Pintexx Workplace

1 — Letzte Änderung: Jul 14, 2022

Pintexx GmbH

Inhaltsverzeichnis

1. Pintexx Workplace

Pintexx Workplace ist eine umfassende Lösung für den digitalen Arbeitsplatz.

Einen ersten Eindruck vermittelt der Workplace-Flyer.

1.1. Zum Einstieg

Pintexx Workplace wird als Virtuelle Maschine geliefert, welche von der Pintexx Download-Seite für VMWare oder HyperV heruntergeladen werden kann.
Um eine minimale Größe zu erzielen ist die VM im 7z-Format gepackt.

Nach dem Entpacken kann die VM in das jeweilige System geladen werden.

1.1.1. Vorbereitung

Pintexx Workplace wird als Virtuelle Maschine (VM) für unterschiedliche Hypervisors geliefert.

Anforderungen VM

HyperV
VMWare (vmdk, ova)

Single VM Betrieb

min. 1 Core
min. 2 GB Ram (empfohlen 4 GB)
30 GB Storage

Multi VM Betrieb (Load Balancing)

1 VM Portal
Min. 2 VM Gateway

Die Anforderungen an CPU und Speicher hängen von der Anzahl an Benutzern ab.

Statische IP

Wenn kein DHCP-Server verwendet werden soll werden folgende Informationen benötigt:

Statische IP
Gateway
DNS
Netzmaske

Netzwerk Routen

Werden verschiedene Netze verwendet dann müssen evtl. Netzwerk-Routen im System eingetragen werden.

Anforderungen SSL

Single VM Betrieb
Wenn ein eigenes Zertifikat verwendet werden soll, wird ein Zertifikat im p12-Format inkl. Passwort benötigt.

Multi VM Betrieb
Empfohlen wird ein Sub-Domain-Zertifikat, ansonsten ein Zertifikat für Portal und Gateways

DNS

Single VM Betrieb
Es wird ein DNS-Eintrag mit IP der VM benötigt

Multi VM Betrieb
Es werden DNS-Einträge für das Portal und jedes Gateway benötigt

Portweiterleitung

Single VM Betrieb
Es wird eine Portweiterleitung in der Firewall auf Port 80 und 443 der VM benötigt (empfohlen)

Multi VM Betrieb
Es werden Portweiterleitungen für das Portal und jedes Gateway benötigt. Es können dafür unterschiedliche Ports verwendet werden.

Anforderungen Active Directory/LDAP

IP/Host des AD/LDAP Servers
OU, die eine Gruppe enthält, welche die Benutzer enthält, die das System nutzen sollen
OU der Benutzer, um Benutzer-Informationen auslesen zu können
AD Domäne
AD Lese Benutzer, Login/Passwort eines Benutzers mit dem sich Gruppen und Benutzer auslesen lassen
Wenn die IP Adresse des PC’s aus AD gelesen werden soll, dann einen Feldnamen aus AD für IP
Wenn die MAC Adresse des PC’s aus AD gelesen werden soll, dann einen Feldnamen aus AD für MAC
Wenn die Telefon-Nr. des PC’s aus AD gelesen werden soll, dann einen Feldnamen aus AD für Telefon

Radius

IP/Host des Radius Servers
Secret
Protokoll (PAP/CHAP)
Port

Zugriff auf RDS mit Load Balancing

Wird auf einen MS RD Broker mit mehreren Terminal Servern zugegriffen wird die Load Balancing Info benötigt.

tsv://MS Terminal Services Plugin.1.

Benutzer

Wird zur Authentifizierung Radius verwendet oder soll direkt über einen lokalen Benutzer authentifiziert werden dann müssen diese Benutzer im System angelegt werden.

Sollen viele Benutzer angelegt werden so können unsere Import-Tools angefragt werden.

WakeOnLan

Für das Aufwecken eines PC’s wird seine Mac Adresse benötigt.

Steht der PC in einem anderen Netzwerk kann ein WOL-Dienst verwendet werden.
Dieser kann von der Pintexx HomePage geladen werden.

2-Faktor-Authentifizierung

Im Falle einer 2-Faktor-Authentifizierung müssen für jeden Typ unterschiedliche Daten bereitgestellt werden:

E-Mail: Wenn AD, dann muss E-Mail im AD vorhanden sein., ansonsten im lokalen Benutzer
SMS: SMS Provider Url
Googler Authenticator: APP auf SmartPhone
Radius: Key Generator

Drucken

Soll auf dem lokalen Drucker gedruckt werden können und wird ein Client-Betriebssystem < Windows 10 verwendet, dann muss der Druck-Konverter aktiviert werden. (Remote Admin -> Einstellungen -> Drucken)

Logo

Für das Anwender-Portal kann ein Logo konfiguriert werden. Das Logo kann als png, gif, jpeg konfiguriert werden.

Benachrichtigung

Wird als 2-Faktor Auth. E-Mail verwendet, dann müssen die Verbindungsdaten eines SMTP-Servers bekannt sein.

Backup

Soll ein Backup der Konfigurationsdatenbanken durchgeführt werden, werden die Verbindungsdaten eines FTP Servers benötigt

Updates

Für das Einspielen von Updates muss ein Zugriff auf

https://pinapps.pintexx.com

möglich sein.

Reporting

Für den Report der Zugriffszahlen zur Abrechnung muss ein Zugriff auf

https://pinapps.pintexx.com

möglich sein

Monitoring

Wenn ein Monitoring erfolgen soll, z.B. über SNMP dann wird eine entsprechendes Tool benötigt, dazu die IP-Adresse des Tool-Servers

Netzwerk

Um auf vorgesehene PC’s im Netzwerk zugreifen zu können, muss evtl. der Zugriff in einer Firewall freigeschaltet werden.

Wird auf ein Netzwerk mit der IP
172.17.x.x
zugegriffen?

Sicherheit

Für erweiterte Sicherheit kann eine TLS-Version z.B. TLSv1.2 konfiguriert werden.
Des Weiteren können entsprechende http-Headern gesetzt werden.

Lizensierung

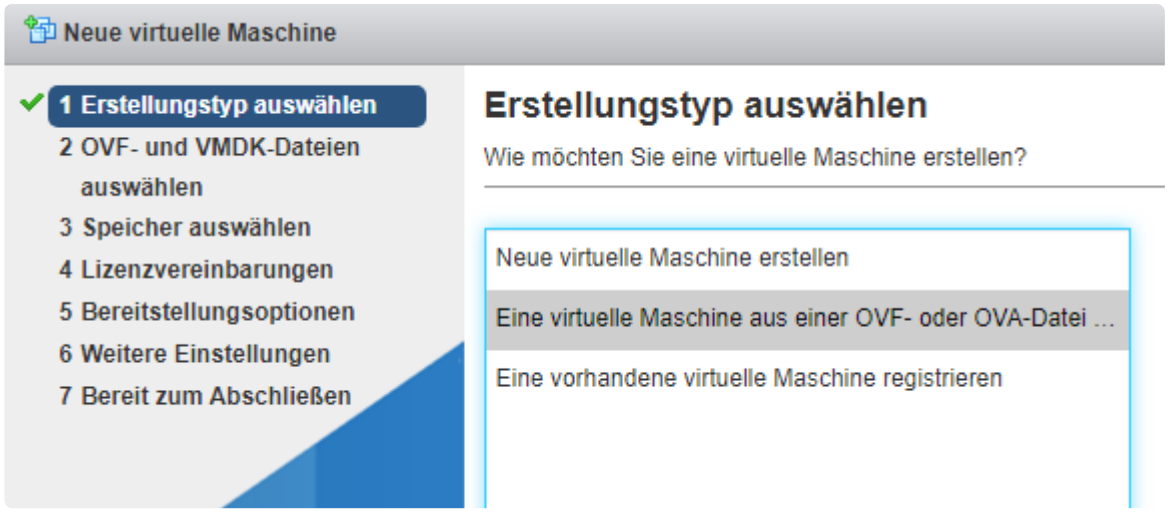
Vor dem Release muss ein gültige Lizenz in “System” installiert sein.

1.1.2. VM einrichten

VMWare

Nach dem Download und dem Entpacken sollten folgende Dateien vorliegen:
pintexx-workplace.ovf
pintexx-workplace-disk1.vmdk

In VMWare “Neue VM erstellen/registrieren”



Als Erstellungstyp “Eine virtuelle Maschine aus einer OVF…” auswählen

“Weiter”

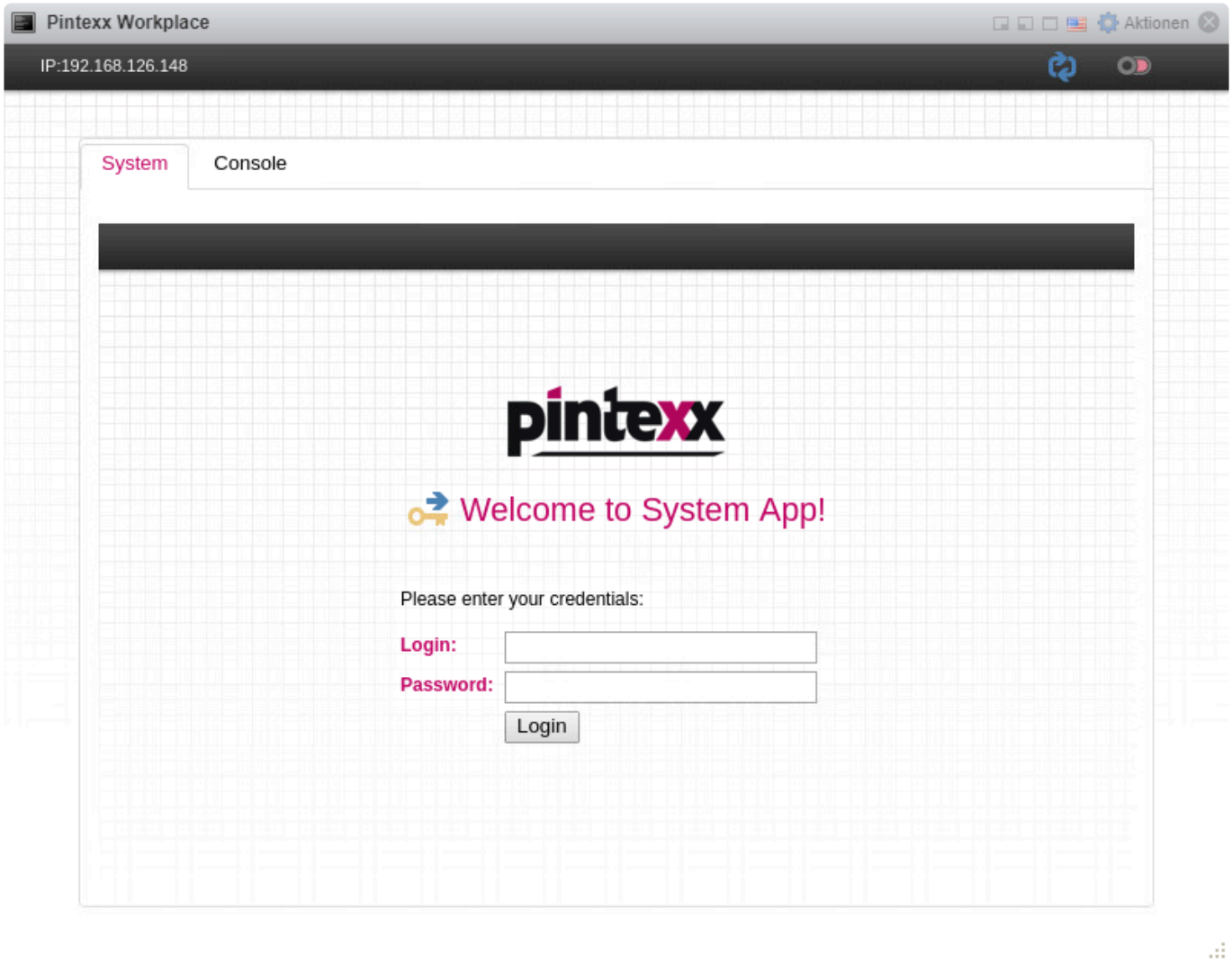
Einen Namen für die VM eingeben und die beiden Dateien auswählen.

Dann immer auf “Weiter” und letztendlich auf Beenden.

Die VM sollte nun importiert und i.d.R. auch gestartet sein.

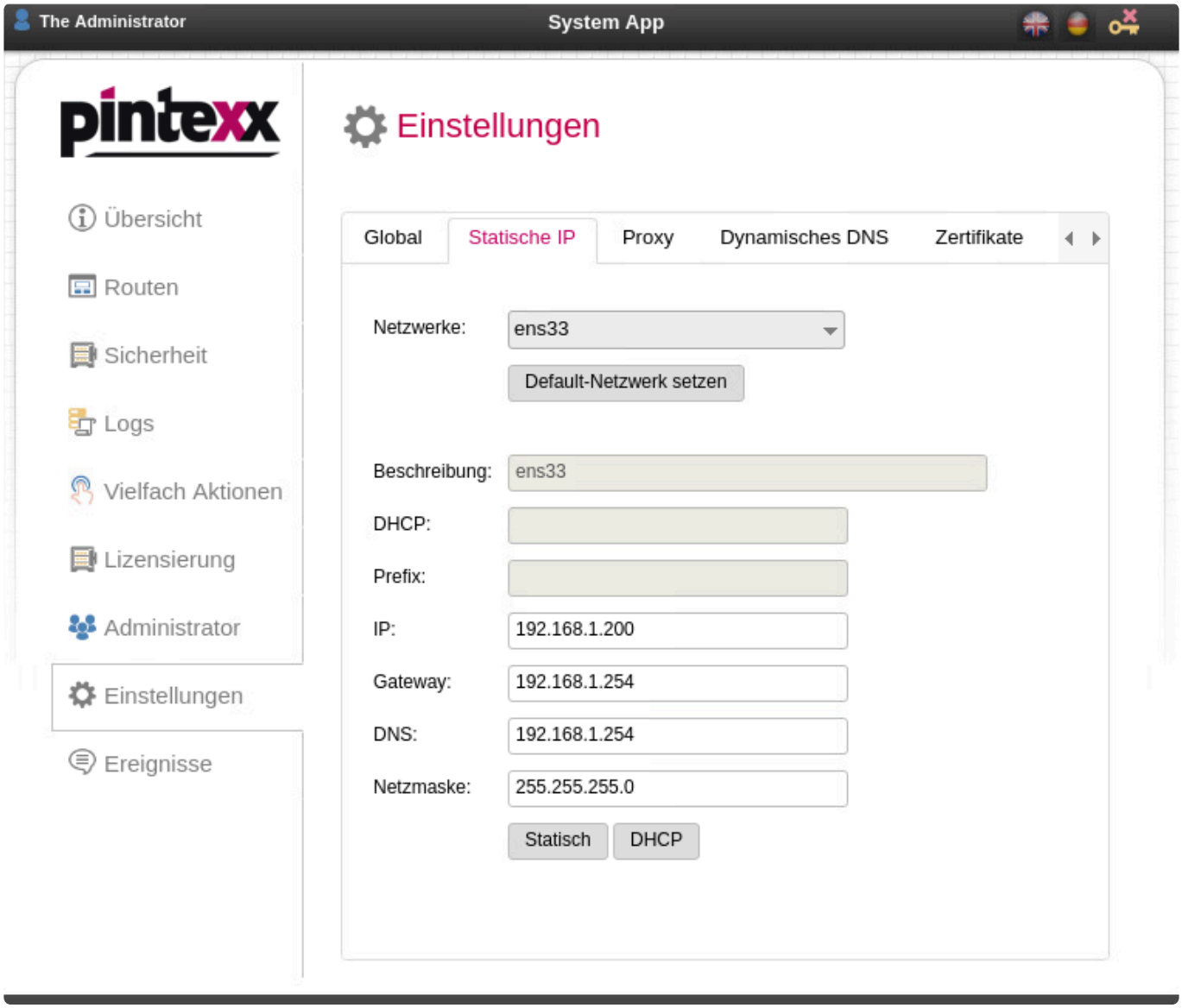
1.1.3. Statische IP setzen

In der VM Konsole sollte ein Anmeldebildschirm für “System” angezeigt werden.



Anmelden mit:
Login: administrator
Passwort: 12345678

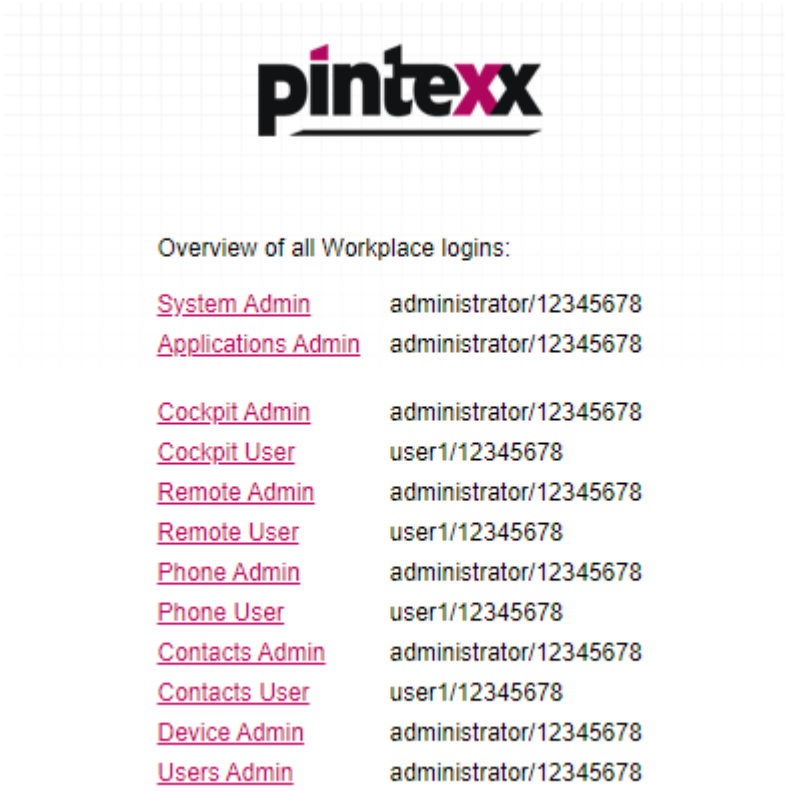
Dann auf “Einstellungen” – “Statische IP”.



Dann die statische IP, Gateway, DNS und Netzmaske setzen.
Dann auf “Statisch”.
Das System muss nun neu gestartet werden. Dies kann in der Konsole am oberen rechten Rand über den blauen “Neustart”-Button durchgeführt werden.

1.1.4. Schnelltest

Nach dem Setzen der statischen IP sollte diese direkt im Browser aufrufbar sein.
Als Ergebnis sollte eine Übersichtsseite über die aktuellen Zugänge der Workplace Anwendungen mit Login/passwort erscheinen.



Damit lassen sich alle Zugänge testen.

Zum Test der Remote-Funktion auf “Remote User”.
Anmelden mit
Login: user1
Passwort: 12345678

Angezeigte Verbindung öffnen.
Anmelden am Windows Desktop mit
Login: user1
Passwort: 12345678

Ist ein Zugang in alle Anwendungen möglich ist das System korrekt installiert und kann nun konfiguriert werden.

1.2. Workplace Anwendungen

Pintexx Workplace umfasst zahlreiche Anwendungen.
Dazu gehören administrative Anwendungen sowie Anwendungen mit Benutzerzugang.

Zu den administrativen Anwendungen gehören “System” und “Applications”.
Über “**System**” werden alle system-relevanten Konfigurationen durchgeführt.
Über “**Applications**” können Anwendungen aus einem App Store installiert und aktualisiert werden.
“System” und “Applications” sind immer vorhanden und benötigt keine Lizenzierung.

Über “**Device**” können alle “Business Devices” verwaltet werden.

Zu den Anwendungen mit Benutzer-Zugang gehören:
“**Cockpit**”: Web Desktop und zentrales Authentifizierungs-System
“**Remote**”: Zugriff auf Windows-Desktop über Browser
“**Phone**”: Web-basiertes Telefon mit Zugriff auf Telefon-Anlage (SIP-Client)
“**Contacts**”: Anlegen von Addressbüchern mit REST-API

1.2.1. Workplace “System”

“System” verwaltet systemnahe Einstellungen.

Dazu gehört z.B. die Proxy-Konfiguration (Routen), die Zertifikatsverwaltung, die Lizenzierung und das Setzen der statischen IP-Adressen.

1.2.1.1. Aufruf

“System” kann direkt über folgende Url aufgerufen werden:

<IP/Domäne>/system

“System” hat nur einen Administrator-Zugang.

1.2.1.2. Übersicht

In der Übersicht wird der aktuelle System-Status angezeigt.

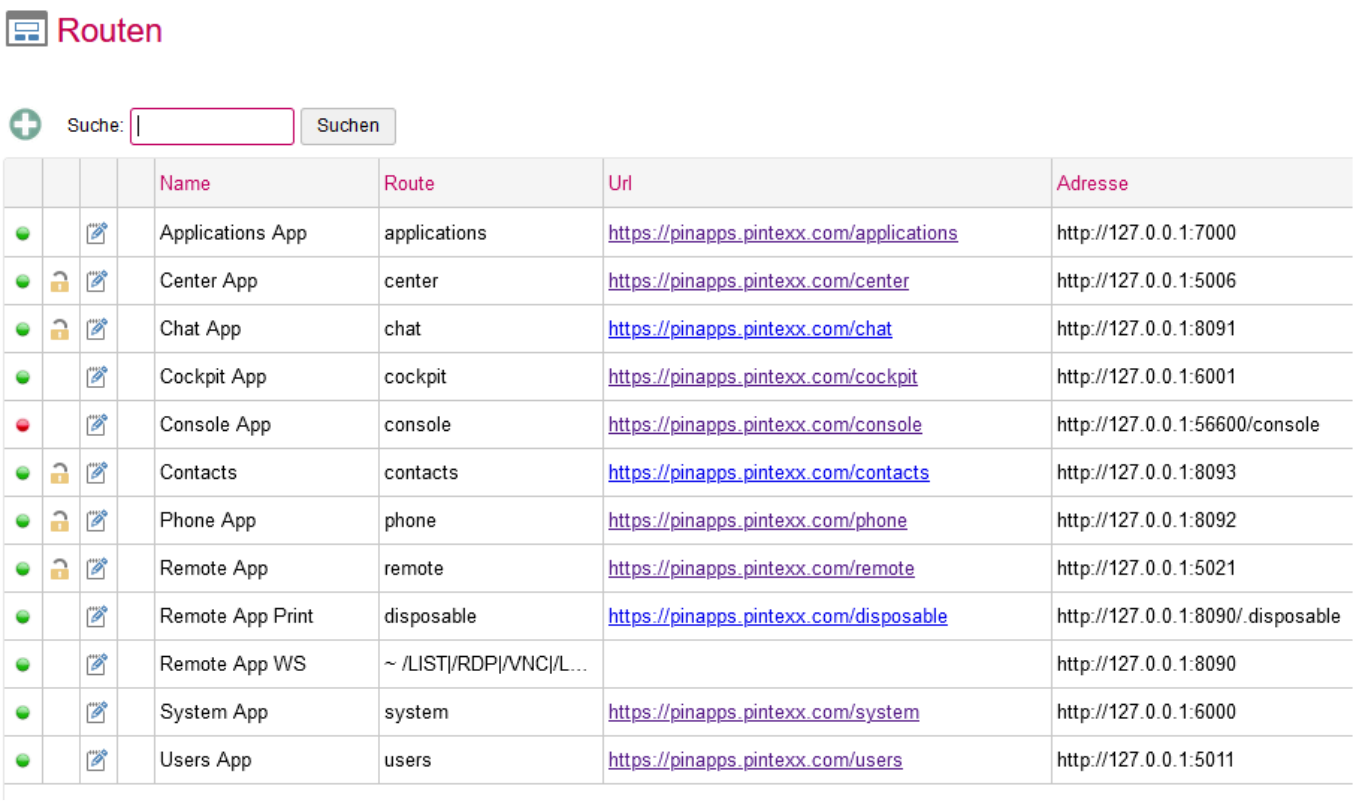
Es wird empfohlen die Prozessor-Auslastung, die Speicher-Auslastung vor allem aber die Laufwerksauslastung regelmäßig zu prüfen.
Durch kontinuierliches Schreiben von Log-Dateien über einen längeren Zeitraum kann das Laufwerk volllaufen.
Über Einstellungen -> System -> Freigeben kann Laufwerks-Platz freigegeben werden.

1.2.1.3. Routen

“System” kann über sog. Routen Anwendungen über einen Namen unterhalb derselben Domäne zugänglich machen.

Beispiel:
https://workplacedemo.pintexx.com/myroute

Nach der Installation sind Routen auf alle Apps eingetragen. Die vom System verwendeten Routen können nicht gelöscht oder verändert werden.
Die Konsole App ist nicht aktiviert.



Name	Route	Url	Adresse
Applications App	applications	https://pinapps.pintexx.com/applications	http://127.0.0.1:7000
Center App	center	https://pinapps.pintexx.com/center	http://127.0.0.1:5006
Chat App	chat	https://pinapps.pintexx.com/chat	http://127.0.0.1:8091
Cockpit App	cockpit	https://pinapps.pintexx.com/cockpit	http://127.0.0.1:6001
Console App	console	https://pinapps.pintexx.com/console	http://127.0.0.1:56600/console
Contacts	contacts	https://pinapps.pintexx.com/contacts	http://127.0.0.1:8093
Phone App	phone	https://pinapps.pintexx.com/phone	http://127.0.0.1:8092
Remote App	remote	https://pinapps.pintexx.com/remote	http://127.0.0.1:5021
Remote App Print	disposable	https://pinapps.pintexx.com/disposable	http://127.0.0.1:8090/.disposable
Remote App WS	~ /LIST|/RDP|/VNC|/L...		http://127.0.0.1:8090
System App	system	https://pinapps.pintexx.com/system	http://127.0.0.1:6000
Users App	users	https://pinapps.pintexx.com/users	http://127.0.0.1:5011

In der ersten Spalte wird der Status der Route angezeigt. Ein grünes Symbol bedeutet aktiv, ein rotes Symbol inaktiv.
Durch Aktivieren des Symbols kann der Status verändert werden.

Befindet sich in der 2.Spalte ein Symbol, so kann der Zugriff auf diese Route so eingeschränkt werden, dass ein Zugriff nur über das Cockpit möglich ist.

Befindet sich in der 4. Spalte ein rotes Kreuz, dann kann diese Route gelöscht werden.
In den folgenden Spalten wird die Routen-Bezeichnung, die Route, die Url (als Link) sowie die interne IP-Adresse/Port angezeigt.

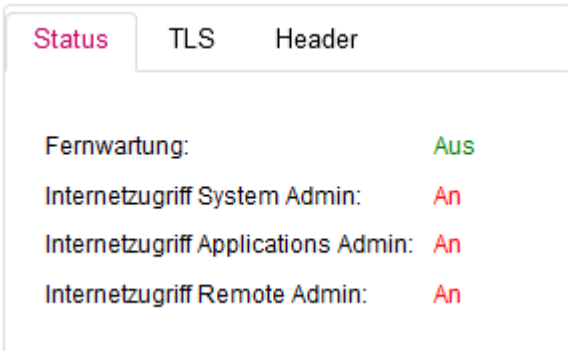
Die Routen von Anwendungen aus dem App Store müssen nicht selbst angelegt werden. Diese werden nach der Installation der Anwendung von “Applications” selbst angelegt.

1.2.1.4. Sicherheit

Über das Menü “Sicherheit” kann der aktuelle Status angezeigt werden sowie der TLS-Level und Header eingestellt werden.

1.2.1.4.1. Status

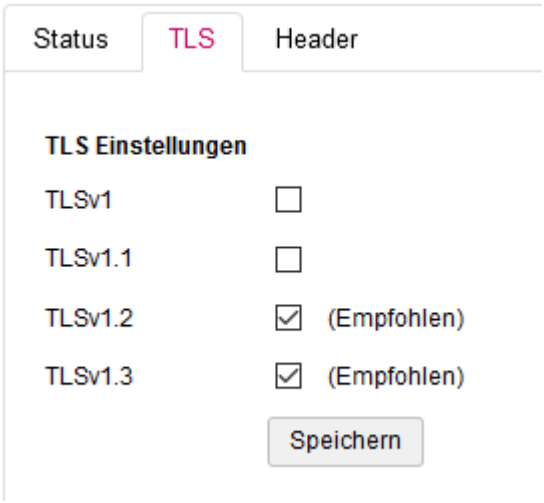
Im Status-Tab wird der aktuelle Status- der Sicherheits-Einstellungen angezeigt.



Hier kann überprüft werden, ob die Fernwartung (Konsole) aktiv ist und ob Admin-Zugriffe über das Internet freigegeben sind.

1.2.1.4.2. TLS-Level

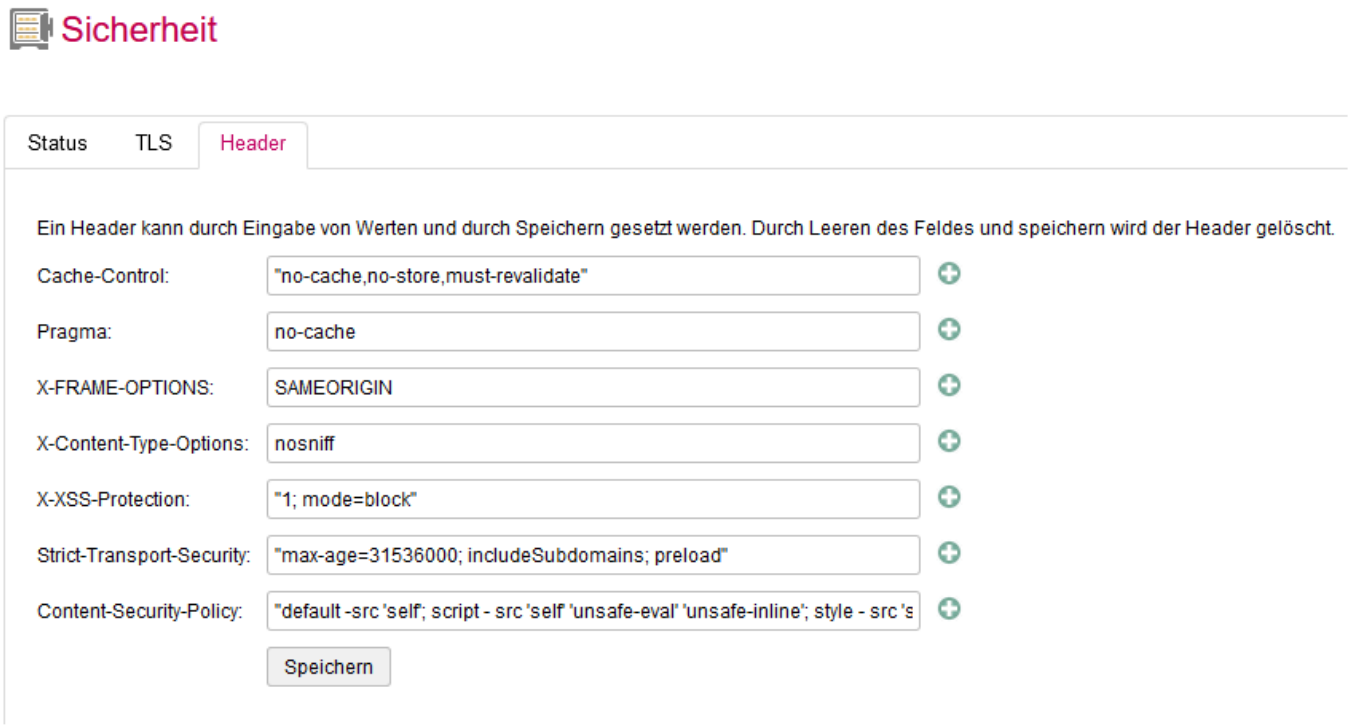
Im TLS-Tab kann der TLS-Level eingestellt werden.



Achtung:
Diese Einstellungen sollten ganz zum Schluss getätigt werden, z.B. bevor Let’s Encrypt eingerichtet wird.

1.2.1.4.3. Header

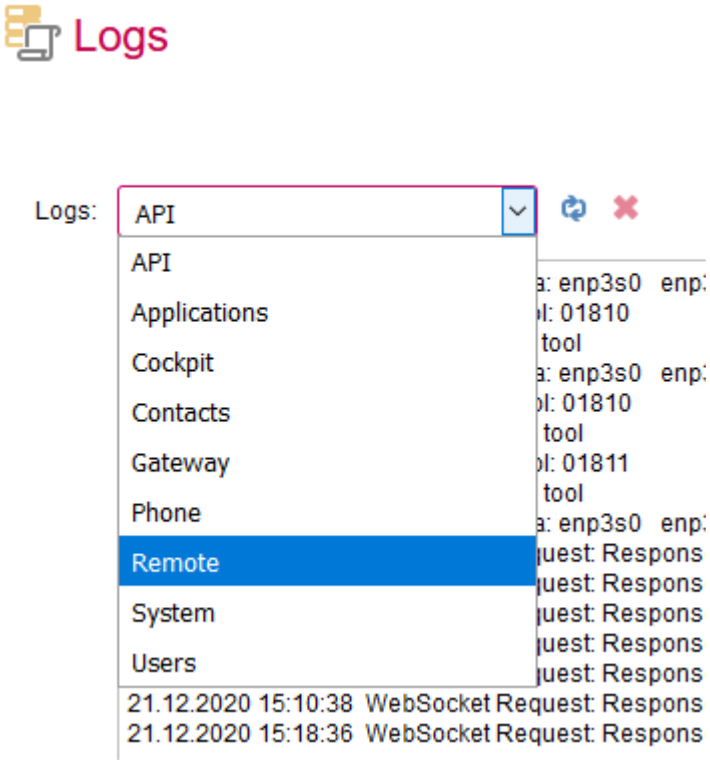
Im Header-Tab können weitere Sicherheits-Merkmale durch Konfiguration von Headern eingestellt werden.



Achtung:
Diese Einstellungen sollten ganz zum Schluss getätigt werden, z.B. bevor Let's Encrypt eingerichtet wird.
Werden hier andere Einstellungen als die Default-Einstellungen vorgenommen kann diese u.U. zu einem Zugriffs-Verlust auf das System führen!

1.2.1.5. Logs

Im Logs-Menü können alle Log-Dateien aller installierten Anwendungen eingesehen werden.

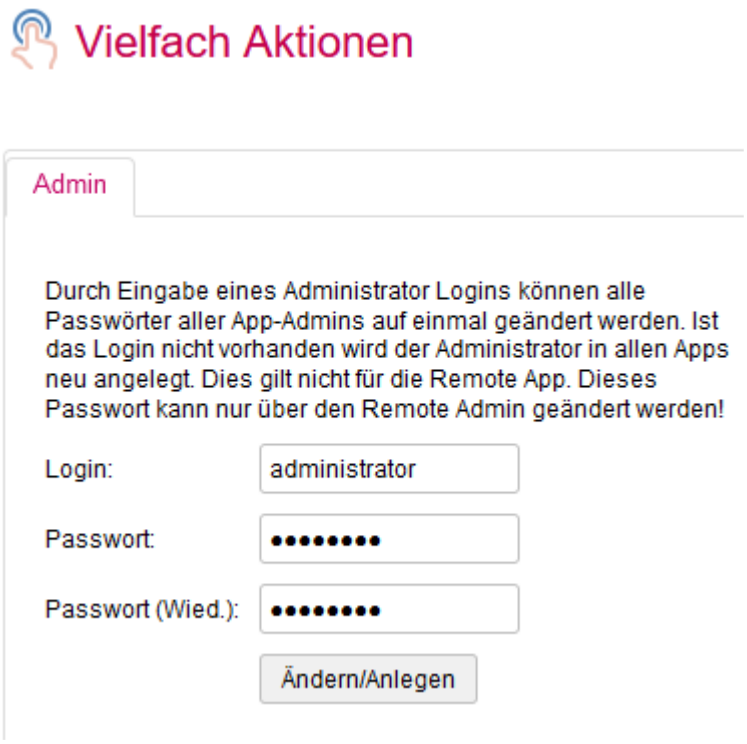


Durch den Refresh-Button kann die Anzeige aktualisiert werden.
Durch den Löschen-Button kann die Log-Datei gelehrt werden.

Ausnahme:
Die Gateway-Log-Datei kann nur über den Remote-Admin gelöscht werden.

1.2.1.6. Vielfach Aktionen

Bei den Vielfach-Aktionen handelt es sich aktuell um die Möglichkeit, das Administrator-Passwort in allen Anwendungen auf einmal zu setzen.
Weitere Aktionen können später hinzugefügt werden.



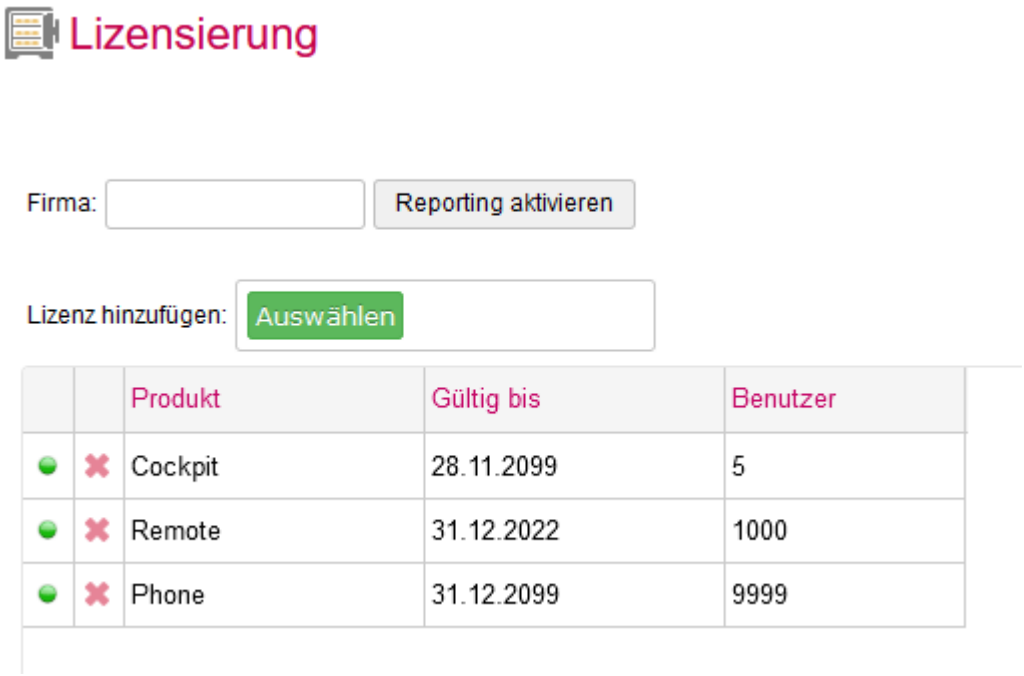
Durch Angabe eines bestehenden Admin-Logins wird das Passwort für alle Admins aller installierten Anwendungen neu gesetzt.
Ist das Login nicht vorhanden, wird ein neuer Admin angelegt.

Ausnahme:
Dieses Feature gilt nicht für den “Remote” Admin.

1.2.1.7. Lizenzierung

Hier kann die Lizenzierung aller Anwendungen durchgeführt werden.
“System” , “Applications” und “User” gehören zu den Verwaltungs-Anwendungen und müssen nicht lizenziert werden.

Für alle weiteren Anwendungen gibt es vom Hersteller entsprechende Lizenz-Dateien, die über den Auswählen-Button eingespielt werden können.



Nach Installation der VM oder Starten der pinBox wird eine Demo-Lizenz installiert, welche für 45 Tage gültig ist.

Wird das System zahlungspflichtig in Betrieb genommen, muss im Feld “Firma” einmalig der Firmenname eingegeben werden und das Reporting aktiviert werden.

1.2.1.8. Administrator

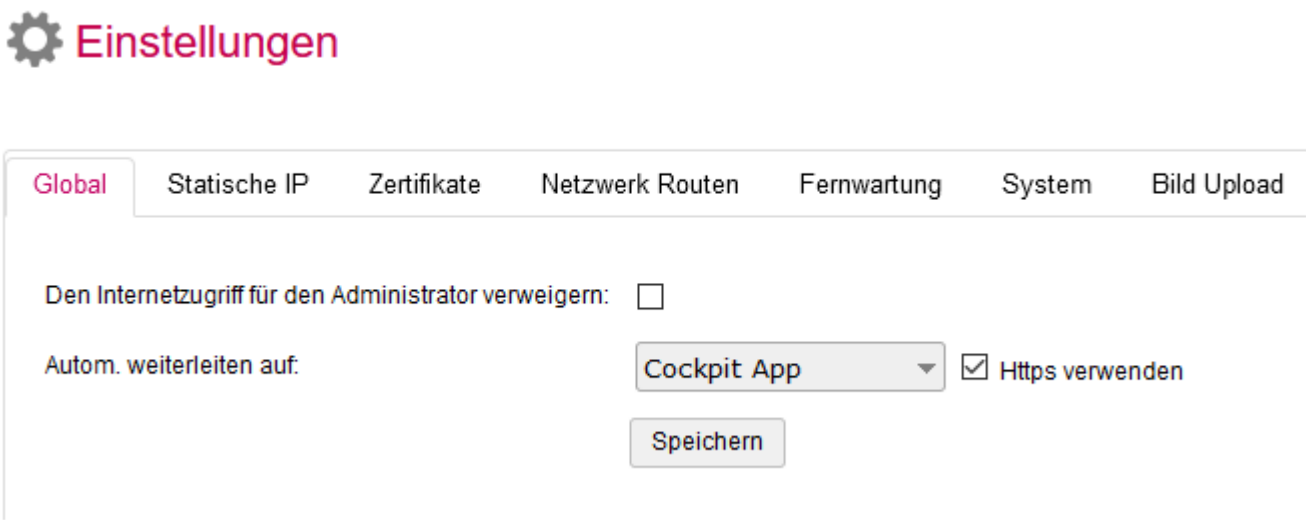
Siehe Administrator

1.2.1.9. Einstellungen

Hier können die verfügbaren Einstellungen gesetzt werden.

1.2.1.9.1. Global

Im “Global”-Tab können verschiedene Einstellungen gesetzt werden.



Administrator-Zugriff verweigern

Durch Aktivieren ist kein Zugriff auf “System” über das Internet mehr möglich, sondern nur noch über die interne IP-Adresse.
Sollten mehrere Netzwerkkarten verwendet werden (VM) bestimmt das Default-Netzwerk die IP.

Empfehlung:
Nach Konfiguration diese Einstellung immer aktivieren

Automatische Weiterleitung

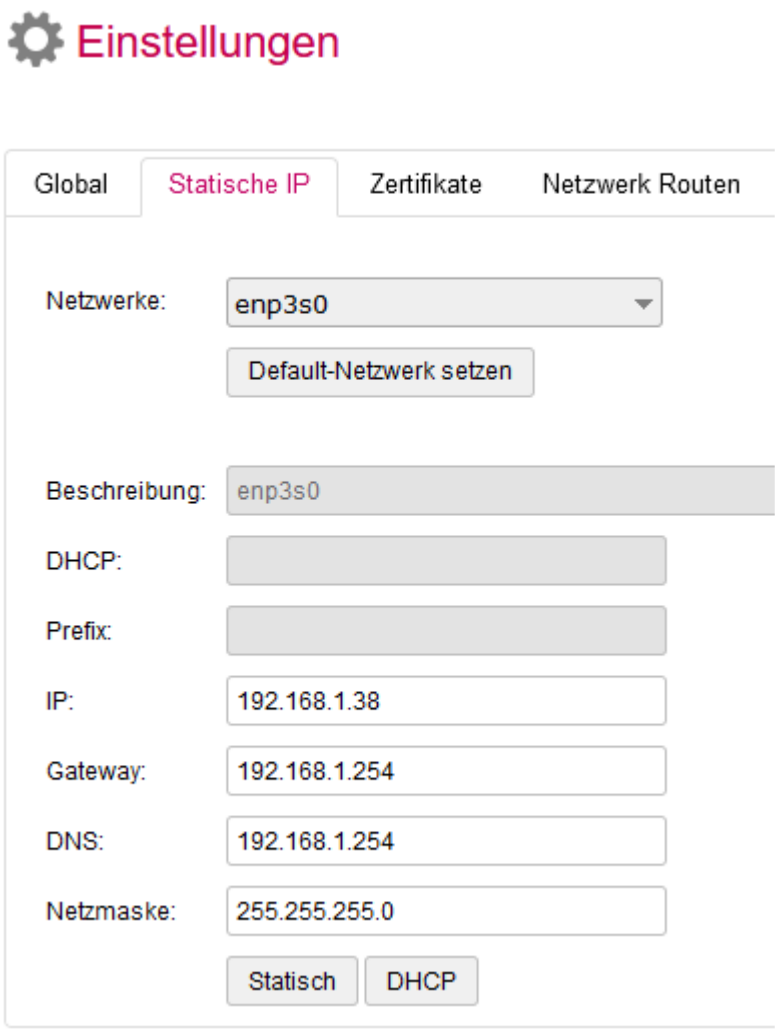
Hier kann eine automatische Weiterleitung auf eine installierte Anwendung konfiguriert werden.
D.h. durch Eingabe der IP-Adresse oder Domäne wird automatisch auf die Anwendung umgeleitet.

Wird auch noch “https” aktiviert, erfolgt eine Umleitung auf https://domäne.

Achtung:
Zum Zeitpunkt des Speicherns mit aktiviertem “https” muss “System” über eine Domäne aufgerufen sein.

1.2.1.9.2. Statische IP

Hier kann für eine oder mehrere Netzwerk-Karten eine statische IP-Adresse gesetzt werden.



Die verfügbaren Netzwerke (Netzwerkkarten über VM) werden in der Liste angezeigt.
Es besteht aktuell leider keine Beziehung zwischen dem Netzwerknamen in der VM und dem hier angezeigten Netzwerknamen.
Dies kann nur durch Try/Error herausgefunden werden.

Werden mehrere Netzwerkkarten verwendet kann über den “Default”-Button das Default-Netzwerk gesetzt werden.
Über dieses Netzwerk ist dann das System erreichbar.

Über den “Statisch”-Button kann dann die stat. IP-Adresse zugewiesen werden.
Über den “DHCP”-Button wird die stat. IP-Adresse entfernt und das System versucht über DHCP eine IP-Adresse zu erhalten.

Achtung:
Durch die Eingabe falscher Werte kann das System nicht mehr zugreifbar werden.

1.2.1.9.3. Zertifikate

Das System bietet die Möglichkeit, sowohl eigene Zertifikate als auch Let’s Encrypt zu verwenden.

Let’s Encrypt

Ein LE-Zertifikat kann installiert werden, sobald “System” über eine Domäne aufgerufen wird.
Danach muss noch eine E-Mail angegeben werden. Diese dient bei LE zur Zusendung von Informationen, sobald das Zertifikat abgelaufen ist.
“System” sorgt aber dafür, dass das Zertifikat nach Ablauf automatisch verlängert wird.

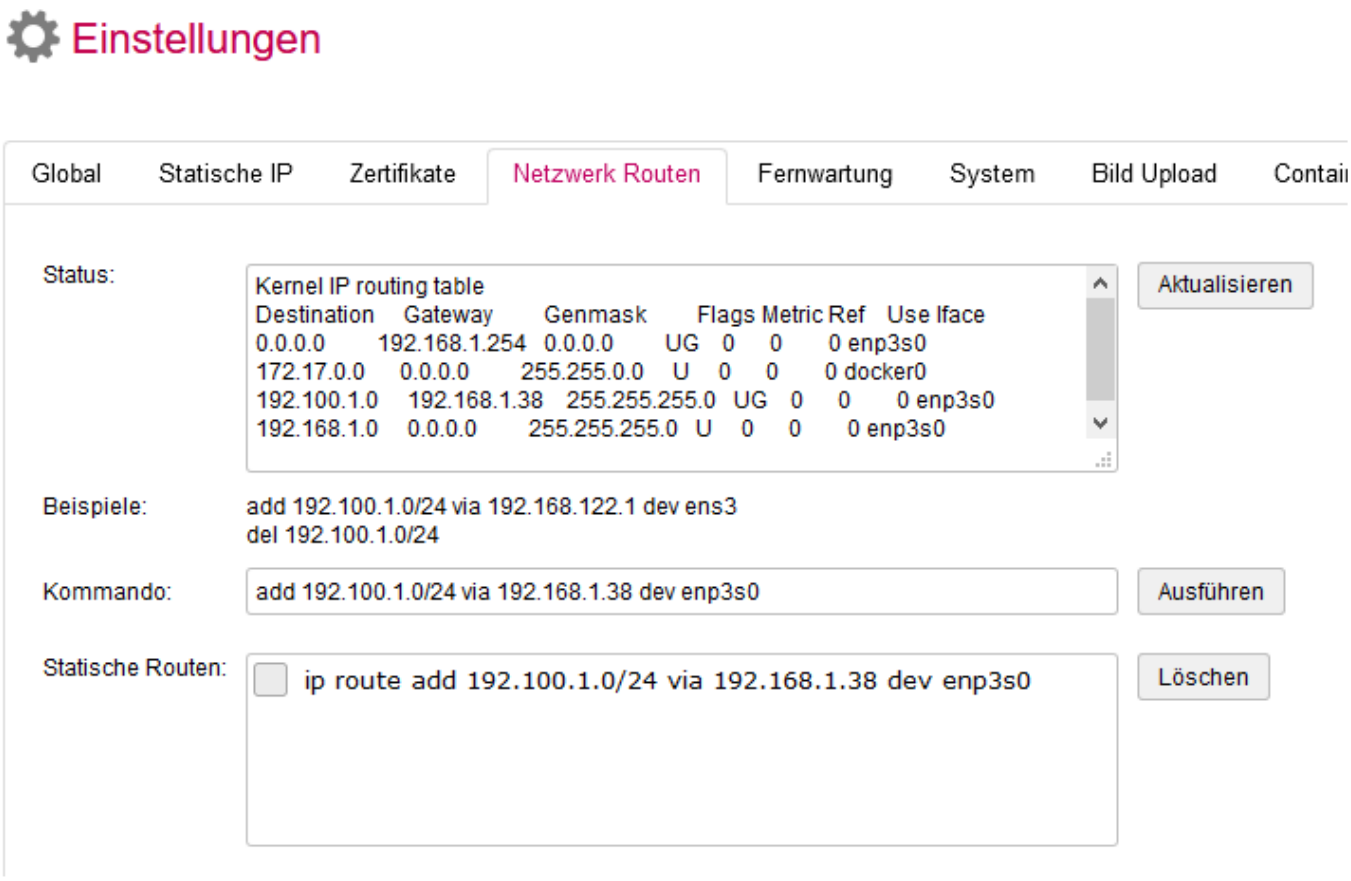
Eigene Zertifikate

Ein Standard-Zertifikat, welches im Format .p12 vorliegen muss, kann über “Durchsuchen”-Button vom lokalen Laufwerk geladen werden.
Zusätzlich wird das Zertifikats-Passwort benötigt.
Dann kann durch den “Installieren”-Button das Zertifikat installiert werden.

Hinweis:
Nach der erfolgreichen Installation des Zertifikates können ALLE installierten Anwendungen über https aufgerufen werden.

1.2.1.9.4. Netzwerk Routen

Um verschiedene End-Punkte im Netzwerk erreichen zu können ist u.U. das Setzen von Netzwerk-Routen erforderlich.



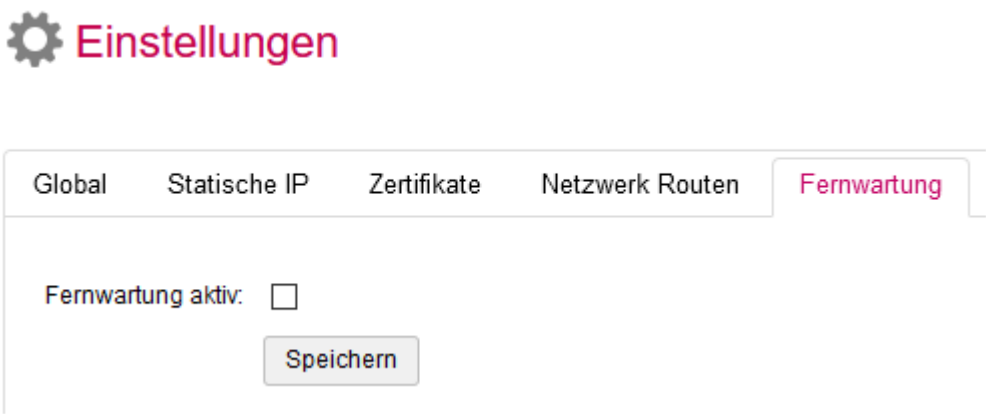
Der aktuelle Status wird im Status-Bereich angezeigt und kann über den “Aktualisieren”-Button aktualisiert werden.

Durch Ausführen eines Kommandos können weitere Routen hinzugefügt werden.
Diese Routen stehen auch nach Neustart des Systems zur Verfügung und können ebenfalls wieder gelöscht werden.

Achtung:
Dieser Bereich sollte nur von Experten verwendet werden da Falscheingaben den Zugriff auf das System beeinträchtigen können!

1.2.1.9.5. Fernwartung

Wird der Fennzugang aktiviert, dann wird die Konsole freigegeben.



Über
<ip/domäne>/console
kann dann ein Hersteller-Mitarbeiter auf das System zugreifen.

Achtung:
Die Fernwartung sollte nur auf ausdrückliche Empfehlung eines Hersteller-Mitarbeiters oder dessen Beauftragten aktiviert werden!

1.2.1.9.6. System

Über den “System”-Tab können grundlegende System-Aktionen durchgeführt werden.

System neu starten

Bitte das System NIE einfach nur ausschalten sondern immer kontrolliert über diese Funktion neu starten.

System herunterfahren

Bitte das System NIE einfach nur ausschalten sondern immer kontrolliert über diese Funktion herunterfahren.

System-Check

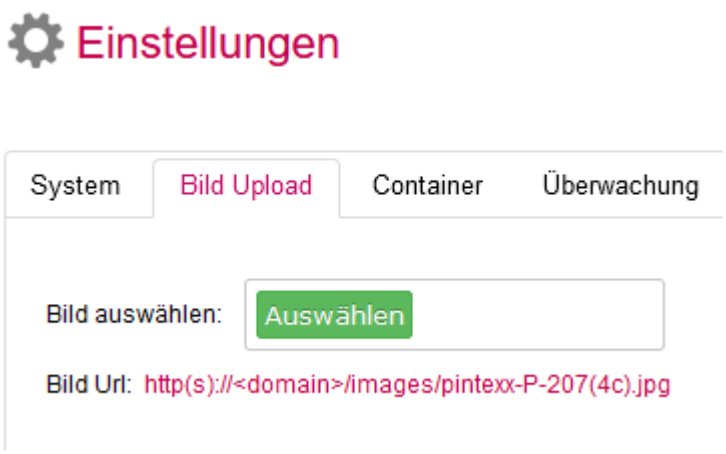
Hier können verschieden System-Einstellungen überprüft werden. Bei Fehlern bitte an den Support wenden.

Speicherplatz freigeben

Über die Zeit können Log-Dateien zu einer Verringerung des Speicherplatzes führen.
Über diese Funktion kann deshalb eine Speicherbereinigung durchgeführt werden.

1.2.1.9.7. Bild Upload

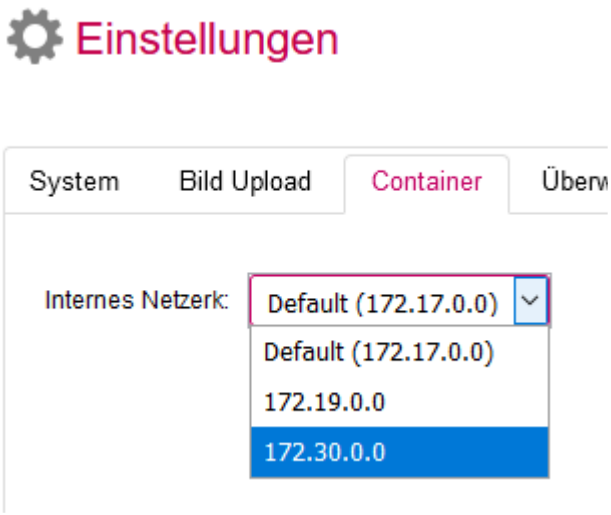
Für die Verwendung von Logos oder Hintergründen für verschiedene Anwendungen können hier zentral Bilder hochgeladen werden.



Nach dem Hochladen wird die Url des Bildes angezeigt, welche dann in andere Anwendungen übernommen werden kann.

1.2.1.9.8. Container

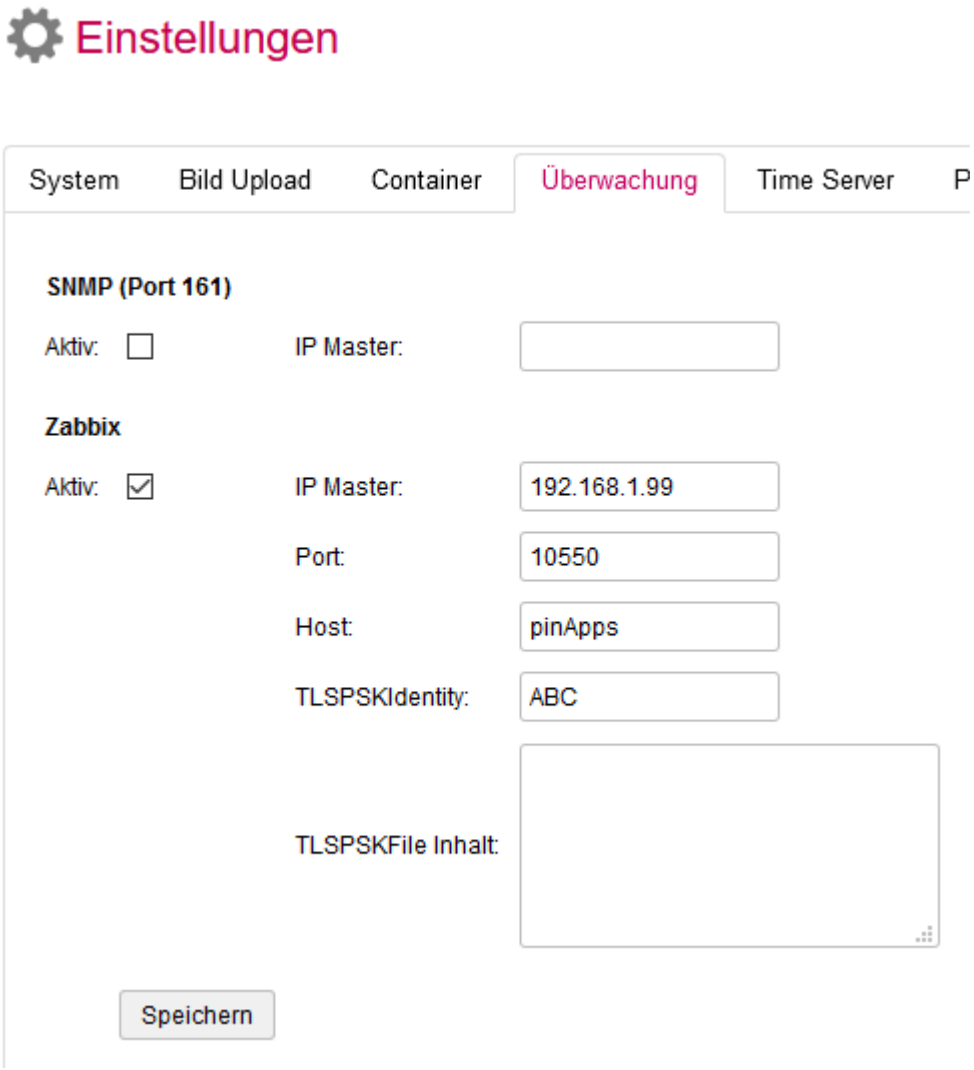
Die interne Verwendung der IP 172.17.x.x kann in machen Netzwerken zu Problemen führen.



Deshalb kann diese interne IP verändert werden.

1.2.1.9.9. Überwachung

Das System verfügt über einen Anbindung an die Monitoring-Systeme SNMB und Zabbix.



SNMP

Bei SNMP muss lediglich die IP des zugreifenden Systems angegeben werden.

Zabbix

Bei Zabbix müssen die Master IP, der Port, der Host sowie die TLSPSKIdentity und TLSPSKFile angegeben werden.

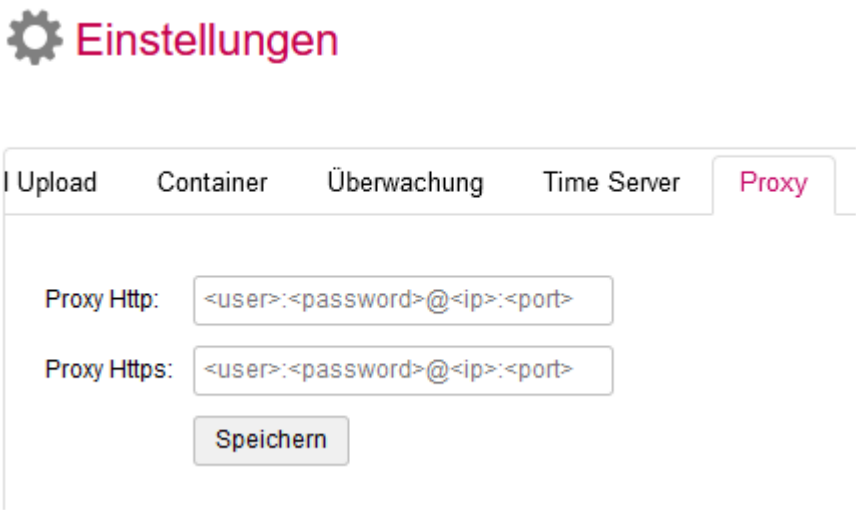
1.2.1.9.10. Time Server

Für mache Anwendungen ist eine genaue Uhrzeit erforderlich.
Dazu gehört z.B. “Remote” mit 2-Faktor-Auth. über den Google Authenticator.

Deshalb kann hier ein eigener Time Server angegeben werden.

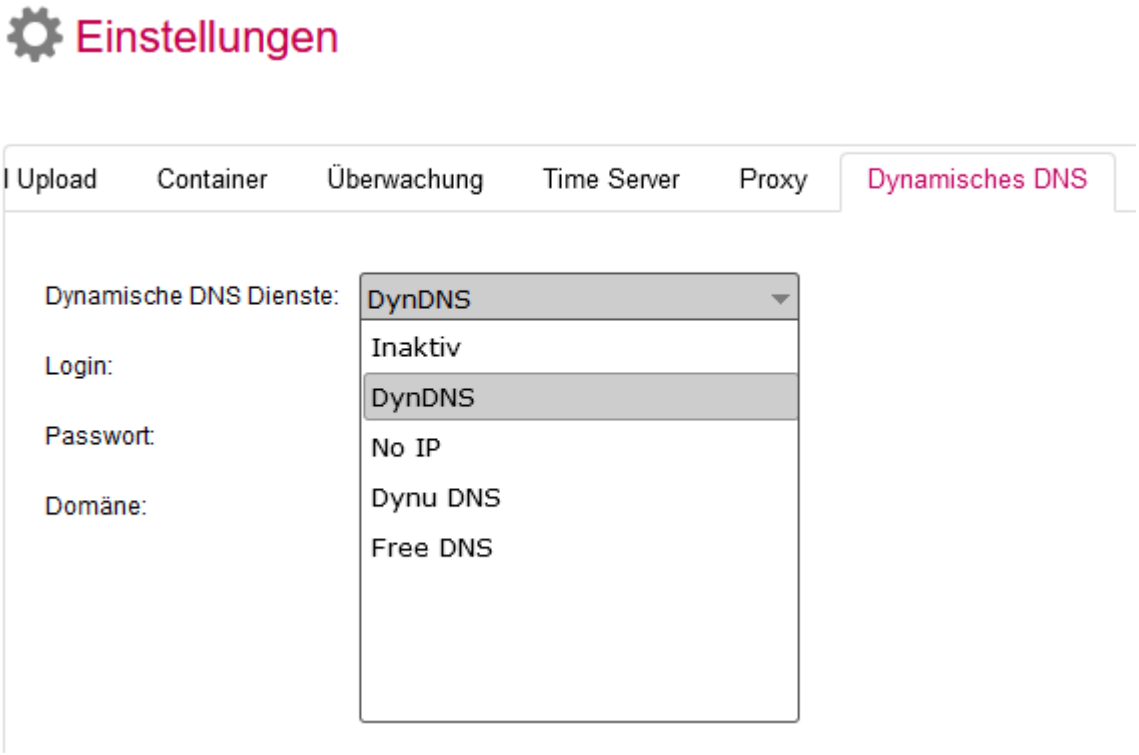
1.2.1.9.11. Proxy

Für spezielle Anforderungen kann ein Proxy-Server angegeben werden.



1.2.1.9.12. Dynamisches DNS

Für die pinBox kann hier dynamisches DNS über verschiedene Provider eingerichtet werden.



1.2.1.9.13. Backup

Siehe Backup

1.2.1.9.14. Software Update

Hier können die neuesten Updates für “System” eingespielt werden.

Achtung:
Nach dem Update wird “System” UND “Applications” neu gestartet, da beide am selben internen Dienst hängen.

1.2.1.9.15. Info

Siehe Info

1.2.1.10. Ereignisse

Siehe Ereignisse

1.2.2. Workplace “Cockpit”

1.2.2.1. Aufruf

Das “Cockpit” hat 2 Zugänge, einen für den Administrator und einen für den Benutzer.

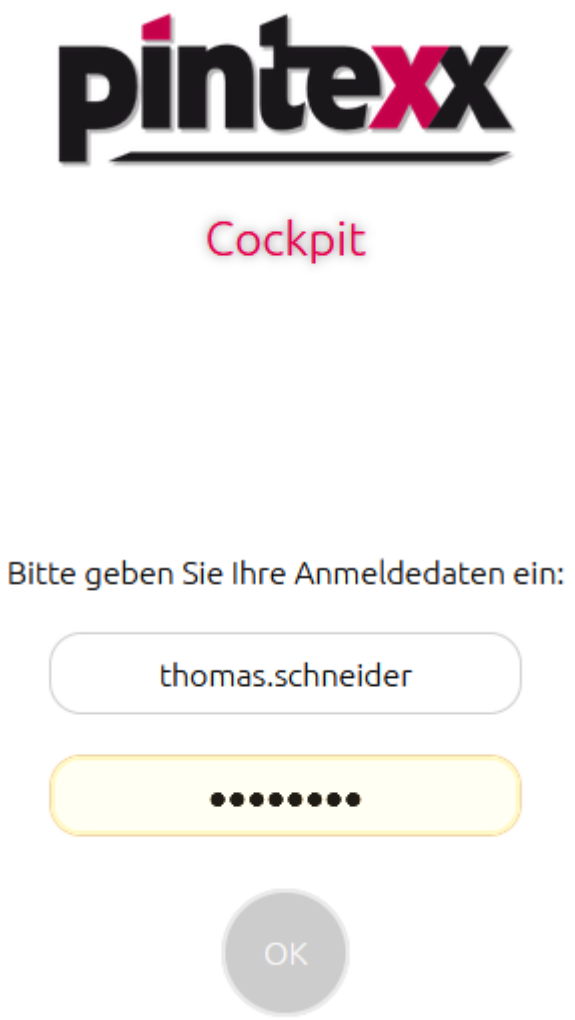
Benutzer:
<IP/Domäne>/cockpit

Administrator:
<IP/Domäne>/cockpit/adminlogin

1.2.2.2. Benutzer-Bereich

Der Benutzer-Bereich wird durch Aufruf der Benutzer-Login-Seite erreicht.

In Abhängigkeit der eingestellten Authentifizierung wird hier entweder ein Anmelde-Bildschirm für Login/ Passwort angezeigt

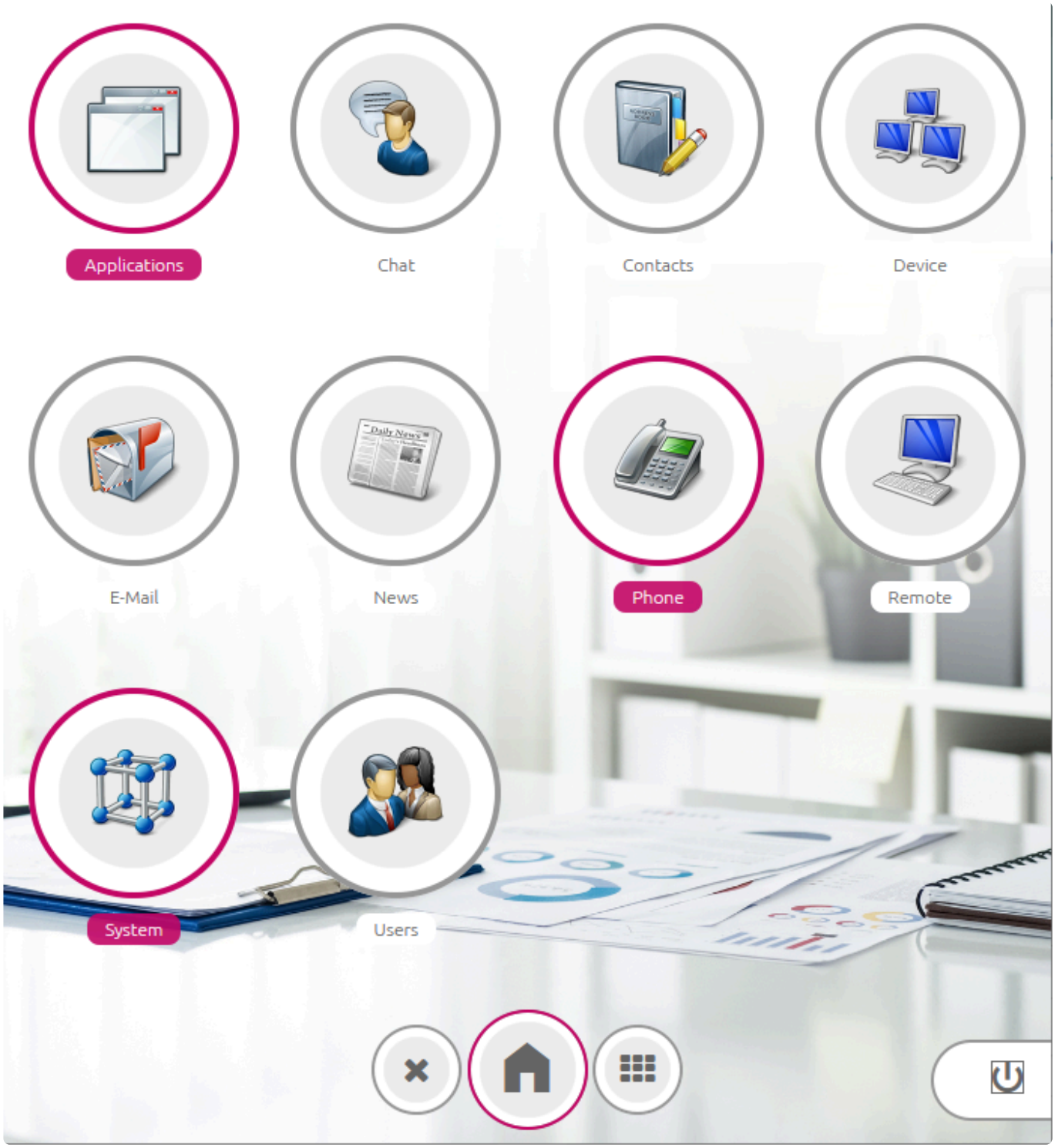


oder ein QR-Code im Falle der Authentifizierung über den elektr. Personalausweis.

Der Stil der Login-Seite einschließlich Logo können im Admin unter “Einstellungen” – “Stil” konfiguriert werden.

1.2.2.2.1. Web Desktop

Nach der Anmeldung gelangt der Benutzer auf den Web Desktop.



Alle vom Admin konfigurierten Anwendungen werden angezeigt und können durch Klick gestartet werden.
Ist eine Anwendung gestartet, wird dies durch eine Umrandung angezeigt.
Über den Home-Button gelangt man wieder in der Home-Bereich.
Über einen Klick auf eine gestartete Anwendung wird diese angezeigt.

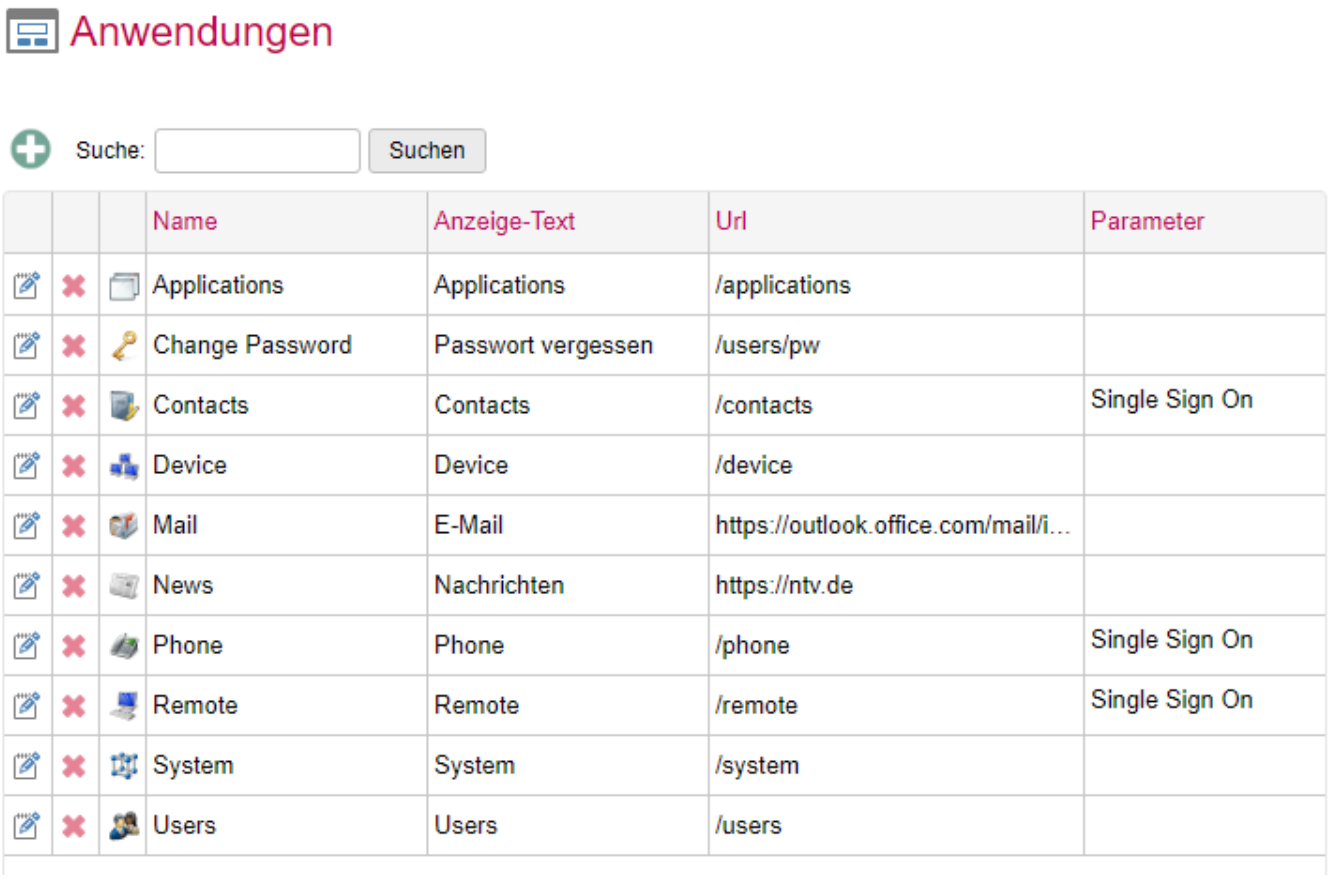
Gleichzeit erscheint in der Toolbar ein Beenden-Button, über den eine Anwendung beendet werden kann.
Über den rechten Auswahl-Button kann direkt auf eine geladene Anwendung zugegriffen werden.

Über den “Exit”-Button kann das Cockpit verlassen werden.

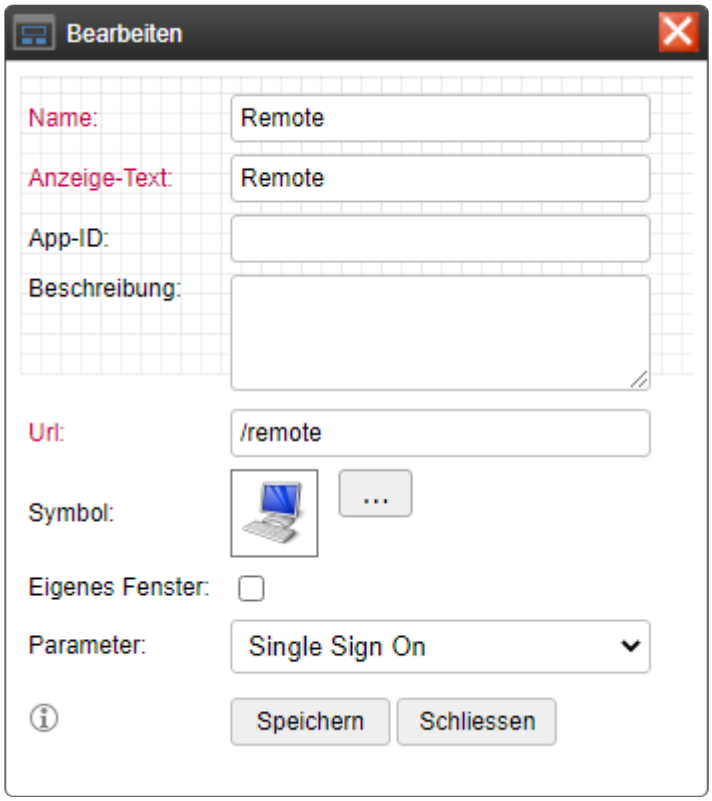
1.2.2.3. Admin-Bereich

1.2.2.3.1. Anwendungen

Hier können alle Anwendungen verwaltet werden, die auf dem Cockpit Desktop erscheinen sollen.



Über den Plus-Button kann eine neue Anwendung konfiguriert werden.



Folgende Einstellungen können konfiguriert werden:

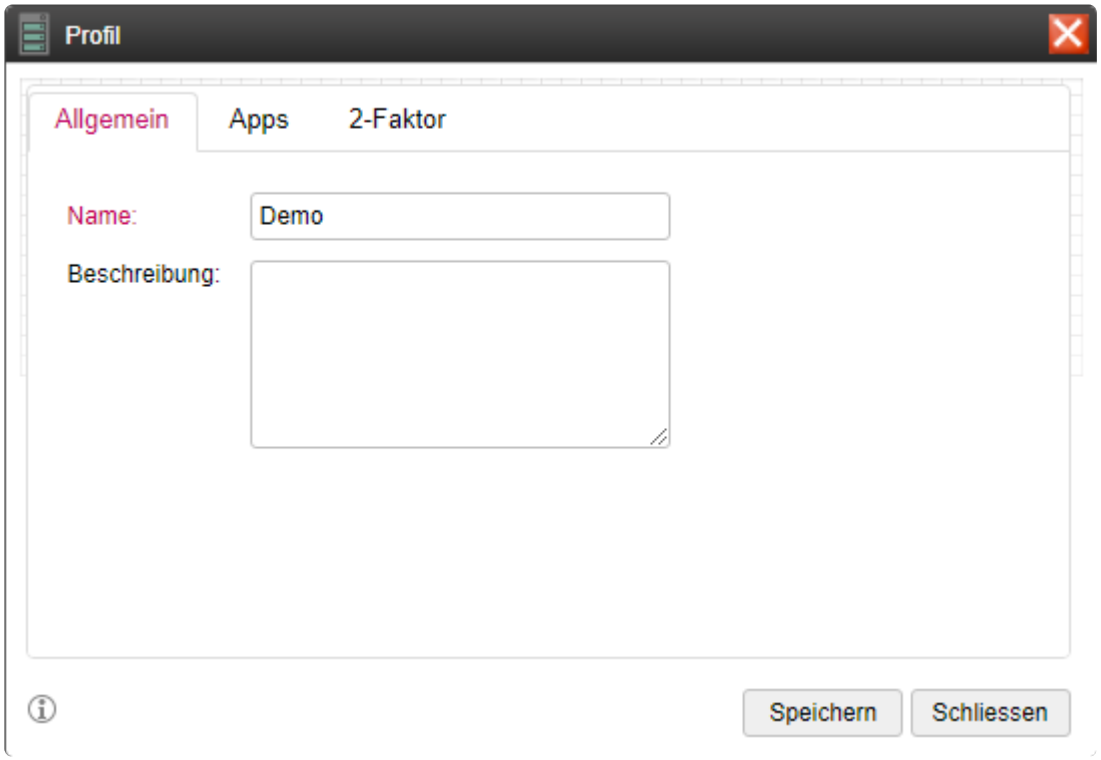
Einstellung	Beschreibung
Name	Der interne Name der Anwendung.
Anzeige-Text	Der Text, der unterhalb des Symbols im Desktop angezeigt wird.
App-ID	Für zukünftige Anwendungen.
Beschreibung	Beschreibungs-Text der Anwendung.
Url	Url der Anwendung. Es kann eine relative Url (eine installierte Anwendung) wie z.B. “/remote” angegeben werden, oder eine absolute Url.
Symbol	Aus einer Symbol-Liste kann das Anwendungs-Symbol ausgewählt werden.
Eigenes Fenster	Zeigt die Anwendung in einem eigenen Browser-Fenster an.
Parameter	Hier kann z.B. das Signle Sign On aktiviert werden.

1.2.2.3.2. Profile

Über ein Profil kann eine Anwendung einem Benutzer oder einer Gruppe zugeordnet werden.

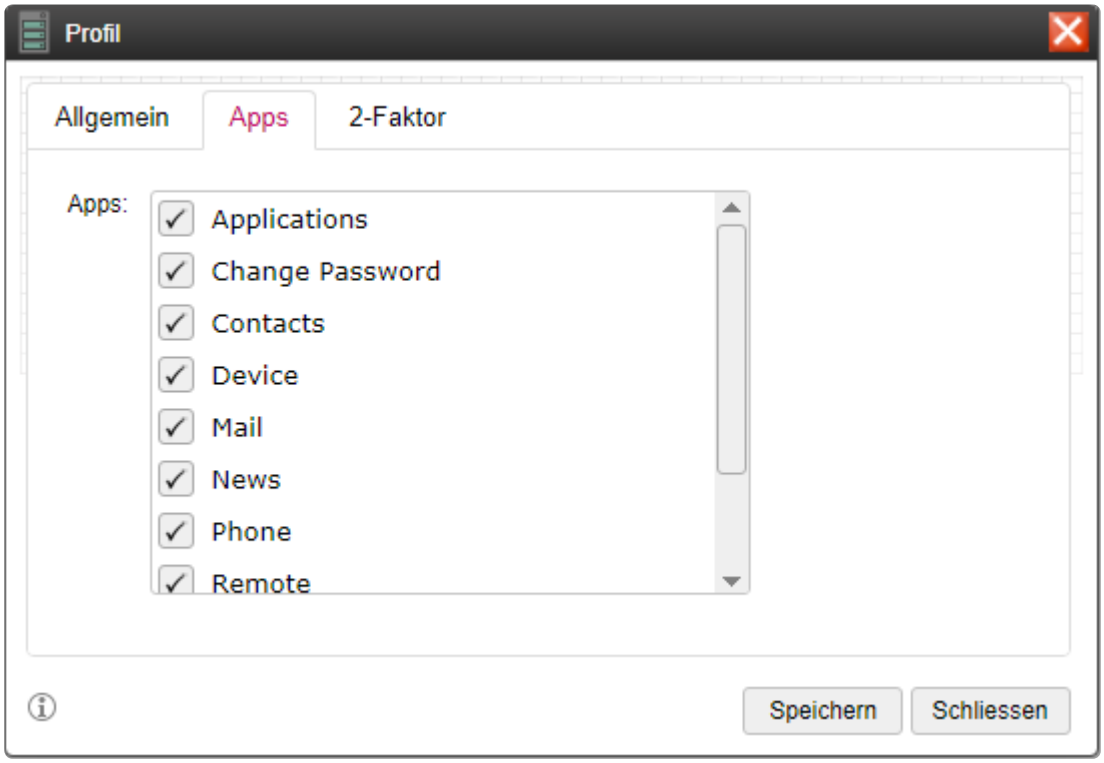
1.2.2.3.2.1. Allgemein

Hier kann eine interne Bezeichnung und eine Beschreibung des Profils angegeben werden.



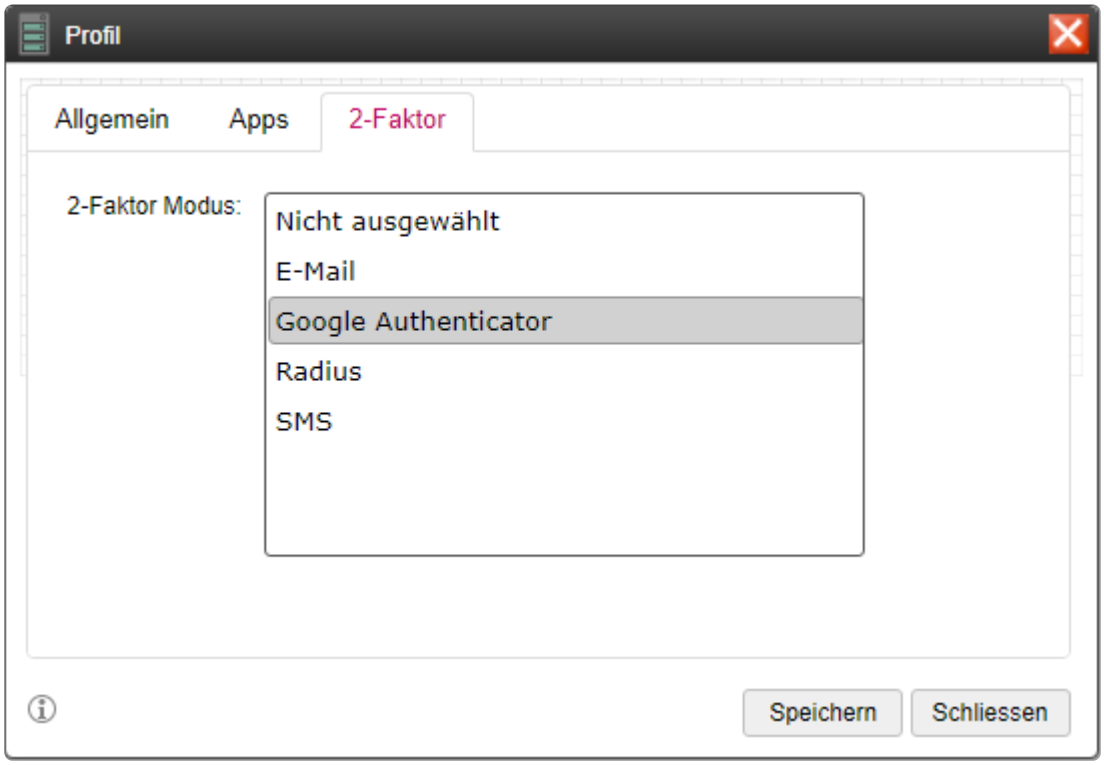
1.2.2.3.2.2. Anwendungen

Hier kann dem Profil eine Anwendung zugewiesen werden.



1.2.2.3.2.3. 2-Faktor

Hier kann für das Profil eine 2-Faktor-Authentifizierung ausgewählt werden.



E-Mail

Es muss für den Benutzer eine E-Mail konfiguriert sein. Des weiteren muss der Benachrichtigungs-Dienst (SMTP-Server) aktiviert sein.

Google Authenticator

Dazu wird die GA App auf einem Smartphone benötigt. Ein QR-Code zum Einrichten des Kontos in der App wird im Benutzer-Bereich angezeigt.

Radius

Dazu muss der Radius-Server konfiguriert werden.

SMS

Dazu muss ein SMS-Dienst konfiguriert werden und eine Telefon-Nummer zur Verfügung stehen.

1.2.2.3.3. Benutzer

Die Benutzer-Funktionen entsprechen exakt den “Remote”-Benutzer-Funktionen

1.2.2.3.4. Gruppen

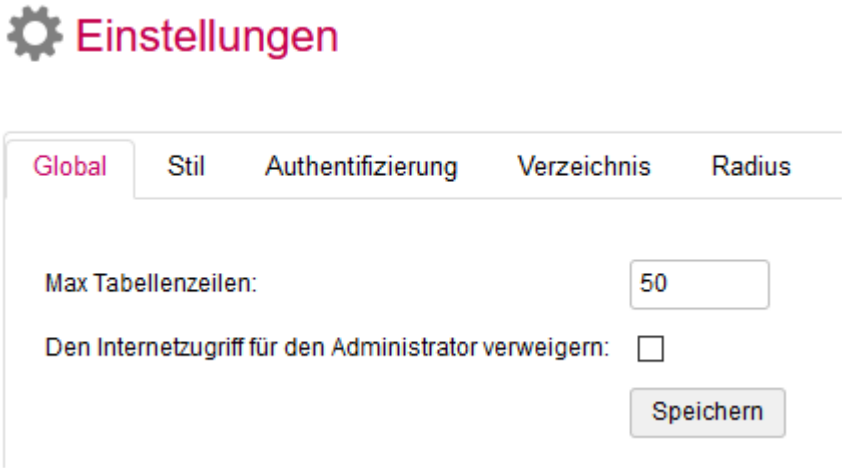
Die Gruppen-Funktion entspricht der “Remote”-Gruppen-Funktion

1.2.2.3.5. Administrator

Siehe Administrator

1.2.2.3.6. Einstellungen

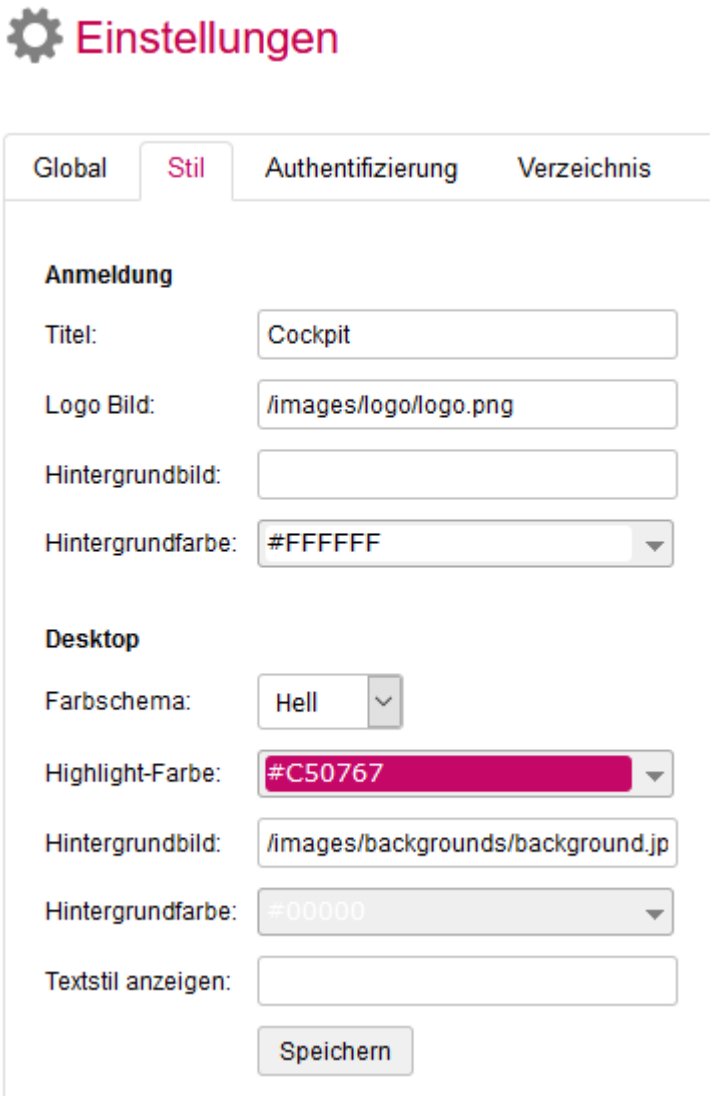
1.2.2.3.6.1. Global



Hier kann die Anzahl der Suchergebnisse sowie der Zugriff auf den Admin-Bereich konfiguriert werden.

1.2.2.3.6.2. Stil

Hier kann der Login-Bildschirm des Benutzers und der Desktop konfiguriert werden.



Login-Bildschirm

Die Überschrift wird unter dem Logo angezeigt.

Ein entsprechendes Logo kann hier über einen absoluten Pfad angegeben werden.
Das Logo kann in “System” unter “Einstellungen” -> “Bild Upload” auf das System geladen werden.
Nach dem Hochladen wird die exakte Url angezeigt. Diese kann hier verwendet werden.

Ein Hintergrundbild kann auf dieselbe Weise wie ein Logo gesetzt werden.

Die Hintergrund-Farbe kann aus einem Farbauswahl-Dialog gesetzt werden.

Desktop

Das Farbschema kann zwischen Hell und Dunkel eingestellt werden.
Die Highlight-Farbe kann über einen Farbauswahl-Dialog gesetzt werden.

Ein Hintergrund-Bild kann gesetzt werden (Upload s.o.)
Wird keine Hintergrundbild verwendet so kann eine Hintergrundfarbe gesetzt werden.
Der Textstil (Text unter Symbol im Desktop) kann über CSS-Stile gesetzt werden, z.B. font-size:10px

1.2.2.3.6.3. Authentifizierung

Der Authentifizierungs-Modus kann hier ausgewählt werden.

Benutzer

Die Authentifizierung wird über ein lokales Benutzer-Konto durchgeführt.

Verzeichnis

Die Authentifizierung wird über einen Verzeichnis-Dienst durchgeführt. Dieser muss unter “Einstellungen” – “Verzeichnisdienst” konfiguriert werden.

Radius

Die Authentifizierung wird über einen Radius-Server durchgeführt. Dieser muss unter “Einstellungen” – “Radius” konfiguriert werden.

Elektronischer Personalausweis

Soll über den elektronischen Personalausweis authentifiziert werden so werden hier unterschiedliche Anbieter unterstützt.
Ist eine Ausweisapp2 oder Open eCard App installiert, dann wird diese automatisch erkannt.
Das System fordert dann zur Eingabe der Pin bzw. zum Auflegen des Ausweises auf ein Lesegerät auf.

Wird keine lokale Anwendung gefunden wird ein QR-Code angezeigt.
Dieser muss mit einer speziellen App gescannt werden.
Der Authentifizierungsvorgang findet dann über die App statt.

1.2.2.3.6.4. Verzeichnis

Die Verzeichnis-Funktion entspricht exakt der “Remote”-Verzeichnis-Funktion

1.2.2.3.6.5. Radius

Die Radius-Funktion entspricht exakt der “Remote”-Radius-Funktion

1.2.2.3.6.6. Google Authenticator

Die Google Authenticator-Funktion entspricht exakt der “Remote”-Google Authenticator-Funktion

1.2.2.3.6.7. SMS

Die SMS-Funktion entspricht exakt der “Remote”-SMS-Funktion

1.2.2.3.6.8. Benachrichtigung

Siehe Benachrichtigung

1.2.2.3.6.9. Backup

Siehe Backup

1.2.2.3.6.10. Info

Siehe Info

1.2.2.3.7. Ereignisse

Siehe Ereignisse

1.2.3. Workplace “Remote”

“Remote” ermöglicht den Zugriff auf Windows-Desktops über das RDP-Protokoll.

“Remote” besteht aus einem “Portal” und einem “Gateway”.
Das “Portal” stellt zum einen einen Zugang für den Benutzer zum öffnen seiner Rechner-Verbindungen, zum anderen den Admin-Zugang für die Konfiguration zur Verfügung.

Das “Gateway” übernimmt die Umsetzung des RDP nach HTML5.

1.2.3.1. Aufruf

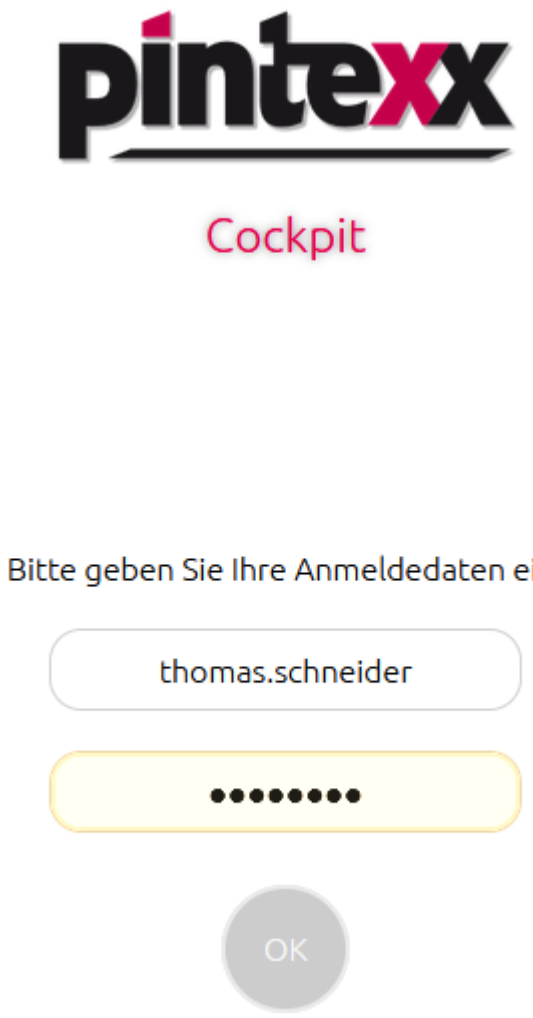
“Remote” hat 2 Zugänge, einen für den Administrator und einen für den Benutzer.

Benutzer:
<IP/Domäne>/remote

Administrator:
<IP/Domäne>/remote/adminlogin

1.2.3.2. Benutzer-Bereich

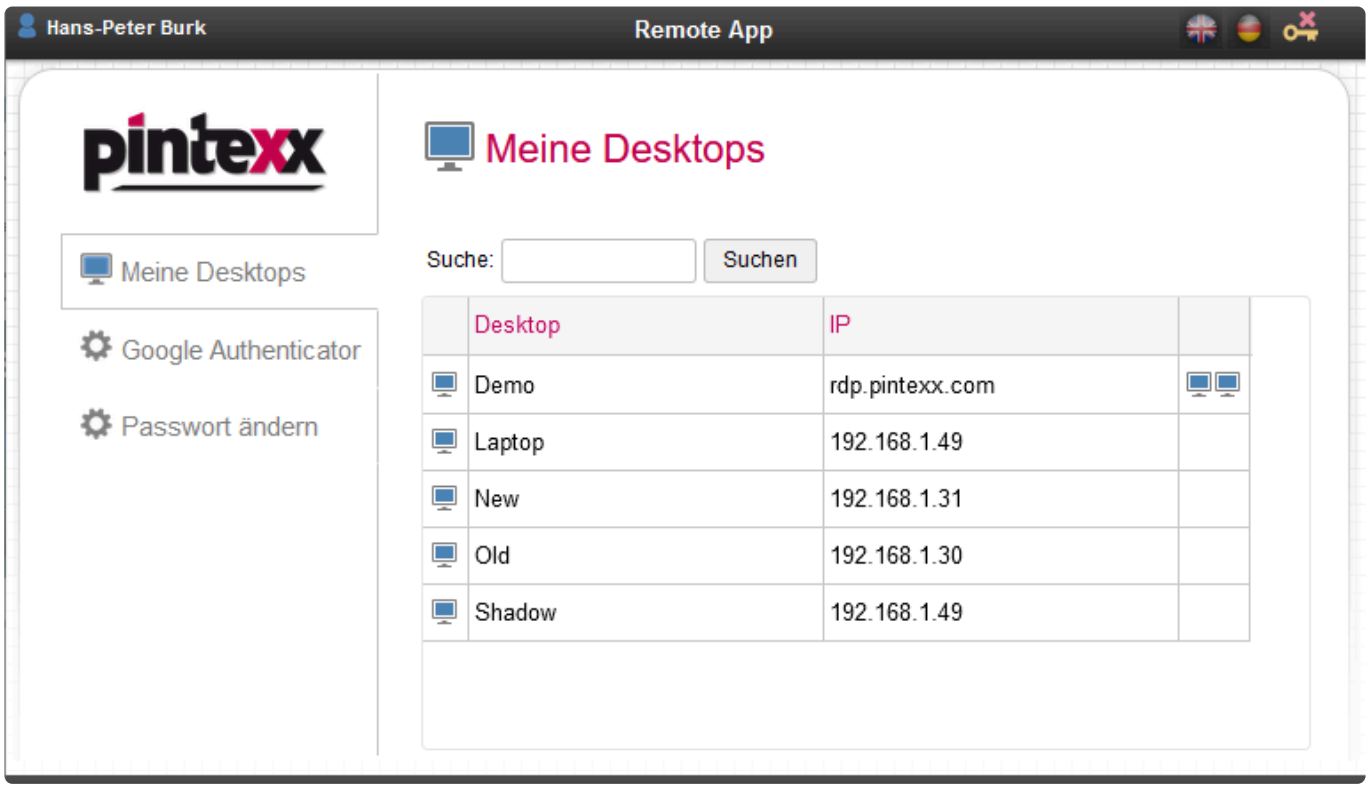
Der Benutzer-Bereich wird durch Aufruf der Benutzer-Login-Seite erreicht.



Der Stil der Login-Seite einschließlich Logo können im Admin unter “Einstellungen” – “Stil” konfiguriert werden.

1.2.3.2.1. Verbindungen

Nach erfolgreichem Login werden alle Verfügbaren Verbindungen in einer Liste angezeigt.



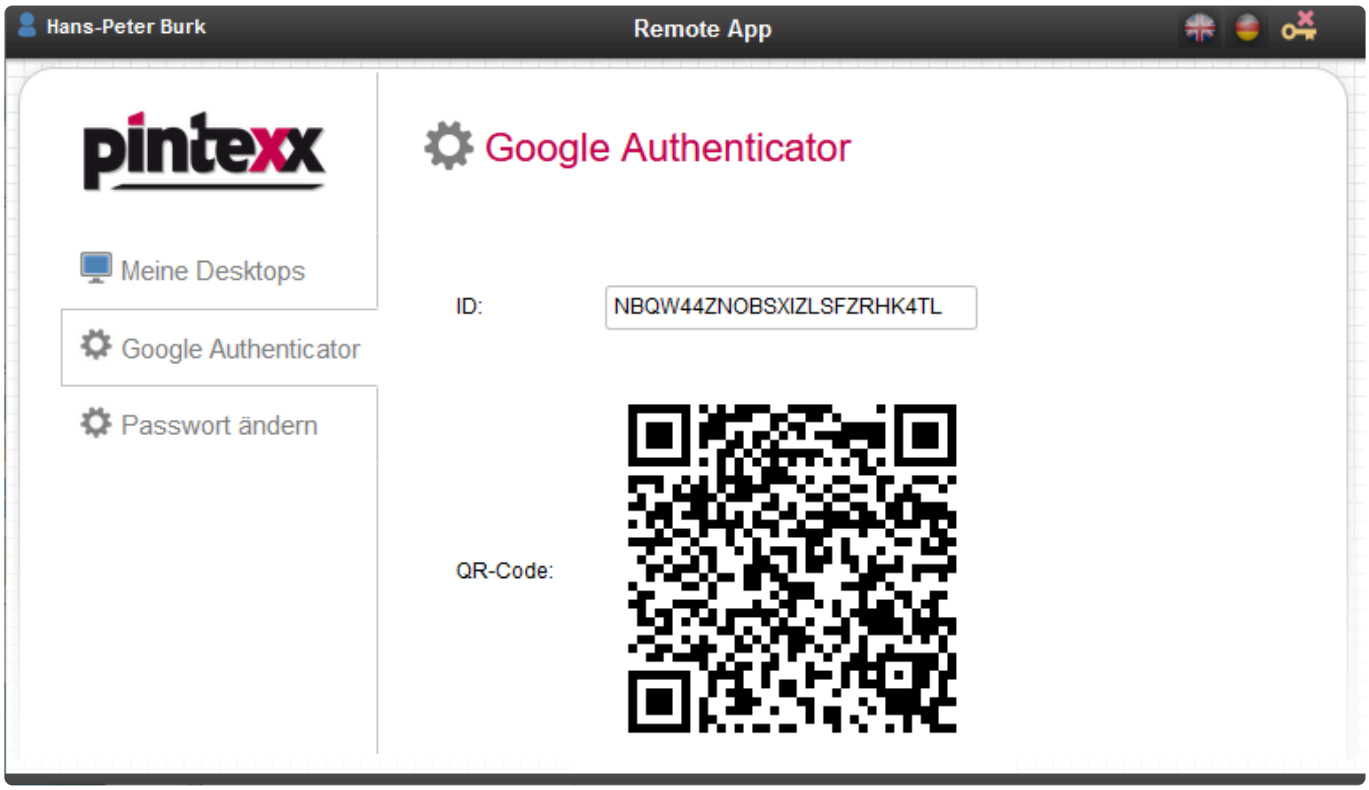
Durch Klick auf das Verbindungssymbol oder durch Doppel-Klick in eine Zeile wird die Verbindung aufgebaut.

Wurde ein Profil mit der Eigenschaft “Dual-Monitor” konfiguriert, dann erschein in der 3. Spalte ein Symbol mit 2 Monitoren.
Um den zweiten Monitor zu verwenden, muss zuerst diesen Symbol geklickt werden.
Daraufhin wird ein neues Browser-Fenster geöffnet. Dieses muss nun auf den 2. Bildschirm verschoben werden.
Danach muss dieser Bildschirm über F11 oder das Browser-Menü auf Vollbild umgeschaltet werden.

Dann muss vor der Verbindungsaufnahme der Browser im ersten Bildschirm auf Vollbild umgeschaltet werden.
Jetzt kann die Verbindung aufgebaut werden und auf beiden Monitoren angezeigt werden.

1.2.3.2.2. Google Authenticator

Wurde ein Profil mit 2-Faktor-Authentifizierung über den Google Authenticator aktiviert, dann einmal das Menü “Google Authenticator” mit einem QR-Code angezeigt.



Mit dem QR-Code kann dann ein Konto in der GA App angelegt werden.
Beim nächsten Login des Benutzers wird das Menü nicht mehr angezeigt.

1.2.3.2.3. Passwort ändern

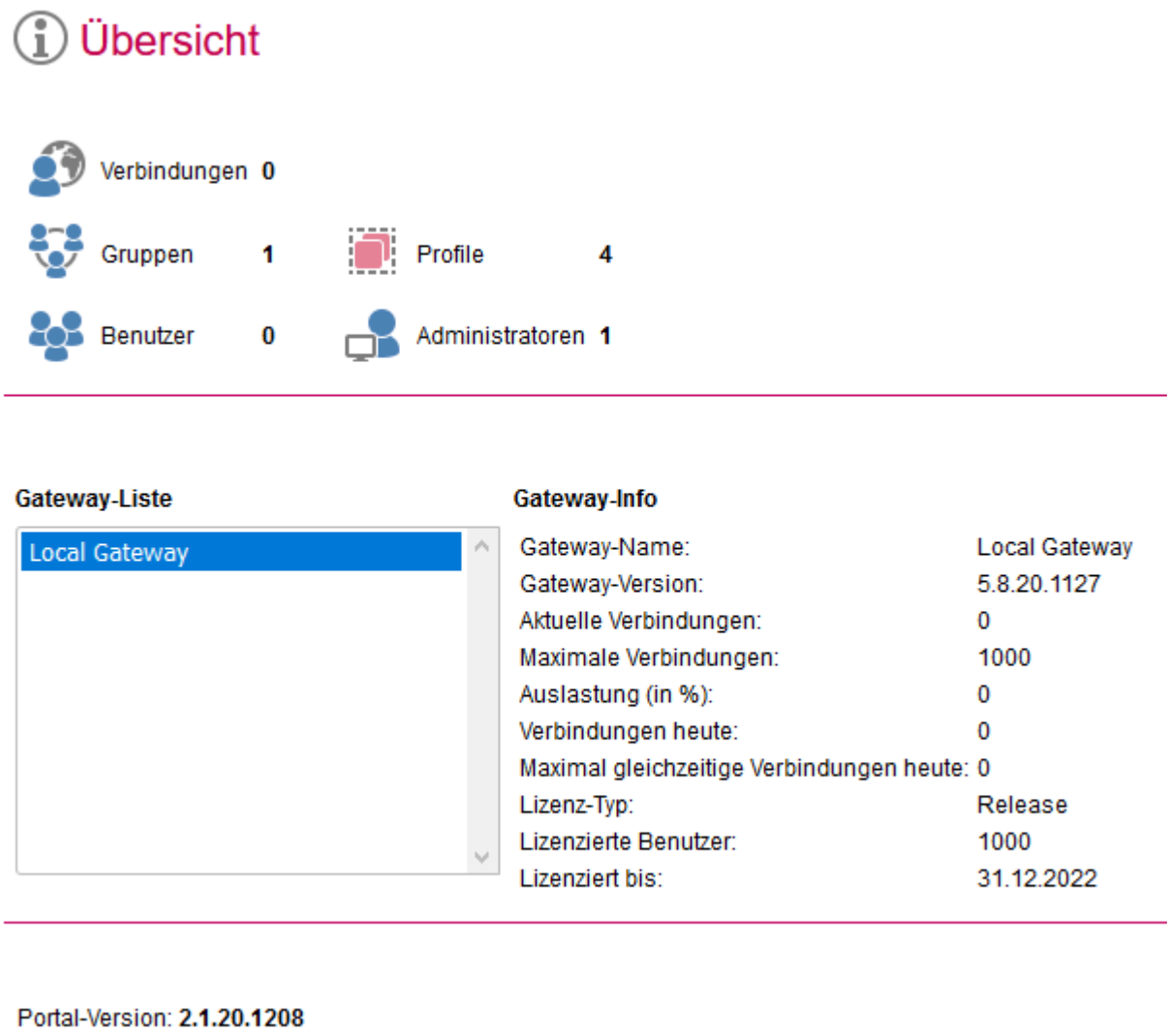
Wurde im Admin unter “Einstellungen” – “Global” die Option “Passort-Änderung zulassen” aktiviert, so erscheint ein weiteres Menü für die Passwort-Änderung.

Hier muss das aktuelle, und das neue Passwort mit Wiederholung eingegeben werden.
Die Passwort-Änderung funktioniert nur bei lokalen Benutzern, nicht bei Benutzern eines Verzeichnisses oder eines Radius-Servers.

1.2.3.3. Admin-Bereich

1.2.3.3.1. Übersicht

Die Übersichts-Seite zeigt eine Übersicht über den aktuellen Stand von “Remote”.

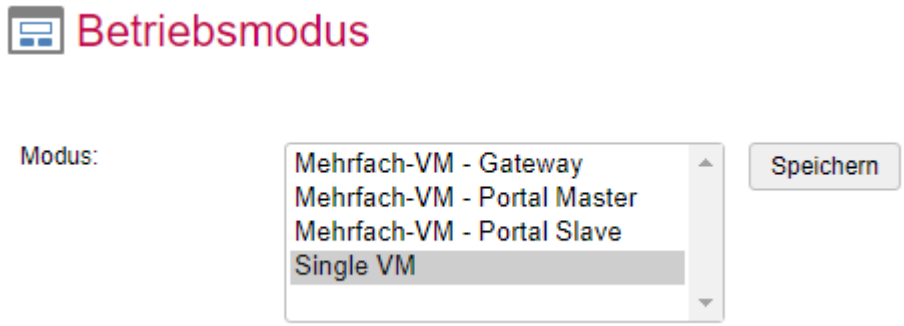


Die Anzeige ist abhängig vom Betriebs-Modus.
Es werden immer alle aktuellen Verbindungen für alle Gateways angezeigt.
Dazu die Anzahl der angelegten Gruppen, Profile, Benutzer und Admins.

Gibt es mehrere Gateways so werden diese in der Gateway-Liste aufgelistet.
Durch Klick auf ein Gateway werden aktuelle Informationen zum aktuellen Gateway angezeigt.

1.2.3.3.2. Betriebsmodus

“Remote” kann in verschiedenen Betriebsmodi betrieben werden.



Es kann sowohl eine einzelne VM (Standard), als auch ein Verbund aus mehreren VMs je nach Anforderungen an die Benutzerzahl verwendet werden.
Mehrere VMs erlauben Fail-Over und Load-Balance Funktionen.

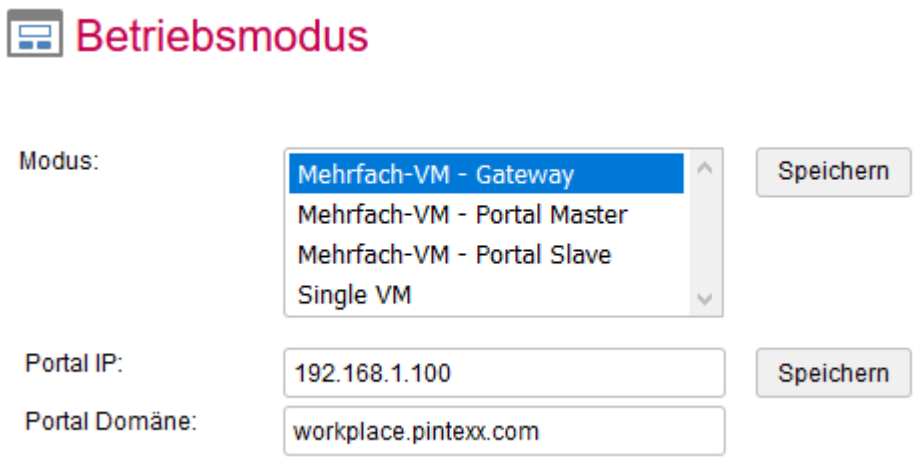
1.2.3.3.2.1. Single VM

Im Single-VM Modus ist das Portal und das Gateway innerhalb einer VM.

Dieser Modus empfiehlt sich bis zu einer Benutzeranzahl von ca. 500 gleichzeitigen Benutzern.

1.2.3.3.2.2. Mehrfach VM – Gateway

In diesem Modus wird das Portal von den Gateways getrennt um die Last auf mehrere Gateways zu verteilen.
Also z.B. 1 Portal VM und 2+ Gateway VMs.



Dieser Modus wird empfohlen ab einer Benutzerzahl > 500 gleichzeitigen Benutzern.

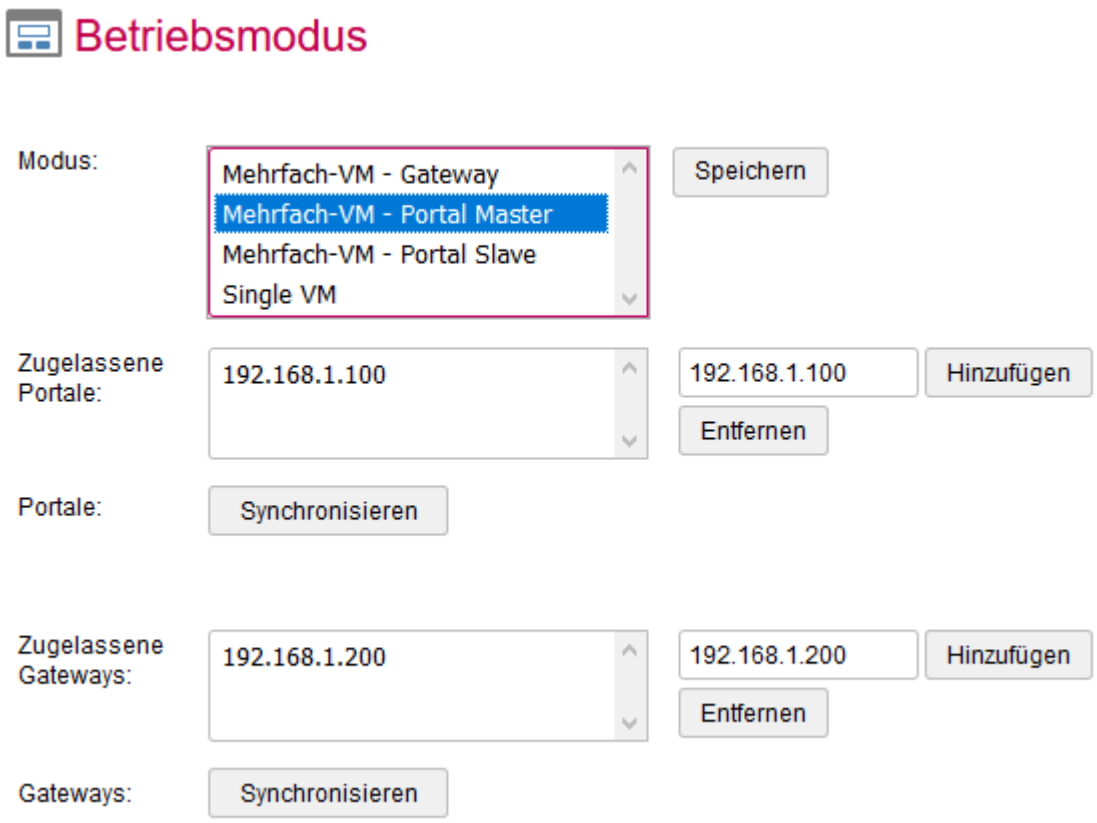
Als Parameter muss die interne IP Adresse der Portal-VM und die Portal-Domäne angegeben werden.

Die Kommunikation zwischen Portal und Gateway verläuft ausschließlich im internen Netzwerk.
Der Benutzer-Zugriff auf eines der Gateways im Falle einer Verbindung erfolgt direkt vom Browser zum Gateway.

Achtung:
Werden mehrere Gateways verwendet muss der Gateway-Name eindeutig sein.
Dieser kann durch Bearbeiten des Gateways eingestellt werden.

1.2.3.3.2.3. Mehrfach VM – Portal Master

Dieser Modus ist der High Availability Modus (HA).
Es kann sowohl mehrere Portal-VMs als auch mehrere Gateway-VMs geben.



Wird diese Konfiguration über einen vorgeschalteten Load Balancer betrieben, so werden die Benutzer auf eines der Portal-VMs geleitet.
Der Load Balancer muss dabei das “Session Stickiness” unterstützen.
D.h. wurde einmal ein Portal ausgewählt, muss dieses auch in nachfolgenden Zugriffen verwendet werden.
Es können sowohl Software- als auch Hardware-Balancer verwendet werden.
Der Load Balancer ist aktuell nicht Teil der Pintexx Workplace Lösung.

Das System unterstützt ebenfalls eine sog. Floating IP ohne Load Balancer.
Dabei wird den Portal-VMs eine Floating IP zugewiesen. Ist eine IP nicht erreichbar leitet das System automatisch auf die andere IP um.
In diesem Fall handelt es sich um ein Fail-Over System, da immer nur ein Portal Betrieben wird.

Es müssen folgende Parameter konfiguriert werden:

Portal-VMs

Die zugehörigen Slave-Portale müssen über ihre IP konfiguriert werden.

Über den “Synchronisieren”-Button wird die aktuelle Konfiguration an alle Portal-VMs übertragen.

Dieser Vorgang sollte nach jeder Änderungen an lokalen Benutzern, Gruppen und Profile oder Einstellungen durchgeführt werden.

Gateway-VMs

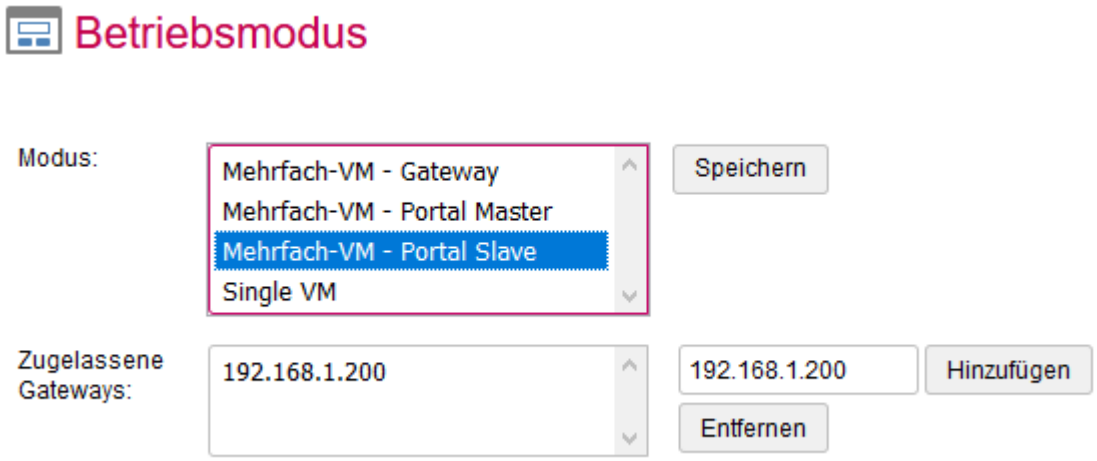
Die zugehörigen Gateway-VMs werden über ihre IP konfiguriert.

Über den “Synchronisieren”-Button wird die aktuelle Konfiguration an alle Gateway-VMs übertragen. Dieser Vorgang sollte nach jeder Änderungen an Profilen durchgeführt werden.

Achtung:
Wird eine Synchronisierung durchgeführt ist das System so konfiguriert, dass jedes Portal immer auf alle Gateways zugreifen kann.
Wird dies nicht gewünscht, so muss nach der Synchronisierung eine entsprechende Nach-Konfigurierung in den Portal erfolgen.

1.2.3.3.2.4. Mehrfach VM – Portal Slave

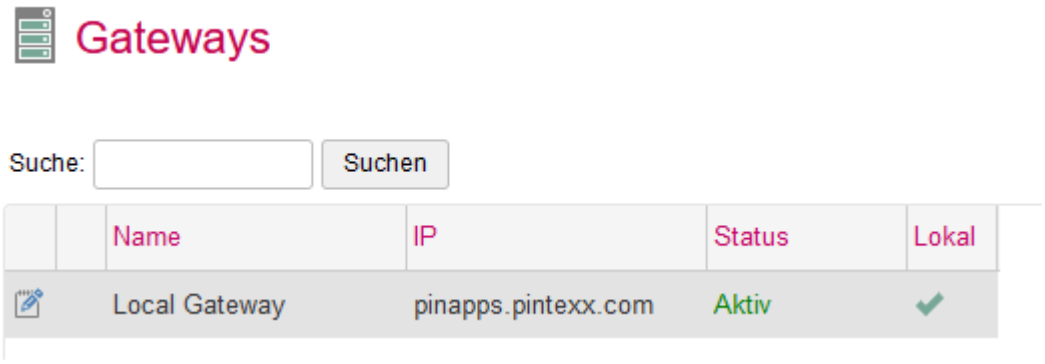
Dieser Modus wird für die Portal-VM eingestellt, die als Slave dienen soll.



Für diese VM können auch die zugehörigen Gateway über die IP individuell konfiguriert werden.

1.2.3.3.3. Gateways

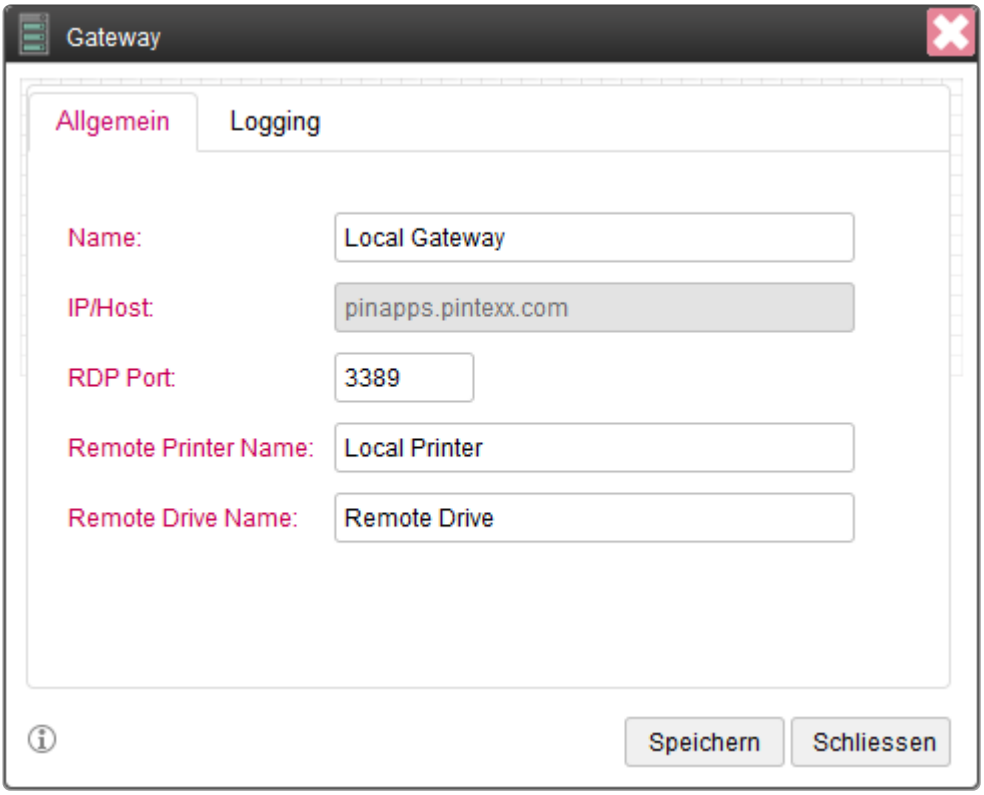
Hier werden alle verfügbaren Gateways in Abhängigkeit vom Betriebs-Modus angezeigt.



Am Falle einer Single-VM wird das in der VM integrierte Gateway angezeigt.
Im Fall einer Mehrfach-VM-Konfiguration werden die konfigurierten Gateways angezeigt.

Achtung:
Bei mehreren Gateways muss der Gateway-Name eindeutig sein!

Tab “Allgemein”



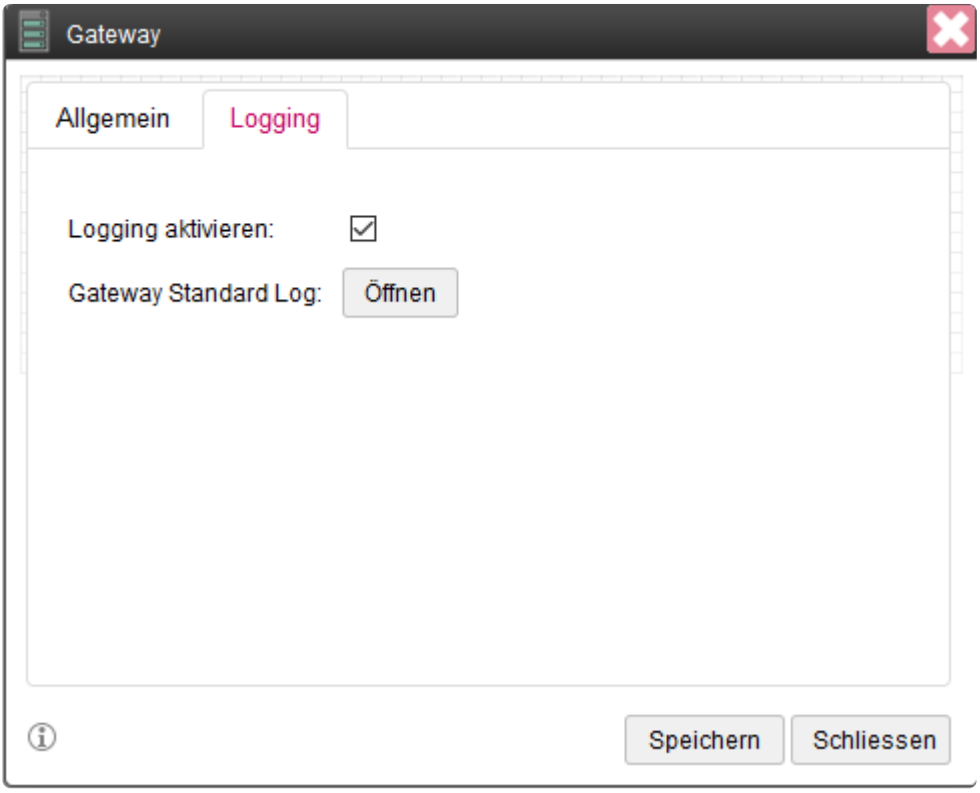
Hier kann der Gateway-Name gesetzt werden.
Der Standard-Port für den Zugriff auf RDP ist auf 3389 voreingestellt, kann aber hier verändert werden.

Achtung:
Wird der Port geändert gilt dies für alle Zugriff über dieses Gateway!

Der Port kann auch im Profil hinter der IP-Adresse gesetzt werden, also z.B. 192.168.1.200:3388

Der Name des Druckers, welcher im Druck-Dialog der Remote-Sitzung erscheint, kann hier gesetzt werden.
Der Name des Laufwerks, welches in der Remote-Sitzung erscheint, kann hier gesetzt werden.
Über dieses Laufwerk erfolgt der Up/Download von Dateien.

Tab “Logging”



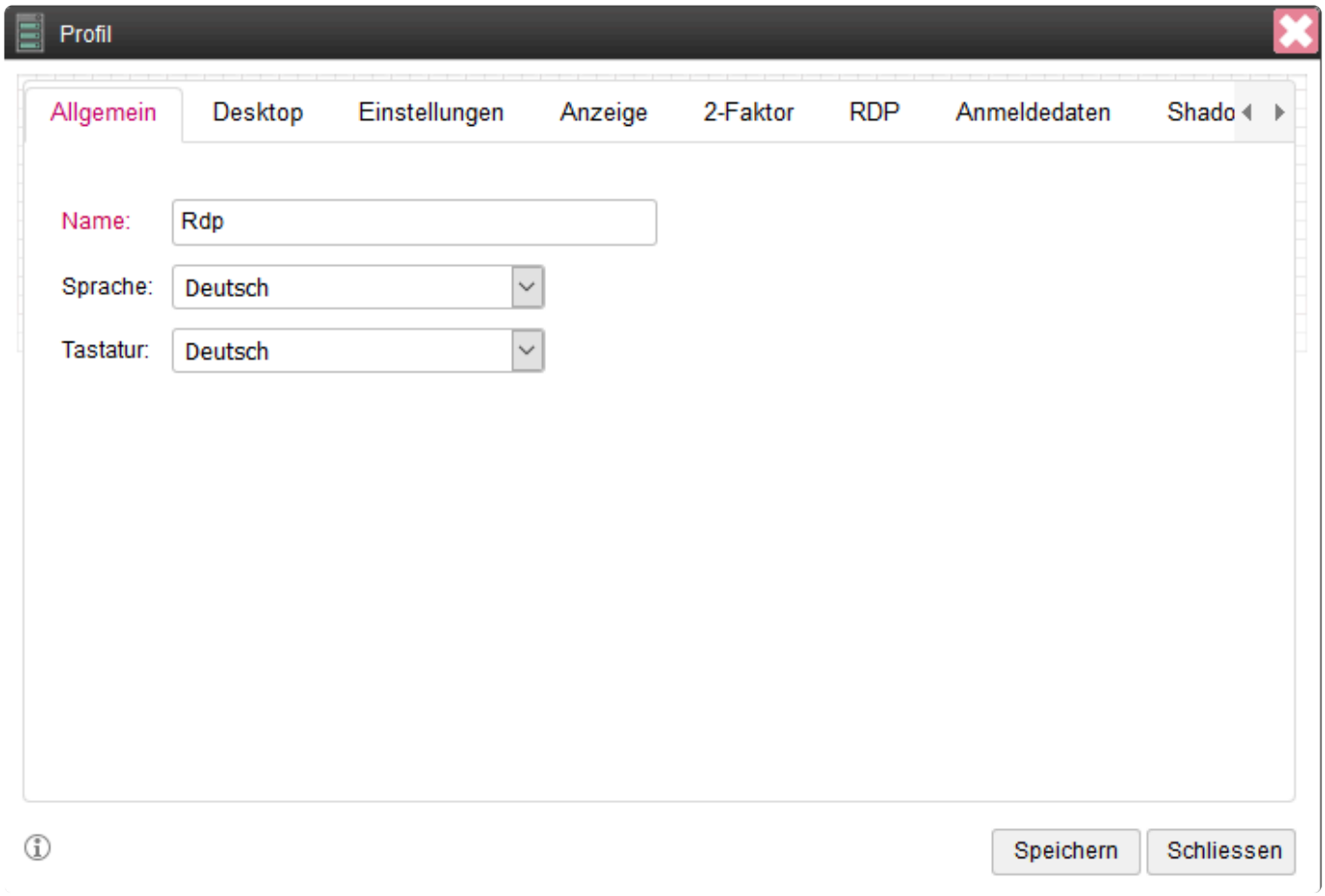
Hier kann das Logging aktiviert werden bzw. die Log-Datei des Gateways eingesehen werden.

1.2.3.3.4. Profile

Über ein Profil wird die Verbindung zu einem RDP-Ziel definiert und dessen Eigenschaften festgelegt.

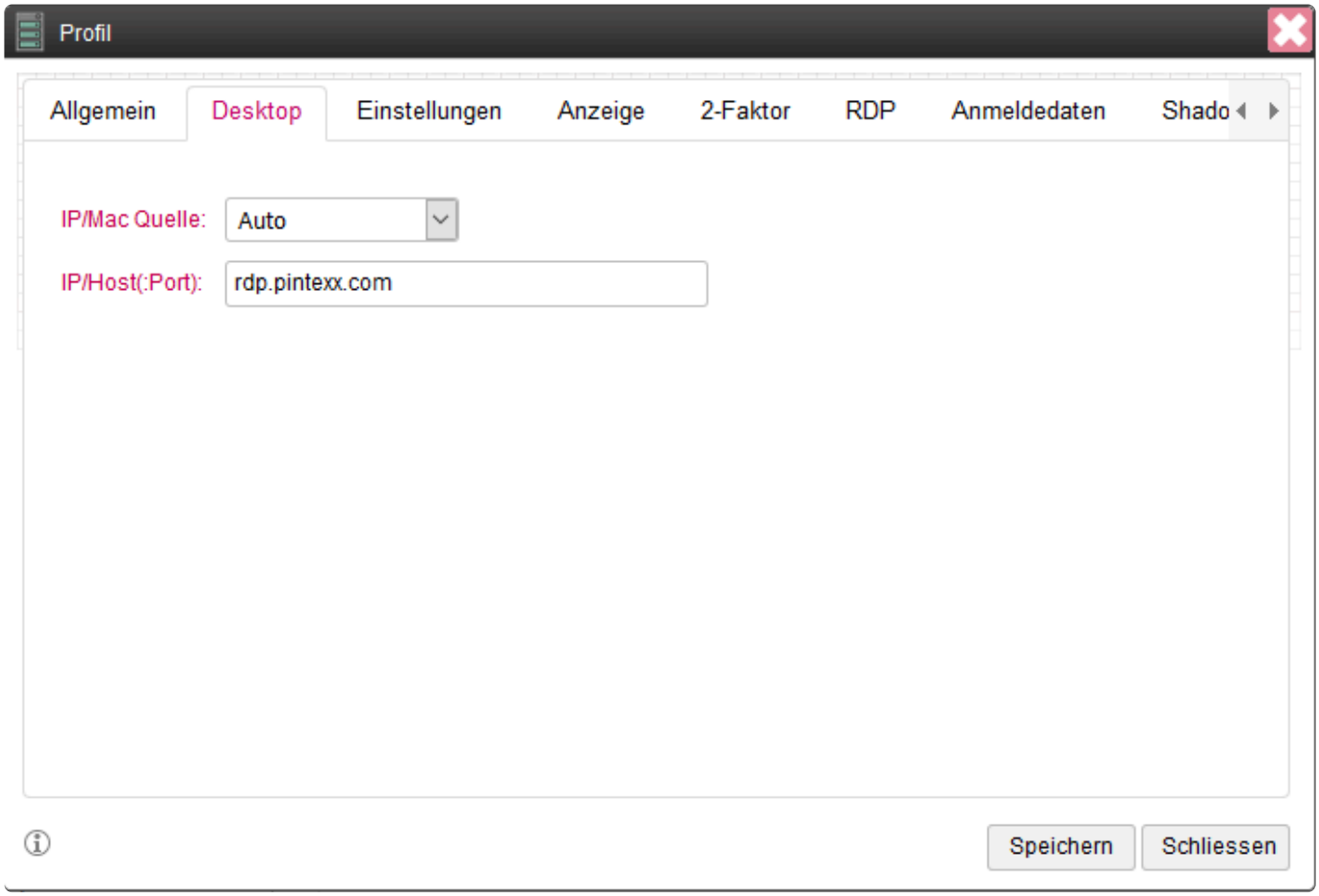
1.2.3.3.4.1. Allgemein

Auf dem Tab “Allgemein” wird der Name des Profils, die Sprache für Meldungen sowie das Tastatur-Layout eingestellt.



1.2.3.3.4.2. Desktop

Auf dem Tab “Desktop” wird bestimmt, woher die IP-Adresse für die Verbindung kommen soll.



Es gibt verschiedene Quellen für die IP/Mac-Adresse.

Auto

Es wird versucht, die IP/Mac-Quelle automatisch zu ermitteln. Diese Option ist nur aus Kompatibilitätsgründen vorhanden und sollte durch andere Optionen ersetzt werden.

Profil

Die IP-Adresse wird aus dem Feld IP/Host des Profils entnommen, die Mac-Adresse von Tab “Einstellungen” -> WakeOnLAN -> Mac.
Sollte der RDP-Port vom Standard abweichen, kann hier ein spezieller Port angehängt werden, z.B. 192.-168.1.200:3344

Verzeichnis

Die IP/Mac-Adresse wird aus dem Verzeichnis unter Menü “Einstellungen” -> “Verzeichnis” ausgelesen, wenn ein Feldname für IP oder Mac angegeben wird.
Allerdings nur dann, wenn auch die Authentifizierung über das Verzeichnis erfolgt.

Lokaler Benutzer

Die IP/Mac-Adresse wird von einem im Menü “Benutzer” angelegten Benutzer ermittelt, der dasselbe Login hat wie bei der Authentifizierung.

Shadow

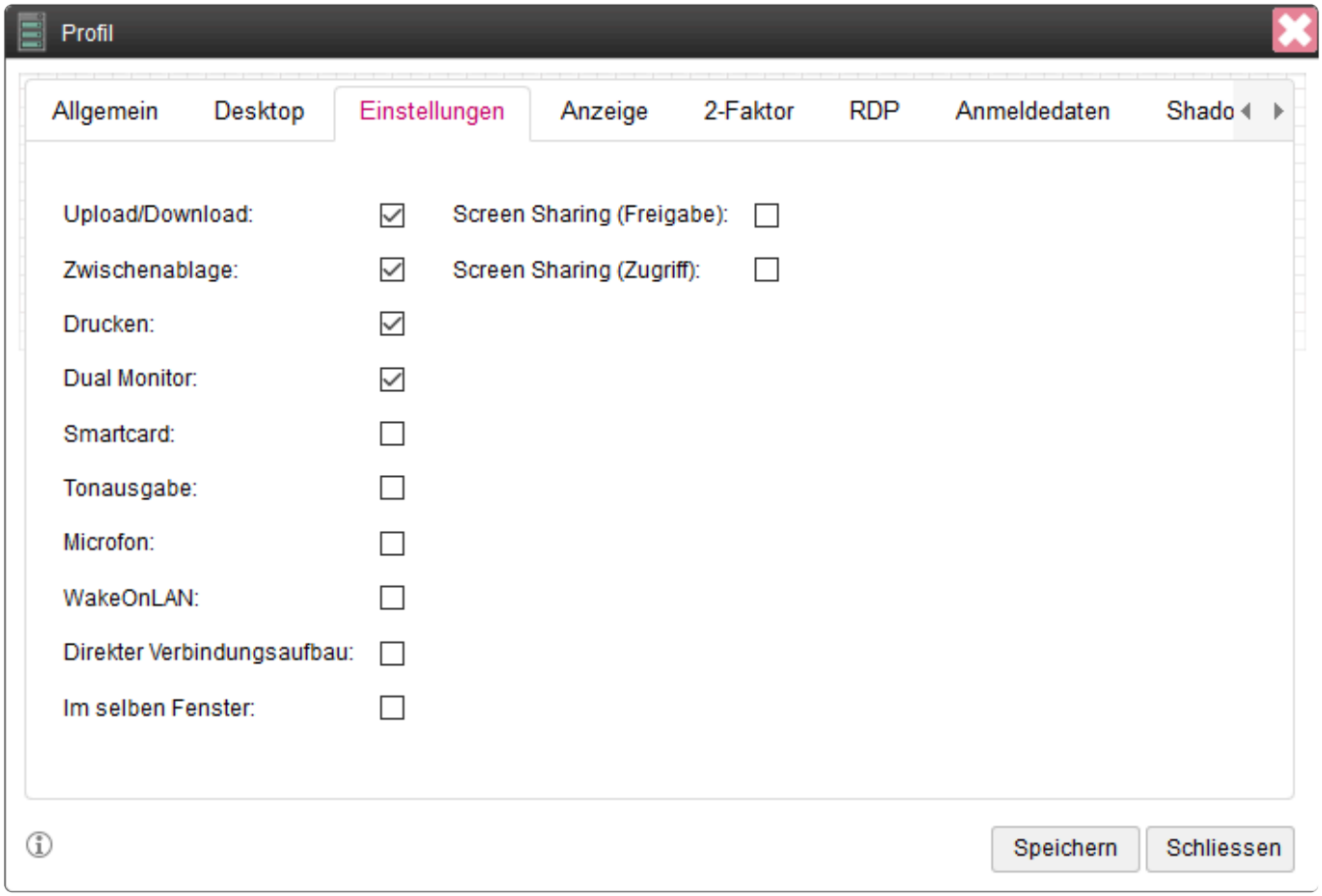
Mit dem Shadow-Profil kann sich ein Experte auf einen PC aufschalten, an dem ein anderer Benutzer arbeitet.
Dazu müssen im Tab “Shadow” entsprechende Angaben gemacht werden.

Pool

In dieser Einstellung wird ein PC-Pool erstellt, dessen IP/Mac im Tab “Pool” definiert werden.

1.2.3.3.4.3. Einstellungen

Spezielle Einstellungen für das Profil um erlaubt Aktionen zu definieren.

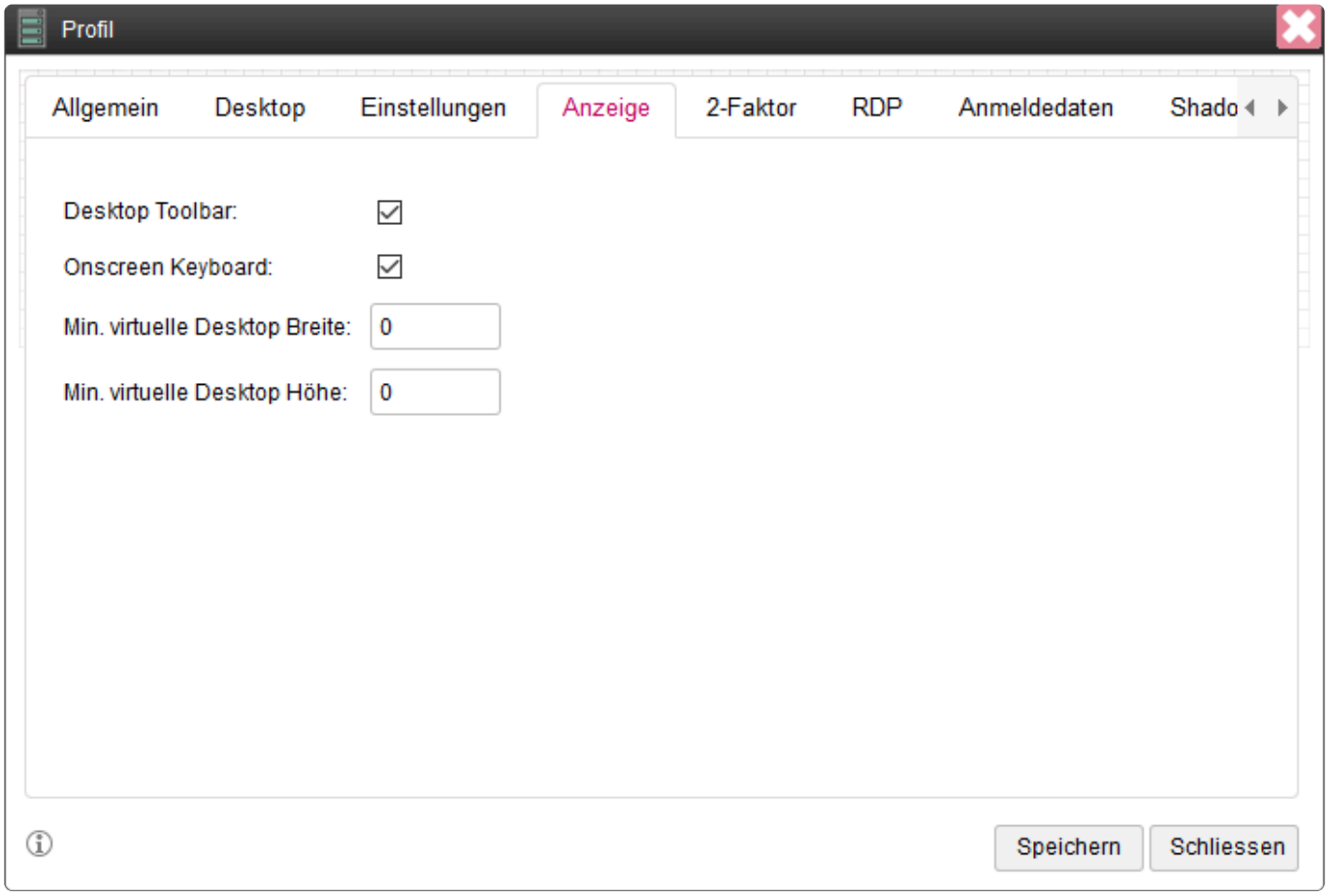


Feature	Beschreibung
Upload/Download	Nach der Anmeldung an der Remote-Sitzung erscheint ein Toolbar am oberen Rand, wenn die Maus dorthin bewegt wird. Dort können Dateien hoch- und heruntergeladen werden
Zwischenablage	Über die Zwischenablage können Texte in/von der Remote-Sitzung kopiert werden
Drucken	Das Drucken über die Remote Sitzung wird aktiviert
Dual Monitor	Es werden 2 Monitore unterstützt
Smartcard	Es wird eine Smartcard über die USB-Schnittstelle unterstützt (für Datev Benutzer)
Tonausgabe	Es wird die Ton-Weiterleitung aus der Remote-Sitzung unterstützt
Mikrofon	Es wird die Sprach-Weiterleitung in die Remote-Sitzung unterstützt
WakeOnLAN	Es wird das automatische Aufwecken eines PC's vor dem Zugriff unterstützt
Direkter Verbindungsaufbau	Wurde einem Benutzer nur eine Verbindung zugeordnet dann wird diese nach der Anmeldung direkt geöffnet
Im selben Fenster	Die Verbindung wird im selben Browser-Fenster geöffnet

Screen Sharing	Ein Experte kann sich auf eine bestehende Remote-Sitzung schalten und die Kontrolle übernehmen
Screen Sharing (Zugriff)	Die Experten-Freigabe für den Zugriff auf eine Sitzung

1.2.3.3.4.4. Anzeige

Diese Einstellungen betrifft die Remote-Sitzung.



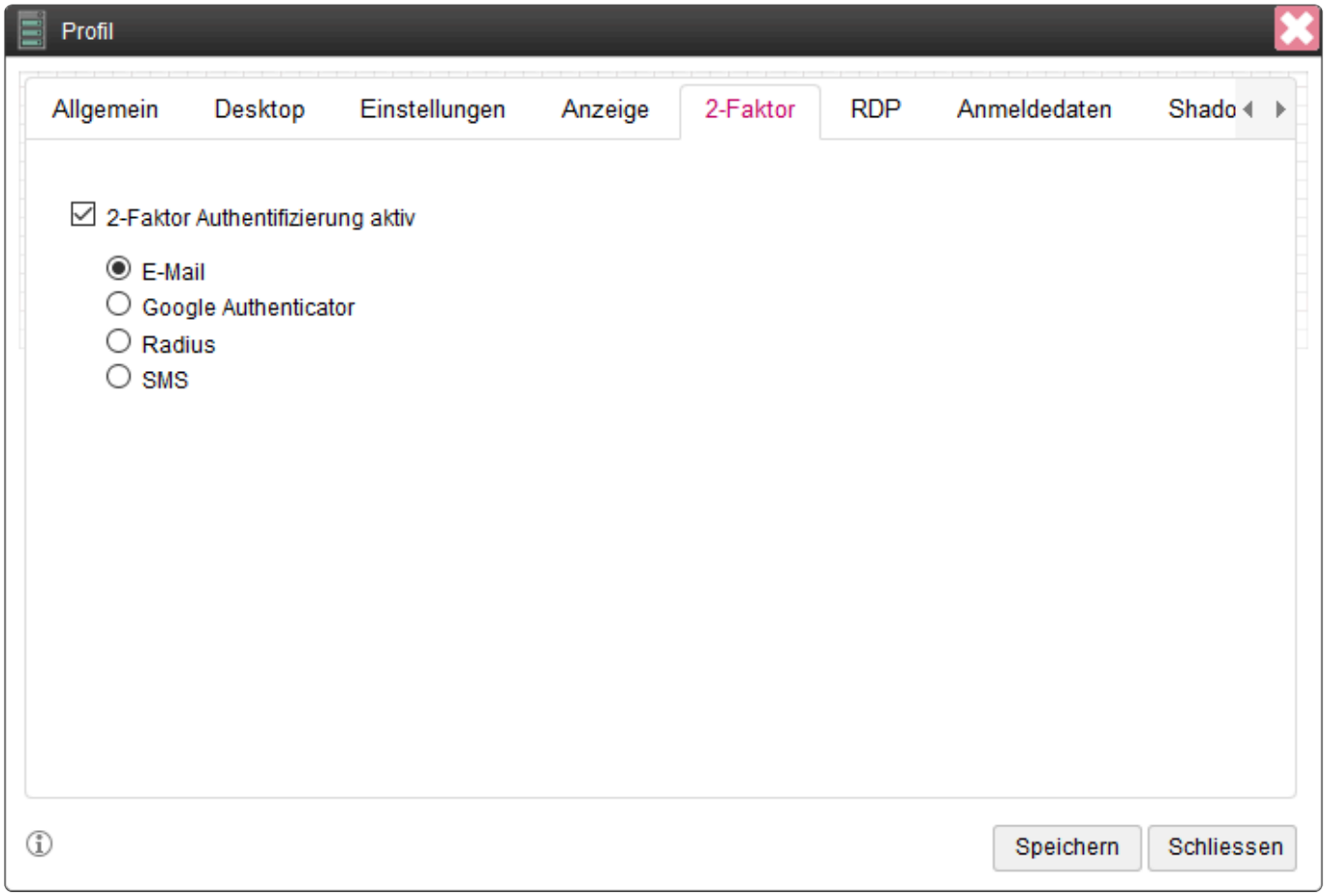
Es kann nach dem Verbindungs-Aufbau eine Toolbar angezeigt werden.
Diese ist notwendig für Up/Download und Screen-Sharing

Es kann nach dem Verbindungs-Aufbau ein OnScreen-Keyboard angezeigt werden.
Dies kann bei mobilen Geräten hilfreich sein.

Auf mobilen Geräten kann eine Bildschirmgröße angeben werden, die größer als der Bildschirm des mobilen Gerätes ist.

1.2.3.3.4.5. 2-Faktor

Hier wird eine 2-Fakot-Authentifizierung definiert.



Die 2-Faktor-Authentifizierung unterstützt folgende Modi:

E-Mail

Vor dem Verbindungsaufbau wird eine E-Mail an den Benutzer gesendet, welche einen OTP enthält (Einmal-Code).
Dieser muss vor dem Verbindungsaufbau eingegeben werden.
Dieses Feature erfordert die Konfiguration eines Mail-Servers im Menü “Einstellungen” -> “Benachrichtigung”.
Soll die E-Mail-Adresse aus einem Verzeichnis geholt werden, muss bei der Verzeichnis-Konfiguration unter “Einstellungen” -> “Verzeichnis” ein Feld für E-Mail angegeben werden.

Google Authenticator

Für den GA wird die GA App auf einem Smartphone benötigt. Diese kann über die entsprechenden Stores kostenlos installiert werden.
Die GA App muss einmal einen QR-Code für das Anlegen eines Kontos scannen.
Dieser Code wird dem Benutzer bei der Benutzer-Anmeldung einmalig angezeigt.
Die GA App generiert dann einen Code, der vor dem Verbindungs-Aufbau eingegeben werden muss.
Der QR-Code kann für alle Benutzer oder für einen speziellen Benutzer unter “Einstellungen” -> “Google

Authenticator” neu einmalig angezeigt werden.

Radius

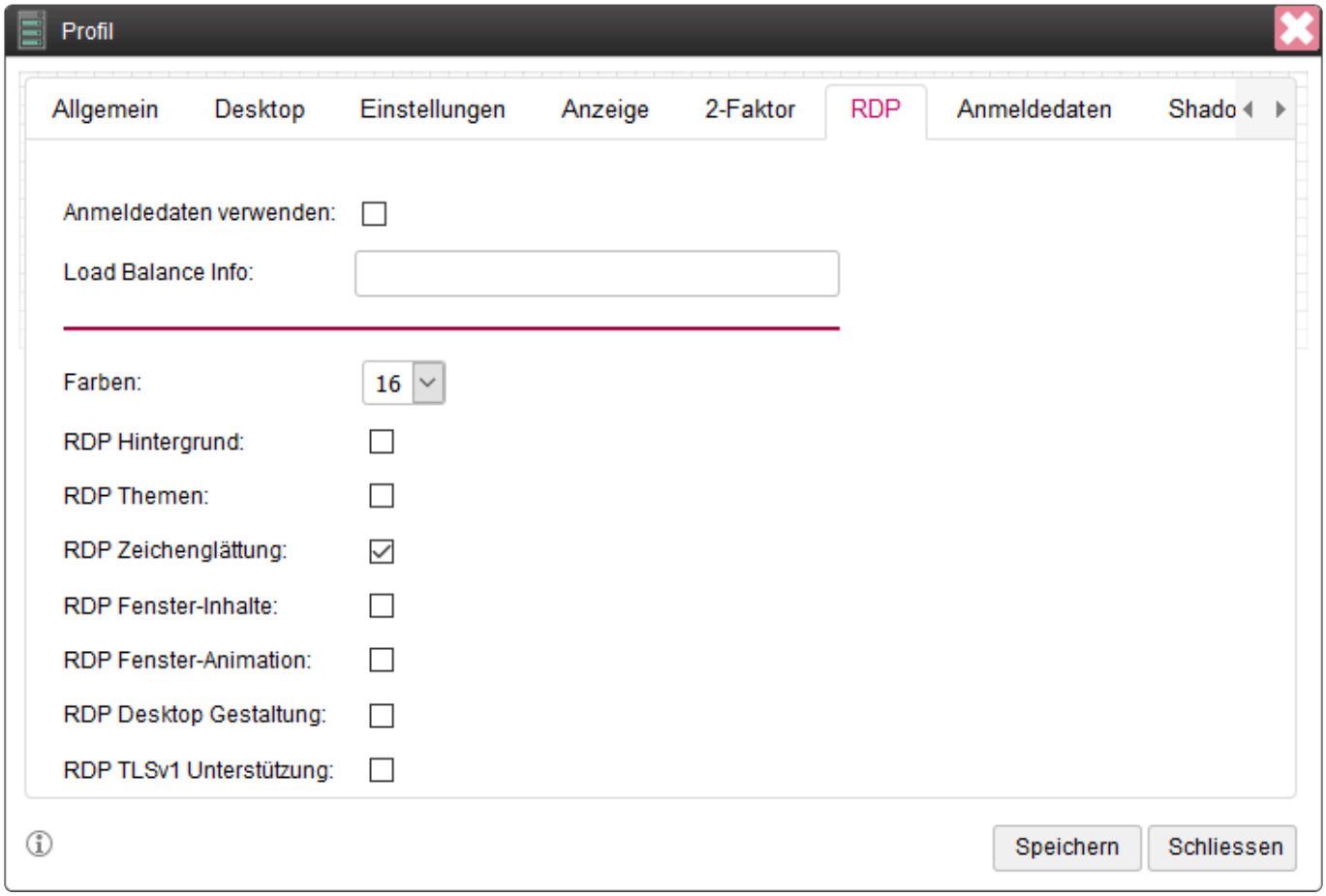
In diesem Fall wird über einen Radius-Server ein Code generiert. Dieser muss dann vor dem Verbindungs-Aufbau angegeben werden.

SMS

Der Benutzer erhält vor der Anmeldung eine SMS an eine angegebene Nummer mit einem Code.
Dieser muss vor dem Verbindungsaufbau eingegeben werden.
Um die SMS zu versenden muss unter “Einstellungen” -> “SMS” ein entsprechender Dienst konfiguriert werden.
Die Telefon-Nummer muss je nach Profil-Einstellung entweder über ein Verzeichnis oder über einen lokalen Benutzer ermittelbar sein.

1.2.3.3.4.6. RDP

Hier können u.a. die vom RDP-Protokoll definierten Einstellungen vorgenommen werden.



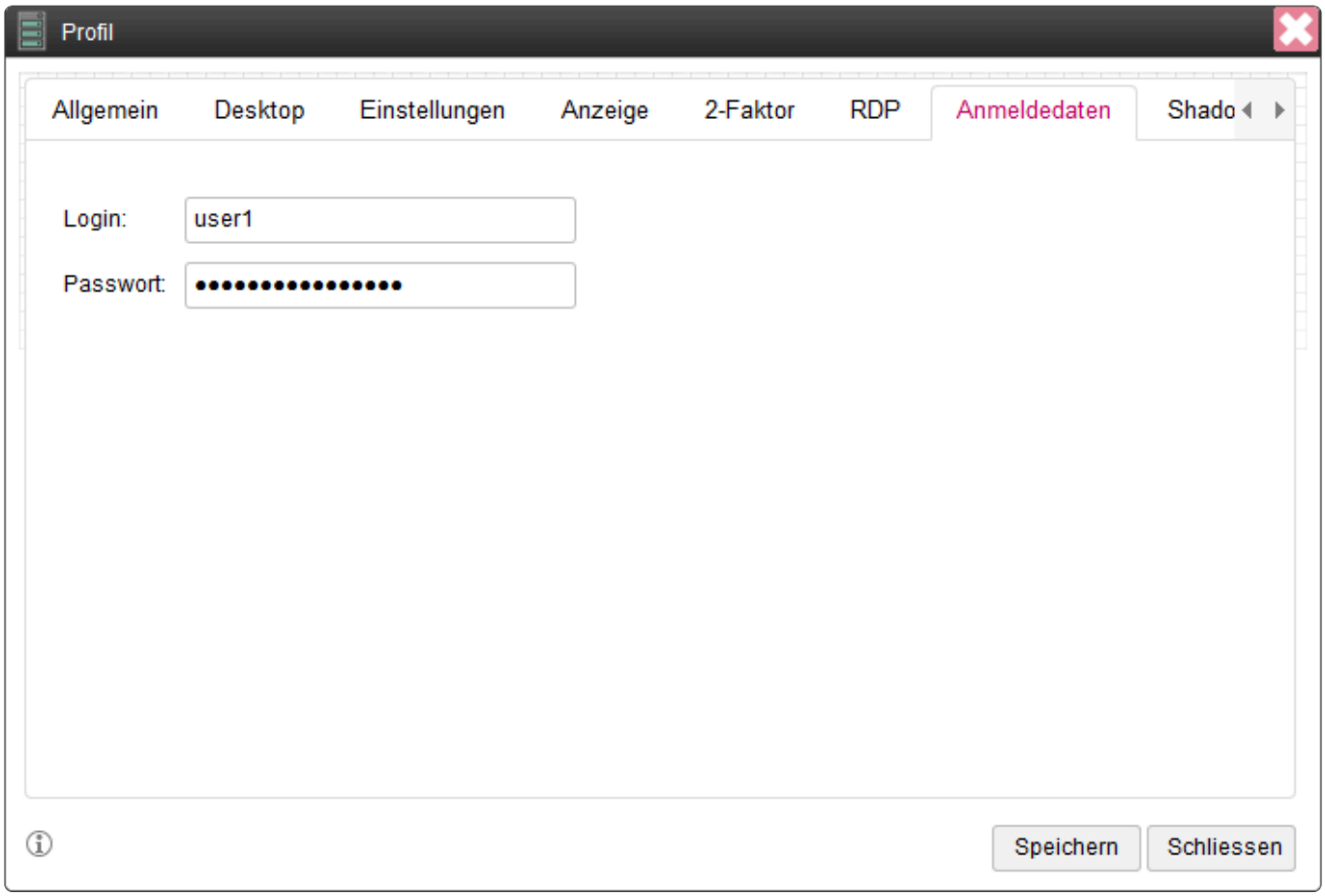
Bei “Anmeldedaten verwenden” werden die zur Anmeldung am Portal verwendeten Anmeldedaten auch für die Anmeldung an der Remote-Sitzung verwendet.

Die “Load Balance Info” ist erforderlich, wenn es sich bei dem Terminal-Server um eine Farm handelt. Die LBI besteht aus einer festgelegten Zeichenfolge + dem Collection-Namen:
“tsv://MS Terminal Services Plugin.1.” + ““

Alle weiteren Parameter entsprechen dem RDP-Protokoll.

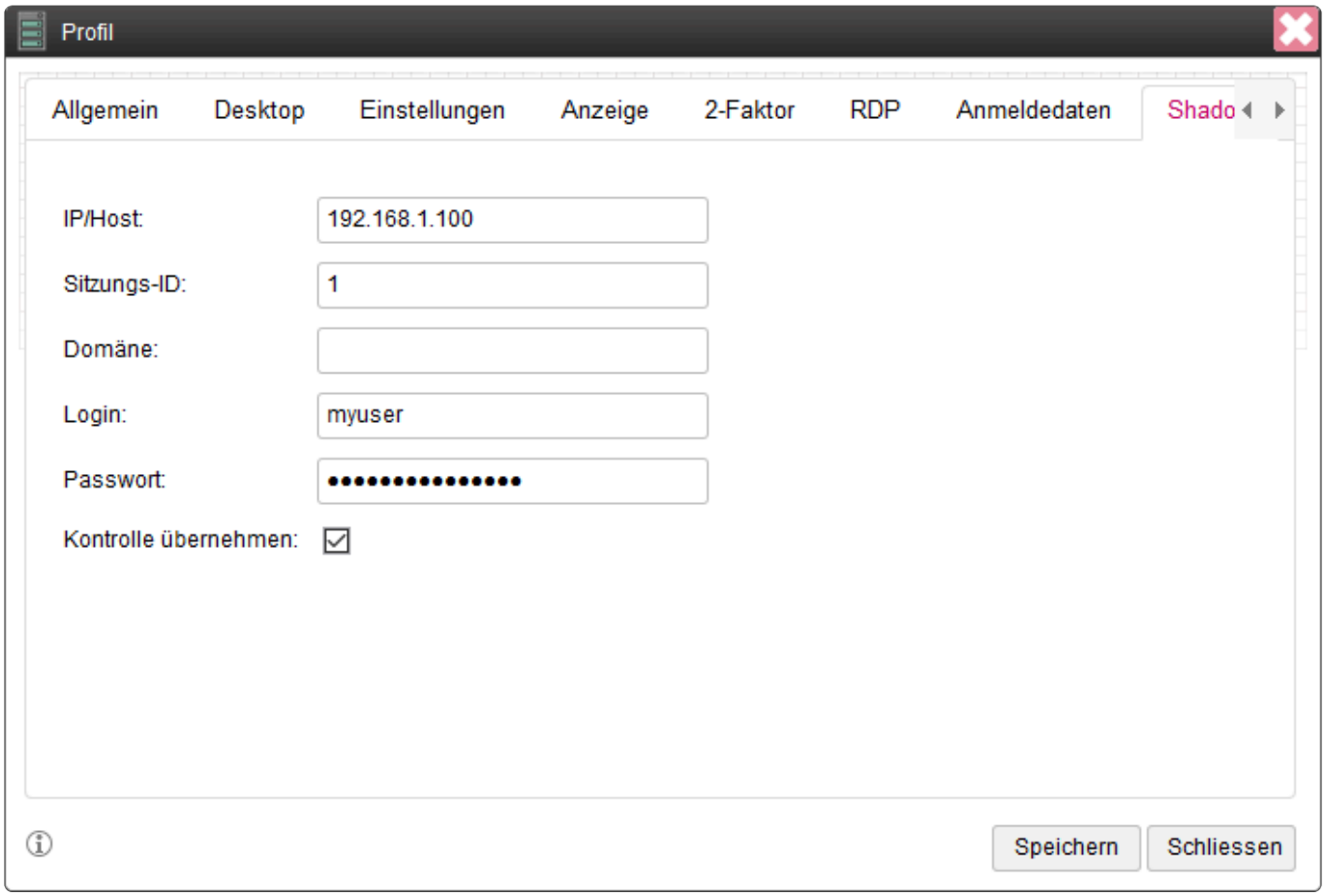
1.2.3.3.4.7. Anmeldedaten

Soll die Anmeldung an der Remote-Sitzung mit vordefinierten Anmelde-Daten erfolgen, so können diese hier definiert werden.



1.2.3.3.4.8. Shadow

Wird ein Profil mit der Einstellung “Shadow” versehen, so kann sich ein Experte auf einen PC schalten, an dem bereits ein andere Benutzer angemeldet ist.



Für dieses Feature ist keine Remote-Sitzung über ein Gateway erforderlich.

Folgende Daten müssen angegeben werden:

Name	Beschreibung
IP/Host	IP/Host des Rechners, auf den der Experte zugreifen soll
Sitzungs-ID	Die Sitzungs-ID der Sitzung des angemeldeten Benutzers. Diese ist i.d. R. immer gleich und kann auf dem PC über das Kommando “quser” ermittelt werden
Domäne	(Optional) Die Domäne des PC’s
Login	Login eines lokalen Benutzers oder Administrators
Passwort	Passwort eines lokalen Benutzers oder Administrators

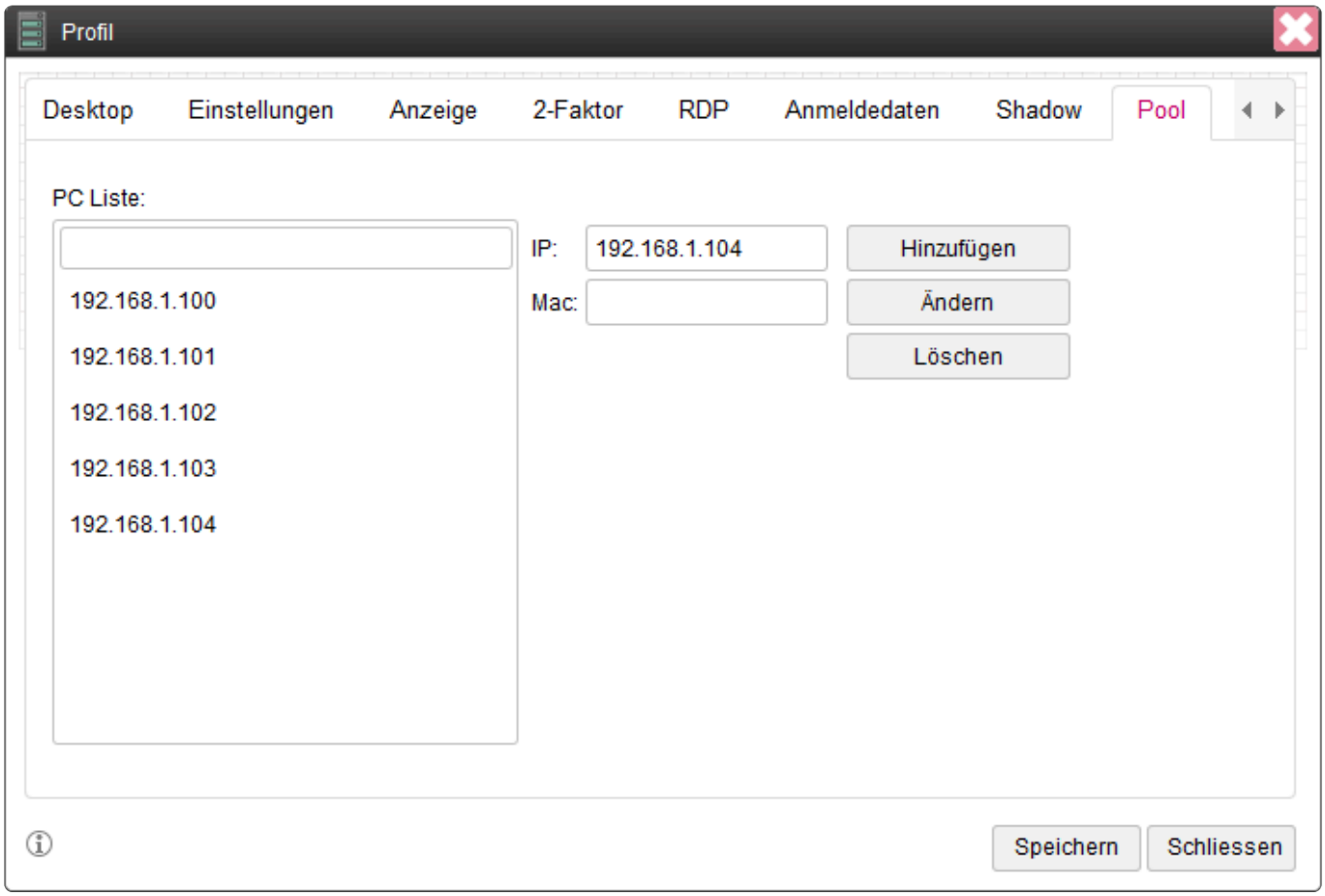
Für den Zugriff auf den PC gelten folgende Voraussetzungen:

- Funktioniert nur mit Win10
- Das Netzwerk darf nicht öffentlich sein

- Die Firewallregel INBOUND: RDP SHADOWING (TCP 445) muss aktiv sein
- Remote Desktop (nicht Remote Access) muss aktiviert sein
- Remote Identifizierung mit NLM
- Diese Gruppenrichtlinie muss angepasst werden:
  gpedit |\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Set rules for remote control of Remote Desktop Services user sessions
- In den Gruppenrichtlinien prüfen ob in „Deny access from this network ..“ nicht „everyone“ eingetragen ist.
- In den Gruppenrichtlinien prüfen ob in „Allow access from this network ..“ auch die „RemoteDesktopUser“ eingetragen sind.

1.2.3.3.4.9. Pool

Hier können PC’s zu einem PC-Pool zusammengefasst werden.
Dieses Feature wurde speziell für das PC Rack entwickelt.



Es kann hier eine Liste an PC’s mit IP und Mac-Adressen angelegt werden.
Ist eine Mac-Adresse verfügbar, so wird der Rechner vor dem Aufruf geweckt.

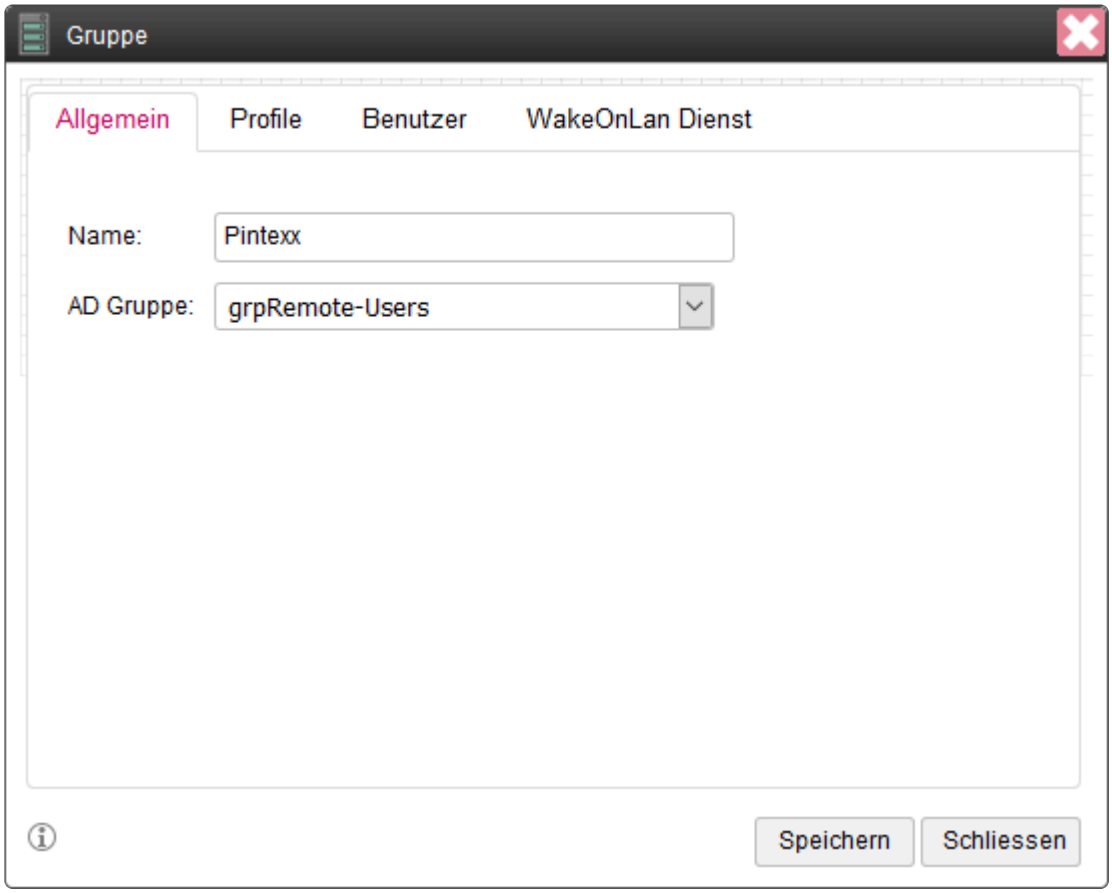
Beim Verbindungs-Aufbau prüft das System auf PC’s, welche aktuell nicht in Verwendung sind.
Mit diesem PC wird der Benutzer dann verbunden. Meldet sich der Benutzer ab, steht der PC wieder zur Verfügung.

1.2.3.3.5. Gruppen

Bei vielen Benutzern macht es Sinn, für unterschiedliche Konfigurationen Benutzer zu einer Gruppe zusammenzufassen.
Eine Gruppe kann aus den Benutzern eines Verzeichnisses bestehen oder aus lokalen Benutzern.

1.2.3.3.5.1. Allgemein

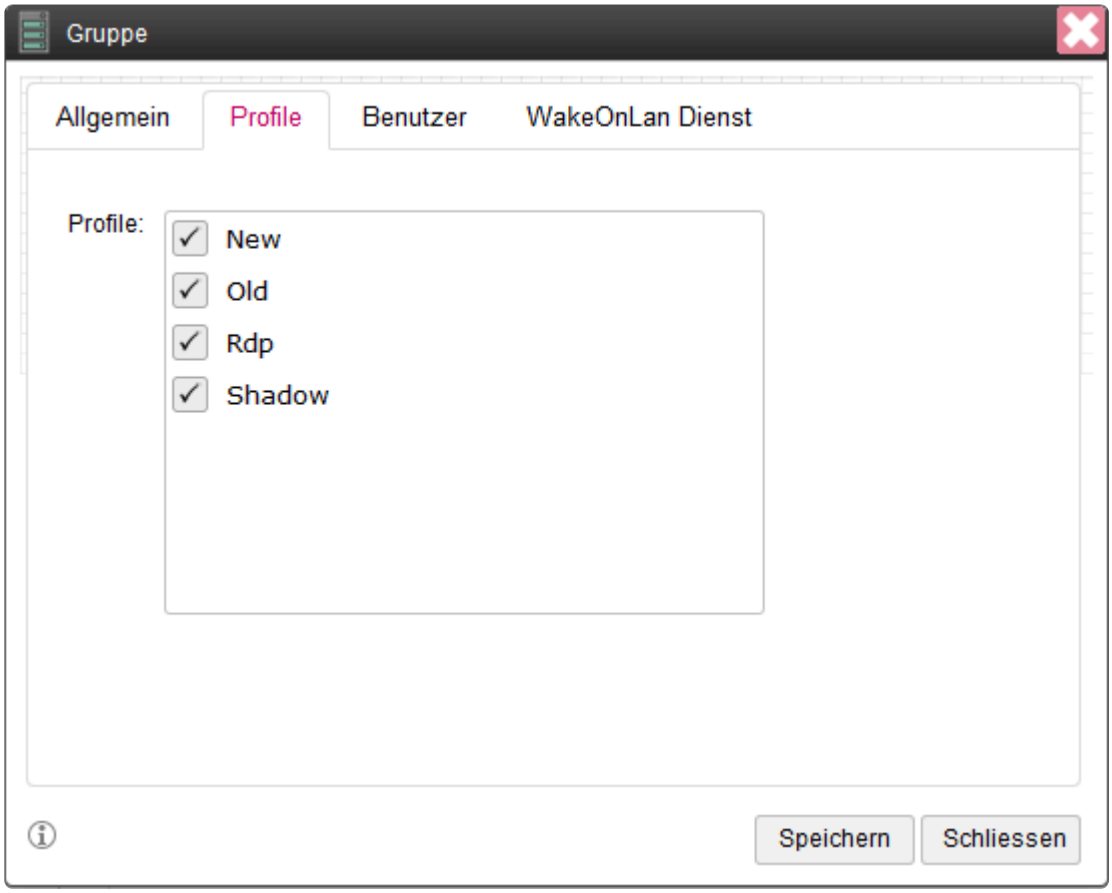
Hier kann der Name der Gruppe angegeben werden und eine Verzeichnis-Gruppe ausgewählt werden.



Die Verzeichnis-Gruppen-Liste ist dann gefüllt, wenn unter “Einstellungen” – “Verzeichnis-Dienst” entsprechende Daten konfiguriert wurden.
Die Gruppen werden aus der Basis OU ausgelesen.

1.2.3.3.5.2. Profile

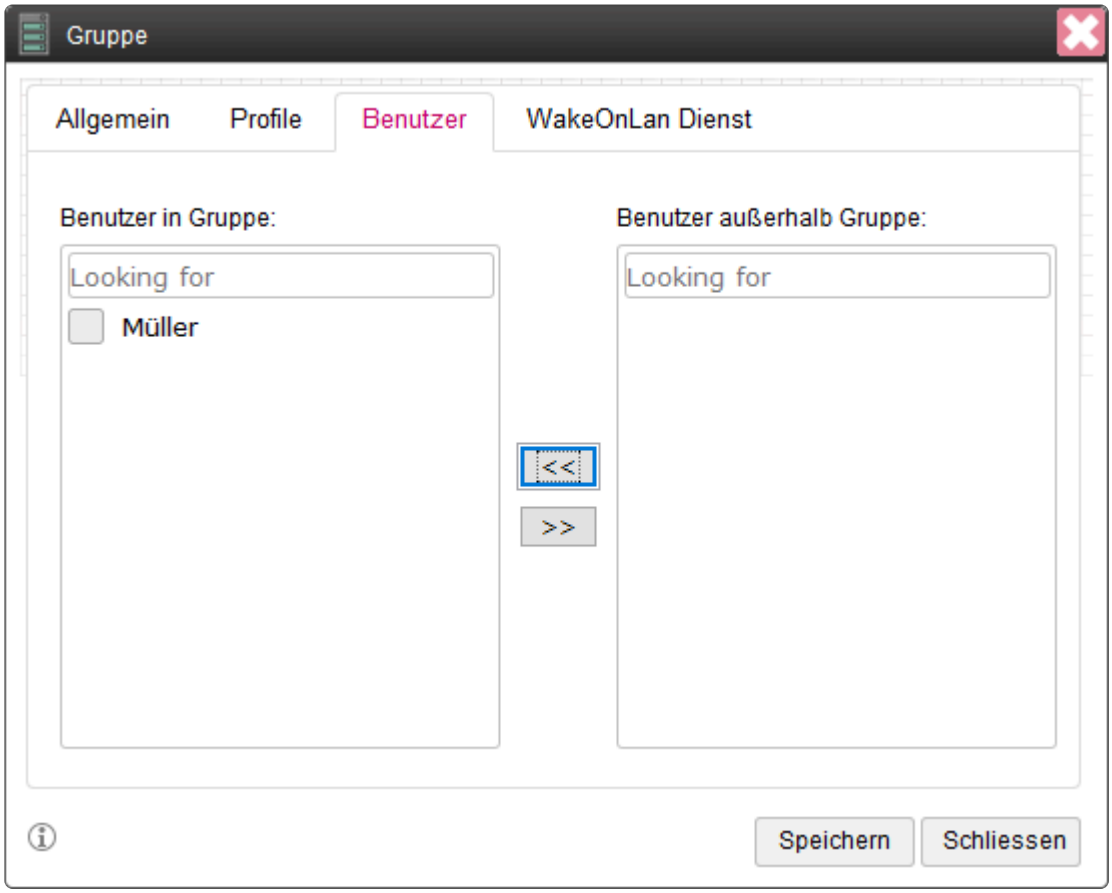
Jeder Gruppe kann ein oder mehrere Profile haben.



Für alle Benutzer innerhalb der Gruppe wird im Benutzer-Bereich pro Profile eine Verbindung angezeigt.

1.2.3.3.5.3. Benutzer

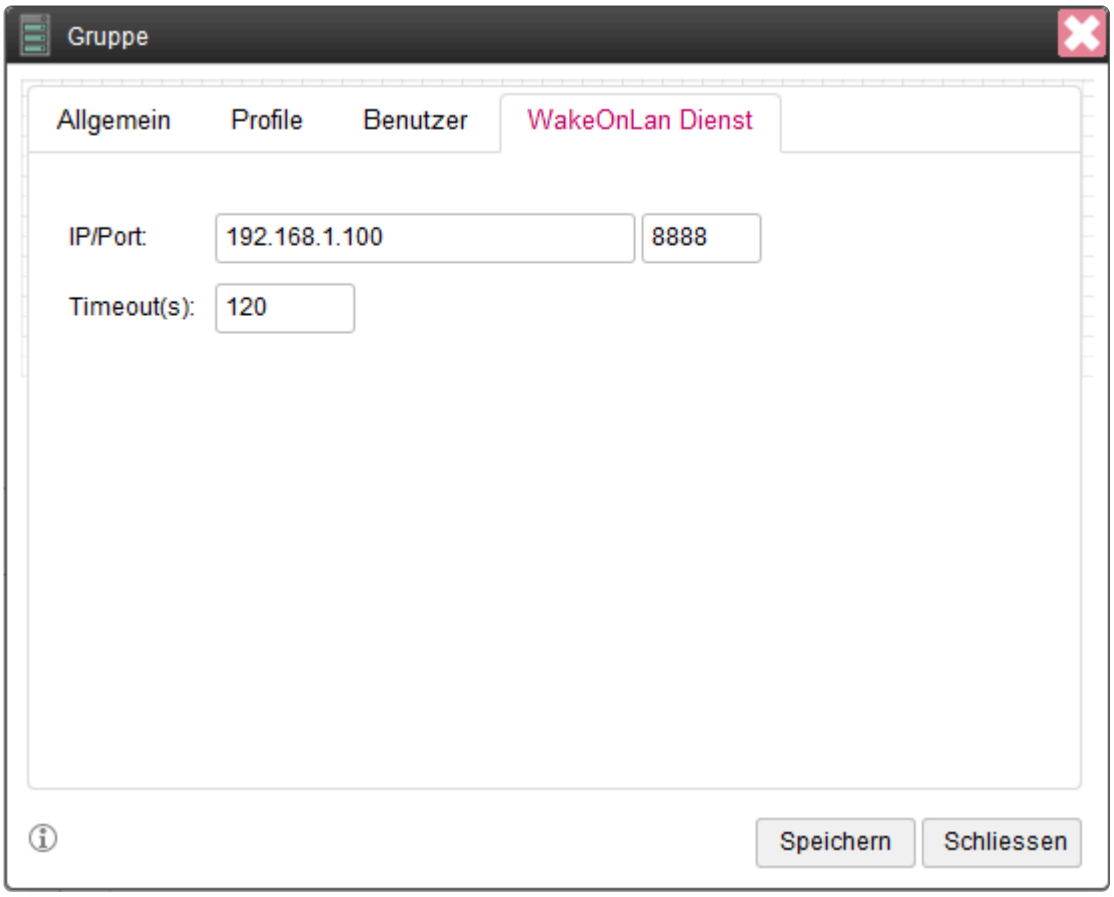
Eine Gruppe kann auch die unter “Benutzer” angelegten Benutzer enthalten.



Ein Benutzer kann nur einmal zu einer Gruppe hinzugefügt werden.

1.2.3.3.5.4. WakeOnLAN Dienst

Kann ein PC im Netzwerk nicht direkt aufgeweckt werden, so kann ein WakeOnLAN-Dienst verwendet werden.



Beim dem Dienst handelt es sich um einen Windows-Dienst, der auf einem Windows-Rechner installiert werden kann.
Für den Dienst kann der Port über eine Konfigurations-Datei eingestellt werden.

Um den Dienst anzusprechen, wird die IP-Adresse und ein Port benötigt.
Diese muss vom System aus erreichbar sein.

Ein Timeout bestimmt, wie lange auf das Wecken des PC's gewartet werden soll.

1.2.3.3.6. Benutzer

Ist eine Nutzung existierender Benutzer über ein Verzeichnis nicht möglich, können hier Benutzer verwaltet werden.

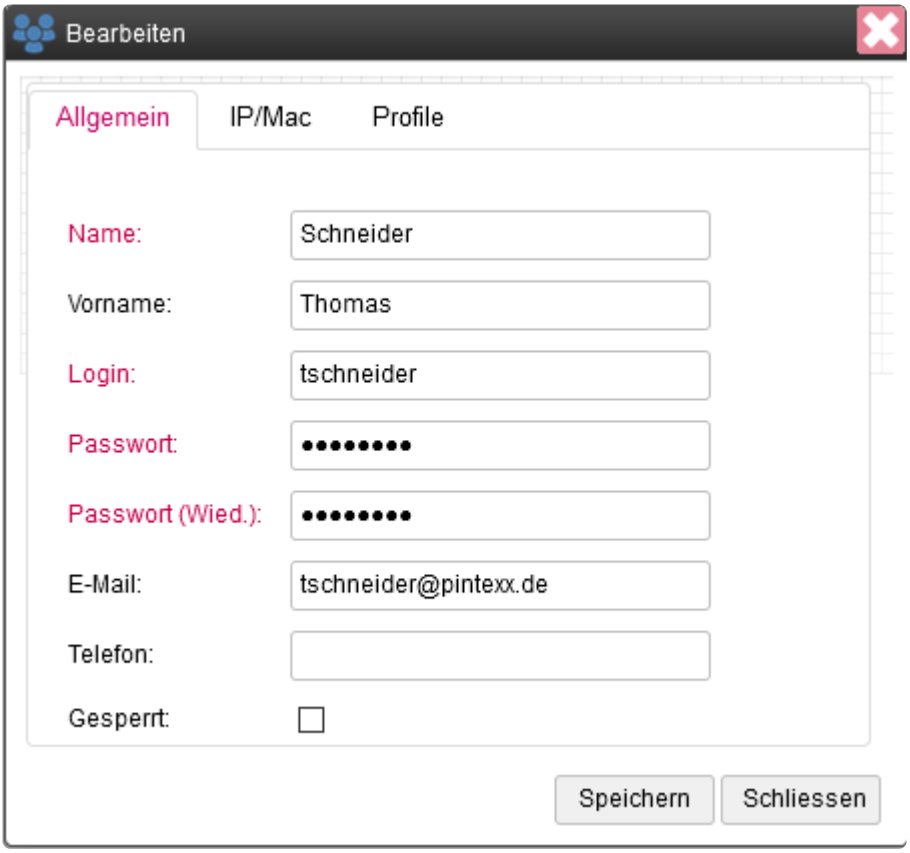
1.2.3.3.6.1. Benutzer-Liste

In der Benutzer-Liste werden alle lokalen Benutzer aufgelistet.

Über den Plus-Button kann ein neuer Benutzer angelegt werden.
Über den Löschen-Button kann ein Benutzer gelöscht werden.

1.2.3.3.6.1.1. Allgemein

Hier können die Basisdaten des Benutzers eingegeben werden.

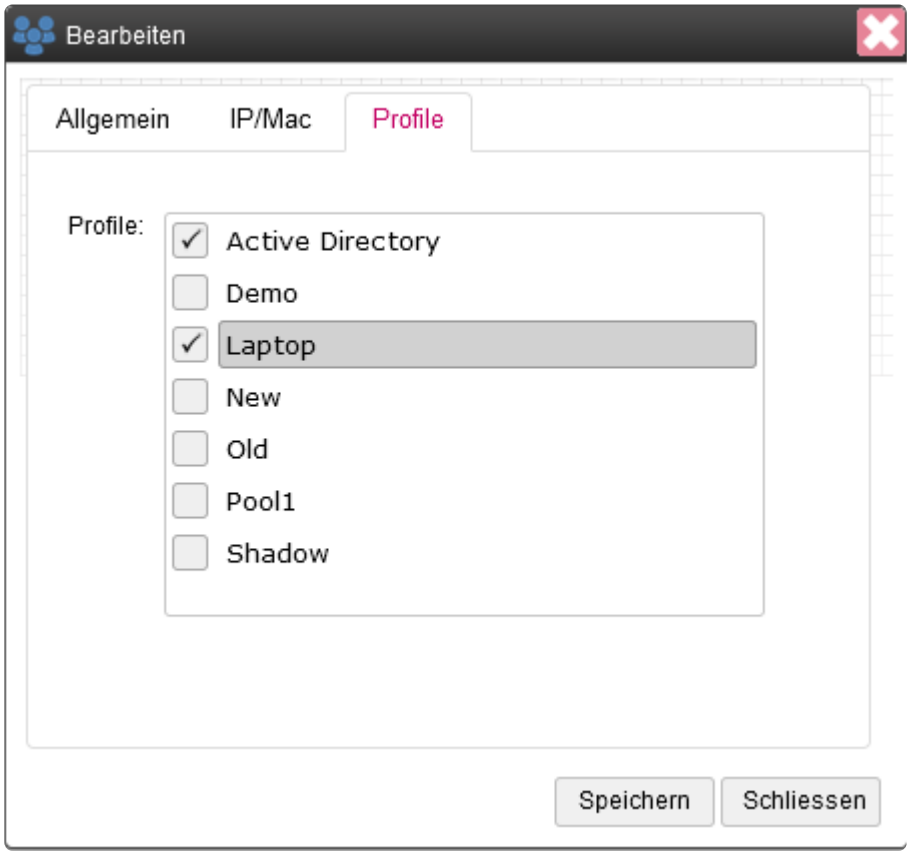


1.2.3.3.6.1.2. IP/Mac

Hier kann die IP- und die Mac-Adresse eingetragen werden.

1.2.3.3.6.1.3. Profil

Einem Benutzer können ein oder mehrere Profile zugeordnet werden.



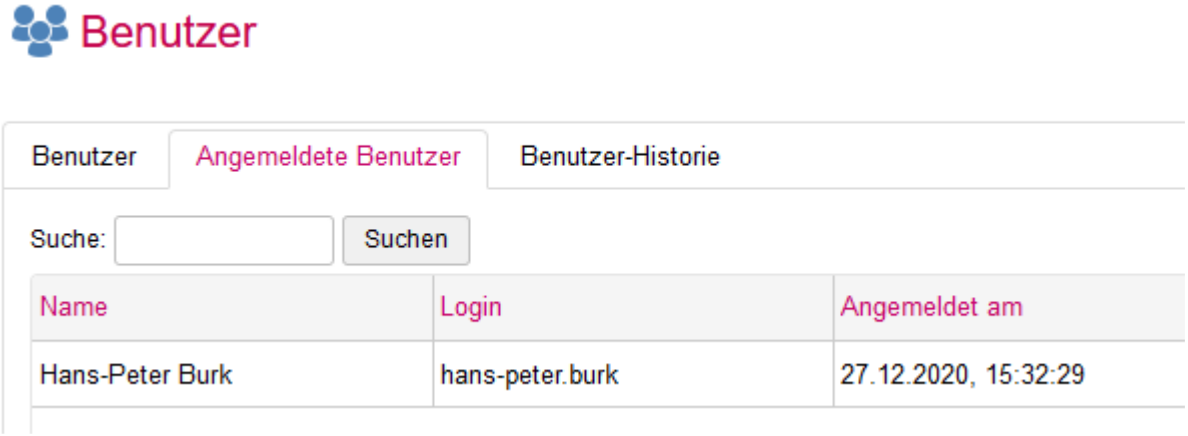
Für jedes Profil wird im Benutzer-Bereich eine Verbindung angezeigt.

1.2.3.3.6.1.4. Import

Benutzer können über eine CSV-Datei importiert werden.
Die einzelnen Felder können über die Überschriften den internen Feldern zugeordnet werden.

1.2.3.3.6.2. Angemeldete Benutzer

Hier werden alle aktuell angemeldeten Benutzer angezeigt.

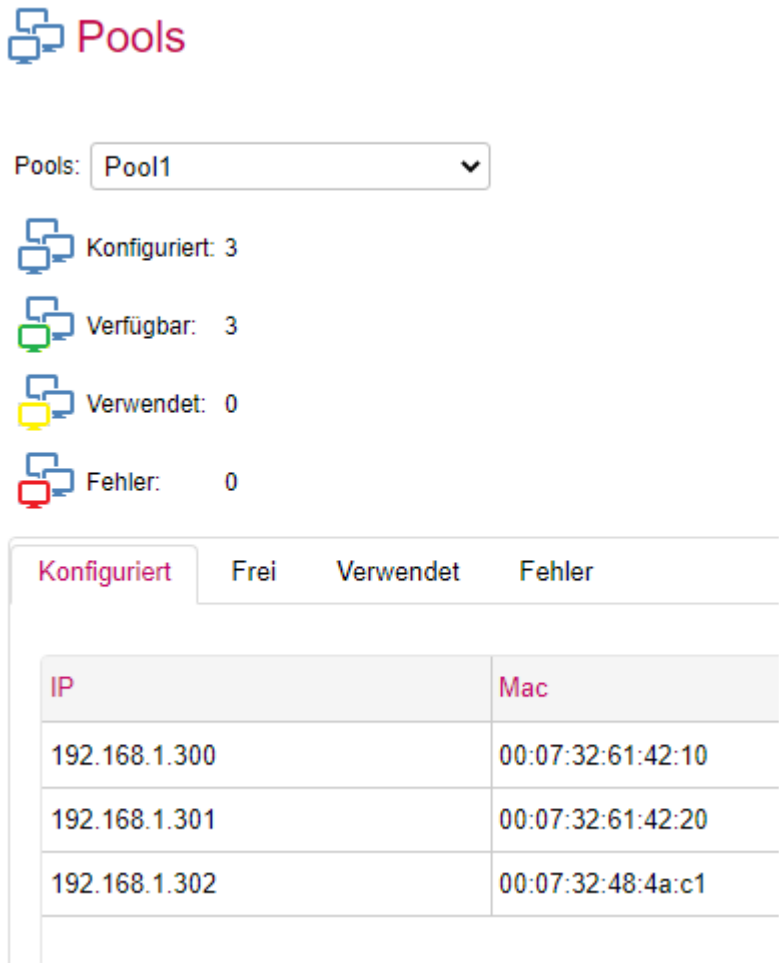


1.2.3.3.6.3. Benutzer-Historie

Die Benutzer-Historie erfasst alle An- und Abmeldungen aller Benutzer.

1.2.3.3.7. Pools

Wurde ein Profil mit der IP-Quelle “Pool” definiert, so wird der Status hier angezeigt.

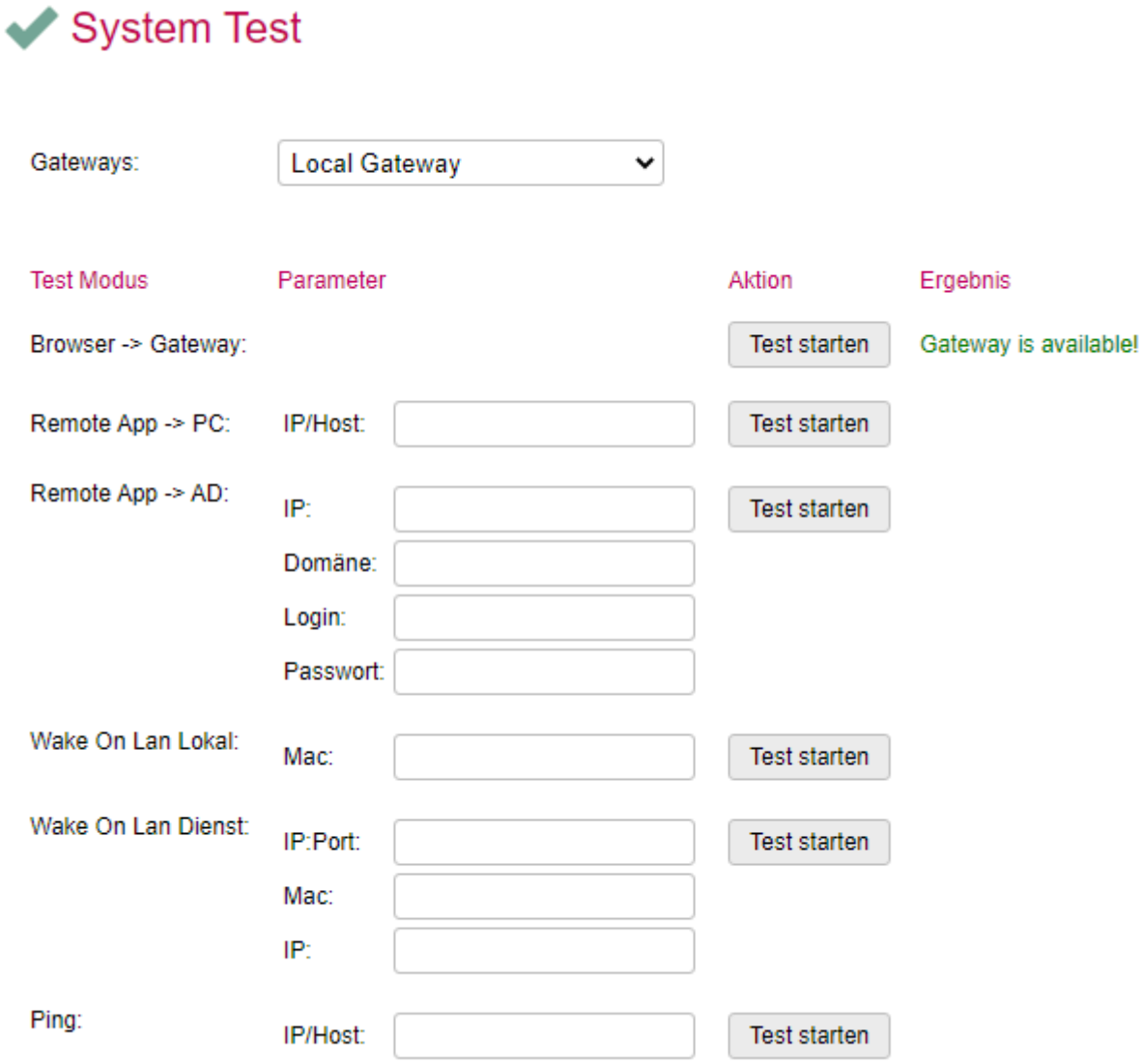


Angezeigt werden die Anzahl der konfigurierten, verfügbaren, verwendeten und nicht verfügbaren PC’s.

In der unteren Liste werden jeweils IP/Mac pro Typ angezeigt.

1.2.3.3.8. System Test

Der System Test dient bei Problemen dazu, jeden möglichen Weg im Netzwerk zu testen.



Test	Beschreibung
Browser -> Gateway	Prüft, ob eine Verbindung zwischen Browser und Gateway vorhanden ist.
“Remote” -> PC	Prüft, ob ein PC über seine IP-Adresse und den RDP-Port erreichbar ist. Durch Angabe eines anderen Ports kann auch dieser getestet werden.
“Remote” -> Verzeichnis	Prüft, ob der Zugang zum Verzeichnis-Dienst möglich ist.
Wake On LAN	Prüft, ob ein PC von “Remote” aus aufgeweckt werden kann.
Wake On LAN-Dienst	Prüft, ob ein PC über den WOL-Dienst aufgerufen werden kann.
Ping	Sendet einen Ping an die angegebene IP.

1.2.3.3.9. Administrator

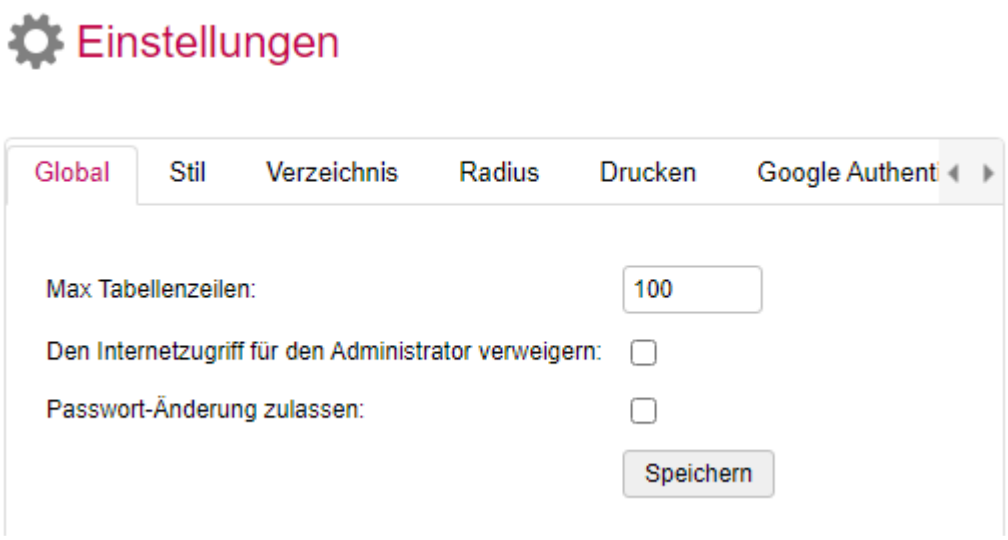
Siehe Administrator

1.2.3.3.10. Einstellungen

Hier können alle “Remote”-Einstellungen vorgenommen werden.

1.2.3.3.10.1. Global

Hier können allgemeine Einstellungen durchgeführt werden.



Mit “Max. Tabellenzeilen” wird die Anzahl der Suchergebnisse definiert.
Des weiteren kann der Administrator über das Internet verweigert werden.
Wird die Passwort-Änderung zugelassen, dann kann im Benutzer-Bereich das Passwort eines lokalen Benutzers geändert werden.

1.2.3.3.10.2. Stil

Hier kann das Aussehen der Benutzer-Login-Seite definiert werden.

Die Überschrift wird unter dem Logo angezeigt.

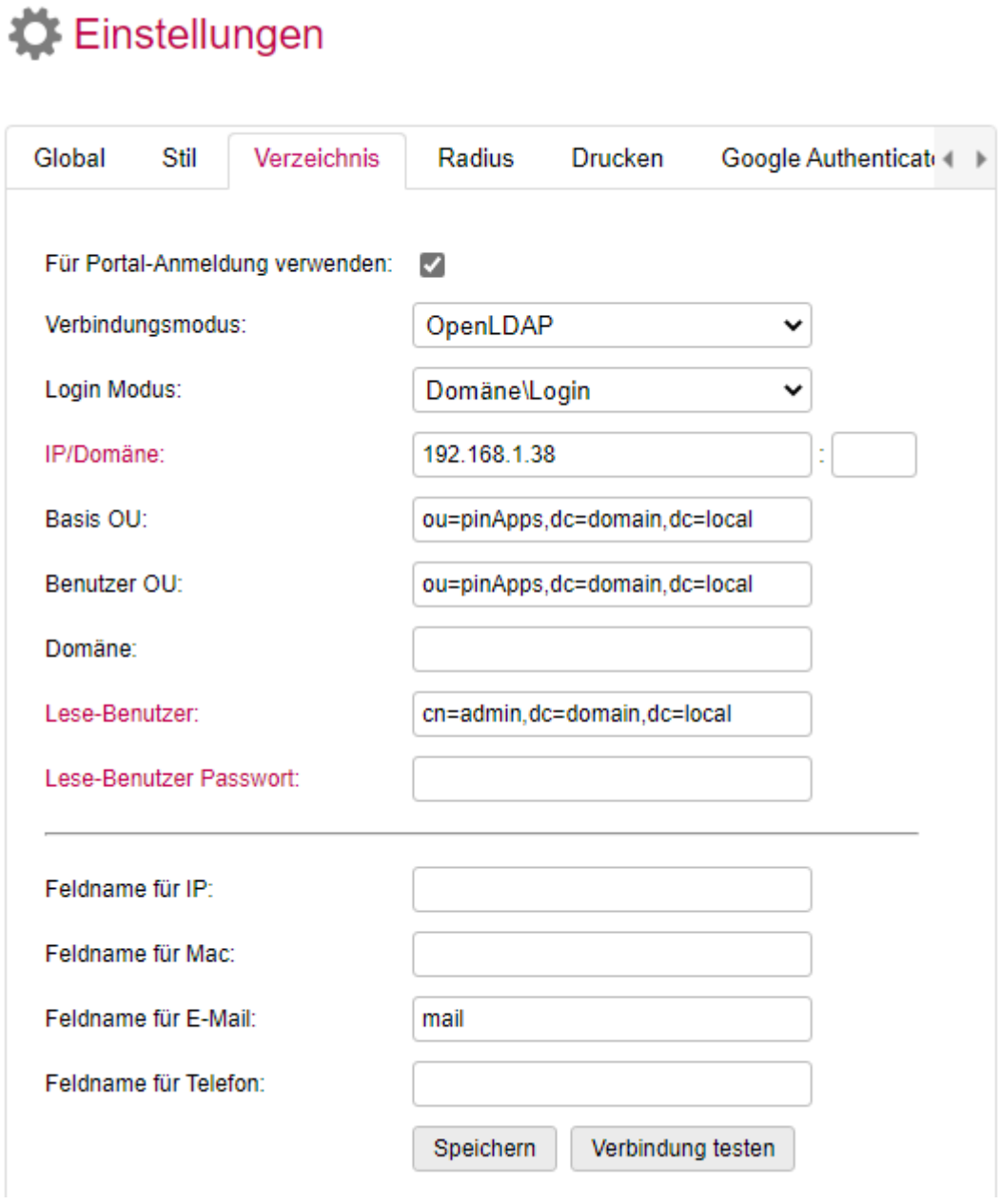
Ein entsprechendes Logo kann hier über einen absoluten Pfad angegeben werden.
Das Logo kann in “System” unter “Einstellungen” -> “Bild Upload” auf das System geladen werden.
Nach dem Hochladen wird die exakte Url angezeigt. Diese kann hier verwendet werden.

Ein Hintergrundbild kann auf dieselbe Weise wie ein Logo gesetzt werden.

Die Hintergrund-Farbe kann aus einem Farbauswahl-Dialog gesetzt werden.

1.2.3.3.10.3. Verzeichnis

Für die Authentifizierung kann hier ein Verzeichnis-Dienst konfiguriert werden.



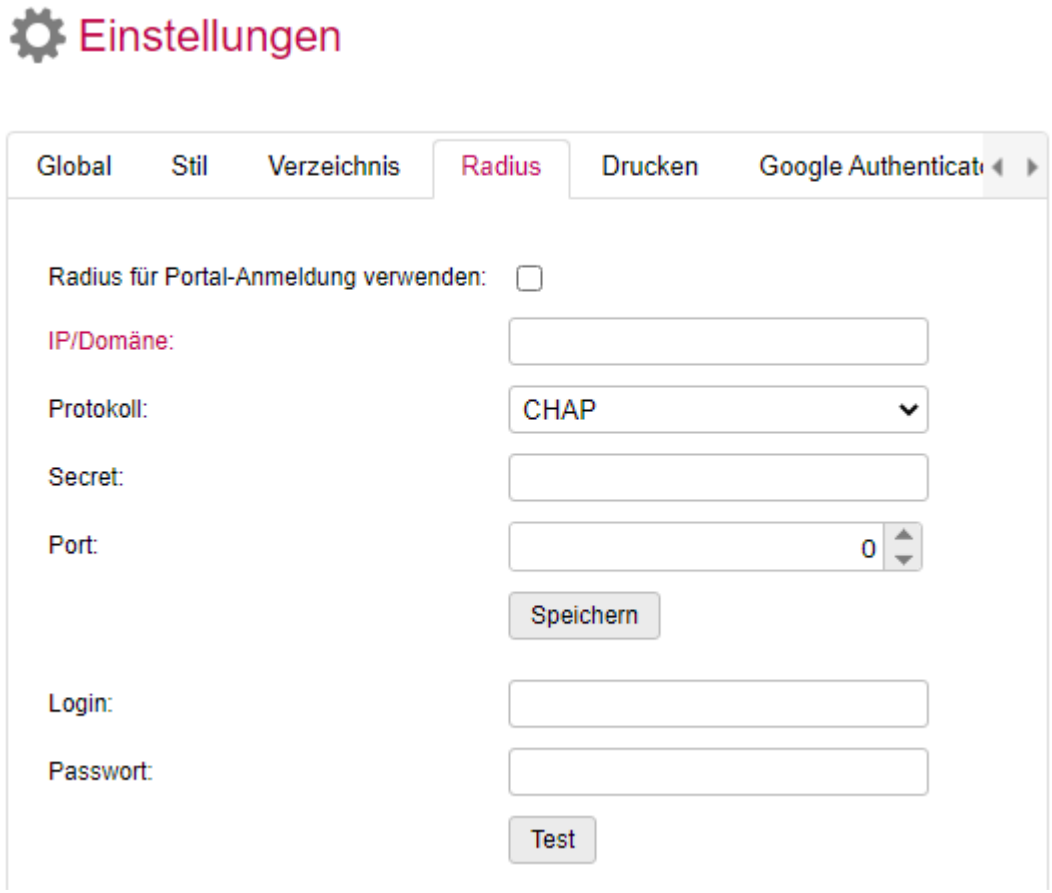
Folgende Eigenschaften können gesetzt werden:

Eigenschaft	Beschreibung
Für Portal-Anmeldung verwenden	Durch Aktivieren wird bei der Benutzer-Anmeldung eine Authentifizierung über den angegebenen Dienst durchgeführt.
Dienst-Typ	Aktuell wird das Active Directory (LDAP) sowie OpenLDAP unterstützt
Login Modus	Für das AD kann die Kombination aus Login und Domäne ausgewählt werden
IP/Domäne	Die IP-Adresse oder Domäne des Verzeichnis-Servers

Basis OU	Die Organisational Unit aller für “Remote” relevanten Gruppen, in denen sich die für das System freigegebenen Benutzer befinden
Benutzer OU	Die Organisational Unit innerhalb der sich die Benutzer befinden
Domäne	Die Domäne, die beider Authentifizierung verwendet werden soll
Lese-Benutzer	Bei AD ein Login, bei OpenLDAP eine DN eines Benutzers der Lesezugriffe auf Gruppen und Benutzer hat, die “Remote” verwenden soll
Lese-Benutzer-Passwort	Das Passwort des Lese-Benutzers
Feldname für IP	Soll die IP-Adresse aus dem Verzeichnis-Dienst gelesen werden, so kann hier ein Feldname (Attribute) angegeben werden
Feldname für Mac	Soll die Mac-Adresse aus dem Verzeichnis-Dienst gelesen werden, so kann hier ein Feldname (Attribute) angegeben werden
Feldname für E-Mail	Soll die E-Mail-Adresse aus dem Verzeichnis-Dienst gelesen werden, so kann hier ein Feldname (Attribute) angegeben werden
Feldname für Telefon	Soll die Telefon-Nummer aus dem Verzeichnis-Dienst gelesen werden, so kann hier ein Feldname (Attribute) angegeben werden

1.2.3.3.10.4. Radius

Für die Authentifizierung kann auch ein Radius-Server verwendet werden.



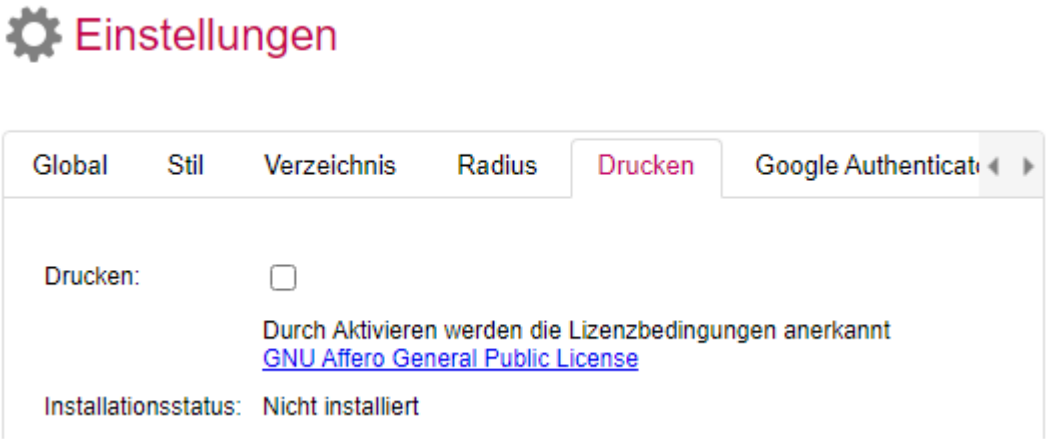
Folgende Eigenschaften können gesetzt werden:

Eigenschaft	Beschreibung
Für Portal-Anmeldung verwenden	Durch Aktivieren wird bei der Benutzer-Anmeldung eine Authentifizierung über den angegebenen Server durchgeführt.
IP/Domäne	Die IP-Adresse oder Domäne des Radius-Servers
Protokoll	Es wird sowohl das CHAP also auch das PAP-Protokoll unterstützt
Secret	Das Radius-Secret
Port	Der Port des Radius-Servers

Durch die Angabe eines Login/Passworts kann der Zugriff auf den Radius-Server getestet werden.

1.2.3.3.10.5. Drucken

Diese Einstellung wird nur bei Verwendung von Betriebssystemen < Windows 10 benötigt.

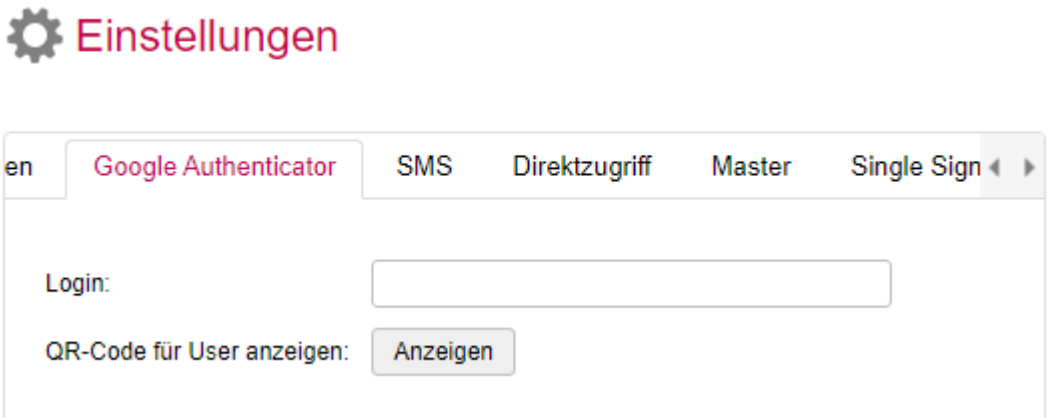


Durch Aktivierung kann ein Postscript->PDF-Konverter aktiviert werden, welcher für das Drucken benötigt wird.

Achtung:
Bitte die Lizenzbedingungen beachten

1.2.3.3.10.6. Google Authenticator

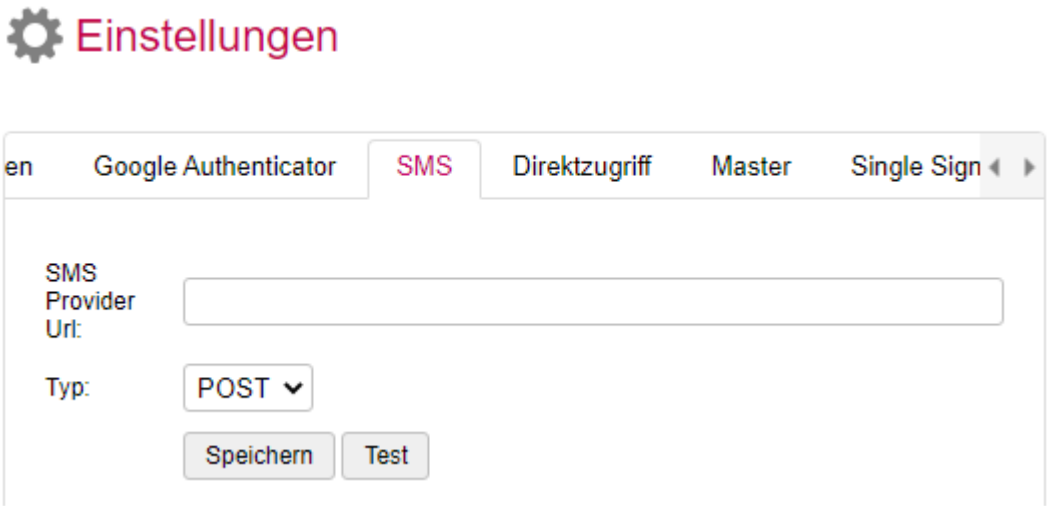
Wird der Google Authenticator als 2-Fakttor-Medium verwendet, so muss dafür ein QR-Code angezeigt werden.



Wird hier ein Login angegeben, dann wird dieser QR-Code dem Benutzer nach der Anmeldung einmalig angezeigt.
Wird kein Login angegeben gilt dies für alle Benutzer.

1.2.3.3.10.7. SMS

Wird SMS als 2-Faktor-Medium verwendet, so kann hier ein entsprechender Dienst über eine Url konfiguriert werden.



Dieser Dienst übernimmt das Versenden der SMS und wird über folgende Parameter innerhalb der Url konfiguriert:

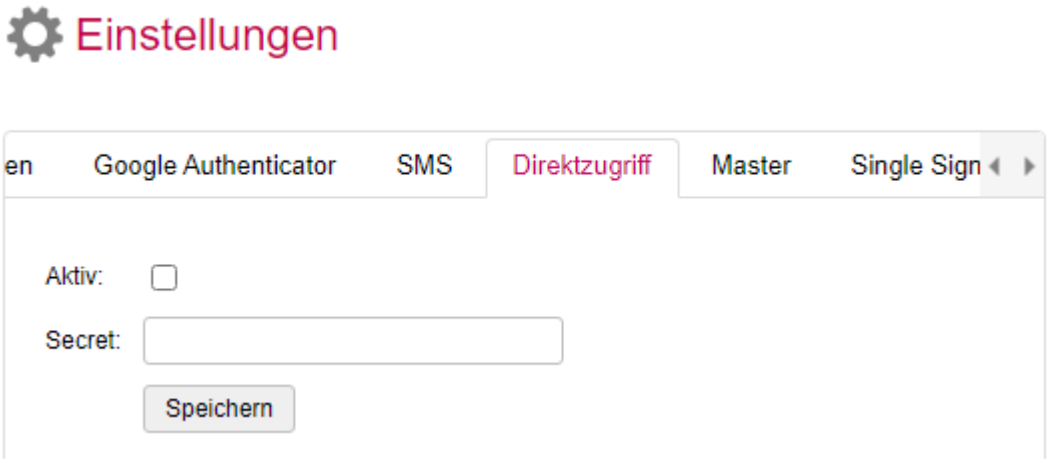
Beispiel:
https://<domäne>/…/…/…&mobile=#PHONENUMBER#&code=#TOKEN#

Die Url muss nach Angaben des Providers konfiguriert werden. Für die Variablen #PHONENUMBER# und #TOKEN# wird dann von “remote” die konfigurierte telefon-Nummer und der Code (OTP) eingefügt.

Des weiteren kann konfiguriert werden, ob ein GET oder POST gemacht werden soll.

1.2.3.3.10.8. Direktzugriff

Es besteht die Möglichkeit, einem Benutzer einen Link zuzusenden.
Über diesen Link kann dann der Zugriff auf den Desktop-Erfolgen.



Wird der Direktzugriff aktiviert und ein Secret (Passwort) angegeben, dann erscheint in der Profil-Liste in der 2.Spalte ein Symbol.
Über dieses Symbol kann dann der generierte Link in die Zwischenablage kopiert werden.

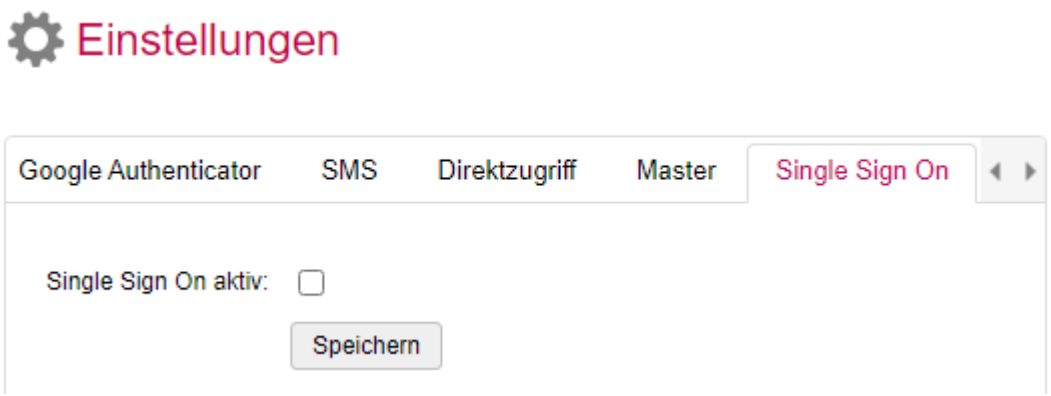
1.2.3.3.10.9. Master

Bei mehreren VM’s gibt es immer einen Master, auf welchem “System” und “Applications” laufen.

Die Master-IP muss dann hier angegeben werden.

1.2.3.3.10.10. Single Sign On

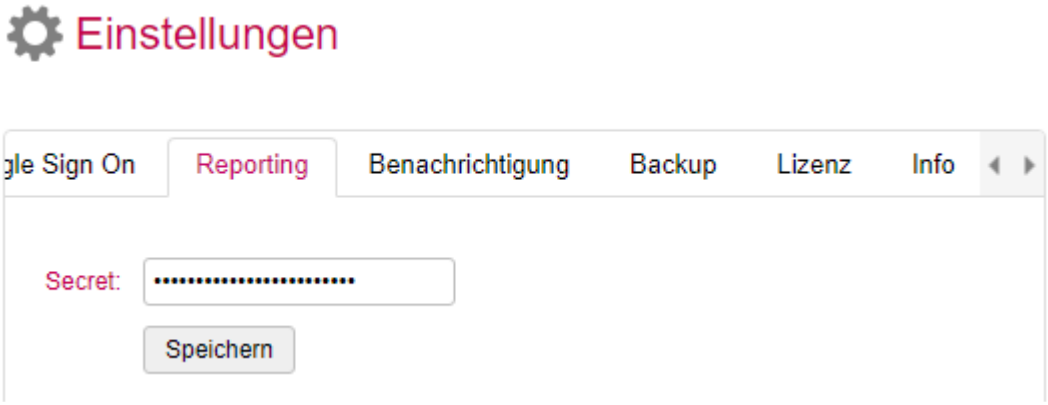
Wird das Pintexx Workplace “Cockpit” verwendet, so kann hier das Single Sign On aktiviert werden.



Allerdings muss SSO auch im Cockpit-Admin für “Remote” aktiviert werden.
Ist SSO aktiviert, ist eine Benutzer-Anmeldung nur noch über das Cockpit möglich.

1.2.3.3.10.11. Reporting

Die aktuellen Daten über die Benutzerzugriff können über einen Link auch von außen abgerufen werden.



Dazu muss ein Secret (Passwort) angegeben werden.

Dann kann über diesen Link eine XML-Datei über den aktuellen Stand abgerufen werden.

Beispiel:
https://workplace.pintexx.com/remote/report?secret=12345678

1.2.3.3.10.12. Benachrichtigung

Siehe Benachrichtigung

1.2.3.3.10.13. Backup

Siehe Backup

1.2.3.3.10.14. Lizenz

Hier kann für spezielle Anforderungen direkt eine Lizenz eingespielt werden.
I.d.R. wird dies aber über “System” durchgeführt.

1.2.3.3.10.15. Info

Siehe Info

1.2.3.3.11. Ereignisse

Siehe Ereignisse

1.2.4. Workplace “Phone”

Workplace “Phone” ist ein browserbasiertes Telefon, welches mit einer Telefonanlage verbunden ist. “Phone” kann auf Adressbücher von “Contacts” zugreifen.

“Phone” umfasst alle Grundfunktionen eines Telefons wie Favoriten, Anrufliste, Kontakte, Halten, Weiterleiten etc.

1.2.4.1. Voraussetzungen

Telefon-Anlage

Voraussetzung für “Phone” ist eine externe oder interne Telefonanlage, die SIP-Konten zur Verfügung stellt.

Für eine Telefon-Verbindung werden folgende Parameter benötigt:

Parameter	Beispiel
Registrar	IP/Domäne der Telefon-Anlage
SIP Login	Login des SIP-Kontos
SIP Passwort	Passwort des SIP-Kontos

Anwendungen

Es werden folgende Anwendungen benötigt:

Anwendung	Beschreibung
Phone	Der Telefon-Client
SIP Gateway	Die Verbindung zur Telefon-Anlage
Contacts	Für den Zugriff auf Telefonnummern aus konfigurierbaren Adressbüchern

Aktionen

Vor der Installation des SIP Gateways in “System” unter “Einstellungen” -> “Zertifikate” -> “Zertifikat bereitstellen”.

1.2.4.2. Aufruf

“Phone” hat 2 Zugänge, einen für den Administrator und einen für den Benutzer.

Benutzer:
<IP/Domäne>/phone

Administrator:
<IP/Domäne>/phone/adminlogin

1.2.4.3. Konfiguration SIP-Konten

Die SIP-Konten können auf unterschiedliche Art und Weise konfiguriert werden.

Über Verzeichnisdienst

In der Verzeichnisdienst-Konfiguration kann ein Feldname angegeben, werden, in welchem die SIP-Konfiguration gespeichert wird.
Verzeichnisdienst konfigurieren

Über Cockpit

Wird “Phone” über Single Sign On an das Cockpit angebunden, dann können die Benutzerdaten direkt in “Phone” übernommen werden.

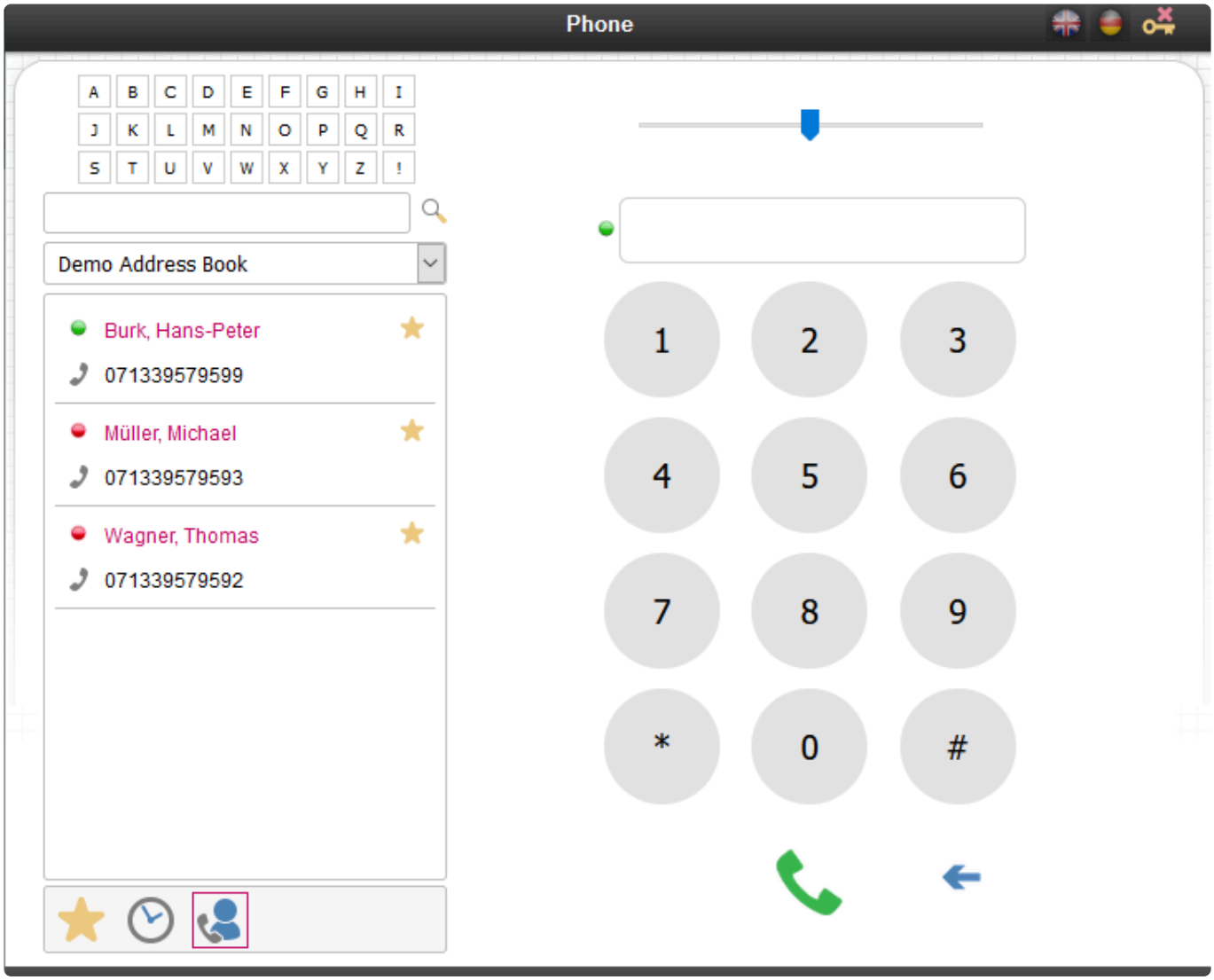
1.2.4.4. Adressbücher

“Phone” kann Adressbücher aus “Contacts” verwenden.
Die Authentifizierung an der “Contacts” REST-API erfolgt mit denselben Anmeldedaten wie für “Phone”.
Alle für den Benutzer konfigurierten Adressbücher stehen dann zur Verfügung.

Sind keine Adressbücher definiert, so kann nur die Wähl-Tastatur verwendet werden.

1.2.4.5. Benutzer-Bereich

Nach erfolgter Authentifizierung wird der Benutzer-Bereich angezeigt.

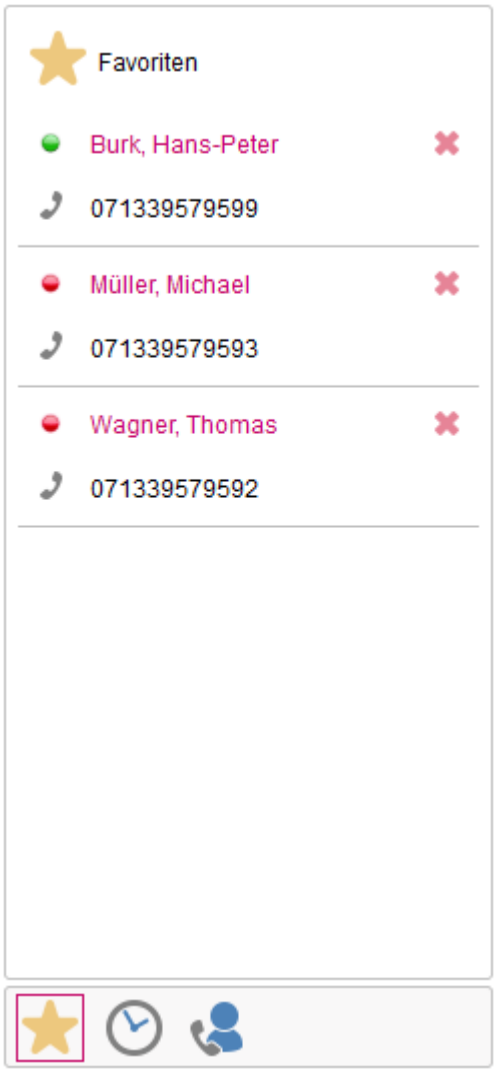


1.2.4.5.1. Auswahl-Bereich

Der Benutzer-Bereich teilt sich in den Auswahl-Bereich auf der linken Seite sowie den Telefon-Bereich auf der Rechten-Seite.
Der Auswahl-Bereich ist in 3 Teile unterteilt, die am unteren Rand aktiviert werden können.

1.2.4.5.1.1. Favoriten

Hier werden alle Favoriten mit Telefon-Nummern angezeigt.



Ein Kontakt kann im Auswahl-Bereich unter “Kontakte” über das Favoriten-Icon erstellt werden.
Über das Löschen-Icon kann der Favorit wieder geköscht werden.

Die Favoriten-Liste enthält auch eine Statusamzeige.
Rot = Benutzer ist nicht angemeldet oder im Gespräch
Grün = Benutzer ist verfügbar

1.2.4.5.1.2. Anruf-Liste

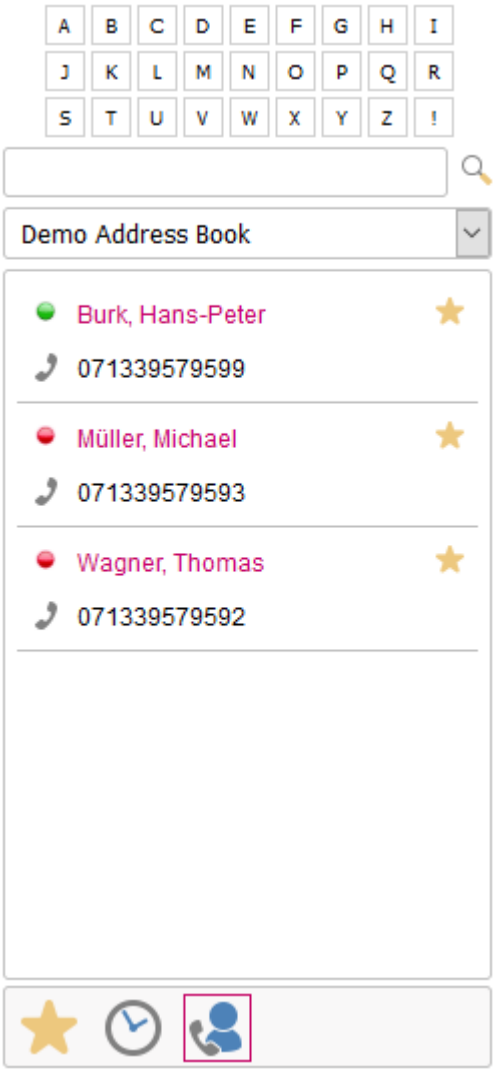
Anzeige aller Anrufe und getätigten Anrufe.

“Phone” zeigt alle ausgehenden, eingehenden und verpassten Anrufe an.

Über den Löschen-Knopf kann die Liste gelöscht werden.

1.2.4.5.1.3. Kontakte

Hier werden alle verfügbaren Adressbücher aus “Contacts” in einer Auswahl-Liste angezeigt.



Ganz oben befindet sich der Direkt-Suchbereich. Durch Anklicken eines Buchstabens werden alle Kontakte angezeigt, die mit diesem Buchstaben beginnen.
Im Suchfeld darunter kann nach beliebigen Kontakten über einen Such-Text Eingabe von “ENTER” oder drücken des Such-Buttons gesucht werden durch.
Ist das Suchfeld leer werden die ersten hundert Kontakte angezeigt.

Durch Aktivieren einer Telefon-Nummer wird diese in das Telefon-Nummern-Feld übertragen.

Über das Favoriten-Icon können Favoriten erstellt werden.

1.2.4.5.2. Telefon-Bereich

Im Telefon-Bereich wird ein Laustärke-Regler, ein Telefon-Nummern-Feld, eine Wähl-Tastatur, ein Icon zur Rufannahme und ein Zurück-Button angezeigt.
Erscheint neben dem Telefon-Nummern-Feld ein grünes Symbol, ist der Benutzer mit der Telefonanlage verbunden.
Bei einem roten Symbol besteht keine Verbindung.

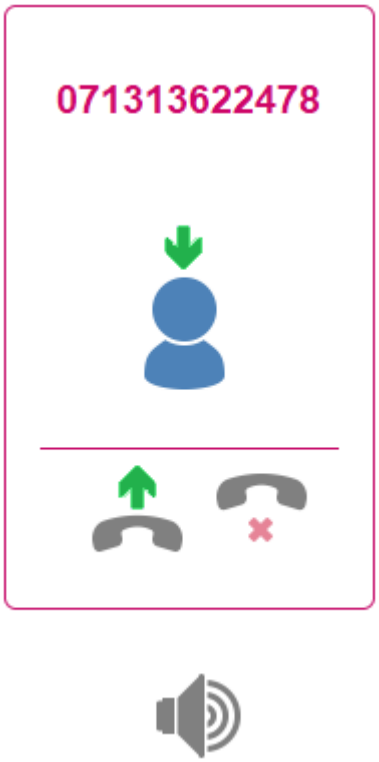
Die Telefon-Nummer kann über die Kontakt-Liste, über die Wähl-Tastatur oder über die Tastatur eingegeben werden.

Wurde im Telefon-Nummern-Feld eine Telefon-Nummer eingegeben, dann kann über die Wähl-Taste ein Anruf getätigt werden.
Ein Wähl-Ton wird hörbar, sofern ein Audio-Ausgabe-Gerät verfügbar ist.

Nimmt der Teilnehmer ab, erscheint Auswahl-Menü mit verschiedenen Optionen:

Über das erste Symbol kann der Anruf beendet werden.
Über das 2. Symbol kann ein weiterer Kontakt zu einer Konferenz hinzugefügt werden.
Über das 3. Symbol kann der Anruf gehalten werden um einen anderen Kontakt anzurufen.
Über das 4. Symbol kann der eigene Ton ein- und ausgeschaltet werden.

Wird das eigene Telefon angerufen ist ein Wählton hörbar und es erscheint ein Auswahl-Menü:

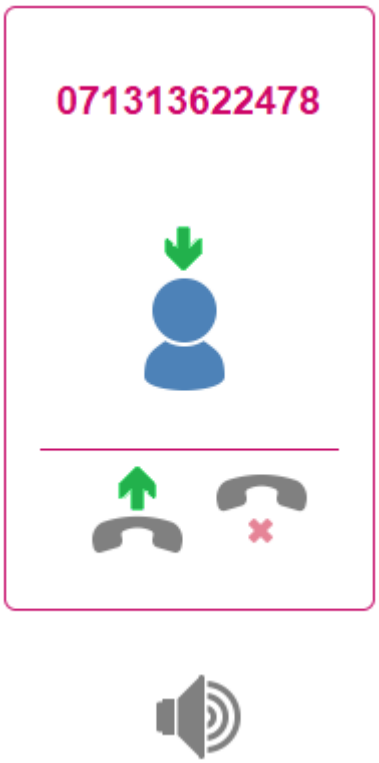


Der Anruf kann über das erste Symbol angenommen oder über das 2. Symbol abgelehnt werden.

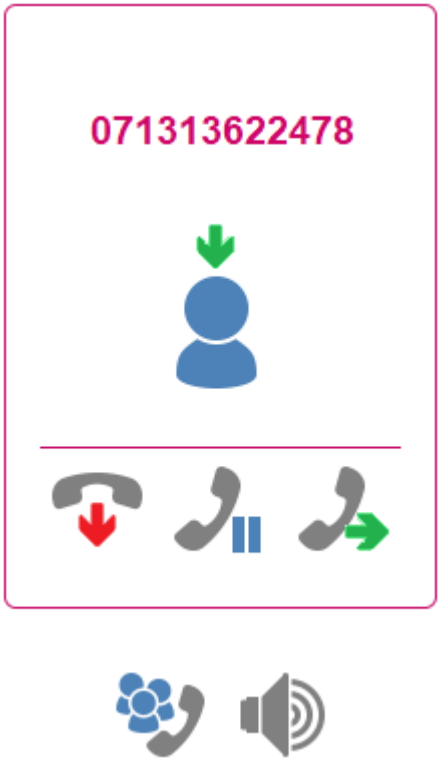
Die beschrieben Features sind nur möglich, wenn sie auch von der Telefon-Anlage unterstützt werden.

1.2.4.5.2.1. Eingehender Anruf

Besteht eine Verbindung zur Telefonanlage (grüne Lampe an) können Anrufe entgegengenommen werden.
Dazu wird ein Klingelton ausgegeben und ein eingehender Anruf angezeigt.
Die anrufende Telefonnummer wird angezeigt. Ist die Nummer in den Kontakten bekannt, wird der Name des Anrufers angezeigt.



Wird der Anruf entgegengenommen, gibt es folgende Optionen:

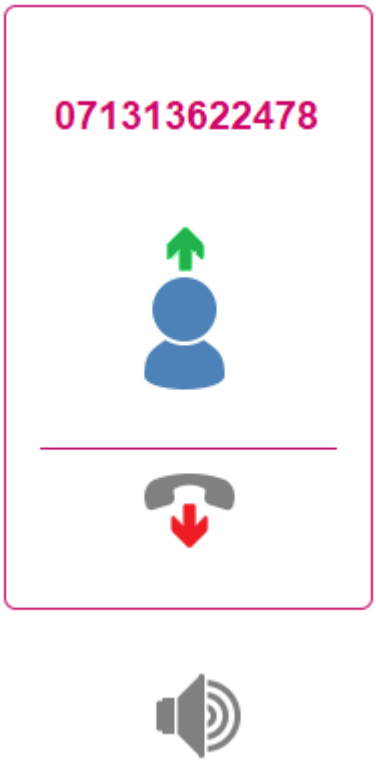


Über das “Auflegen”-Symbol kann der Anruf beendet werden.
Über das “Halten”-Symbol kann der Anruf gehalten werden.
Über das “Weiterleiten”-Symbol kann der Anruf weitergeleitet werden.

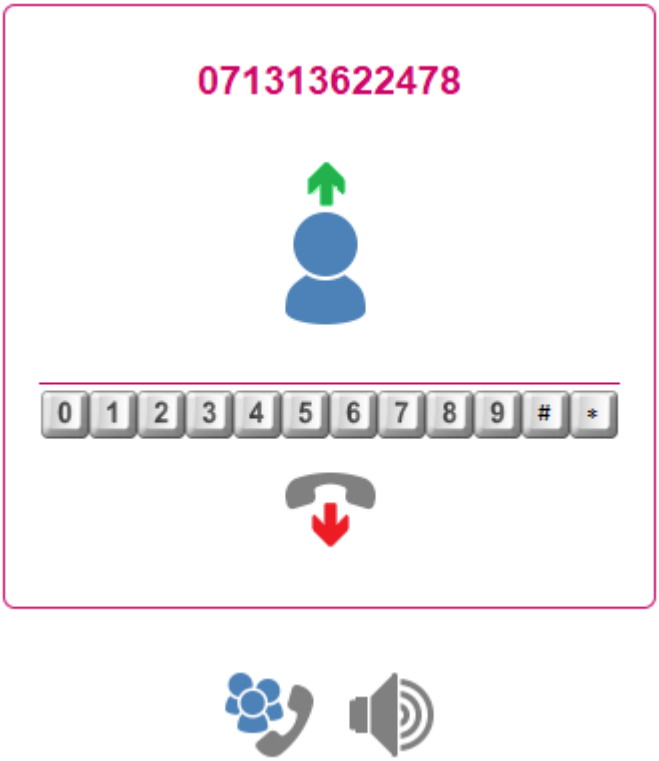
Über die Symbole am unteren Rand kann ein weiterer Anrufer zu einer Konferenz hinzugenommen werden.
Über das “Lautsprecher”-Symbol kann das eigene Mirofon abgeschaltet werden.

1.2.4.5.2.2. Ausgehender Anruf

Die zu wählende Nummer kann entweder aus den Kontakten übernommen oder von Hand eingegeben werden.



Nimmt der Anrufende ab, gibt es folgende Optionen:

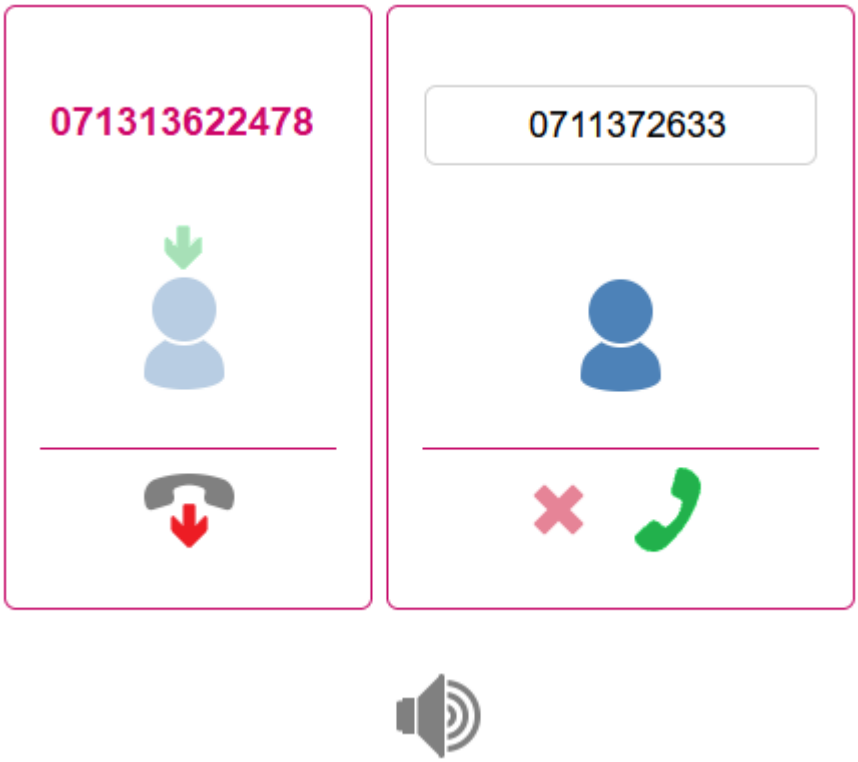


Über die Wähltasten kann ein DTMF-Signal gesandt werden.
(z.B. bei Hotlines mit Auswahlmenü)
Über das “Auflegen”-Symbol kann der Anruf beendet werden.

Über die Symbole am unteren Rand kann ein weiterer Anrufer zu einer Konferenz hinzugenommen werden.
Über das “Lautsprecher”-Symbol kann das eigene Mirofon abgeschaltet werden.

1.2.4.5.2.3. Anruf weiterleiten

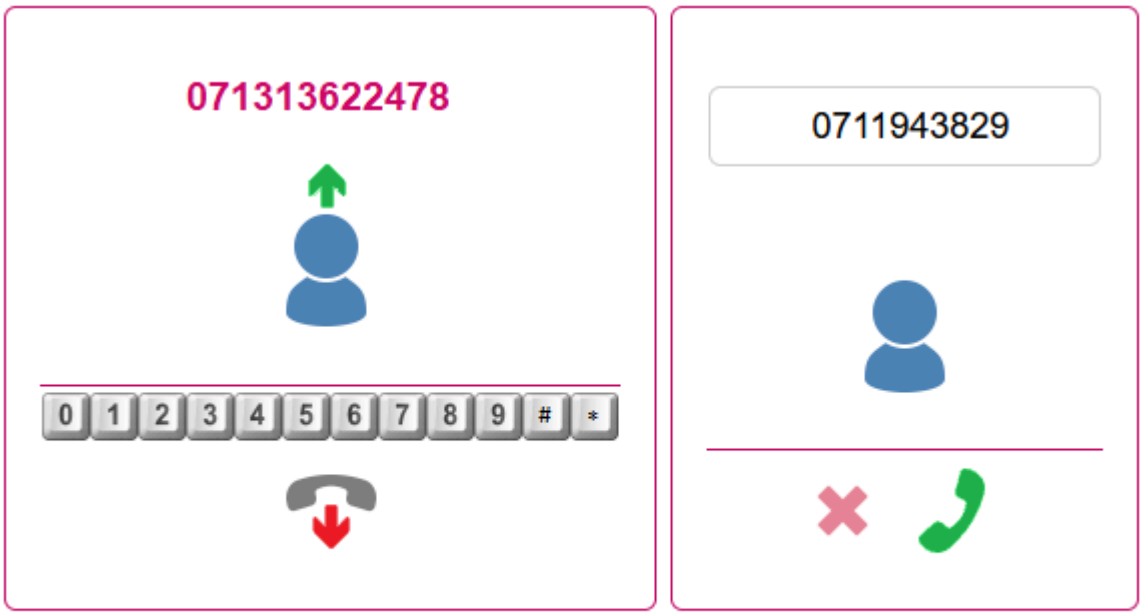
Wurde ein Anruf entgegengenommen und auf das “Weiterleiten”-Symbol geklickt, dann kann eine weitere Nummer ausgewählt oder eingegeben werden.
Die aktuelle Verbindung wird gehalten.



Wird auf das “Wählen”-Symbol geklickt dann wird eine 2. Verbindung aufgebaut.
Ist der 2.Benutzer mit einer Weiterleitung einverstanden kann mit dem “Weiterleiten”-Symbol der Anruf an den ersten Anrufer weitergeleitet werden.
Für den aktuellen Benutzer werden alle Verbindungen beendet.

1.2.4.5.2.4. Telefon-Konferenz

Besteht bereits eine Verbindung, so kann mit dem “Konferenz”-Symbol ein weitere Benutzer hinzugefügt werden.



Wird auf das “Wählen”-Symbol geklickt dann wird eine 2. Verbindung aufgebaut und zur aktuellen Verbindung hinzugefügt.

1.2.4.6. Admin-Bereich

1.2.4.6.1. Administrator

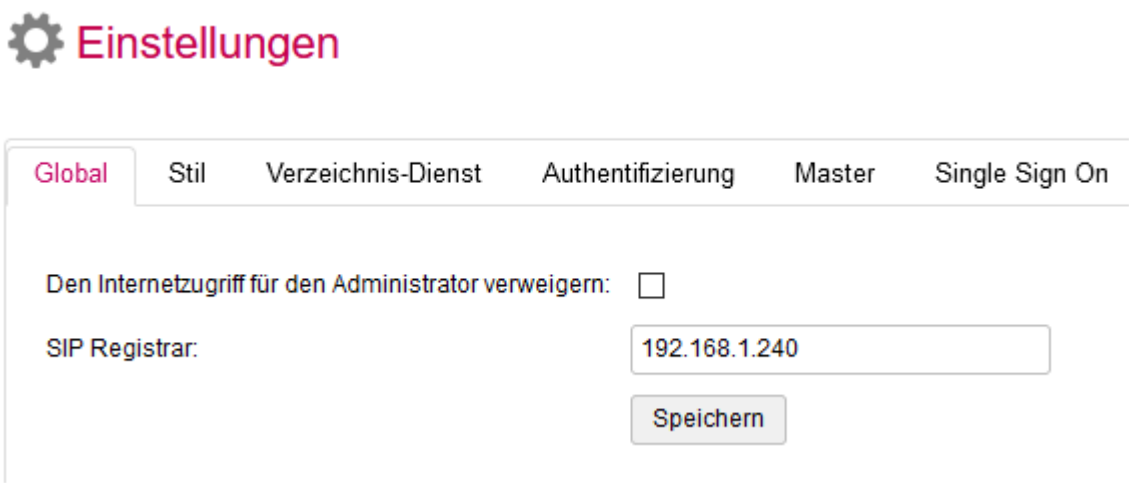
Siehe Administrator

1.2.4.6.2. Einstellungen

Hier können alle “Phone”-Einstellungen vorgenommen werden.

1.2.4.6.2.1. Global

Hier kann der Administrator-Zugriff über das Internet abgeschaltet und ein globaler SIP-Registrar konfiguriert werden.



Durch Aktivieren von “Den Internetzugriff für…” ist kein Zugriff auf den Admin-Bereich über das Internet mehr möglich, sondern nur noch über die interne IP-Adresse.
Sollten mehrere Netzwerkkarten verwendet werden (VM) bestimmt das Default-Netzwerk die IP.

Der global SIP-Registrar kann durch einen pro Benutzer konfigurierten Registrar überschrieben werden.

1.2.4.6.2.2. Stil

Hier kann das Aussehen der Benutzer-Login-Seite definiert werden.

Die Überschrift wird unter dem Logo angezeigt.

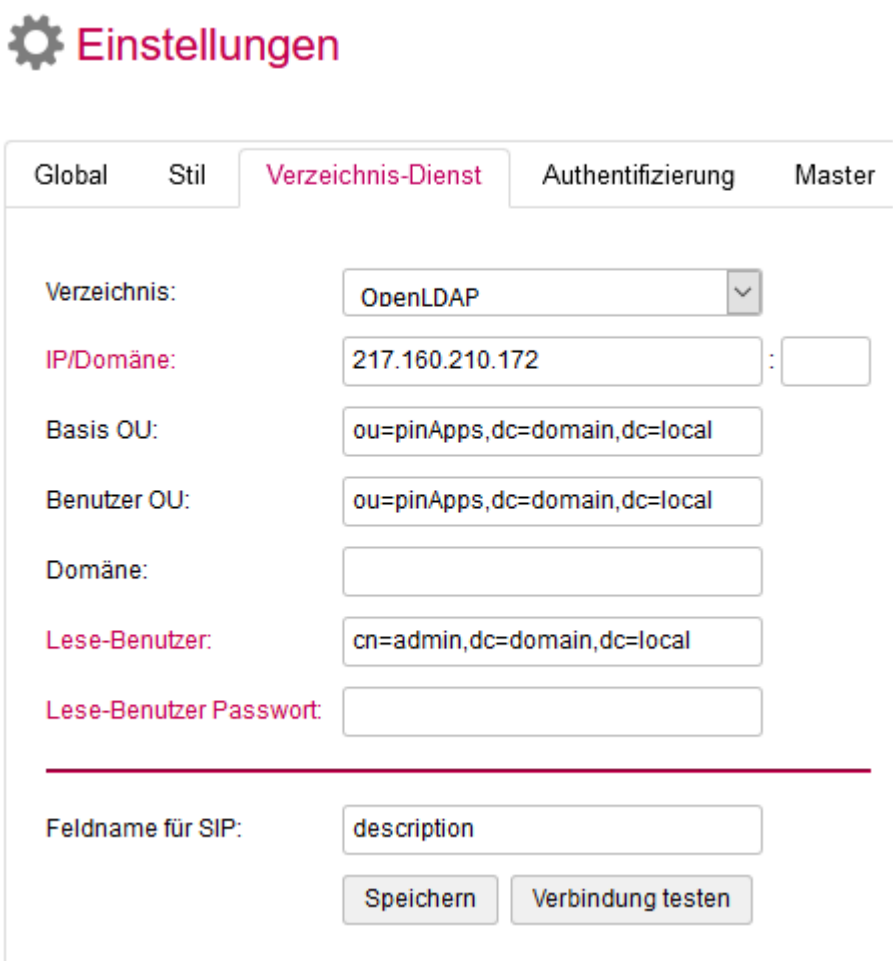
Ein entsprechendes Logo kann hier über einen absoluten Pfad angegeben werden.
Das Logo kann in “System” unter “Einstellungen” -> “Bild Upload” auf das System geladen werden.
Nach dem Hochladen wird die exakte Url angezeigt. Diese kann hier verwendet werden.

Ein Hintergrundbild kann auf dieselbe Weise wie ein Logo gesetzt werden.

Die Hintergrund-Farbe kann aus einem Farbauswahl-Dialog gesetzt werden.

1.2.4.6.2.3. Verzeichnis-Dienst

Hier kann ein Verzeichnis-Dienst für die Authentifizierung verwendet werden.
Die Parameter entsprechen denen aller anderen Workspace Anwendungen.
Die einzige Ausnahme ist das Attribut für die SIP-Konfiguration.



Wird ein Verzeichnis-Dienst verwendet, so kann die SIP-Konfiguration in einem definierbaren Feld gespeichert werden.
Dazu wird in “Feldname für SIP” der Name eines Attributes im Verzeichnisdienst angegeben.

Die SIP-Konfiguration umfasst den Registrar, ein Login/Kennung und ein Passwort.
Diese Informationen stellt die Telefonanlage zur Verfügung.

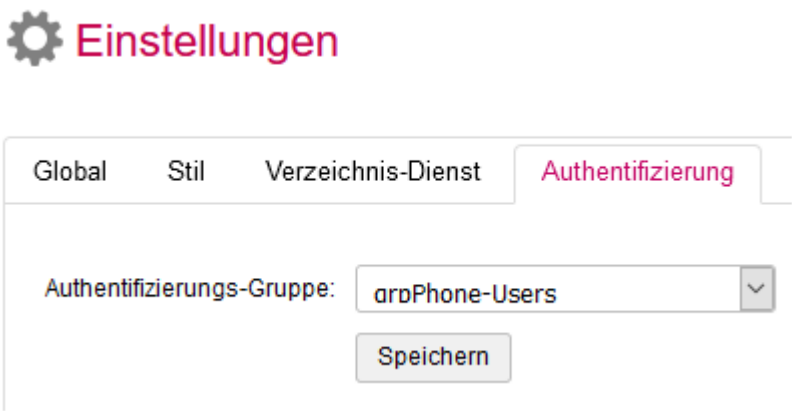
Die Werte müssen im JSON-Format angegeben werden.

{ “Registrar”: “192.168.1.240”, “Login”: “e94633”, “Password”: “8345199” }

Das Feld “Registrar” kann leer sein, wenn unter Einstellungen -> Global -> SIP Registrar ein globaler Registrar konfiguriert wurde.

1.2.4.6.2.4. Authentifizierung

Über die Authentifizierungs-Gruppe wird die Verzeichnis-Gruppe ausgewählt, in welcher sich der Benutzer befinden muss.



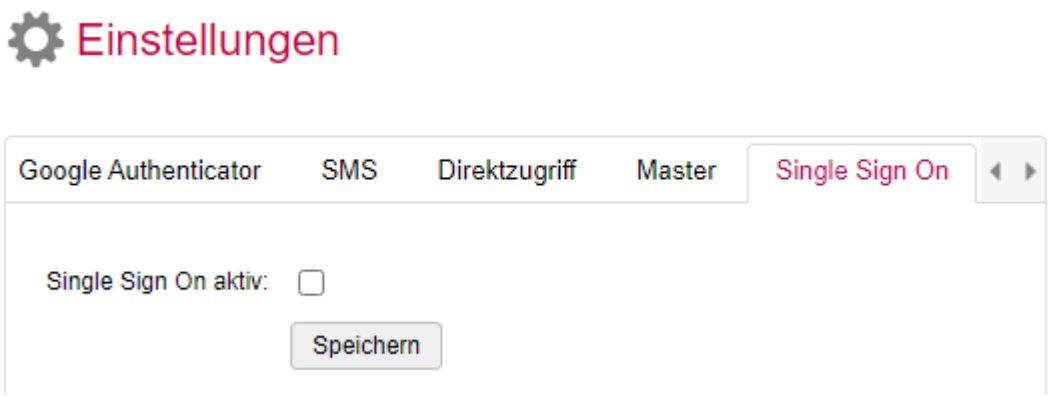
1.2.4.6.2.5. Master

Bei mehreren VM’s gibt es immer einen Master, auf welchem “System” und “Applications” laufen.

Die Master-IP muss dann hier angegeben werden.

1.2.4.6.2.6. Single Sign ON

Wird das Pintexx Workplace “Cockpit” verwendet, so kann hier das Single Sign On aktiviert werden.



Allerdings muss SSO auch im Cockpit-Admin für “Remote” aktiviert werden.
Ist SSO aktiviert, ist eine Benutzer-Anmeldung nur noch über das Cockpit möglich.

1.2.4.6.2.7. Backup

Siehe Backup

1.2.4.6.2.8. Info

Siehe Info

1.2.4.6.3. Ereignisse

Siehe Ereignisse

1.2.5. Workplace “Contacts”

1.2.5.1. Aufruf

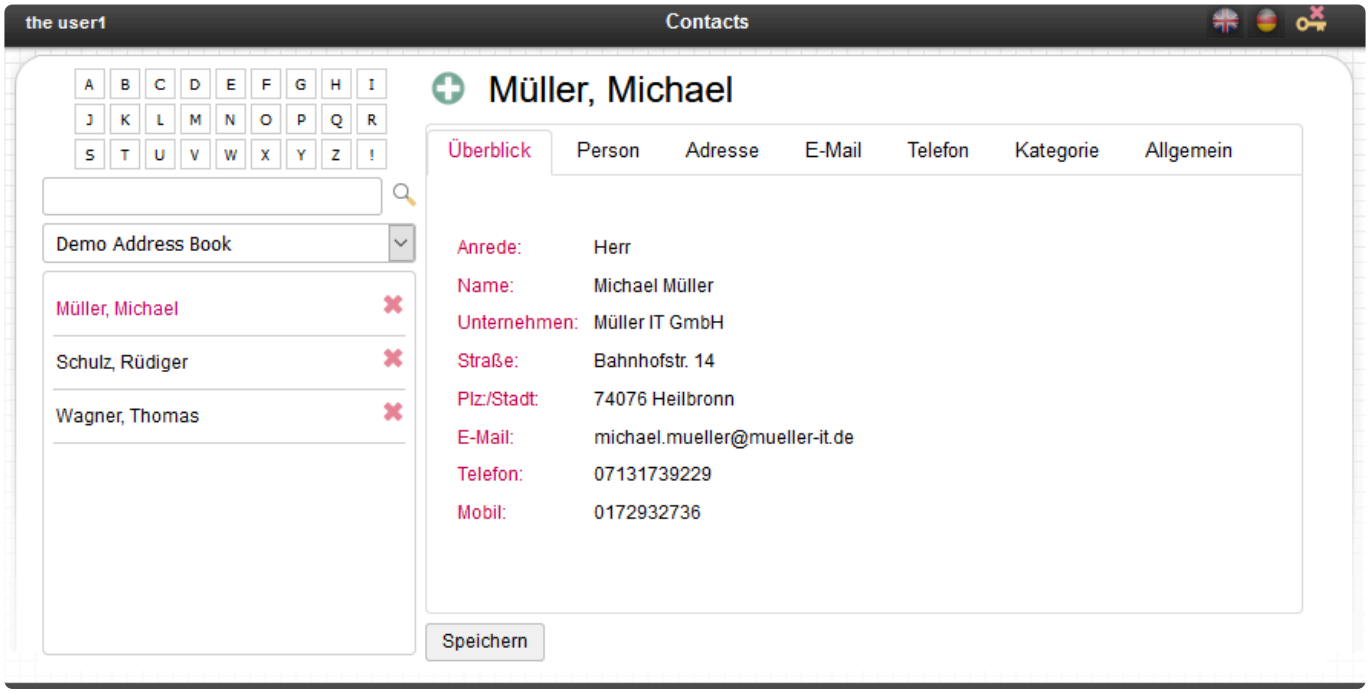
“Contacts” hat 2 Zugänge, einen für den Administrator und einen für den Benutzer.

Benutzer:
<IP/Domäne>/contacts

Administrator:
<IP/Domäne>/contacts/adminlogin

1.2.5.2. Benutzer-Bereich

Der Benutzer-Bereich umfasst den Auswählbereich und den Datenbereich.



1.2.5.2.1. Auswahl-Bereich

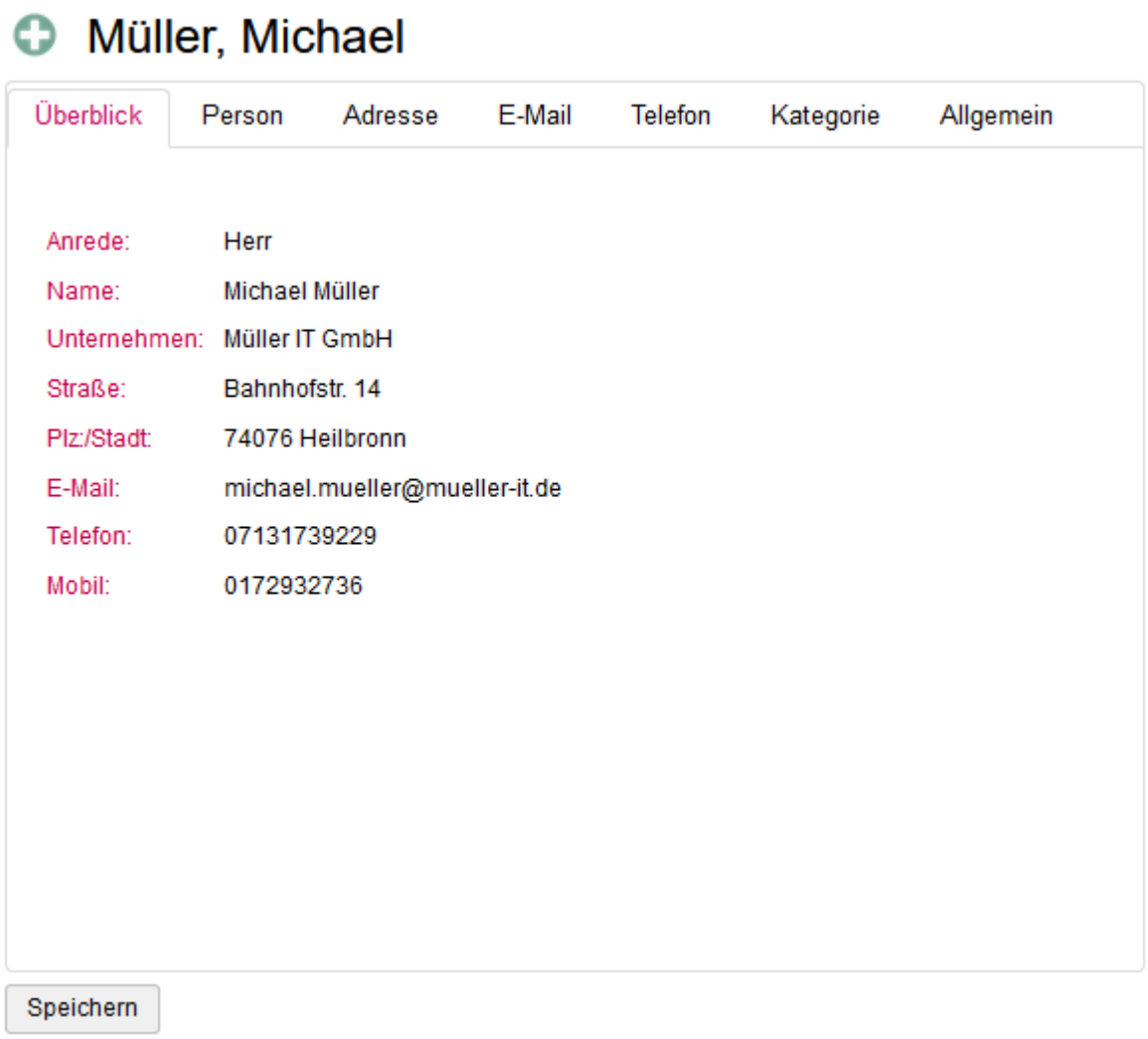
Der Auswahl-Bereich umfasst die Detail-Suche, die Adressbuch-Auswahl und die Kontakt-Liste.

1.2.5.2.2. Daten-Bereich

Im Daten-Bereich können die Daten des Adressbuchs in Abhängigkeit der Rechte verwaltet werden.

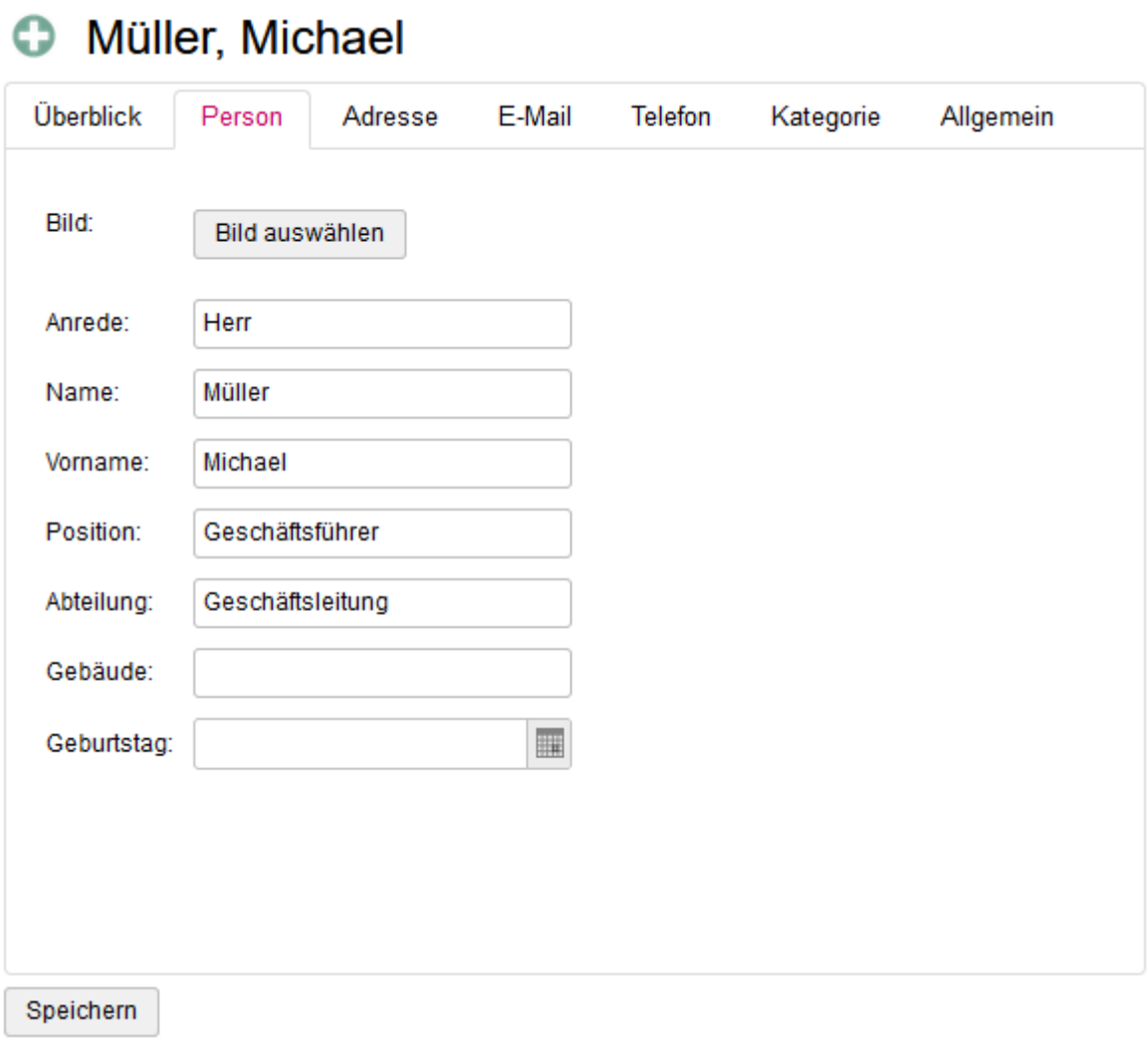
1.2.5.2.2.1. Überblick

Der Überblick-Bereich zeigt die wichtigsten Adress-Daten an:



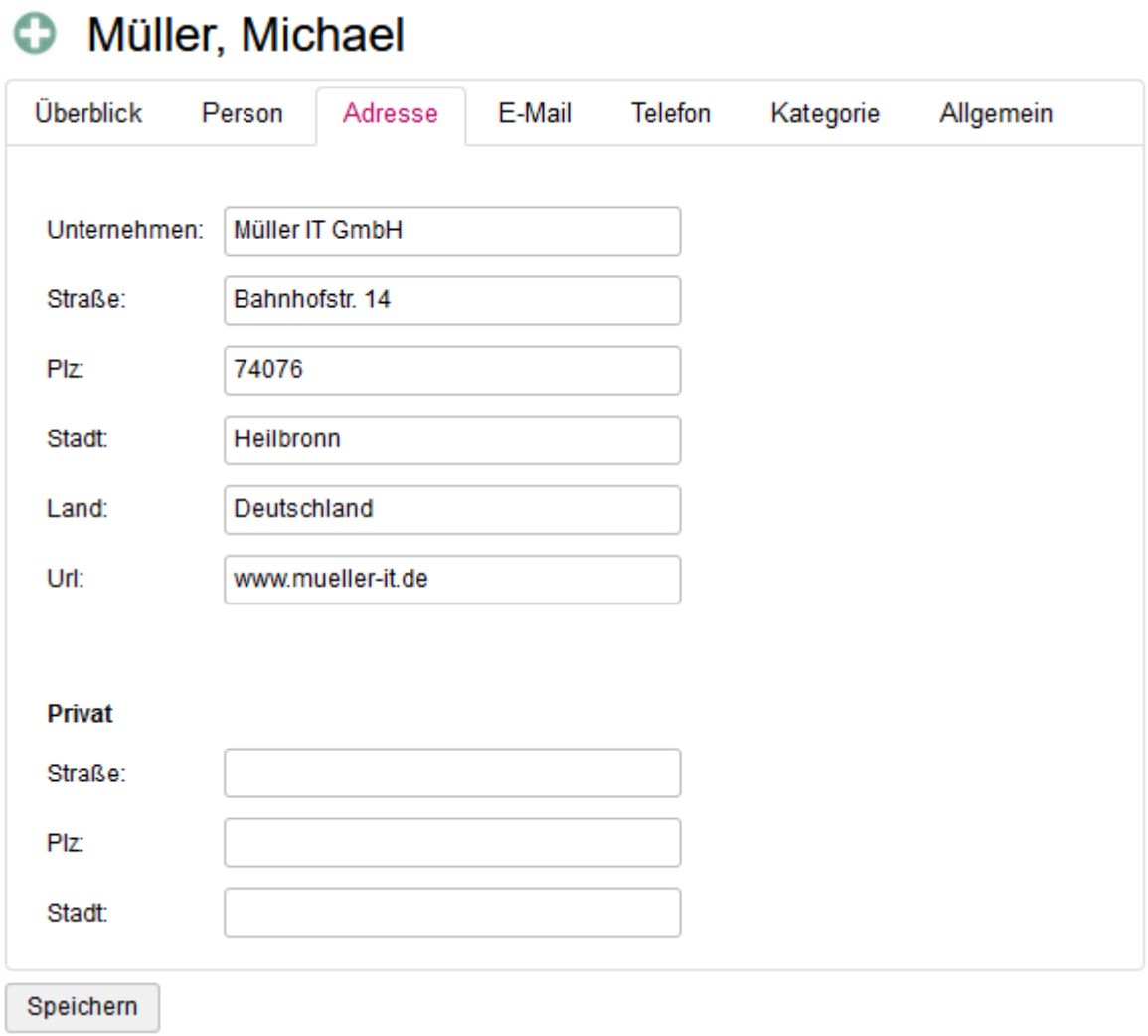
1.2.5.2.2.2. Person

Im Personenbereich können personenbezogene Daten verwaltet werden:



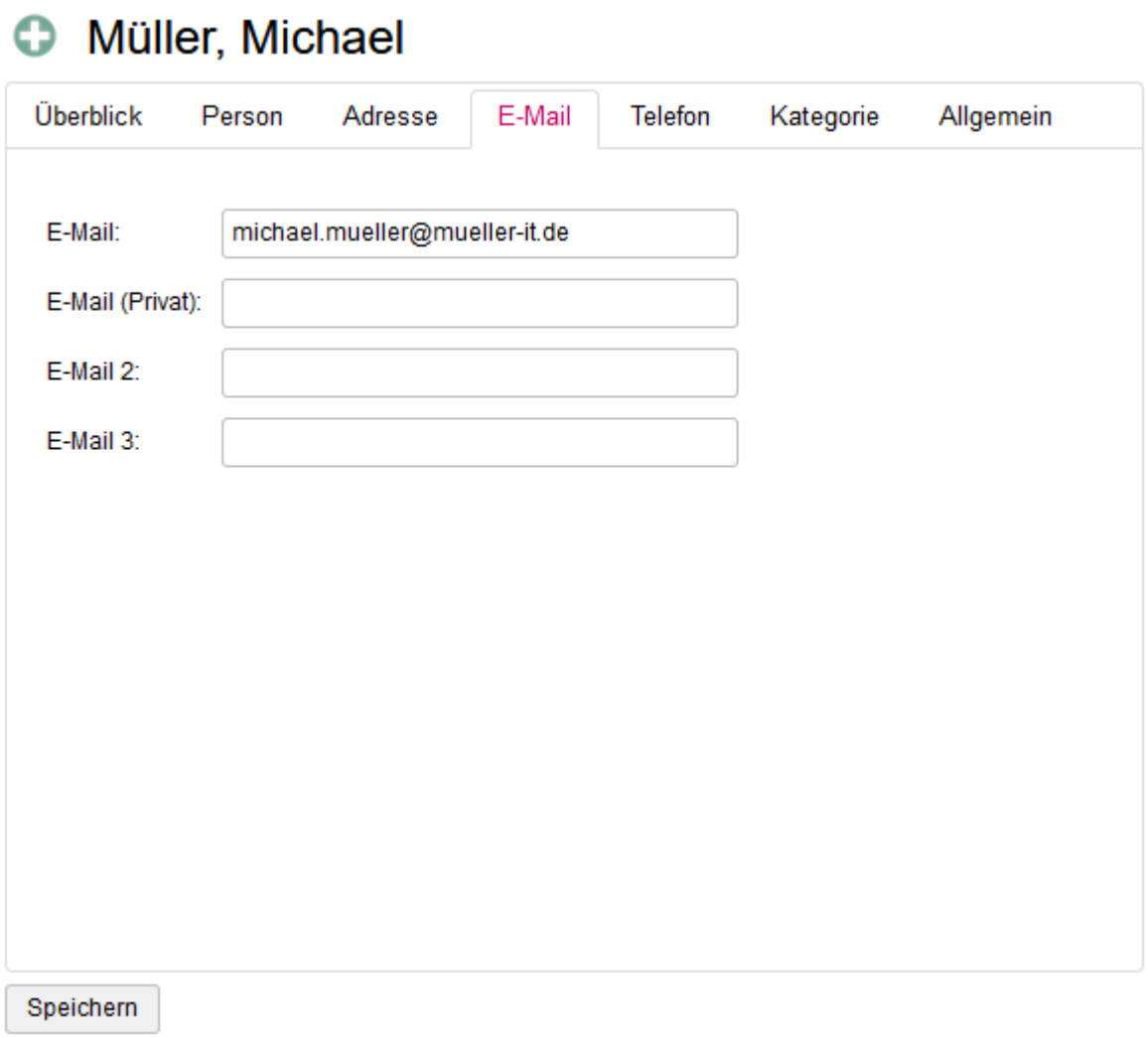
1.2.5.2.2.3. Adresse

Im Adress-Bereich können Adress-Daten verwaltet werden:



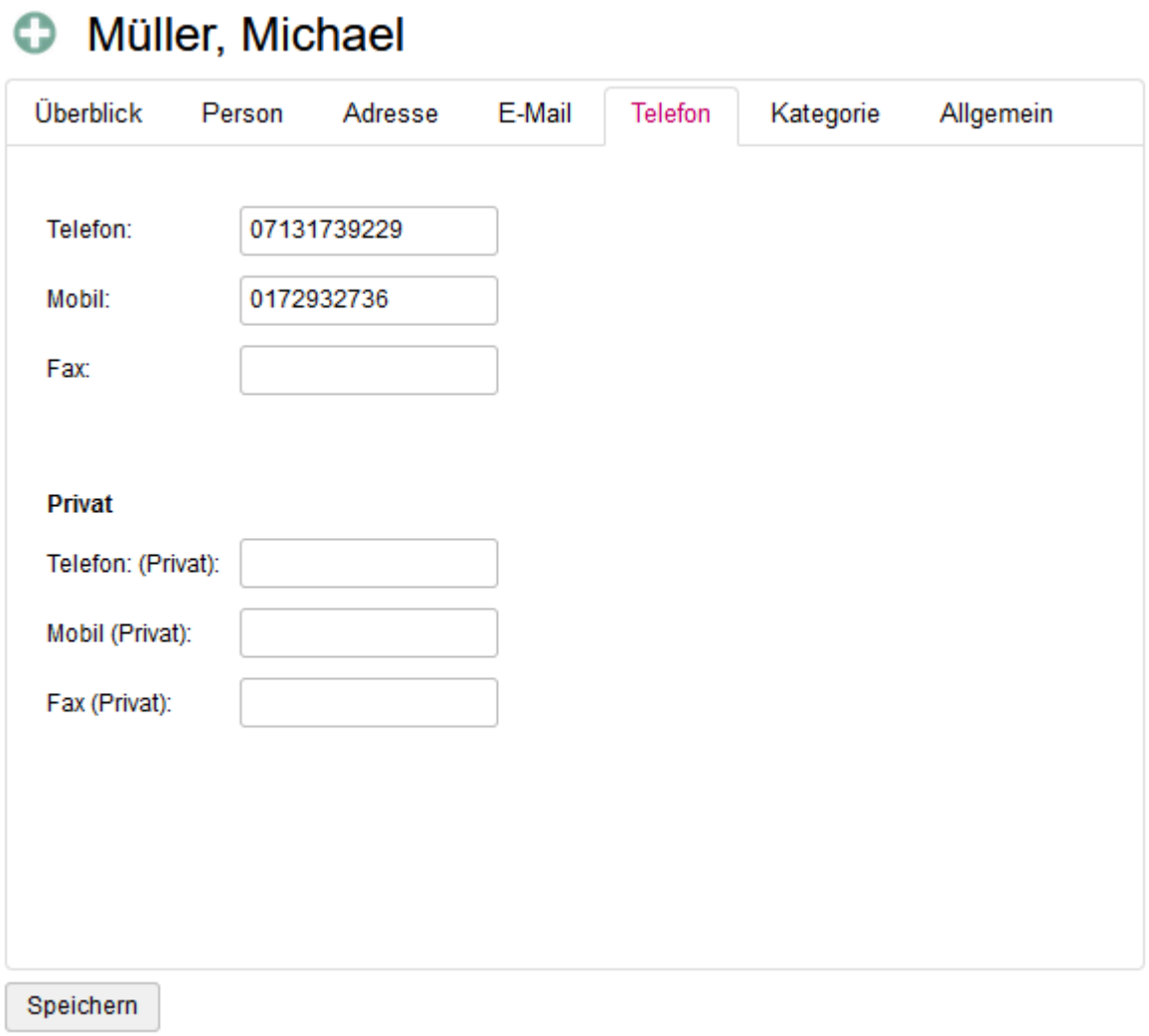
1.2.5.2.2.4. E-Mail

Im E-Mail-Bereich können E-Mails verwaltet werden:



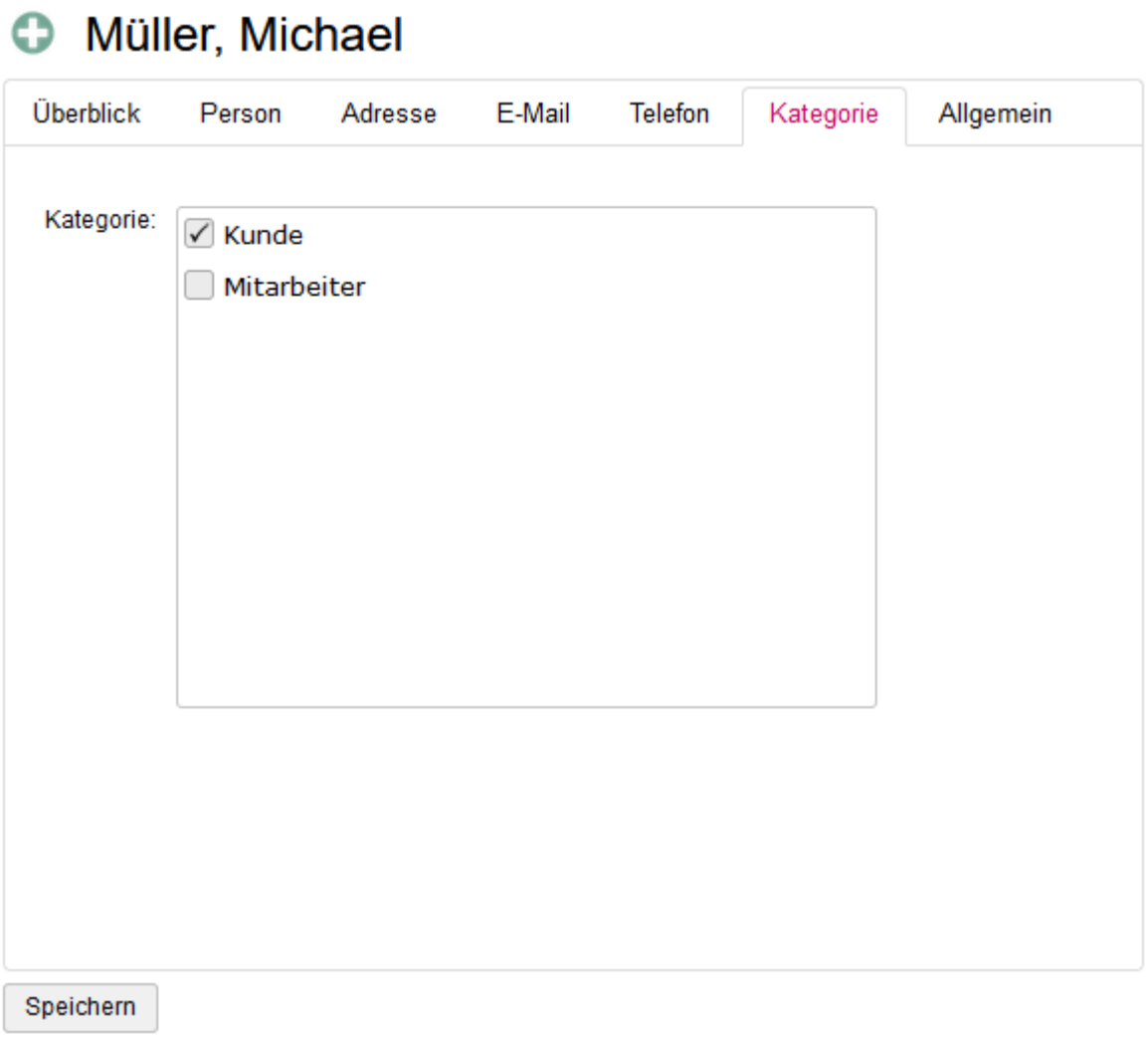
1.2.5.2.2.5. Telefon

Im Telefon-Bereich können Telefon-Daten verwaltet werden:



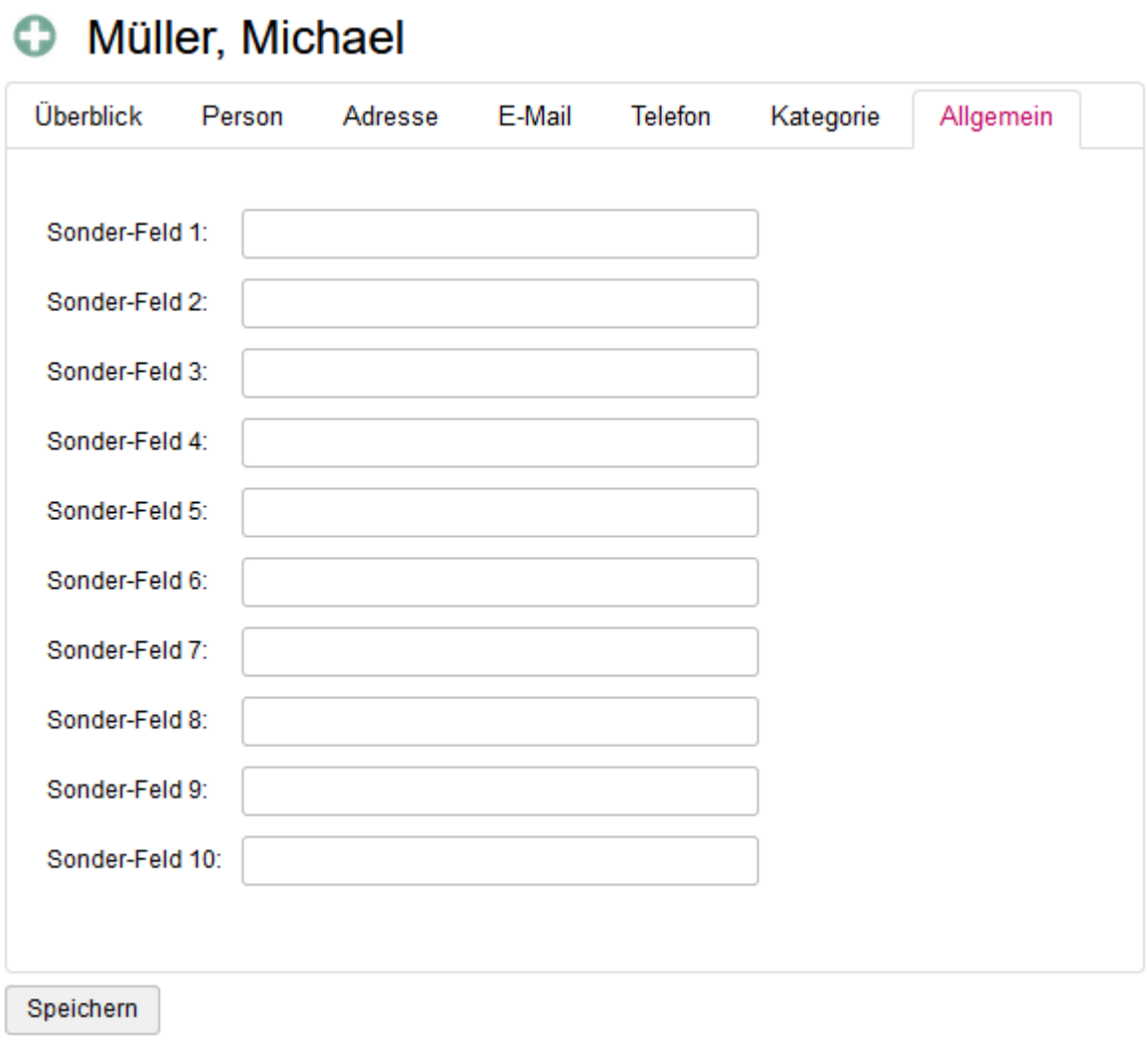
1.2.5.2.2.6. Kategorie

Im Kategorie-Bereich können Kategorien zugeordnet werden:



1.2.5.2.2.7. Allgemein

Im Allgemein-Bereich können individuelle Informationen verwaltet werden:

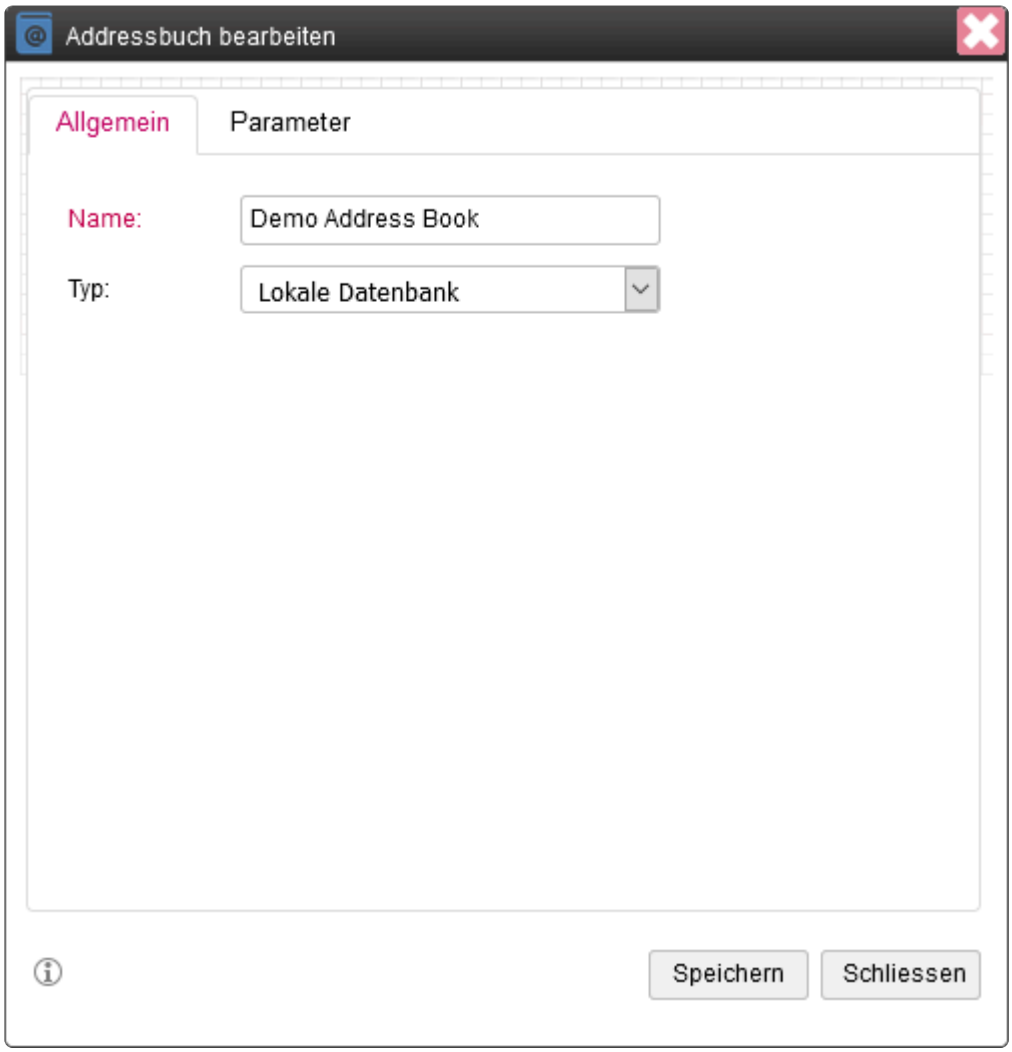


1.2.5.3. Admin-Bereich

1.2.5.3.1. Adressbücher

1.2.5.3.1.1. Datenbank

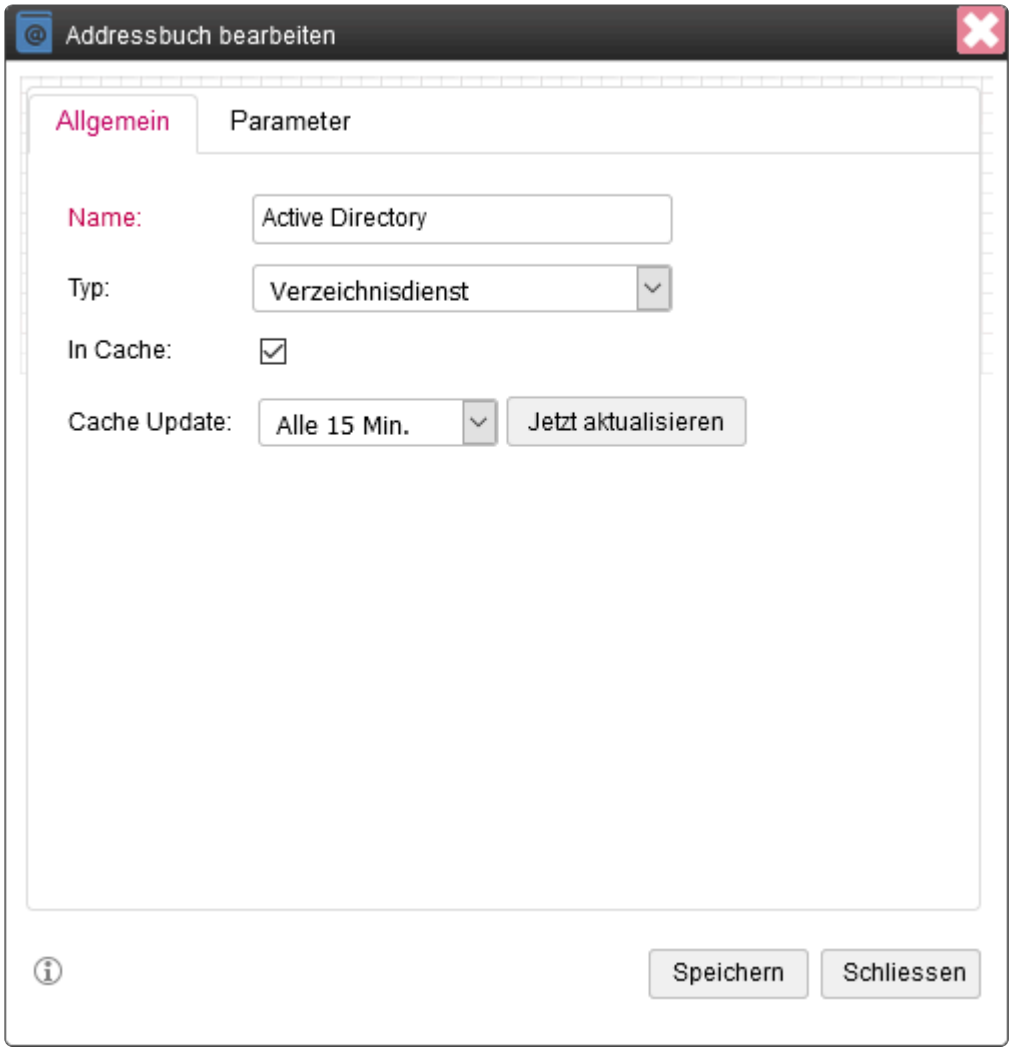
Ein Adressbuch kann über das System erstellt werden und wird lokal in einer Datenbank gespeichert. Es können nahezu beliebig viele Adressbücher angelegt werden.



Als Parameter ist nur der Name des Adressbuchs notwendig.

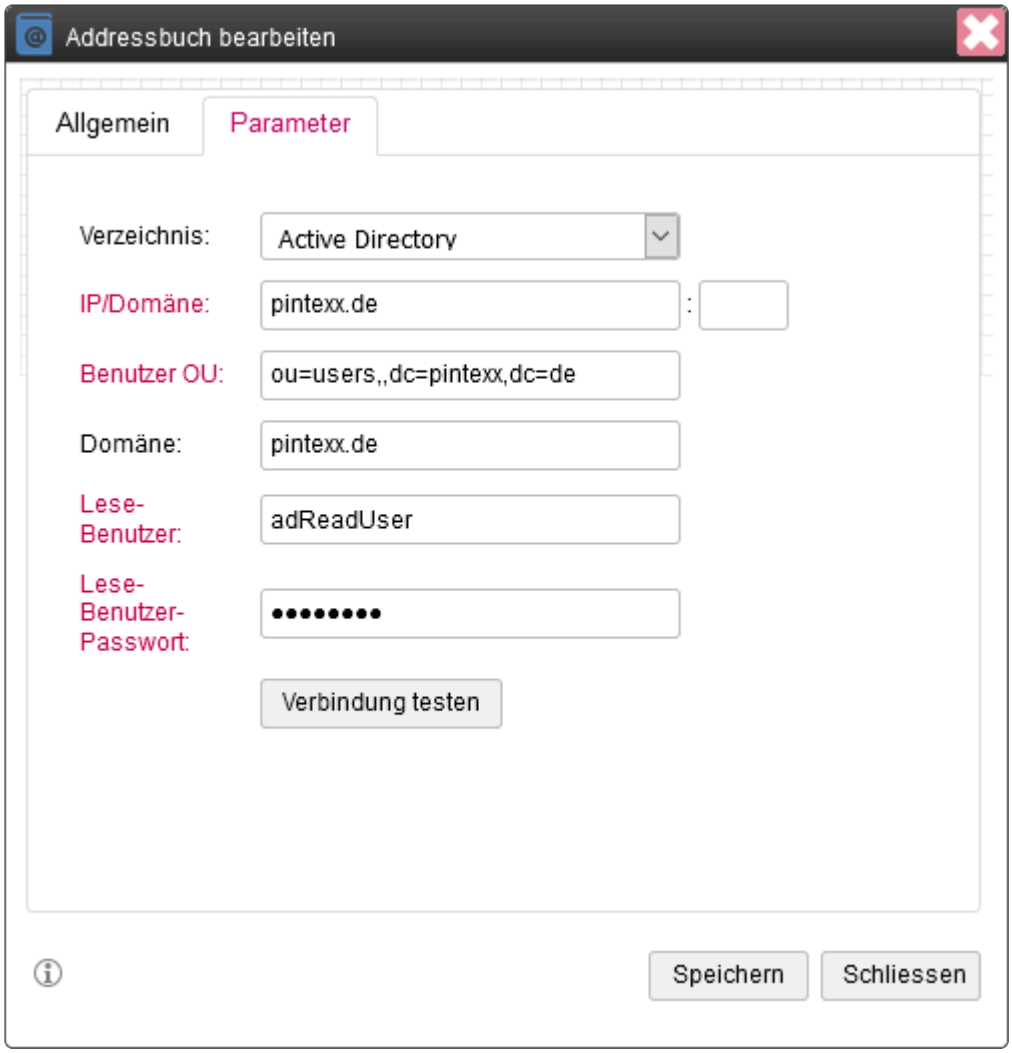
1.2.5.3.1.2. Verzeichnisdienst

Ein Adressbuch kann auch über einen Verzeichnisdienst wie Active Directory oder LDAP erstellt werden.



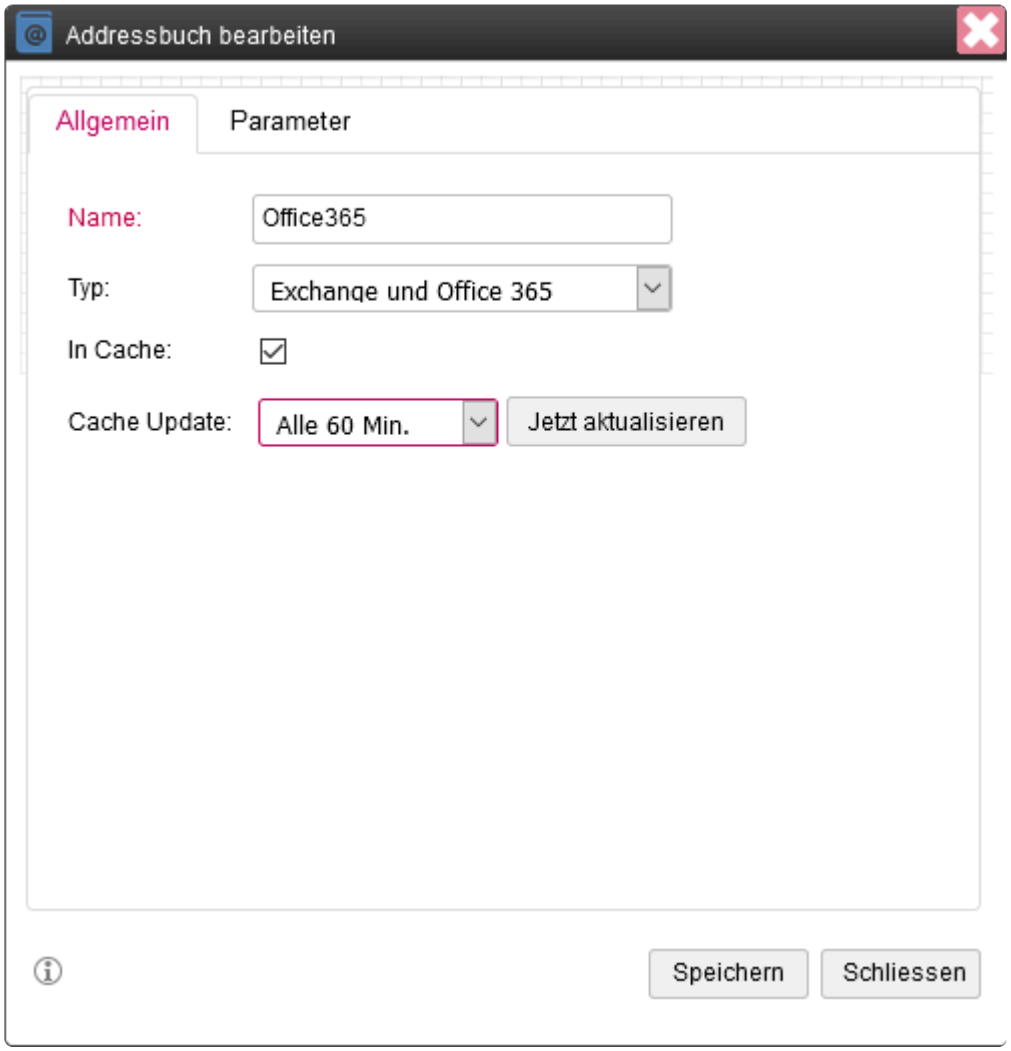
Das Adressbuch kann gecacht (empfohlen) und nach auswählbarer Zeit aktualisiert werden.

Für den Abruf der Daten müssen folgende Parameter konfiguriert werden:


Addressbuch bearbeiten
Allgemein
Parameter
Verzeichnis:
Active Directory
IP/Domäne:
pintexx.de
Benutzer OU:
ou=users,,dc=pintexx,dc=de
Domäne:
pintexx.de
Lese-Benutzer:
adReadUser
Lese-Benutzer-Passwort:
Verbindung testen
Speichern
Schliessen

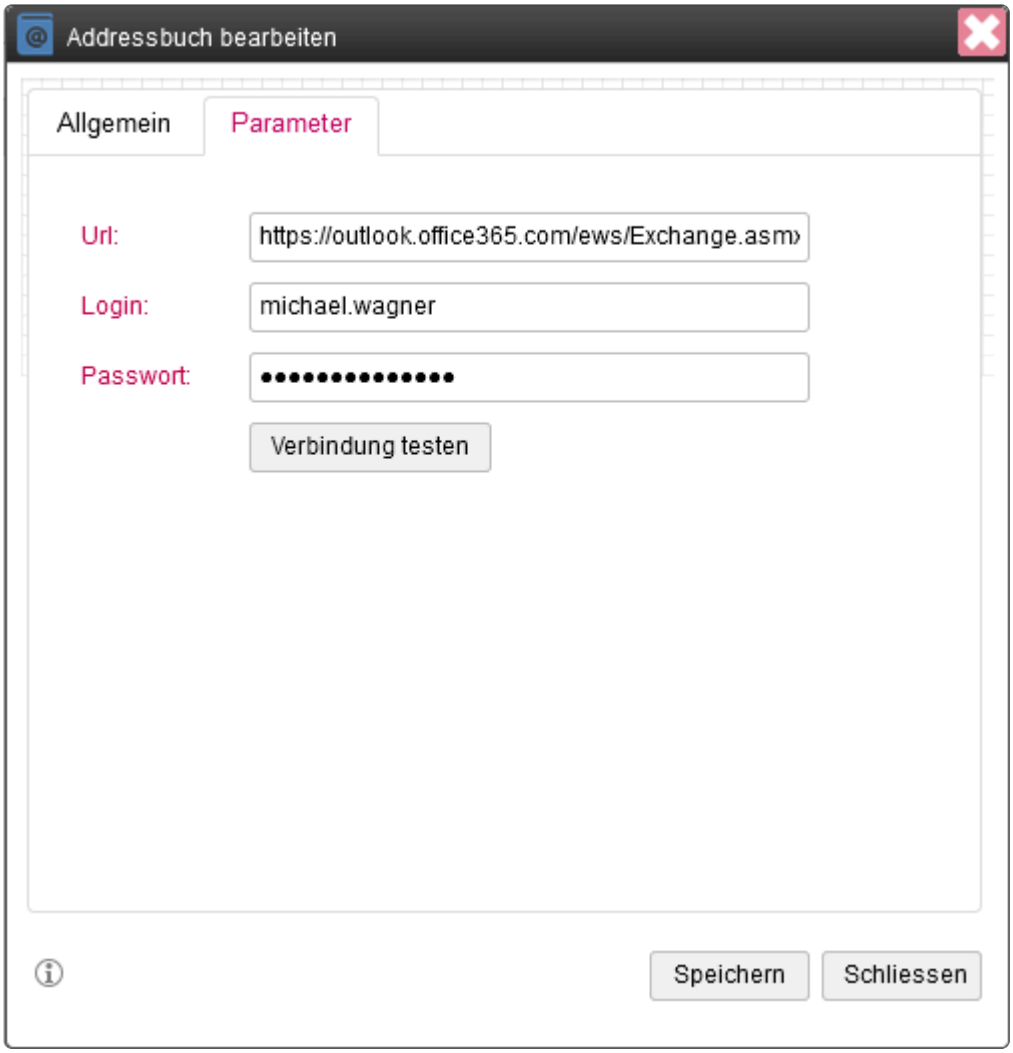
1.2.5.3.1.3. Exchange/Office365

Ein Adressbuch kann auch über Exchange/Office365 erstellt werden.



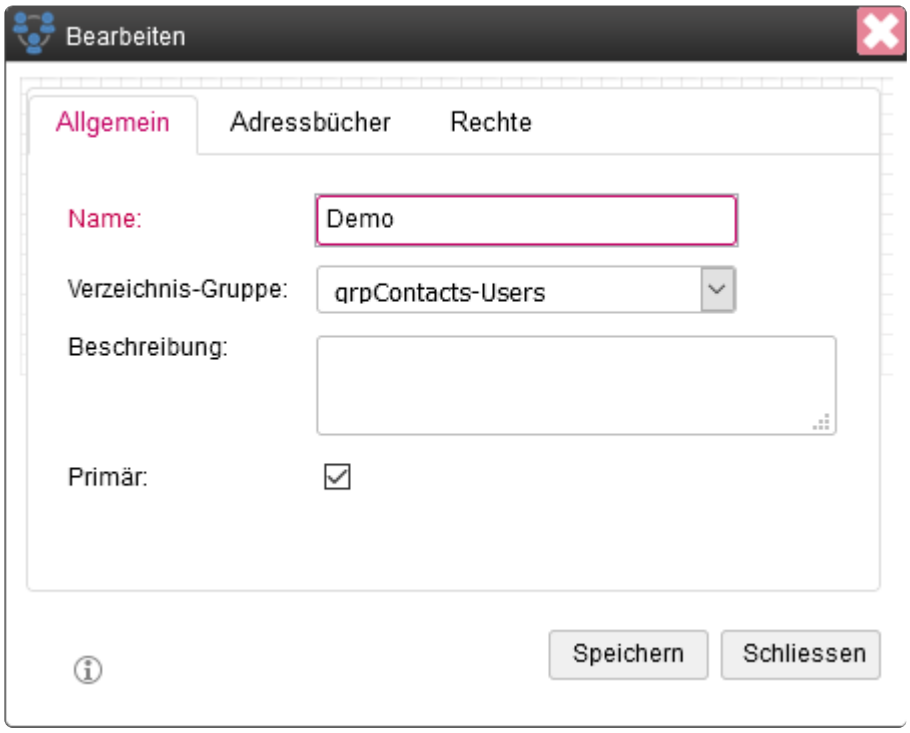
Das Adressbuch kann gecacht (empfohlen) und nach auswählbarer Zeit aktualisiert werden.

Für den Abruf der Daten müssen folgende Parameter konfiguriert werden:

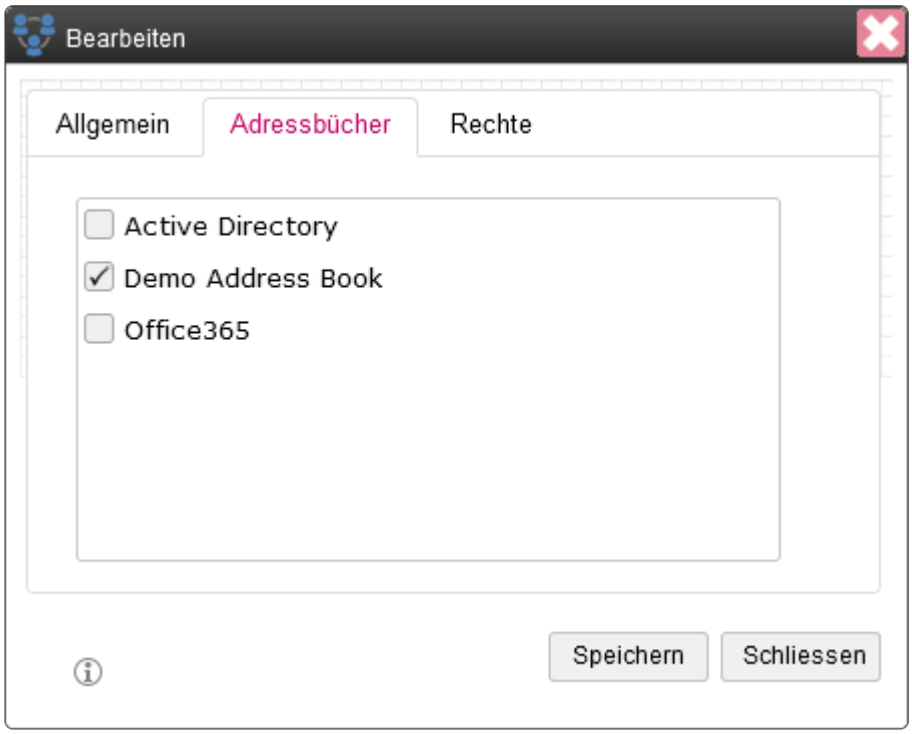

Addressbuch bearbeiten
Allgemein
Parameter
Url:
https://outlook.office365.com/ews/Exchange.asm›
Login:
michael.wagner
Passwort:
Verbindung testen
Speichern
Schliessen

1.2.5.3.2. Gruppen

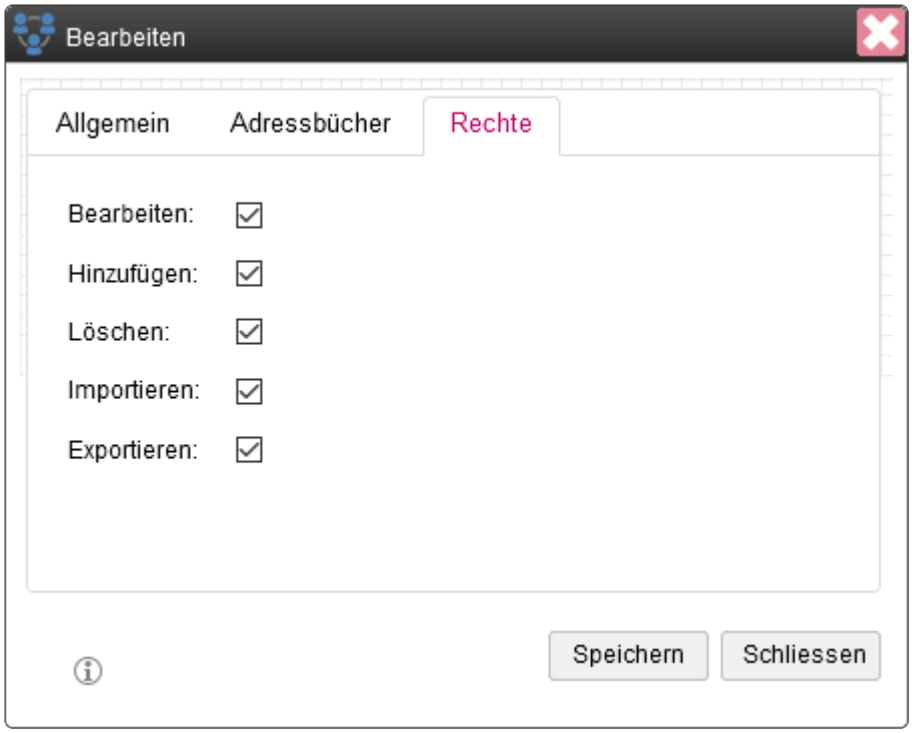
Eine Gruppe umfasst eine Menge an Benutzern, welche über eine Verzeichnisgruppe definiert werden. Alle Gruppenmitglieder erhalten die Gruppenrechte bzw. die der Gruppe zugeordneten Adressbücher.



Jedes Adressbuch kann einer Gruppe zugeordnet werden:

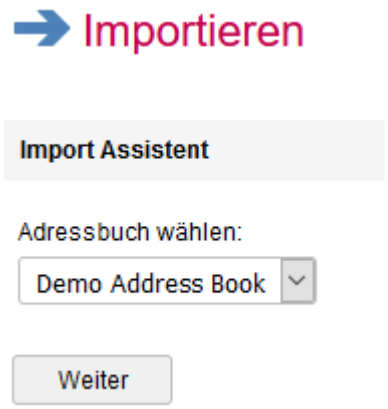


Hier können die Gruppenrechte definiert werden:


Bearbeiten
Allgemein
Adressbücher
Rechte
Bearbeiten:
Hinzufügen:
Löschen:
Importieren:
Exportieren:
Speichern
Schliessen

1.2.5.3.3. Importieren

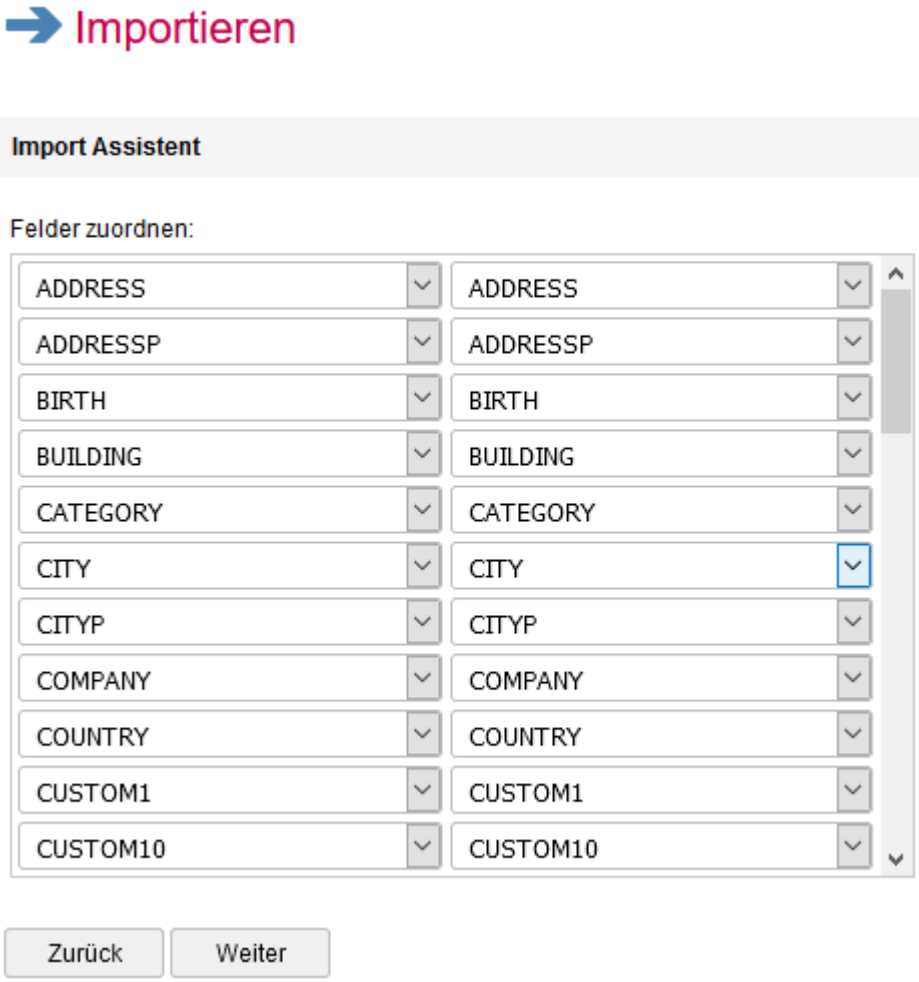
In bestehende Adressbücher können Daten durch externe Dateien importiert werden.
Zuerst muss dazu das Adressbuch ausgewählt werden:



Dann kann der Datei-Typ und das Trennkennzeichen ausgewählt werden:

Dann wird die Import-Datei ausgewählt:

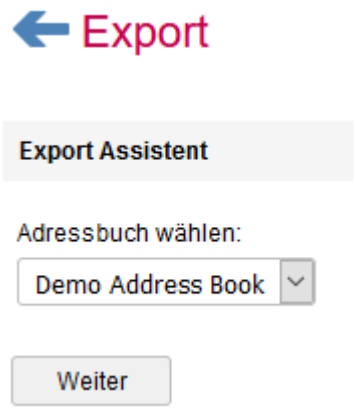
Dann können die Felder den internen Feldern zugeordnet werden:



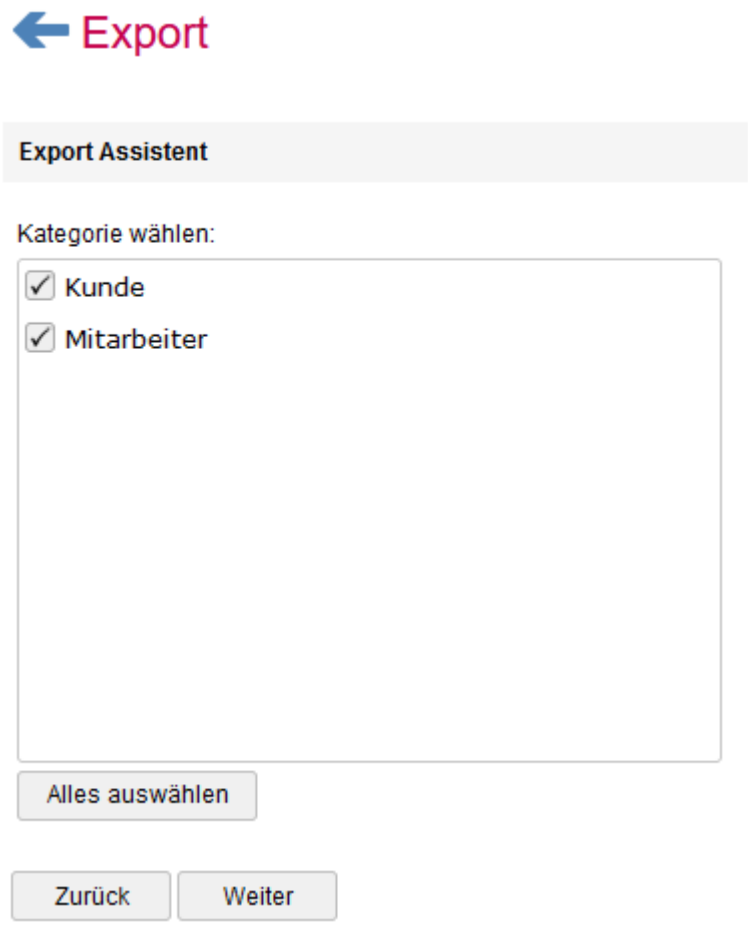
Dann kann der Import-Prozess gestaret werden:

1.2.5.3.4. Export

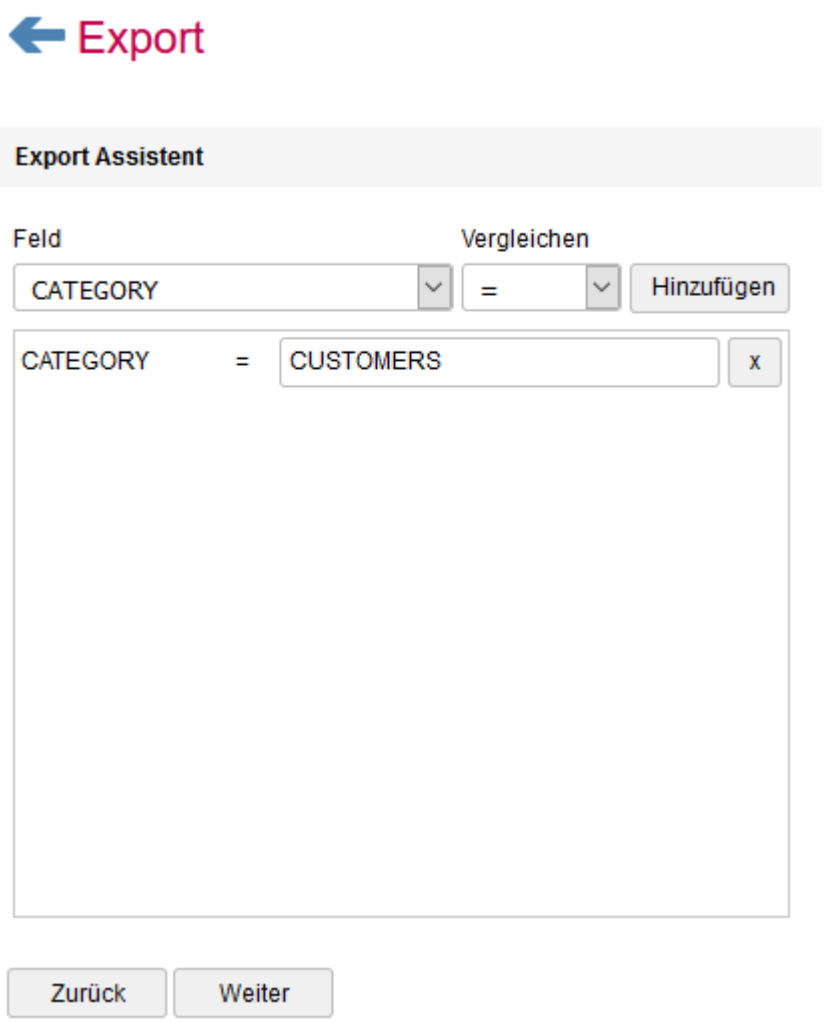
Jedes Adressbuch kann in eine (Text)-Datei exportiert werden.
Dazu muss zunächst das Adressbuch ausgewählt werden:



Dann kann die Kategorie ausgewählt werden:



Dann erfolgt die Feldauswahl:



Letztendlich kann der Datei-Typ und das Trennzeichen ausgewählt und der Export gestartet werden:

1.2.5.3.5. Administrator

Siehe Administrator

1.2.5.3.6. Einstellungen

Hier können alle “Contacts”-Einstellungen vorgenommen werden.

1.2.5.3.6.1. Global

Hier kann der Zugriff auf den Admin-Bereich konfiguriert werden.

1.2.5.3.6.2. Stil

Hier kann das Aussehen der Benutzer-Login-Seite definiert werden.

Die Überschrift wird unter dem Logo angezeigt.

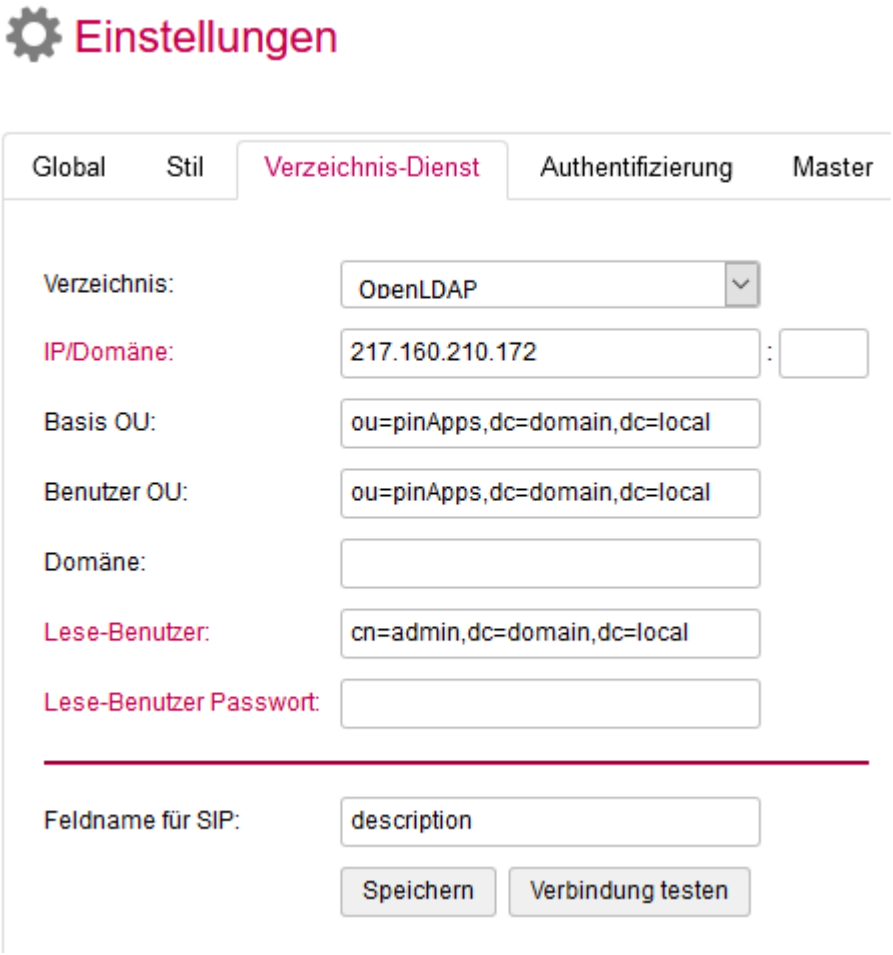
Ein entsprechendes Logo kann hier über einen absoluten Pfad angegeben werden.
Das Logo kann in “System” unter “Einstellungen” -> “Bild Upload” auf das System geladen werden.
Nach dem Hochladen wird die exakte Url angezeigt. Diese kann hier verwendet werden.

Ein Hintergrundbild kann auf dieselbe Weise wie ein Logo gesetzt werden.

Die Hintergrund-Farbe kann aus einem Farbauswahl-Dialog gesetzt werden.

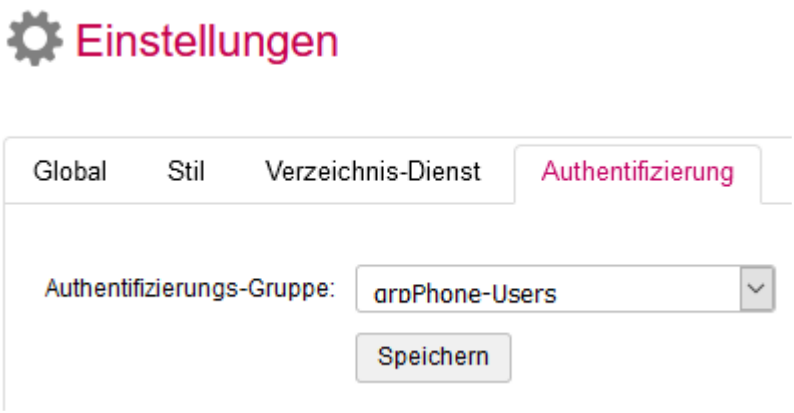
1.2.5.3.6.3. Verzeichnis

Hier kann ein Verzeichnis-Dienst für die Authentifizierung verwendet werden.
Die Parameter entsprechen denen aller anderen Workspace Anwendungen.



1.2.5.3.6.4. Authentifizierung

Über die Authentifizierungs-Gruppe wird die Verzeichnis-Gruppe ausgewählt, in welcher sich der Benutzer befinden muss.



1.2.5.3.6.5. Kategorien

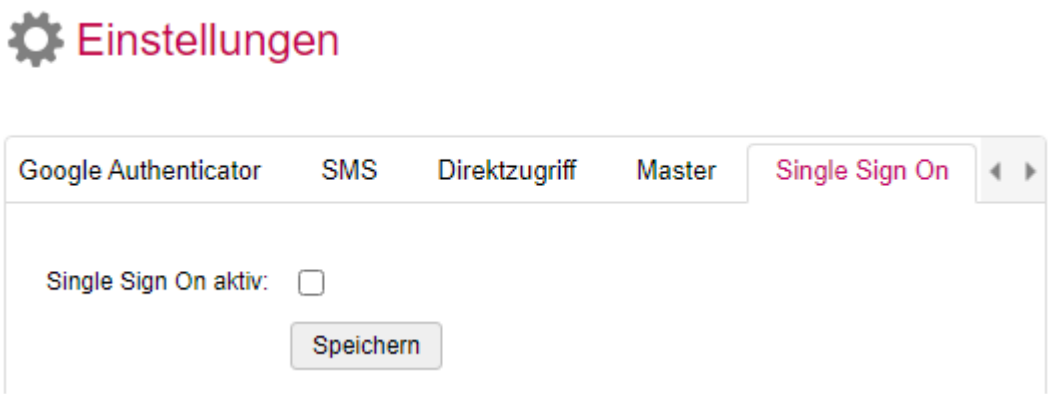
1.2.5.3.6.6. Master

Bei mehreren VM’s gibt es immer einen Master, auf welchem “System” und “Applications” laufen.

Die Master-IP muss dann hier angegeben werden.

1.2.5.3.6.7. Single Sign On

Wird das Pintexx Workplace “Cockpit” verwendet, so kann hier das Single Sign On aktiviert werden.



Allerdings muss SSO auch im Cockpit-Admin für “Remote” aktiviert werden.
Ist SSO aktiviert, ist eine Benutzer-Anmeldung nur noch über das Cockpit möglich.

1.2.5.3.6.8. Backup

Siehe Backup

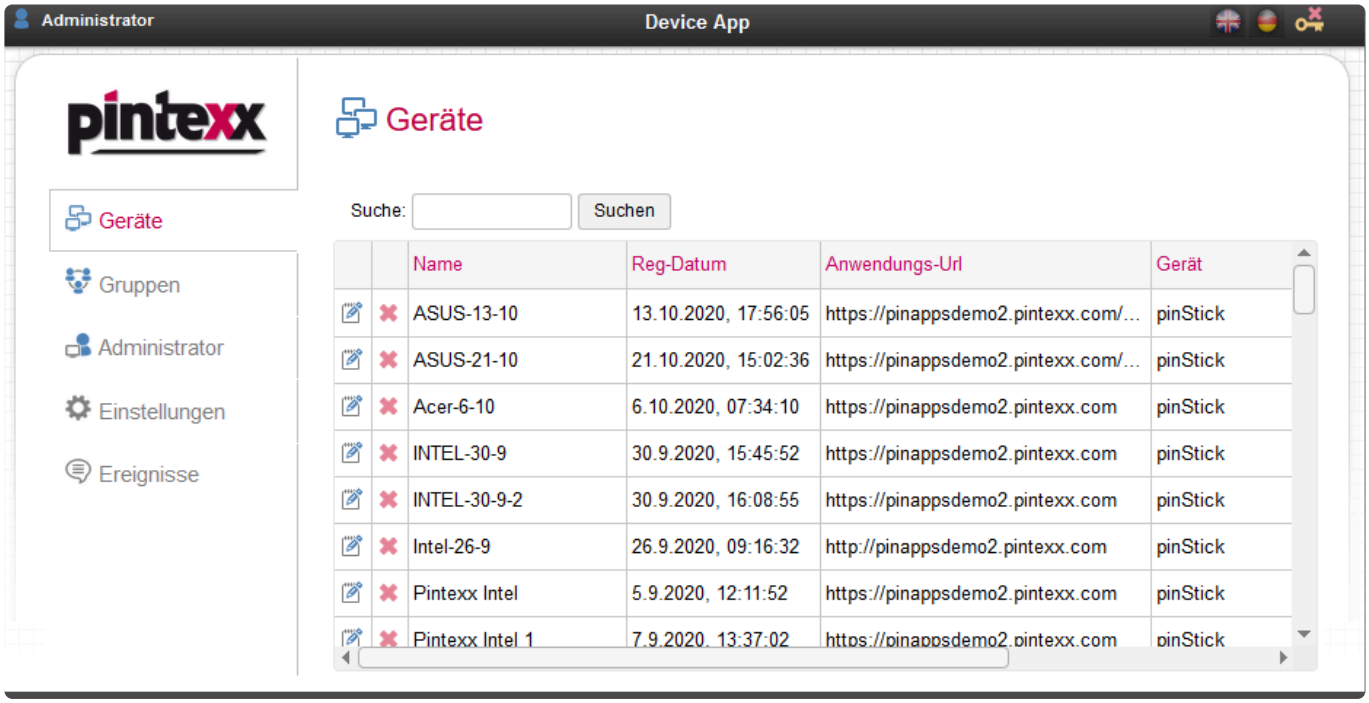
1.2.5.3.6.9. Info

Siehe Info

1.2.5.3.7. Ereignisse

Siehe Ereignisse

1.2.6. Workplace “Device”



1.2.6.1. Aufruf

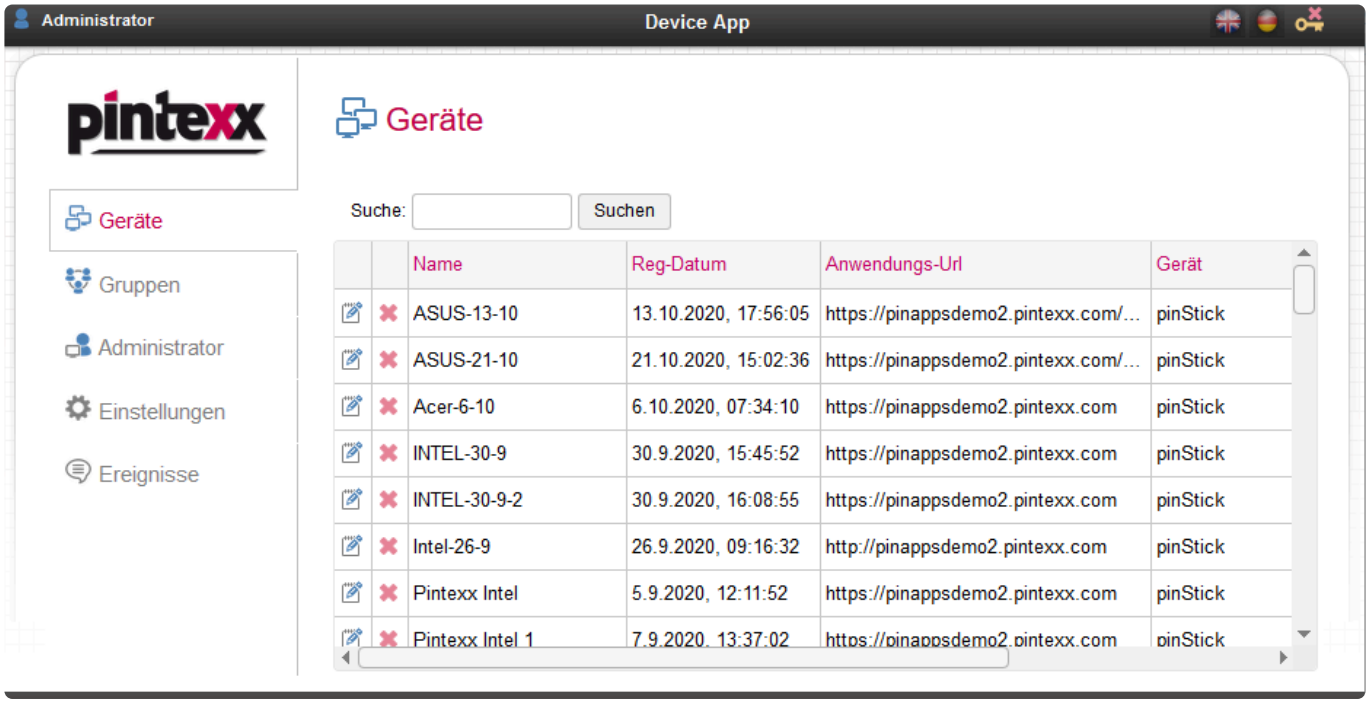
“Device” kann direkt über folgende Url aufgerufen werden:

<IP/Domäne>/device

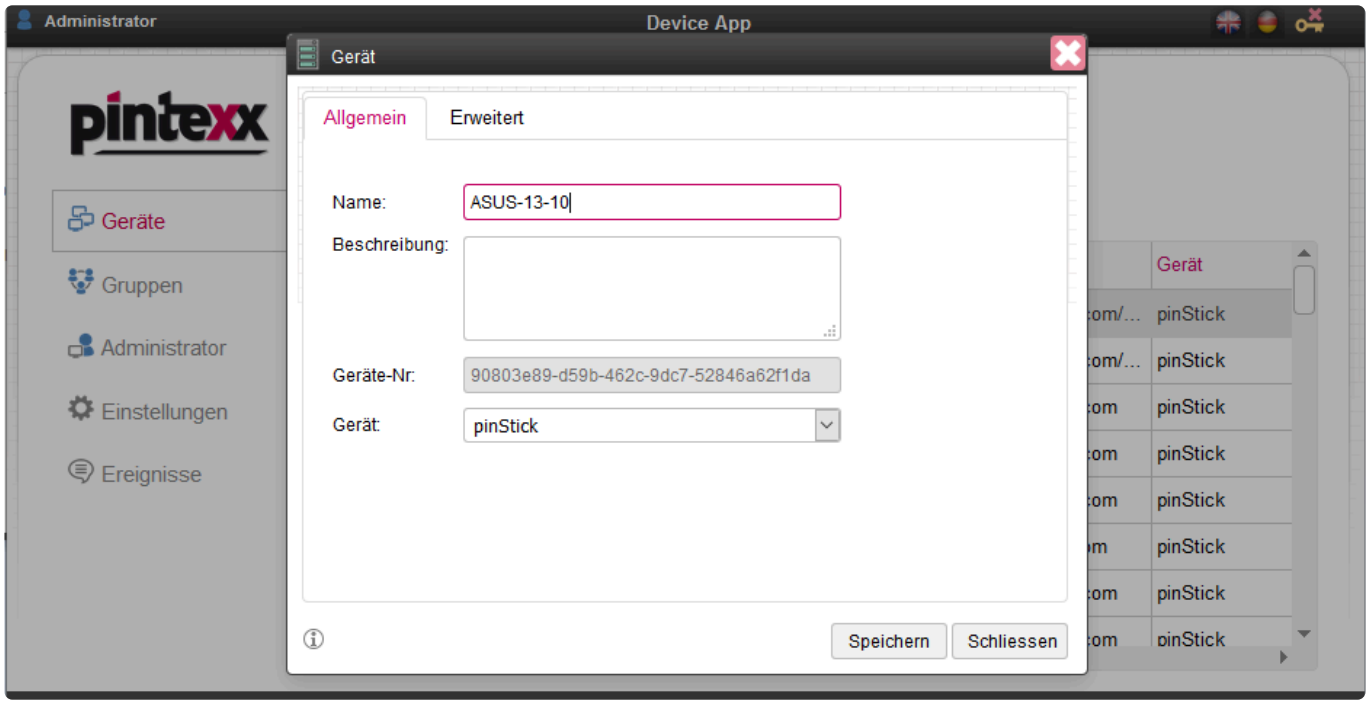
“Device” hat nur einen Administrator-Zugang.

1.2.6.2. Geräteverwaltung

Wird ein Gerät registriert, dann erscheint es in der Auflistung der Geräteverwaltung.



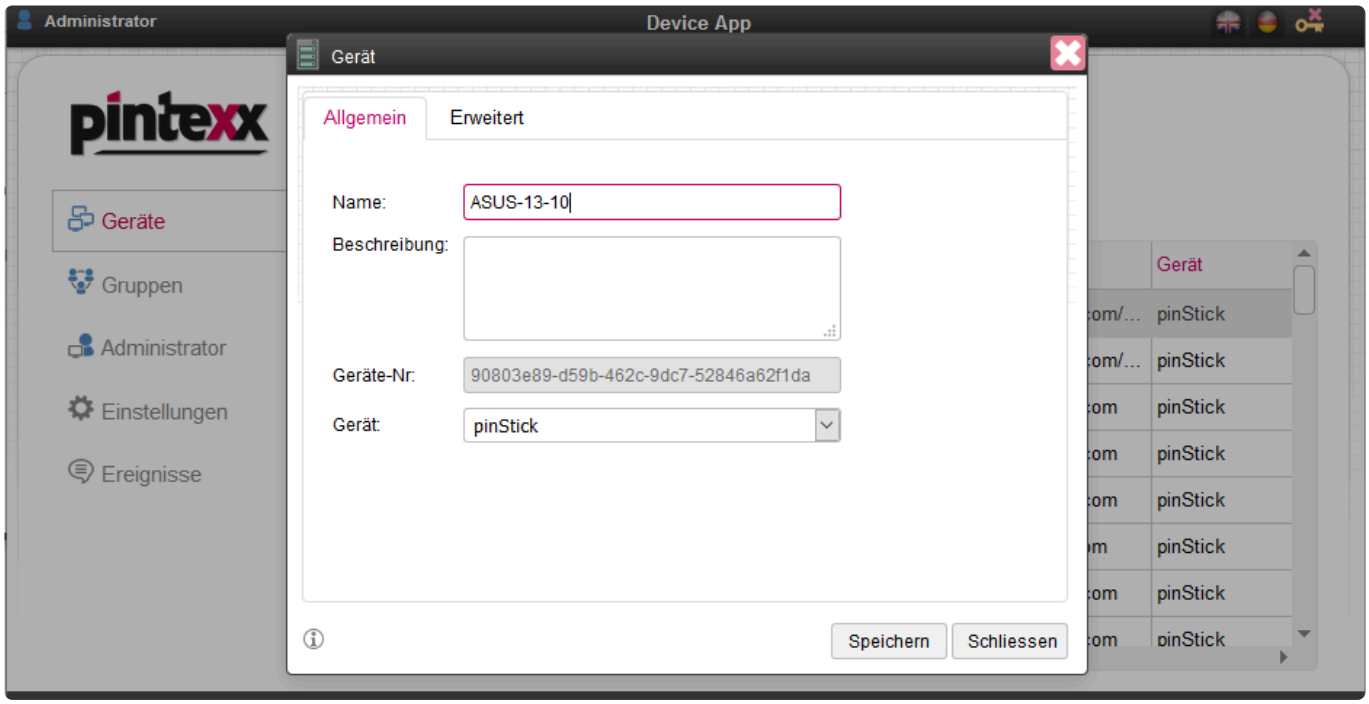
Von dort aus können die Eigenschaften des Gerätes eingestellt werden.



Geräte-Eigenschaften “Allgemein”:

Name	Ein beliebiger Geräte-Name
Beschreibung	Die Beschreibung des Gerätes

Geräte-Nummer	Eindeutige Geräte-Nummer
Geräte-Typ	Der spezifische Typ des Gerätes

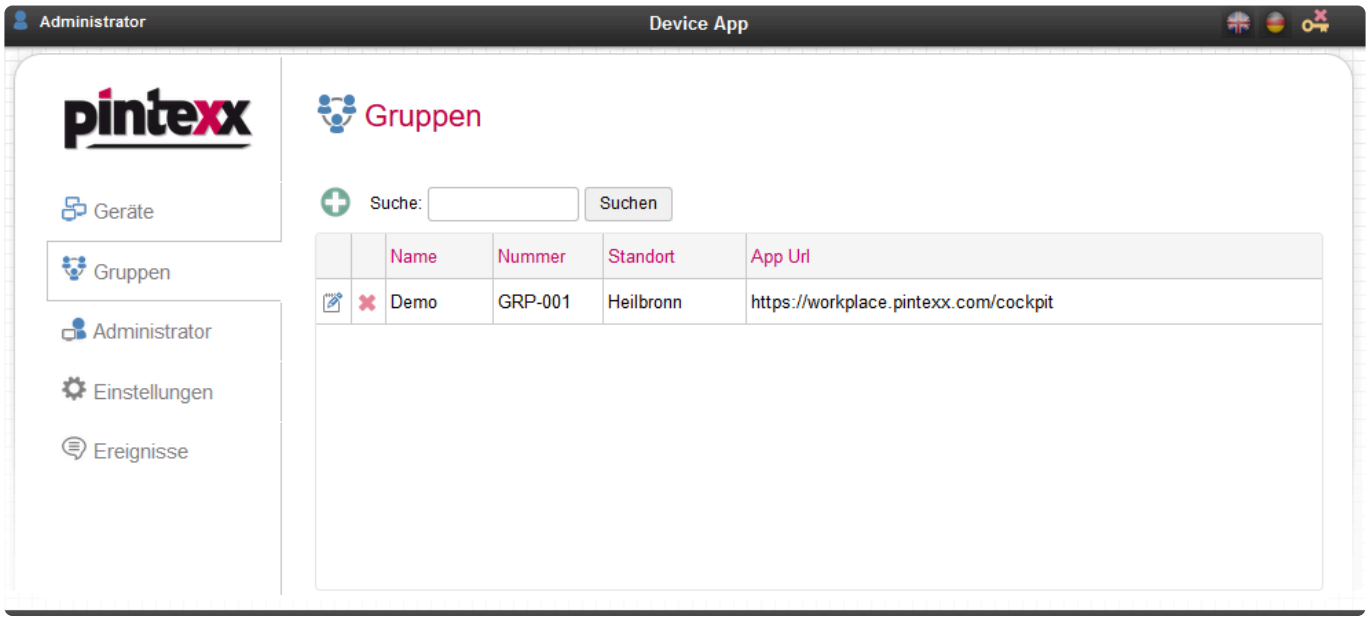


Geräte-Eigenschaften “Erweitert”:

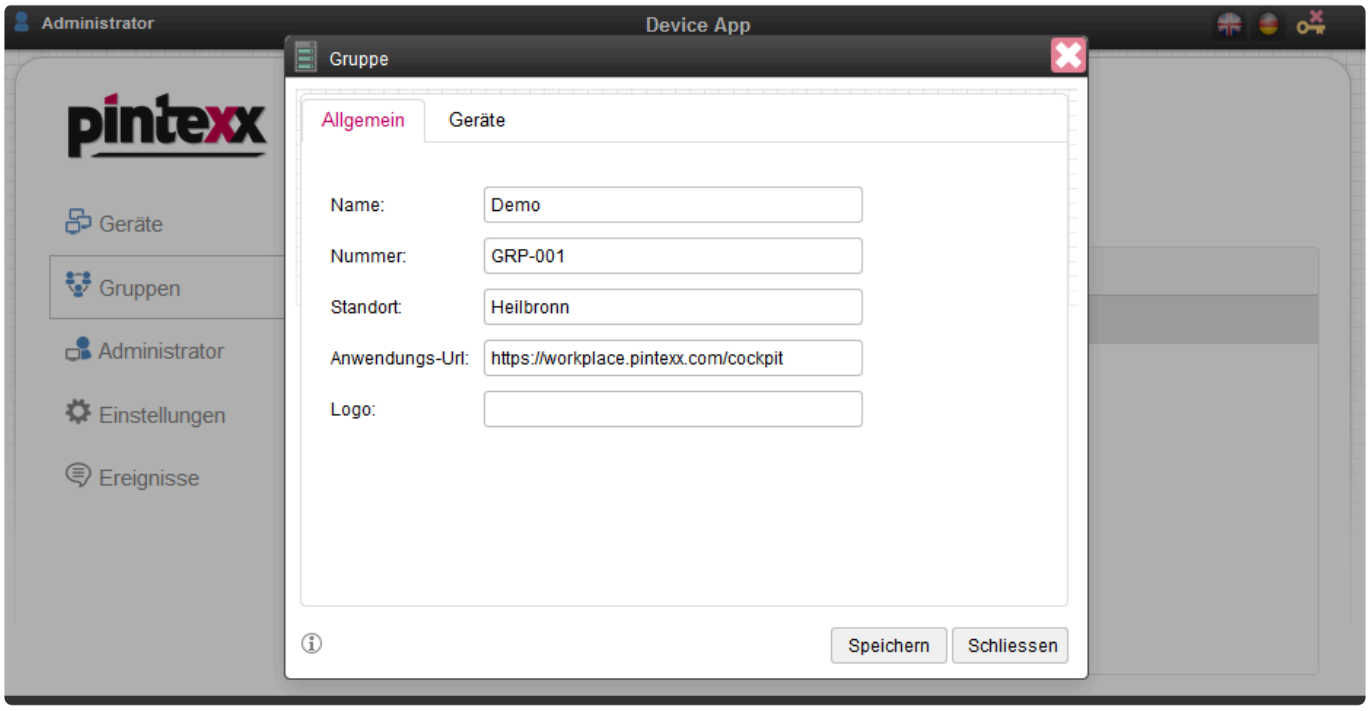
Anwendungs-Url	Die vollständige Url der Web-Anwendung, die im Gerät aufgerufen wird (i.d.R. die “Cockpit”
Nummer	Eine beliebige Nummer
Benutzer	Der aktuelle Benutzer des Gerätes
Standort1	Standort-Angaben des Gerätes
Standort2	Standort-Angaben des Gerätes
Logo	Vollständige Url eines Logos welches auf dem Gerät angezeigt wird

1.2.6.3. Gruppen

Geräte können einer Gruppe zugewiesen werden.
Dadurch lassen sich Einstellungen wie die Anwendungs-Url für alle Geräte auf einmal durchführen.

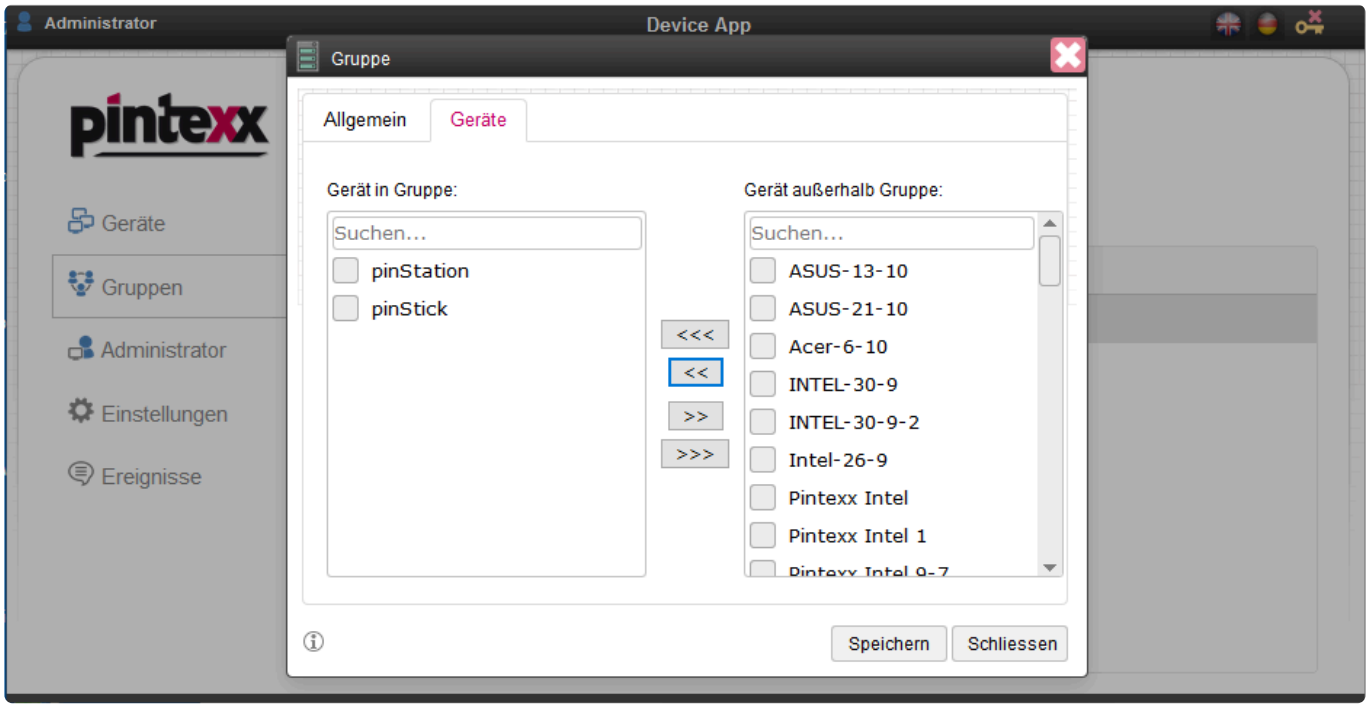


Folgende Einstellungen sind verfügbar:



Name	Ein beliebiger Gruppen-Name
Nummer	Eine beliebige Gruppen-Nummer
Standort	Eine Standort-Angabe
Anwendungs-Url	Die vollständige Url der Anwendung die auf dem Gerät angezeigt wird

Logo	Die vollständige Url eines Logos, welches auf dem Gerät angezeigt wird



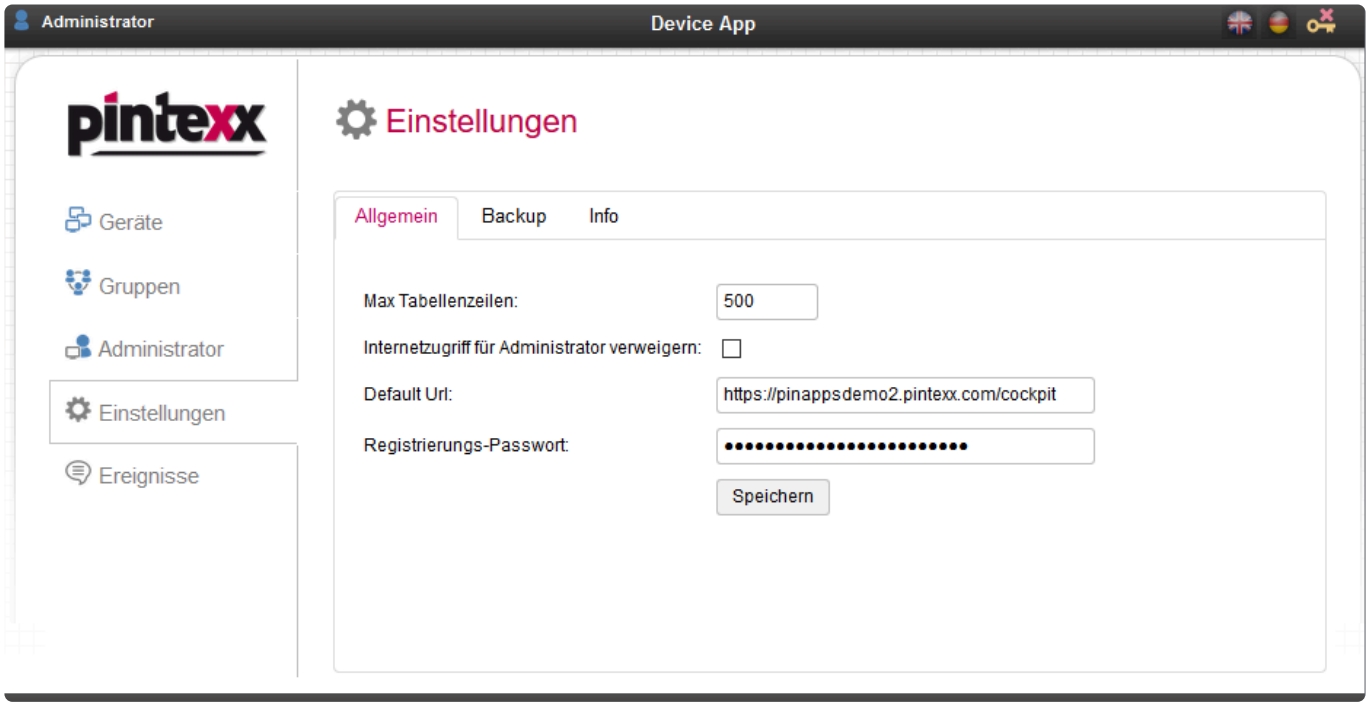
Hier können Geräte zur Gruppe hinzugefügt oder entfernt werden.

1.2.6.4. Administrator

Siehe Administrator

1.2.6.5. Einstellungen

“Allgemein”



Max. Tabellenzeilen	Die max. Anzahl der Zeilen die z.B. in der Geräte-Liste aufgelistet wird.
Internetzugriff für den Administrator verweigern	Durch Aktivierung kann die Geräte-Konfiguration nur noch über eine lokale IP-Adresse erreicht werden
Default-Url	Die Default-Url wird nach der Registrierung des Gerätes automatisch als Anwendungs-Url verwendet
Registrierungs-Passwort	Das Passwort, das zur Registrierung des Gerätes verwendet werden muss.

“Backup”
s. Backup

“Info”
s. Info

1.2.6.6. Ereignisse

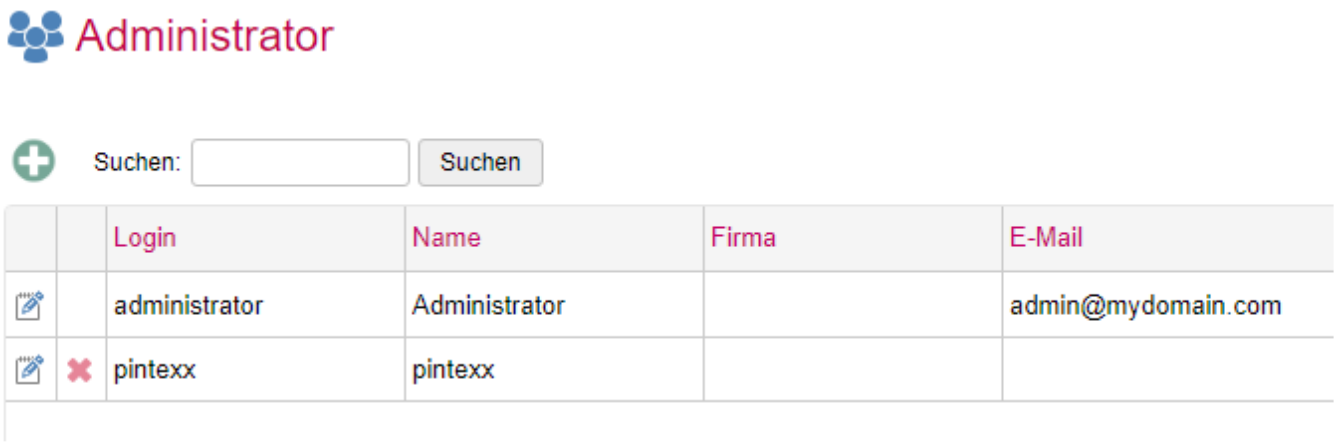
Siehe Ereignisse

1.2.7. Wiederkehrende Funktionen

In den verschiedenen Anwendungen gibt es Funktionen mit demselben Inhalt.
Diese werden hier beschrieben.

1.2.7.1. Administrator

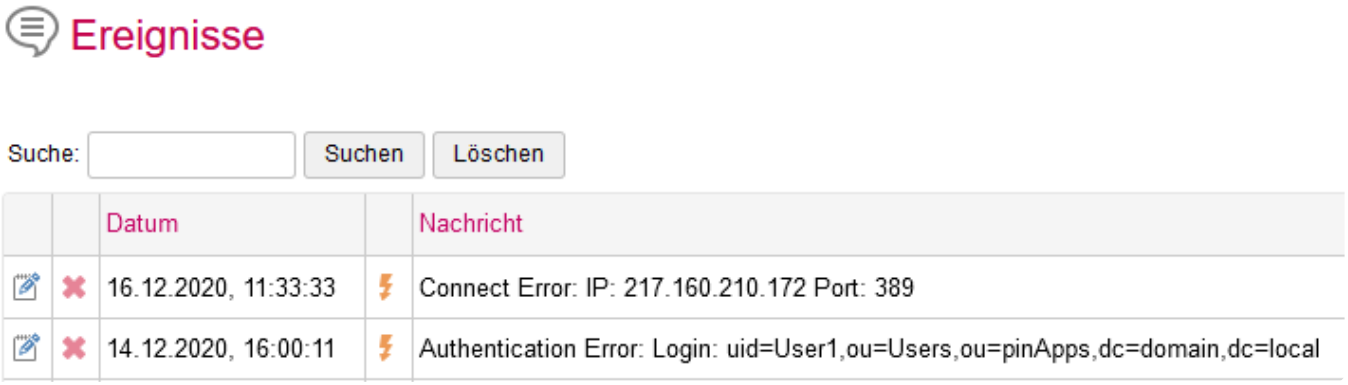
In jeder Anwendung kann es einen oder mehrere Administratoren geben.



I.d.R. gibt es einen Root-Admin, der nicht gelöscht werden kann.
Weitere Admins können über den Plus-Button angelegt werden.

1.2.7.2. Ereignisse

Unter “Ereignisse” werden i.d.R. Informationen über Anwendungs-Fehler oder andere Informationen angezeigt.

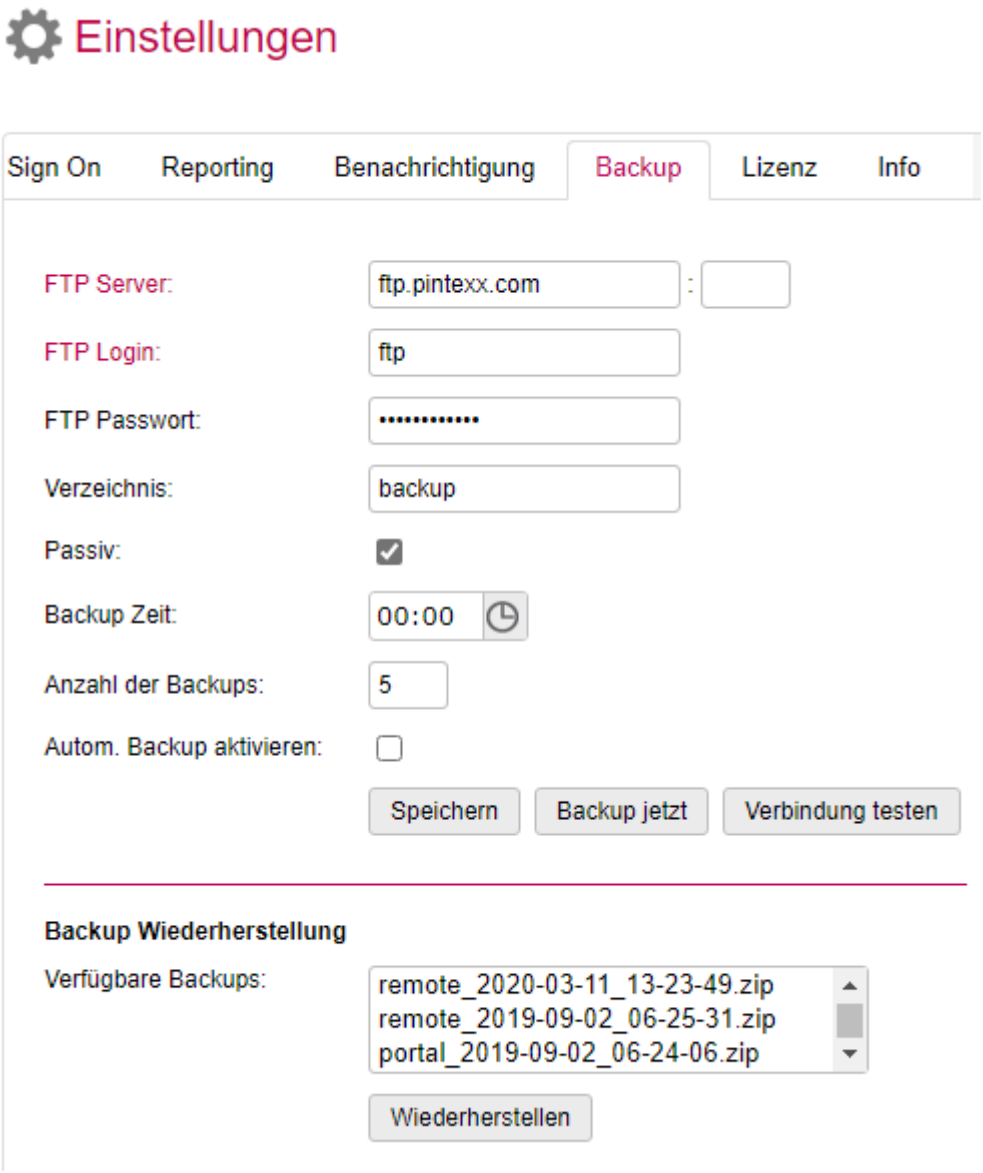


Detailliertere Informationen befinden sich in den Log-Dateien in “System”.

1.2.7.3. Einstellungen

1.2.7.3.1. Backup

Jede Anwendung verfügt über die Möglichkeit die Konfiguration zu sichern und wieder einzuspielen. Andere Formen des Backups wie z.B. sichern der VM bleiben davon unbenommen.



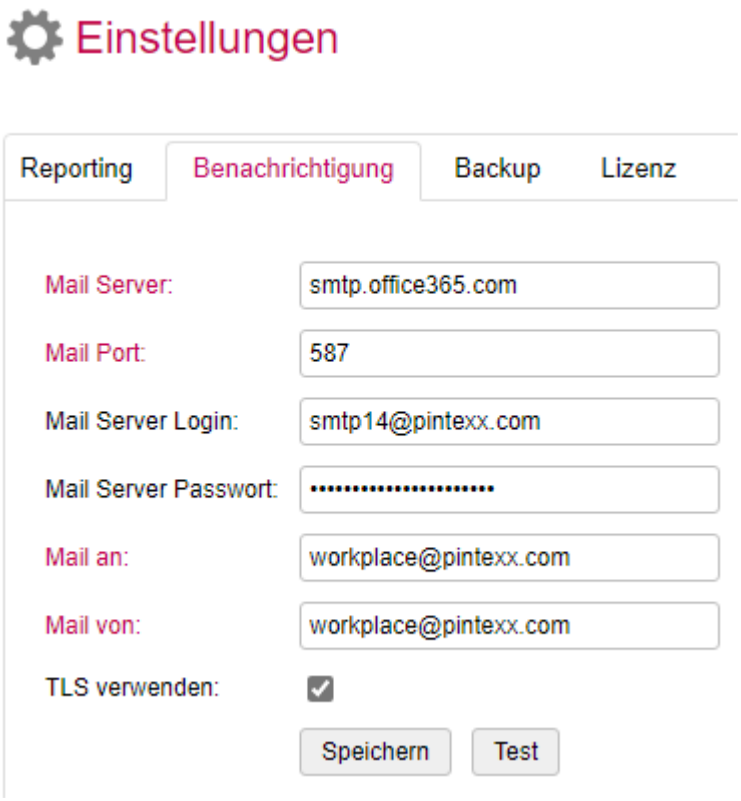
Aktuell besteht die Möglichkeit, die Konfiguration auf einem Ftp-Server abzulegen.
Dazu muss der Zugriff auf den FTP-Server entsprechend konfiguriert werden.

Es wird immer eine angegebene Anzahl an Sicherungen vorgehalten.

Es kann auch ein automatisches Backup konfiguriert werden.

1.2.7.3.2. Benachrichtigung

Um E-Mails zu versenden wird ein SMTP-Server benötigt.



Dieser kann über die entsprechenden Felder konfiguriert und getestet werden.

1.2.7.3.3. Info

Im Info-Bereich werden i.d.R. Informationen über die aktuelle Version und der Lizenz-Status angezeigt.

1.3. Workplace ThinClients

Die Pintexx ThinClients sind speziell für die Nutzung mit der Pintexx Workplace-Lösung angebotene Geräte.

Es handelt sich dabei um ThinClients, mit einem eigens dafür entwickelten Betriebssystem pinOS.

1.3.1. pinOS

Das pinOS ist ein Linux-basiertes Betriebssystem speziell für den Betrieb auf einem ThinClient ausgerichtet.
Jedes Gerät wird damit zu einem Thin Client.

Das pinOS bietet die Möglichkeit, eine über “Device” konfigurierbare Url zu laden.
Im Fall von Pintexx Workplace ist dies das “Cockpit”.

Es ist nicht möglich, auf dem Gerät zu speichern. Downloads sind damit ausgeschlossen.

pinOS unterstützt Netzwerk, WLAN, 2 Monitore und lokales Drucken.

1.3.2. Geräte

Die Business Devices umfassen mehrere unterschiedliche Geräte für unterschiedliche Aufgaben.

1.3.2.1. pinStick

pinStick ist ein USB-Stick mit pinOS für alle INTEL-Geräte.

Das Gerät muss im BIOS so konfiguriert werden, dass vom USB-Stick gebootet werden kann.

1.3.2.2. ThinPhone

ThinPhone ist die Kombination aus

- einem Android oder Apple-Smartphone
- der Pintexx Workplace App
- einer Smartphone-Desktop-Erweiterung wie z.B. DeX von Samsung
- Unterstützung der USB-C Schnittstelle für den Anschluss einen Monitors

Dann kann das System als PC betrieben werden.

1.3.2.3. ThinStation

Die ThinStation ist ein Mini-PC an dem 2 externe Monitore über HDMI angeschlossen werden können.

1.3.3. Gerät einrichten

Nach dem Boot-Vorgang wird der Einrichtungs-Assistent angezeigt.

Es kann die Display-Sprache und die Tastatur ausgewählt werden.

Danach muss die Domäne einer Pintexx Workplace-Installation angegeben werden.
z.B. workplace.<domain.com
Es kann nur https verwendet werden.
Die Url wird nach der Eingabe geprüft.

Schlussendlich muss das Gerät registriert werden.
Dazu muss eine Geräte-Name und ein Registrierungs-Passwort angegeben werden.
Der Geräte-Name erscheint dann in “Device”.
Das Registrierungs-Passwort kann ebenfalls in “Device” konfiguriert werden.

Nach Abschluss der Registrierung wird die konfigurierte Url geladen, sofern eine Intranet/Internet-Verbindung verfügbar ist.
Ist keine Verbindung möglich, wird die Geräte-Konfiguration angezeigt.
Dort kann dann z.B. eine WLAN-Verbindung eingerichtet werden.

1.3.4. Gerät konfigurieren

1.3.4.1. Netzwerk

Ist ein Netzwerkkabel an das Gerät angeschlossen dann wird automatisch eine Netzwerkverbindung aufgebaut.

In der Geräte-Konfiguration kann über “Netzwerk” die zugewiesene IP-Adresse angezeigt werden.

1.3.4.2. W-LAN

Über die Geräte-Konfiguration kann über “WLAN” eine drahtlose Verbindung eingerichtet werden.

Dazu muss aus der Verbindungsliste eine Verbindung ausgewählt und das WLAN-Passwort eingegeben werden.
Es können auch mehrere Verbindungen konfiguriert werden.

1.3.4.3. Mehrere Monitore

Das System unterstützt aktuell bis zu 2 Monitore.

Diese werden in der Geräte-Konfiguration unter “Monitor angezeigt.
Beim Starten einer Anwendung im Cockpit kann dann der Monitor ausgewählt werden, auf dem die Anwendung angezeigt werden soll.

Wird die Multi-Monitor-Unterstützung in “Remote” konfiguriert, dann kann ein Desktop automatisch auf beiden Monitoren angezeigt werden.

1.3.5. Tastatur Kommandos

Folgende Tastatur-Kommandos können unter pinbOS verwendet werden:

F1 ALT-F1 ALT-ESC	Anzeige der konfigurierten Anwendung
F2 ALT-F2	Anzeige Geräte-Konfiguration
F3 ALT-F3	Anzeige System
ALT-TAB	Im Cockpit wird die nächste gestartete Anwendung auf dem entsprechenden Monitor angezeigt
CTRL+ALT+DEL	Anzeige System

1.4. Workplace PC Rack

1.4.1. Inbetriebnahme

Das PC Rack wird als 19”-Einschub in 3HE mit gewählter PC-Austattung geliefert.
Dazu ein 1.5 HE Stromversorgung im 19”-Einschub.

Die Netzwerkkabel aus den einzelnen PC’s müssen mit einem Switch verbunden werden(nicht im Lieferumfang enthalten)
Die Anschlusskabel der einzelnen PC’s müssen mit der Stromversorgung verbunden werden.

Achtung:
PC’s erst nach den vorbereitenden Massnahmen einschalten!

1.4.2. Vorbereitende Massnahmen

Die PC’s können über einen PXE-Boot Server ein individuell konfiguriertes Betriebssystem booten.
Das Betriebsystem (Windows 10) kann als ISO-Datei von unserer Download-Seite pro Hardware-Typ heruntergeladen werden.
Das ISO enthält bereits alle notwendigen Treiber und ein aktuelles System.

Das ISO enthält ebenfalls das “PCRack Static Tool” für das automatisierte Setzen einer statischen IP-Adresse beim erstmailgen Start.
Das Tool verbindet sich mit dem “PCRack Service”, einem Windows-Dienst der eine Liste an statischen IP-Adressen verwaltet.
Dieser Dienst kann z.B. auf dem System installiert werden, auf dem ebenfalls der PXE-Server läuft.

Die Windows-Installation läuft völlig autark mit vorkonfigurierbaren Einstellungen.
Nach der Windows-Installation wird über das “PCRack Static Tool” eine statische IP, DNS,Gateway und Netzmaske abgefragt und auf dem PC gesetzt.
Diese IP wird dann als verwendet markiert und zusammen mit der übergebenen PC-Mac-Adresse in einer separaten Datei gespeichert.

Diese kann dann in “Remote” importiert werden.

1.4.2.1. PXE-Server installieren

Wir empfehlen die Verwendung des Serva-PXE-Servers für Windows.
(Aus rechtlichen Gründen ist keine Lizenz enthalten).

1.4.2.2. ISO-Datei konfigurieren

Für jeden Hardware-Typ kann eine Windows-10 ISO-Datei von unserer Homepage heruntergeladen werden.

Diese kann z.B. mit einer VMWare Workstation zu einer VM konfiguriert werden.
Dort können dann weitere Software-Pakete installiert werden.

1.4.2.3. Windows-Einstellungen konfigurieren

Für die automatische Installation können diverse Parameter wie Sprache, Lizenzschlüssel etc. über einen Online-Konfigurator gesetzt werden.
Dieser generiert dann die autounattended.xml, welche zur PXE-Server-Konfiguration hinzugefügt wird.