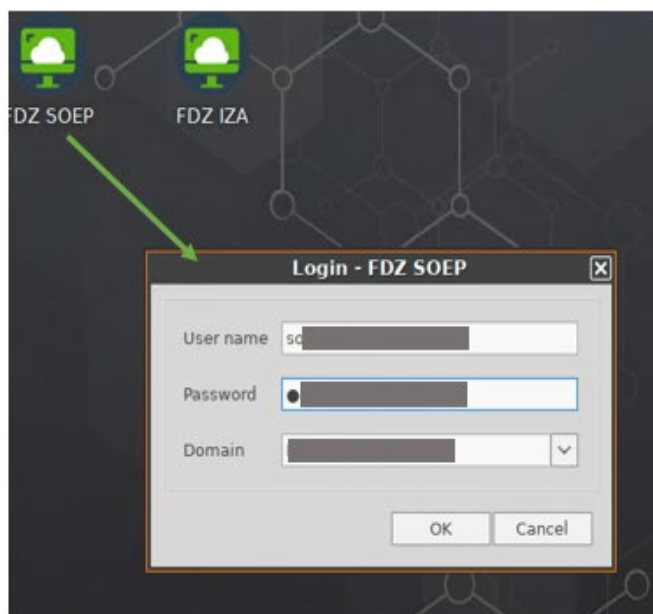


Abbildung 23: Benutzerangaben vordefinierter VMware Horizon Sitzungen
Quelle: Eigene Darstellung

Die Nutzenden müssen dann lediglich ihre Anmeldedaten (Benutzername, Passwort, OTP⁵) eingeben (siehe Abb. 23), um eine Verbindung zu den virtuellen Desktops des datengebenden FDZ herzustellen. Somit wird ein benutzerfreundliches System geschaffen, wobei klar ersichtlich ist, welche Sitzung ausgewählt werden muss, sobald man sich auf dem Desktop befindet. Neben den vordefinierten Sitzungen können Nutzende jedoch keine anderen Anwendungen oder Funktionen auf dem Thin-Client starten. Somit sind keine Möglichkeiten gegeben, um Daten unerlaubt nach außen zu tragen und potenzielle Datenlecks zu verursachen.

Im Folgenden wird beschrieben wie die Konfiguration und Installation des VMware Horizon Clients vorgenommen wird, um die zuvor beschriebenen Sitzungen auf dem Desktop zu definieren.

7.1. Konfiguration VMware Horizon Client

Um den VMware Client zu konfigurieren, muss zunächst ein Profil erstellt werden, in dem sowohl globale als auch sitzungsbezogene Einstellungen definiert werden. Sobald das Profil erstellt wurde, kann es auf beliebigen IGEL-Geräten geladen und aktiviert werden.

Um ein Profil zu erstellen, gehen Sie auf den folgenden Pfad: **Igel Universal Management Suite > Profile** und klicken auf „Neues Profil“ (siehe Abb. 24).

⁵ Grundsätzlich wird die Implementierung einer 2-Faktor-Authentifizierung (2FA), wie zum Beispiel eines One-Time-Passworts (OTP), für jedes datengebende FDZ empfohlen. Innerhalb des RDCnet werden hierzu jedoch keine konkreten Vorgaben gemacht, da dies ein Sicherheitsaspekt ist, der von jedem einzelnen datengebenden FDZ festgelegt werden muss und hierzu keine Informationen mit dem GWAP-stellenden FDZ ausgetauscht werden müssen. Wenn ein FDZ die Notwendigkeit sieht, einen zusätzlichen (dritten) Faktor einzurichten, der durch das FDZ-Personal des GWAP-stellenden FDZ getätigt werden muss, wie beispielsweise ein Mitarbeiterpasswort, ist darauf zu achten, dass dem GWAP-stellenden FDZ dadurch kein zusätzlicher Aufwand entsteht, außer der Eingabe des Passworts am Endgerät. Eine Möglichkeit wäre beispielsweise die Nutzung von Token-Generatoren, die durch die datengebenden FDZ eingerichtet und jedem GWAP-stellenden FDZ ausgegeben werden. Auf diese Weise müsste das Personal des GWAP-stellenden FDZ lediglich das am Generator angezeigte Passwort eingeben, ohne dass für dieses FDZ weiterer Aufwand entsteht.

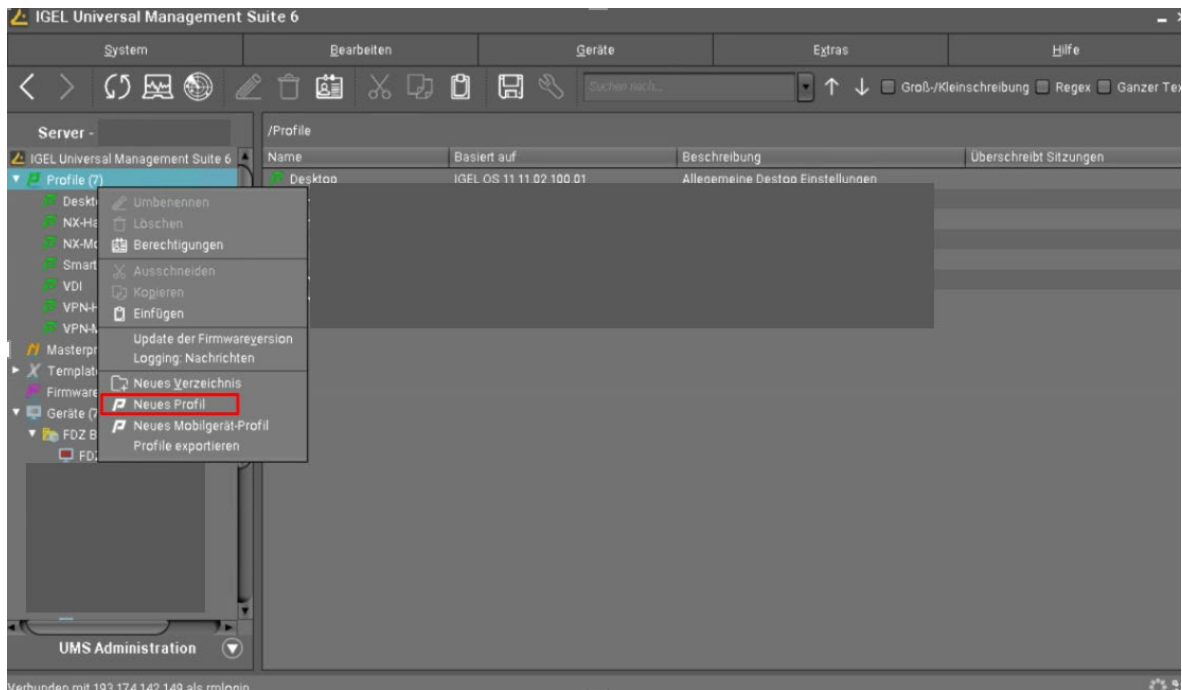


Abbildung 24: Erstellen eines neuen Profils
 Quelle: Eigene Darstellung

Geben Sie einen Namen und Beschreibung für das gewünschte Profil ein und klicken Sie auf „OK“. Das erstellte Profil wird nun auf der linken Seite im Reiter Profile angezeigt. Mit einem Doppelklick auf das neu erstellte Profil öffnen Sie nun die spezifischen Konfigurationen für das Profil:

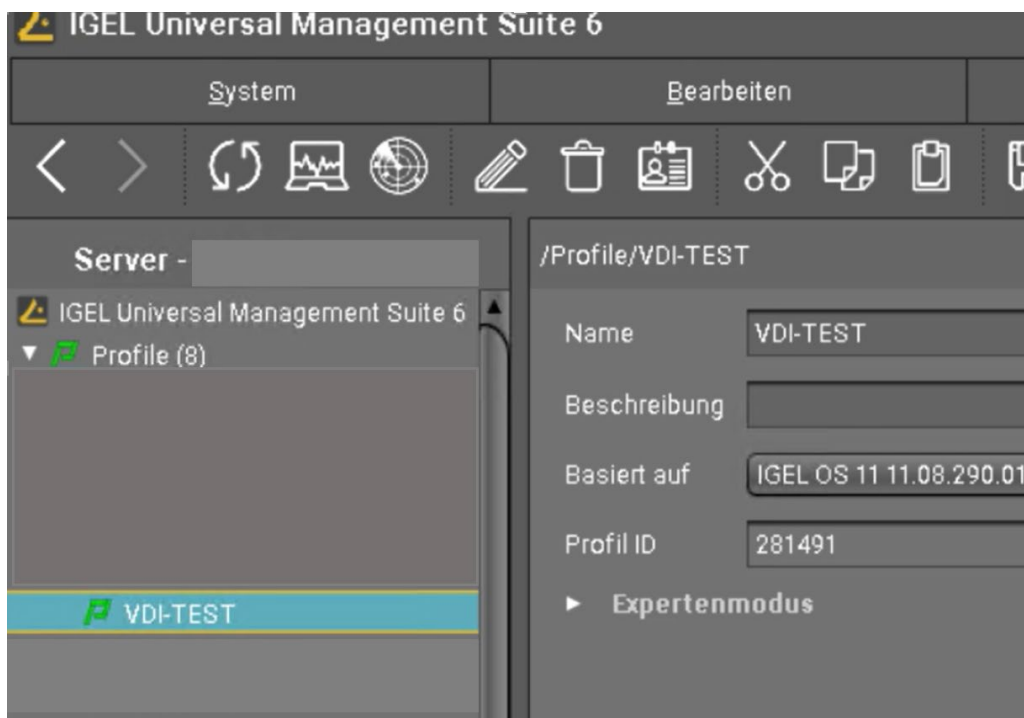


Abbildung 25: Profilkonfiguration
 Quelle: Eigene Darstellung

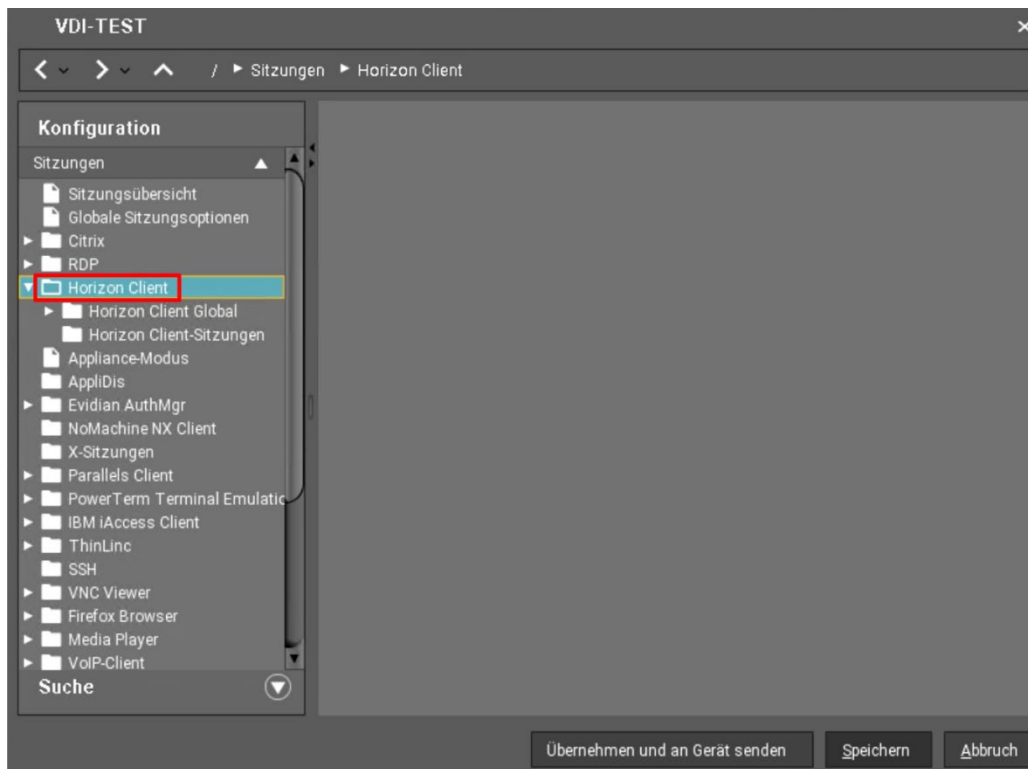


Abbildung 26: Konfiguration VMware Horizon Client
Quelle: Eigene Darstellung

Innerhalb des Konfigurationsmenüs finden Sie nun unter dem Reiter „Sitzungen“ die Möglichkeit, globale und sitzungsbezogene Einstellungen für den VMware Horizon Client vorzunehmen (siehe Abb. 26).

7.1.1. Globale Horizon Client Konfigurationen

Klicken Sie nun auf „Horizon Client Global“ wobei sich folgende Optionen öffnen:

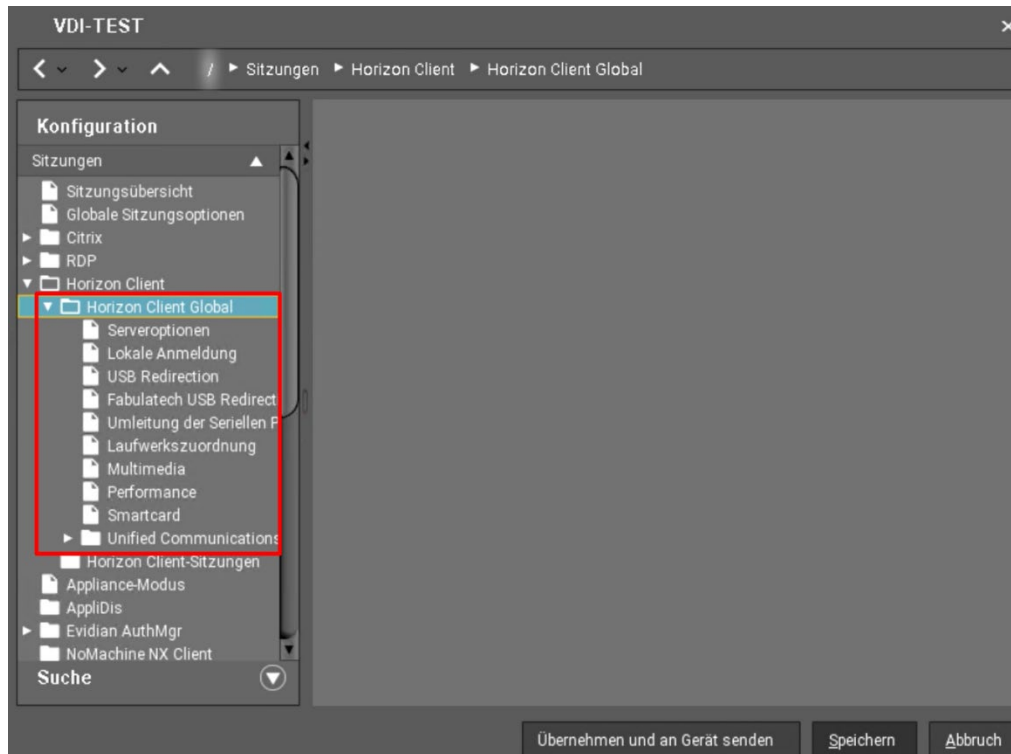


Abbildung 27: Globale Horizon Client Einstellungen

Quelle: Eigene Darstellung

Nehmen Sie nun die folgenden Konfigurationen vor:

1. Serveroptionen

Pfad: Sitzungen > Horizon Client > Horizon Client Global > Serveroptionen

In diesem Bereich legen Sie die Einstellungen für die Verbindung des Horizon Client zum Server fest. Innerhalb der Option „Bevorzugtes Verbindungsprotokoll“ müssen Sie nun die „VMware Blast Option“ auswählen- diese wird am häufigsten für die Verbindung mit Horizon Connection Servern verwendet.

Um diese Option auswählen zu können, muss zuerst das Kontrollkästchen aktiviert werden, indem man auf das gelbe Dreieck klickt, damit das Dropdown-Menü zu einem editierbaren Menü wird (siehe Abb. 27).



Abbildung 28: Konfiguration des Verbindungsprotokolls
Quelle: Eigene Darstellung

2. Lokale Anmeldung

Pfad: Sitzungen > Horizon Client > Horizon Client Global > Lokale Anmeldung

In diesem Bereich können Sie aktivieren, dass Verbindungsparameter vorbelegt werden können. Damit können Sie vermeiden, dass sich Nutzende unter Umständen mehrfach anmelden müssen.

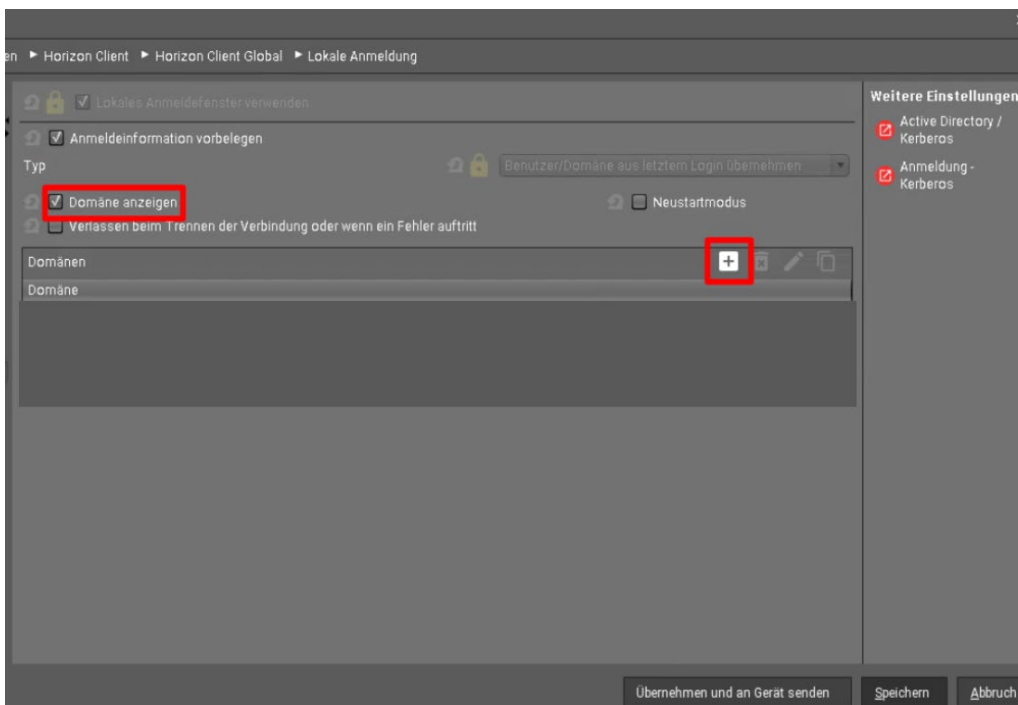


Abbildung 30: Konfiguration lokaler Anmeldungen
Quelle: Eigene Darstellung

Klicken Sie dazu zuerst auf die Schaltfläche "+" (siehe Abb. 28) und geben Sie den Namen des Domänenservers ein. Klicken Sie auf "OK" und überprüfen Sie, ob die Änderung korrekt hinzugefügt wurde.

Aktivieren Sie zudem die Option „Domäne Anzeigen“, so dass bei der Anmeldung überprüft werden kann, ob für die Verbindung die korrekte Domäne genutzt wird.

Nun können Sie die globale Konfiguration abschließen, indem Sie auf „Speichern“ klicken (siehe Abb. 29).

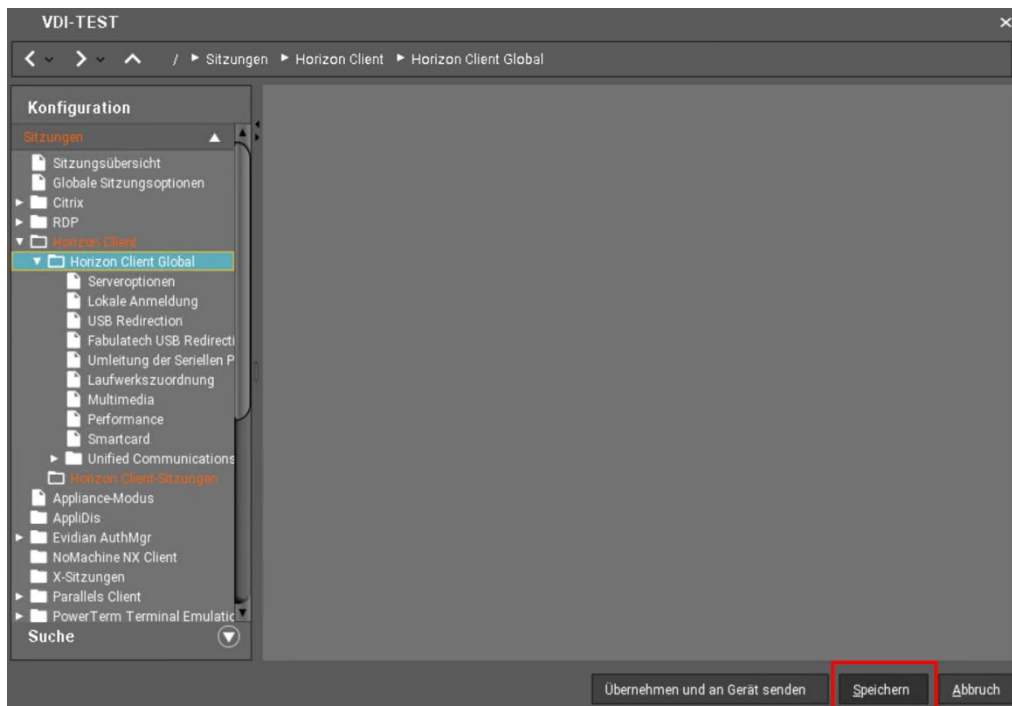


Abbildung 31: Globale Konfiguration speichern.

Quelle: Eigene Darstellung

7.1.2. Konfiguration Horizon Client Sitzungen

Nachdem die globalen Konfigurationen vorgenommen wurden, können nun die Benutzer-Sitzungen definiert werden, welche dann auf dem Desktop angezeigt werden.

Klicken Sie unter dem Pfad **Sitzungen > Horizon Client > Horizon Client-Sitzungen** auf das „+“ Symbol oben rechts auf dem Bildschirm (siehe Abb. 30).

Hinweis: Für jedes datengebende FDZ im RDCnet muss hierbei eine eigene Sitzung definiert werden.

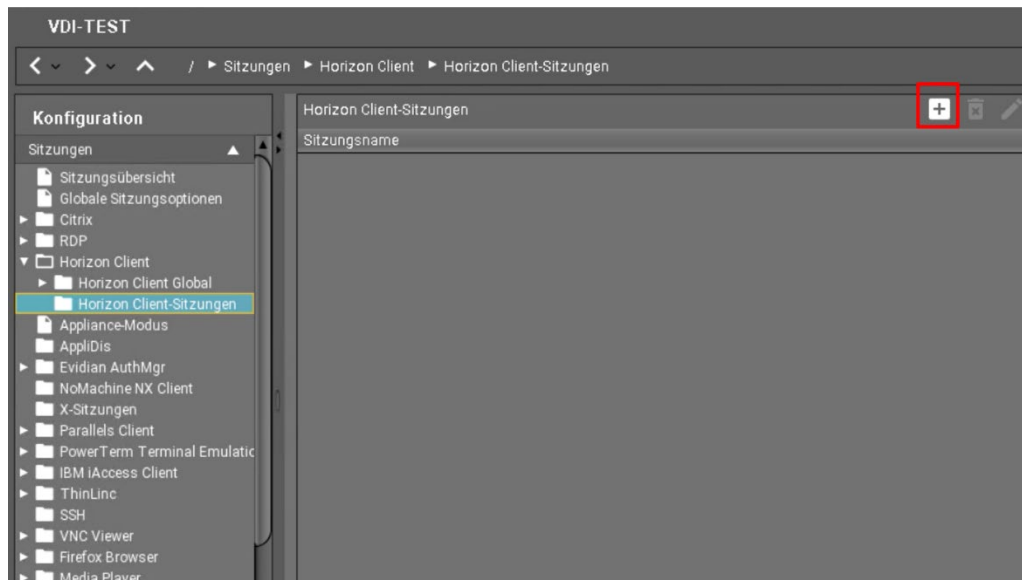


Abbildung 32: Benutzer Sitzung definieren
Quelle: Eigene Darstellung

Daraufhin werden mehrere Optionen angezeigt, die wie folgt konfiguriert werden:

1. Verbindungseinstellungen

Pfad: Sitzungen > Horizon Client > Horizon Client-Sitzungen > [Sitzungsname] > Verbindungseinstellungen

Innerhalb dieser Optionen definieren Sie für eine Sitzung die Verbindungsparameter zu den datengebenden FDZ. Notwendig ist hierfür zum einen die Angabe der Adresse des jeweiligen Verbindungsservers und die hierbei genutzte Domäne (Domäne der Active Directory, in welcher die Gruppe der RDCnet Nutzenden beim datengebenden FDZ hinterlegt sind und die Benutzerangaben authentifiziert werden). Die Felder „Benutzername“ und „Benutzerpasswort“ bleiben leer. Somit ist für die Sitzung zwar der Verbindungsserver definiert, jedoch müssen sich die Nutzenden dann selbst durch die Eingabe von Benutzername und Passwort authentifizieren. Deaktivieren Sie zudem die Option „Automatisch Verbinden“.

IGEL Knowledge Base [6]: Die in diesem Kapitel vorliegenden Informationen sind am 07.06.2023 der „IGEL Knowledge Base“ entnommen und können unter: <https://kb.igel.com/igelos-11.07/de/verbindungseinstellungen-57334505.html> nachgelesen werden.

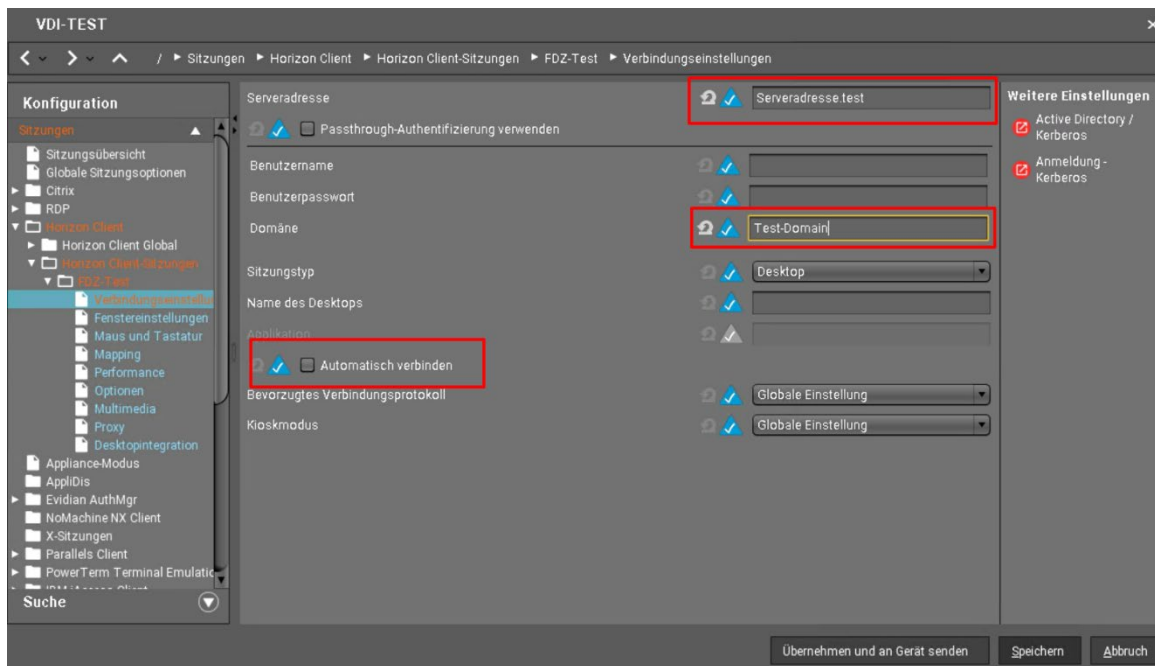


Abbildung 33: Verbindungseinstellungen Horizon Client Sitzung
Quelle: Eigene Darstellung

2. Desktopintegration

Pfad: Sitzungen > Horizon Client > Horizon Client-Sitzungen > [Sitzungsname] > Desktopintegration

Innerhalb dieser Optionen wird festgelegt, wie die konfigurierte Sitzung auf dem Desktop angezeigt wird. Geben Sie einen klaren Namen für die Sitzung ein, der den Nutzenden verdeutlicht, welches FDZ durch die Sitzung angesprochen wird, z.B. „FDZ A“. Deaktivieren Sie außerdem die Optionen „Hotkey“ und „Autostart“ (siehe Abb. 32).

Nun können Sie die Konfiguration der Horizon-Client-Sitzung abschließen, indem Sie auf „Speichern“ klicken.

Wiederholen Sie die Schritte in Kapitel 7.1.2, um jedem teilnehmenden FDZ eine eigene Sitzung zuzuweisen und ein Icon auf dem Desktop zu erstellen.

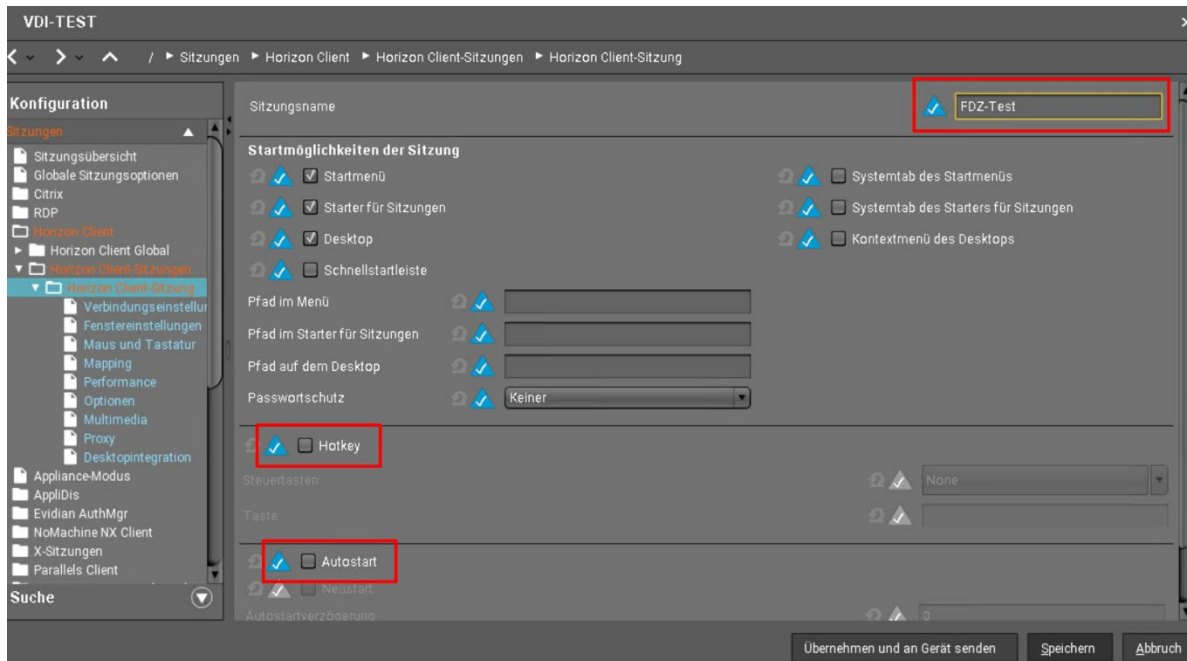


Abbildung 34: Konfiguration der Desktopintegration
Quelle: Eigene Darstellung

7.2. Profil einem IGEL-Gerät hinzufügen

Nachdem das Profil mit den globalen Konfigurationen und Horizon Client Sitzungen definiert wurde, muss es noch auf den zuvor eingereichten IGEL Thin Client übertragen werden.

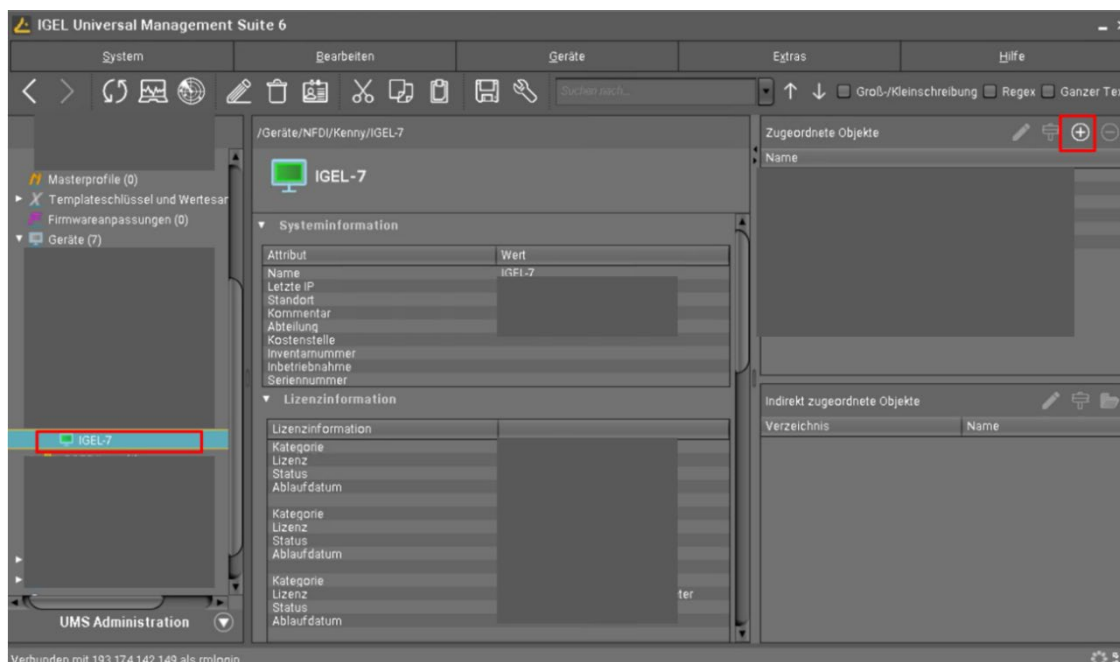


Abbildung 33: Profil auf ein Gerät übertragen (1)
Quelle: Eigene Darstellung

Hierfür gehen Sie auf das Hauptmenü der UMS und wählen im linken Reiter unter „Geräte“ den entsprechenden Thin Client aus, auf dem das Profil aufgespielt werden soll. Anschließend

klicken Sie im Menü „Zugeordnete Objekte“ im oberen rechten Teil des Bildschirms auf das „+“ Symbol (siehe Abb. 33).

Wählen Sie auf dem nun erscheinenden Fenster das Profil aus, das zuvor erstellt wurde, klicken Sie auf den Pfeil nach rechts „>“ und anschließend auf „OK“ (siehe Abb. 34).

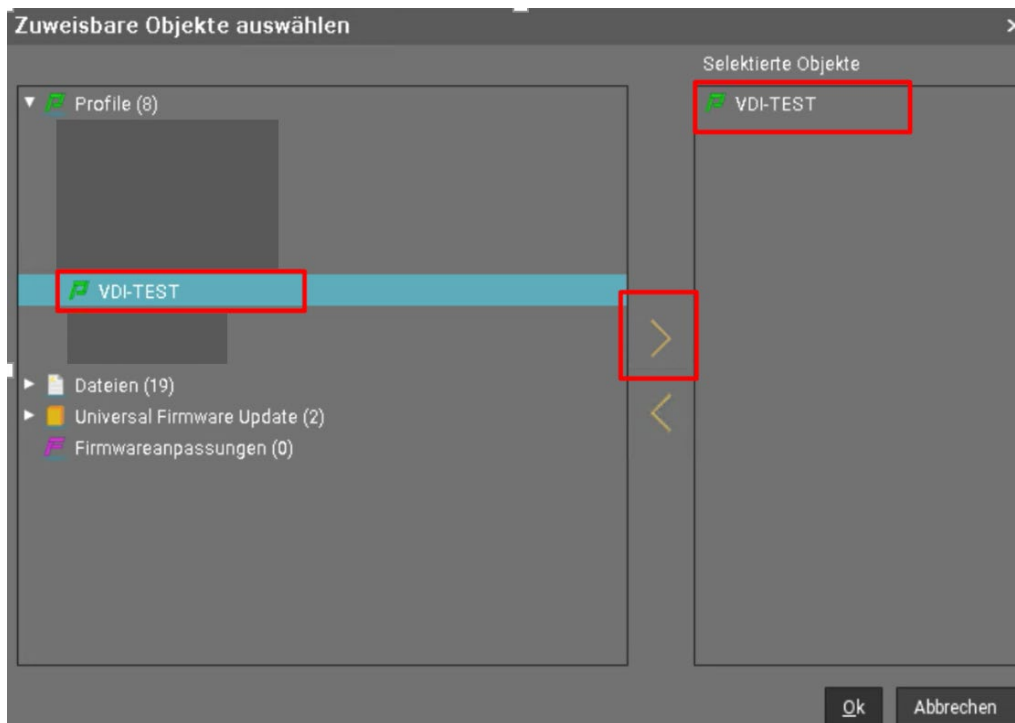


Abbildung 34: Profil auf ein Gerät übertragen (2)
Quelle: Eigene Darstellung

Anschließend werden Sie nach dem Änderungszeitpunkt gefragt, wobei Sie die Option „Beim nächsten Neustart“ auswählen können (siehe Abb. 35).

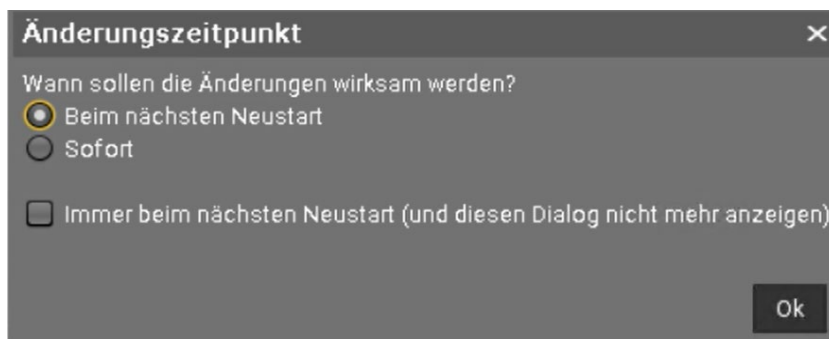


Abbildung 35: Änderungen übernehmen
Quelle: Eigene Darstellung

7.3. Prüfung

In einem letzten Schritt sollte, der Thin Client neu gestartet werden, um zu prüfen, ob die neue Sitzung korrekt angezeigt wird und ausführbar ist.

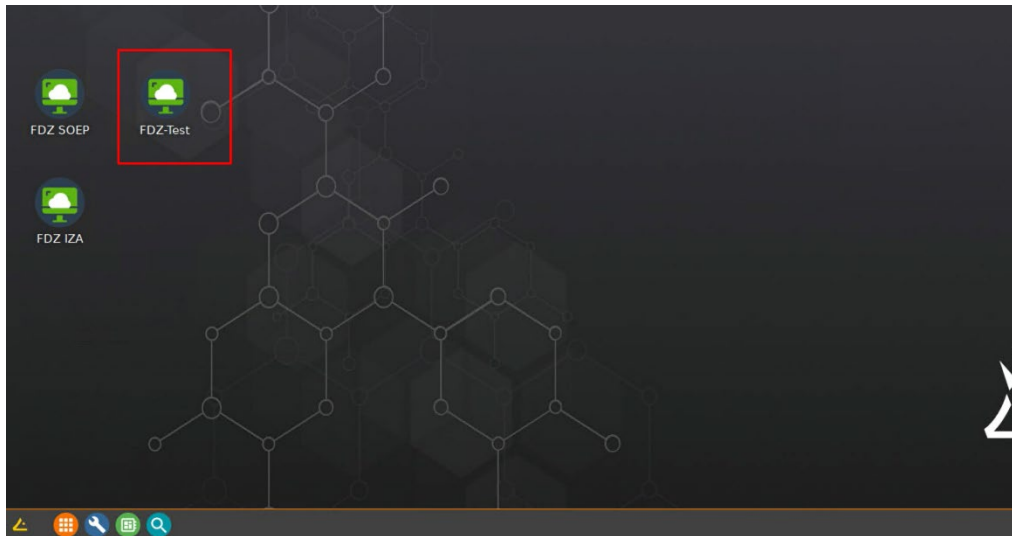


Abbildung 36: Neue Sitzung überprüfen
Quelle: Eigene Darstellung

8. Zusammenfassung

Das RDCnet hat zum Ziel, Gastwissenschaftsarbeitsplätze (GWAP) teilnehmender Forschungsdatenzentren (FDZ) in einem Netzwerk von gesicherten Zugangsstellen zu vereinen. Dadurch wird Forschenden ein höheres Maß an Flexibilität geboten, um auf sensible Daten der verschiedenen FDZ zuzugreifen. Anstatt dass Forschende zwingend zum datengebenden Institut vor Ort reisen müssen, haben sie die Möglichkeit, einen geeigneten Standort aus einer Auswahl teilnehmender Institute zu wählen. Somit können Reise- und Aufenthaltskosten für Forschende reduziert werden, wobei die Daten jedoch nach wie vor von gesicherten Arbeitsplätzen aus analysiert werden.

Das technische Konzept des RDCnet basiert dabei auf dem "FDZ-im-FDZ"-Ansatz (Bender & Heinig, 2011) und erweitert diesen für multilaterale Kooperationen. Jedes FDZ stellt hierbei als „Datenempfänger“ einen GWAP (z. B. in Form eines Thin Clients) bereit, der sich in einem Datensicherheitsraum befindet. Durch die Nutzung von "Secure Remote Access" können Forschende von diesen GWAP aus auf virtuelle Desktops anderer FDZ zugreifen, um formal anonymisierte bzw. sensible Forschungsdaten zu analysieren. Die Umsetzung erfolgt mithilfe einer "Virtuellen Desktop-Infrastruktur" (VDI), bei der die virtuellen Desktops auf den Servern der datengebenden FDZ gehostet werden. Diese Vorgehensweise gewährleistet eine kontrollierte Oberfläche zur Analyse der Daten in geschützten Umgebungen, wobei die Kontrolle über den Datenzugriff stets bei den datengebenden FDZ liegt.

Der Schwerpunkt dieses Working Papers liegt auf einer Beschreibung der technischen Anforderungen und Kriterien für die Rolle des Datenempfängers und bietet eine konkrete technische Anleitung, wie ein Thin Client als GWAP für das RDCnet konfiguriert werden kann. Dabei werden die technischen und organisatorischen Maßnahmen, die innerhalb des multilateralen Kooperationsvertrags des RDCnet (siehe Murray & Goebel, 2022) definiert wurden, berücksichtigt. Grundsätzlich wird die Verwendung von Thin Clients als GWAP empfohlen, da sie maßgeblich für Remote-Access-Anwendungen entwickelt wurden und Merkmale wie restriktive lokale Speicherung, erweiterte Sicherheitsoptionen oder eine effiziente Administration bieten. Die hier vorliegende Anleitung wird anhand eines Thin Clients der Marke "IGEL" dargestellt und umfasst die Lizenzregistrierung, Installation und Konfiguration der zentralen Administrationsoberfläche, Sicherheitskonfigurationen der Clients sowie die Installation und Definition von Sitzungen innerhalb der Remote Access Software VMware Horizon Client.

Das Working Paper bietet insbesondere für die FDZ eine Hilfestellung, die noch keinen GWAP implementiert haben, und soll somit die Hürden für die Umsetzung eines solchen Arbeitsplatzes im RDCnet verringern.

Literaturverzeichnis

Bender, S., and Heining, J. (2011): The Research-Data-Centre in Research-Data-Centre Approach: A First Step Towards Decentralised International Data Sharing. IASSIST Quarterly 35 (3), 10-16.

IGEL Community: Getting Started Guide. Zugriffsdatum 21.06.2023. URL: <https://www.igelcommunity.com/igel-getting-started-guide>

IGEL Knowledge Base [1]: License Portal. Zugriffsdatum 17.05.2023. URL: <https://kb.igel.com/gettingstarted/de/igel-license-portal-ilp-51194193.html>

IGEL Knowledge Base [2]: Installationsanforderungen. Zugriffsdatum 17.05.2023. URL: <https://kb.igel.com/endpointmgmt-6.04/en/installation-requirements-26035258.html>

IGEL Knowledge Base [3]: Ports und Kommunikation. Zugriffsdatum 17.05.2023. URL: <https://kb.igel.com/endpointmgmt-5.09/de/igel-ums-kommunikationsports-22459132.html>

IGEL Knowledge Base [4]: Registrierung Thin Client. Zugriffsdatum 17.05.2023. URL: <https://kb.igel.com/endpointmgmt/en/registering-thin-clients-on-the-ums-server-22459660.html>

IGEL Knowledge Base [5]: Geräte scannen und hinzufügen. Zugriffsdatum 17.05.2023. URL: <https://kb.igel.com/endpointmgmt-6.05/de/netzwerk-nach-geraeten-scannen-und-geraete-an-der-igel-ums-registrieren-31599388.html>

IGEL Knowledge Base [6]: Verbindungseinstellungen. Zugriffsdatum 17.05.2023. URL: <https://kb.igel.com/igelos-11.07/de/verbindungseinstellungen-57334505.html>

Murray, Neil, & Goebel, Jan. (2022). Vertragliche Grundlagen zur Teilnahme am RDCnet. In KonsortSWD Working Paper (Vol. 1). Zenodo. URL: <https://doi.org/10.5281/zenodo.6358334>

Impressum

Kontakt:

Neil Murray
SOEP in DIW Berlin
Mohrenstraße 58
10117 Berlin
Website
nmurray@diw.de

Berlin, September 2023

KonsortSWD Working Paper:

KonsortSWD baut als Teil der Nationalen Forschungsdateninfrastruktur Angebote zur Unterstützung von Forschung mit Daten in den Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften aus. Unsere Mission ist es, die Forschungsdateninfrastruktur zur Beforschung der Gesellschaft zu stärken, zu erweitern und zu vertiefen. Sie soll nutzungsorientiert ausgestaltet sein und die Bedürfnisse der Forschungscommunities berücksichtigen. Wichtiger Grundstein ist dabei das seit über zwei Jahrzehnten durch den Rat für Sozial- und Wirtschaftsdaten (RatSWD) aufgebaute Netzwerk von Forschungsdatenzentren. In dieser Reihe erscheinen Beiträge rund um das Forschungsdatenmanagement, die im Kontext von KonsortSWD entstehen. Beiträge, die extern und doppelblind begutachtet wurden sind entsprechend gekennzeichnet.

KonsortSWD wird im Rahmen der NFDI durch die Deutsche Forschungsgemeinschaft (DFG) gefördert – Projektnummer: 442494171.



Diese Veröffentlichung ist unter der Creative-Commons-Lizenz (CC BY 4.0) lizenziert:
<https://creativecommons.org/licenses/by/4.0/>

DOI: 10.5281/zenodo.8232563

Zitationsvorschlag:

Goebel, J., Murray, N., Pedrique, K., Sieber, I. (2023). *Implementierung eines Gastwissenschaftsarbeitsplatz im RDCnet - Technische Anleitung zur Konfiguration eines Thin Clients*. KonsortSWD Working Paper 6/2023. Konsortium für die Sozial-, Verhaltens-, Bildungs- und Wirtschaftswissenschaften (KonsortSWD).

<https://doi.org/10.5281/zenodo.8232563>