BENUTZER LEITFADEN

EXTERNER ZUGANG VMWARE UNIFIED ACCESS GATEWAY (UAG)

Im Sinne einer verbesserten Lesbarkeit und eines verbesserten Verständnisses wird in diesem Benutzerleitfaden auf die geschlechterspezifische Formulierung verzichtet.

RAITEC IT-Support Telefon: 0599 BLZ 888 oder 66888 (IP-Telefonie) Schriftliche Anfragen senden Sie uns bitte über <u>meineIT – Supportanfrage RAITEC</u>



Inhaltsverzeichnis

Änderu	ngsverzeichnis
1	Auf den Punkt gebracht4
1.1	Voraussetzungen:
1.2	First Login:4
2	Installation und Konfiguration5
2.1	Installationsvorbereitung
2.2	Installation VMware Horizon Client5
2.3	Konfiguration VMware Horizon Client6
3	Erste Schritte in der RAITEC Workplace Cloud7
3.1	Verbindungsaufbau zur Workplace Cloud7
3.2	Registrierung/Kopplung PinglD8
3.3	Verbindungsaufbau zum Desktop starten9
4	FAQs und Tipps10



Änderungsverzeichnis

DATUM	KAPITEL, INHALTE DER ÄNDERUNGEN
08.09.23	Erstellung
16.11.23	Anpassung Multimandanten
04.01.24	Anpassung Support
12.12.24	Anpassung First Login



1 Auf den Punkt gebracht

Der externe Zugang über **UAG** (Unified Access Gateway) ermöglicht den **Zugriff auf die Workplace Cloud** (virtueller Client) **des Benutzers von externen Geräten**, die nicht von der RAITEC verwaltet werden.

Dieses Dokument beinhaltet:

- Voraussetzungen und Passwortwechsel
- Installation und Konfiguration der Softwarekomponenten
- Erste Schritte in der Workplace Cloud
- FAQs und Tipps für Fehlerbehebungen

1.1 Voraussetzungen:

- Windows 10 22H2 oder Windows 11 22H2
- PingID App von "Ping Identity Corporation" am Smartphone oder Desktop (Windows, MAC)
- Empfohlene Mindestbandbreite: 10Mbit Download und 2Mbit Upload

1.2 First Login:

Setzen sie vor der ersten Anmeldung ein neues Passwort.

ACHTUNG: Auch nach dem Rücksetzen durch einen Administrator erforderlich

• Auf <u>https://resetpw.raitec.at</u> -> "Change Password" aufrufen

	verify your new password.
Sign On	USERNAME
Sign On	Username
JSERNAME	CURRENT PASSWORD
PASSWORD	NEW PASSWORD
	CONFIRM NEW PASSWORD
Sign On	(
Change Password? Trouble Signing On?	Submit Submit

Change Password

Please enter your current password and

Abbildung 1: Passwort setzen

Vmware Unified Access Gateway (UAG)



2 Installation und Konfiguration

2.1 Installationsvorbereitung

Für die Installation und den Zugriff auf Ihre Workplace Cloud benötigen Sie:

- Horizon Client Installationsdokumentation und Software (Dataspace RAITEC)
- PingID App für die Authentifizierung PingID Downloads

2.2 Installation VMware Horizon Client

Verwenden Sie für die Installation ausschließlich den am RAITEC Dataspace zur Verfügung gestellten VMware Horizon Client. Falls beim Start der Installation eine Windows Defender Hinweismeldung auftritt, kann diese ignoriert werden und die Installation mit "Ausführen" fortgesetzt werden.

Version 5.5.4 Version 5.5.4 Sie müssen Datenschutzvereinbarung und Lizenzbedingungen zustimmen, bevor Sie das Produkt installieren können	- × Sie müssen Ihr System neu starten, damit die Konfigurationsänderungen für VMware Horizon Client wirksam werden.
Akzeptieren und Installieren	Jetzt neu starten
Installation anpassen	Später neu starten

Abbildung 2: Installation VMware Horizon Client



Vmware Unified Access Gateway (UAG)

2.3 Konfiguration VMware Horizon Client

Die Basiskonfiguration ist nur beim ersten Start erforderlich.

Nach Start des VMware Horizon Clients ist die Option "Nicht authentifizierter Zugriff" rechts oben bei dem grünen Kreis (oder drei waagrechten Punkten) zu aktivieren.

C VMware Horizon Client	- 🗆 X
	+ Server hinzufügen 🔞 Einstellungen 💿
	Software-Updates
	Info über VMware Horizon Client
+	✓ Nicht authentifizierter Zugriff
Server hinzufügen	Auswahl nach Start ausblenden

Abbildung 3: Nicht authentifizierter Zugriff

Öffnen Sie die Einstellungen und passen Sie die Codec Einstellungen unter VMware Blast It. Screenshot (Abbildung 4) an

📮 VMware Horizon Client		<u>11</u> 0		×
	+ Server hinzufügen	🔞 Einstel	lungen	

C VMware Horizon Client × < **VMware Blast** Catenfreigabe Codecs Sicherheit BlastCodec-Decodierung zulassen O VMware Blast D Ein H.264-Decodierung zulassen O Ein Iigh-Definition-Farbe zulassen (kann die Akkulaufzeit und Leistung verringern) HEVC-Decodierung zulassen Aus AV1-Decodierung zulassen Aus

Abbildung 4: Einstellungen des VMware Horizon Clients öffnen

Abbildung 5: VMware Blast Codec Einstellungen



3 Erste Schritte in der RAITEC Workplace Cloud

3.1 Verbindungsaufbau zur Workplace Cloud

Fügen Sie den Server **portal-rwpc.rbgooe.at** durch Doppelklick auf das Plus Symbol -> **Server hinzufügen**

VMware Horizon Client	
+	
Server	
Timzurugen	
Der Name des Verbindungsse	ervers
portal-rwpc.rbgooe.at	
Abbrechen	Verbinden

Abbildung 2: Hinzufügen Server portal-rwpc.rbgooe.at

Anmeldung mit Windows User und Kennwort

A https://portal-rwpc.rbgooe.at			
Geben Sie Ihren Radius-Benutzernamen und Ihr Passwort ein.			
Benutzername			
Passwort			
Abbrechen	Anmelden		

Abbildung 3: Anmeldung Benutzer – Passwort



3.2 Registrierung/Kopplung PingID

Nach der ersten Anmeldung muss einmalig die Kopplung mit der PinglD App am externen Gerät (Smartphone) durchgeführt werden.

1. Am Portal wird der "paring key" angezeigt



Abbildung 8: "pairing key" Anzeige

- 2. App am externen Gerät öffnen und Kopplung starten
 - a. Aufruf und Darstellung kann je Endgeräte Typ und App Version variieren



Abbildung 9: Start manuell Kopplung am externen Gerät

- 3. Geben den angezeigten "paring key" am externen Gerät (PingID App) ein
- 4. Bestätigen Sie mit "Koppeln"



Abbildung 10: "pairing key" Eingabe und Kopplung am externen Gerät



5. Am Portal die Kopplung mit OK bestätigen und Anmelden



Abbildung 11: "pairing key" Bestätigung

Bestätigen Sie die Anmeldung am externen Gerät in der PingID App durch Wischen oder "Yes"



Abbildung 12: PingID Bestätigung am Smartphone

3.3 Verbindungsaufbau zum Desktop starten



Abbildung 13: Verbindungsaubau starten



Vmware Unified Access Gateway (UAG)

4 FAQs und Tipps

- Kein Support für das private Endgerät durch RAITEC
- Jabber kann nur f
 ür Telefonie verwendet werden.
 - Videotelefonie und Bildschirm teilen wird nicht unterstützt.
 - Verwenden Sie hierfür MS Teams.
- Bei einem Update des Horizon Clients, muss die alte Version vorher deinstalliert werden
- USB-Geräte werden nicht in die Session gehängt
- Bluetooth Geräte werden nicht in die Session gehängt
- USB und Bluetooth Geräte die am physischen Client als Tastatur, Maus, Video oder Audio erkannt werden kommen über das Verbindungsprotokoll in die Session nicht über "USB-Redirect"
- Ein Datenaustausch zwischen privatem Gerät und virtuellen Client ist gesperrt
- Nested Mode am Kundensystem (MS Hyper-V, VMware Workstation, MAC OS Parallels Desktop, Xen Desktop) wird nicht unterstützt und führt zu Problemen mit Audio und Video Geräten zb. MS Teams kann nicht auf die Geräte zugreifen
- Nach der Anmeldung mit User/Passwort kommt im Horizon die Fehlermeldung "Authentifizierung fehlgeschlagen- Die maximale Anzahl an Anmeldeversuchen wurde überschritten", hier kann es zu zwei möglichen Fehlern kommen:
 - User nicht berechtigt
 - Passwort abgelaufen oder vom Administrator zurückgesetzt -> Passwort muss immer über <u>https://resetpw.raitec.at</u> "Change Password" neue vergeben werden



Authentifizierung fehlgeschlagen

Die maximale Anzahl an Anmeldeversuchen wurde überschritten.

Abbildung 14: Fehlermeldung im Horizon

• Zugriff auf Clients mit Matrix42 und RDP

Per Matrix42 Remote Control kann auf einen weiteren PC zugegriffen werden. Für eine bessere Qualität und Performance wird empfohlen, die Verbindung per RDP aufzubauen. (Rechtsklick auf den Client und "Verbinden mit RDP")



Abbildung 15: Remote Control Matrix42

