A|S|F|i|N|A|G

ASFINAG Anwenderhandbuch

MSG / SM / ITC / SECURITY

PRIVILEGED IDENTITY & ACCESS MANAGEMENT

Gültigkeitsbereich: MSG		**Gültig ab:** 20.03.2025
Version	**Sicherheitsstatus**	**Dokumentenstatus**
2.1	öffentlich	Freigegeben

Erstellt von	**Geprüft von**	**Freigegeben von/im**
Gesellschaft/Abt./Name: **MSG/SM/ACO**	*Gesellschaft/Abt./Name:* **MSG/SM/JJR**	*Gesellschaft/Abt./Name:* **MSG/SM/ RAH**
Datum: 16.02.2026	**Datum: 16.02.2026**	**Datum:**
Die Dokumentenfreigabe erfolgt mittels Unterschriftenlauf oder im DOXiS mittels Freigabeworkflow (keine Unterschrift notwendig).		
Verteiler	ggf. Verteilerliste	

Inhaltsverzeichnis

1 Allgemein 3
2 Voraussetzungen 3
3 Installation des paloalto GlobalProtect VPN Clients 3
3.1 Herunterladen des paloalto GlobalProtect VPN Clients 3
3.2 Herstellung der VPN-Verbindung 5
4 PIAM Weboberfläche 6
4.1 Öffnen der PIAM Weboberfläche 6
4.2 Ändern des PIAM Benutzer Kennworts 7
4.3 Favoriten 7
4.4 Öffnen einer RDP-Session zum Zielsystem 9
4.5 Öffnen einer RDP-Session und gleichzeitiges Auslesen des aktuellen Passworts 11
4.6 Wiederverbinden einer RDP-Session bzw. erneutes Auslesen des aktuellen Passworts 12
4.7 Beenden einer RDP-Session zum Zielsystem 13
4.8 Requests anzeigen bzw. Requests mit bis zu 23 Stunden Laufzeit anfordern 14
5 Fehlerbehebung 15
5.1 Browser 15
5.2 Pop-Up Blocker 15
5.3 Smart App Control blockiert RDP-Dateien 15
5.4 Fehlermeldung: „Invalid Session Token“ 16
5.5 Fehlermeldung „Failed to Connect RDP Session“ 16
5.6 Fehlermeldung: „Failed to authenticate due to one or more factors” 17
5.7 Fehlermeldung: „An error occurred while trying to submit the Request” 18
5.8 https://piam.asfinag.at kann im Browser nicht geöffnet werden 18
5.9 Deinstallation Cisco Anyconnect 19
6 Fehlermeldungen und Technischer Support 19
7 Anhang 20
7.1 Abkürzungen und Begriffsbestimmungen 20
7.2 Historie 20

1 Allgemein

Dieses Benutzerhandbuch richtet sich in erster Linie jene Benutzer, die einen administrativen Zugriff auf IT-Systeme der ASFiNAG benötigen. Dieser administrative Zugriff wird mit Hilfe des ASFINAG Privileged Identity & Access Management (PIAM) Systems ermöglicht.

2 Voraussetzungen

Um eine Verbindung herstellen zu können, wird ein gültiger PIAM-Benutzeraccount inkl. Microsoft MFA Berechtigung benötigt. Des Weiteren wird ein aktueller Windows PC/Notebook mit installiertem paloalto Globalprotect VPN Client und einer stabilen Internetverbindung vorausgesetzt.

Betriebssystem-Anforderung:

- Windows 11 mit aktuellem Patchlevel
- aktivierte Endpoint-Protection

Für Remote-Desktop-Verbindungen wird der MS RDP Client (=in Windows 11 bereits enthalten) benötigt. Für SSH-Verbindungen wird die Verwendung von PuTTY empfohlen. Alternative RDP-Clients (z.B.: FreeRDP, Linux) werden weder getestet noch unterstützt.

3 Installation des paloalto GlobalProtect VPN Clients

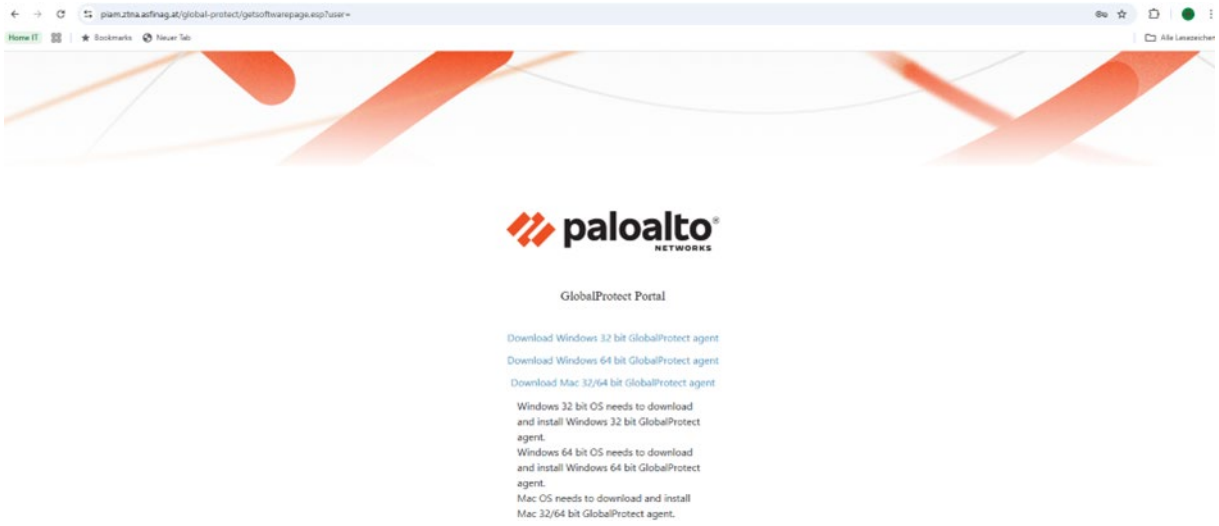
3.1 Herunterladen des paloalto GlobalProtect VPN Clients

Bitte öffnen Sie in einem Webbrowser den folgenden Link.

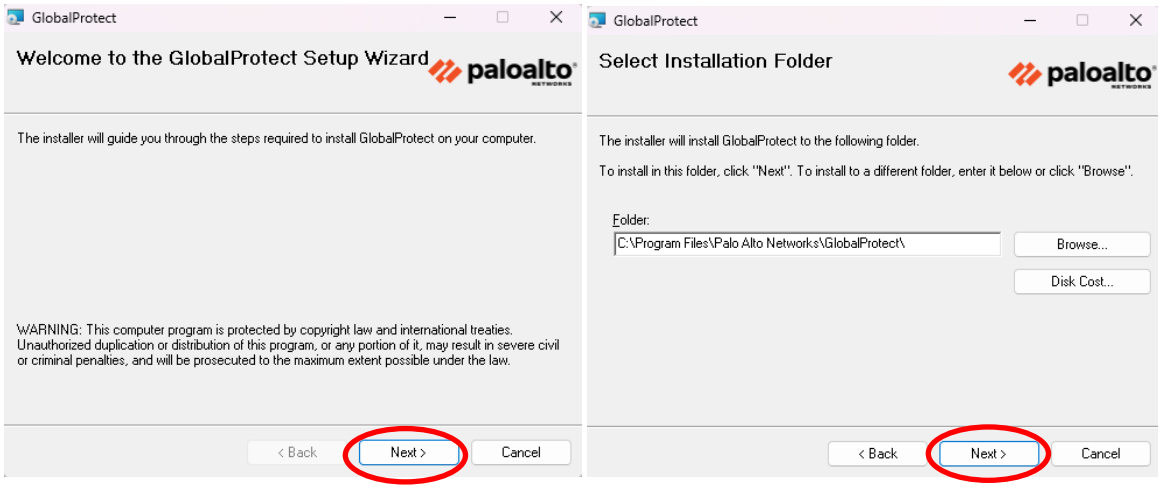
https://piam.ztna.asfinag.at/global-protect/login.esp

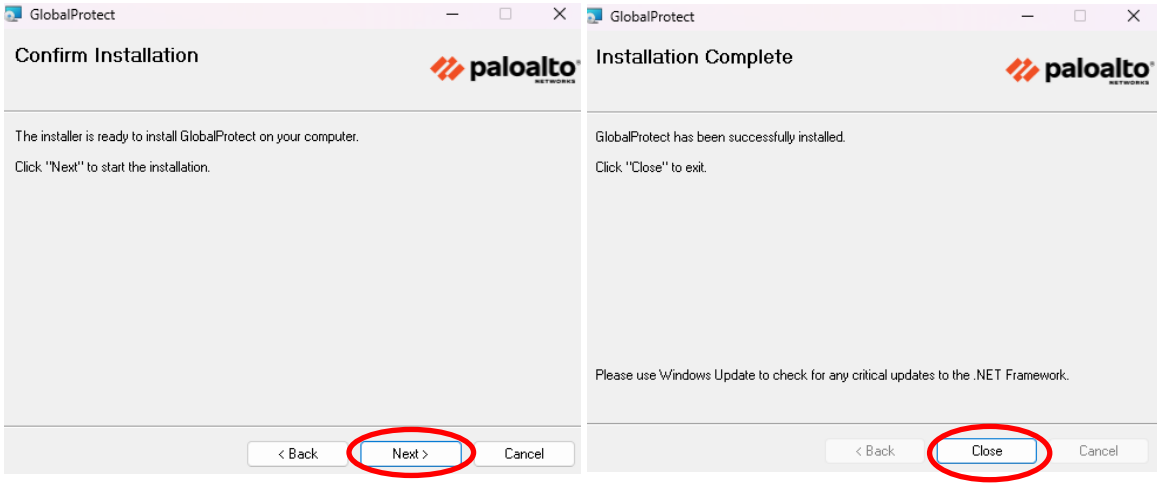
*(Wichtig: **Groß- und Kleinschreibung beachten!)***
USERNAME = PIAM
PASSWORD = siehe Mail mit den Zugangsdaten

Mit „Download Windows 64-bit GlobalProtect Agent“ fortfahren…



Das heruntergeladene Programm kann mit „öffnen“ gestartet werden.





3.2 Herstellung der VPN-Verbindung

Nach erfolgreicher Installation kann der paloalto Globalprotect VPN Client im Startmenü geöffnet werden.

Nach Eingabe von **piam.ztna.asfinag.at** kann die VPN-Verbindung geöffnet werden.

USERNAME = **PIAM** und PASSWORD siehe Mail mit den Zugangsdaten.

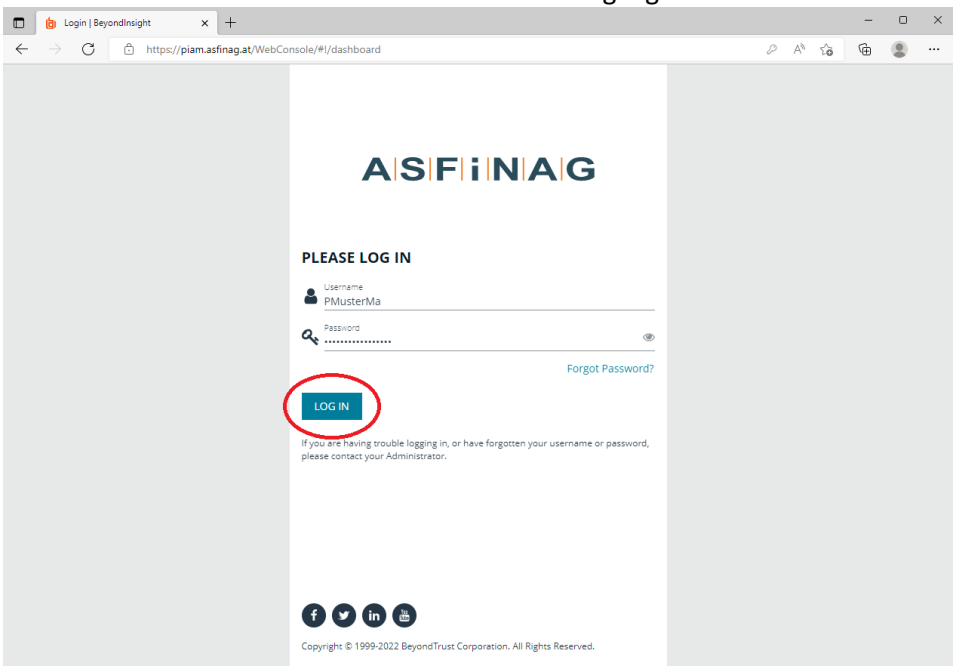
4 PIAM Weboberfläche

4.1 Öffnen der PIAM Weboberfläche

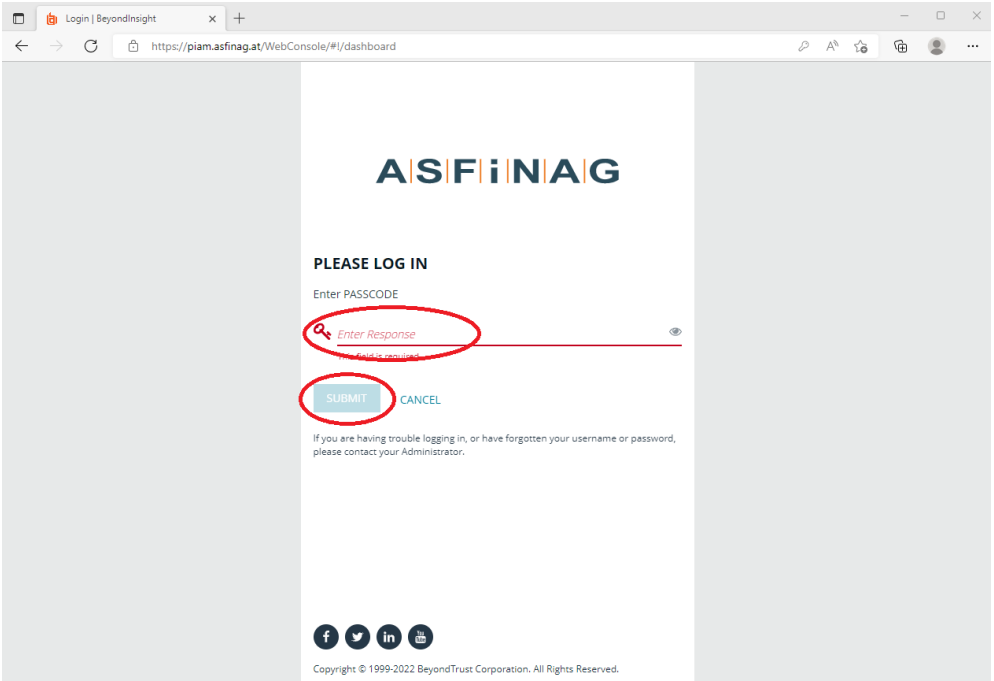
Sobald die VPN-Verbindung aufgebaut wurde, kann mit Hilfe eines Webbrowsers der folgende Link geöffnet werden:

https://piam.asfinag.at

USERNAME und PASSWORD siehe Mail mit den Zugangsdaten.

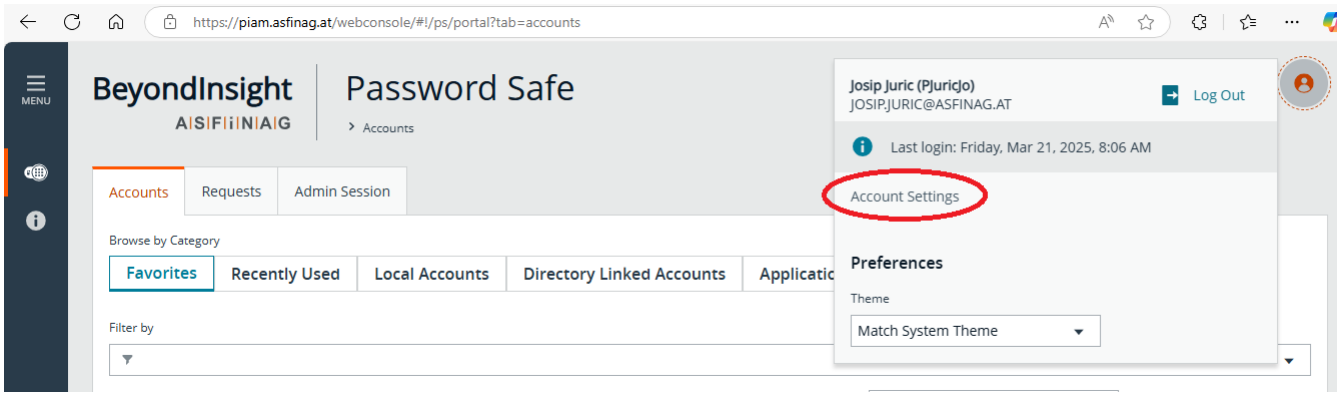


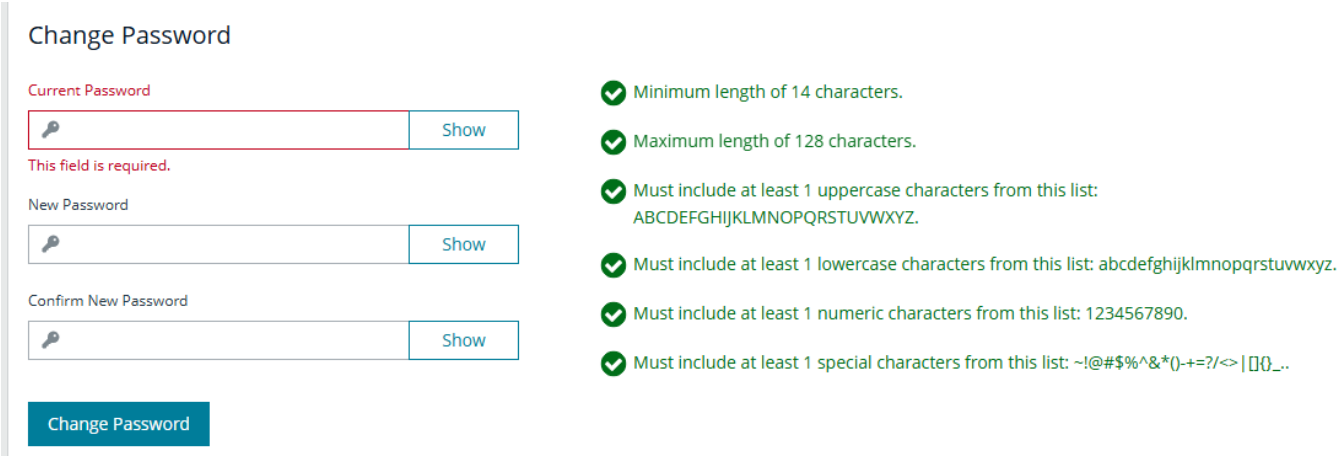
Bitte geben Sie nun den Microsoft Verification Code ein, welchen Sie nach erfolgreicher Authentifizierung per SMS erhalten:



4.2 Ändern des PIAM Benutzer Kennworts

Es wird dringend empfohlen, das 1. Login-Kennwort des PIAM-Benutzers nach dem ersten Login zu ändern!

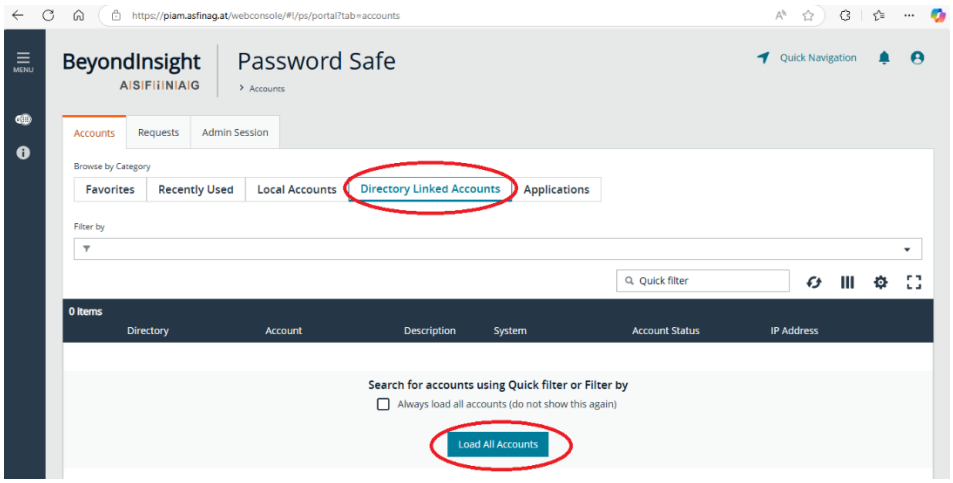




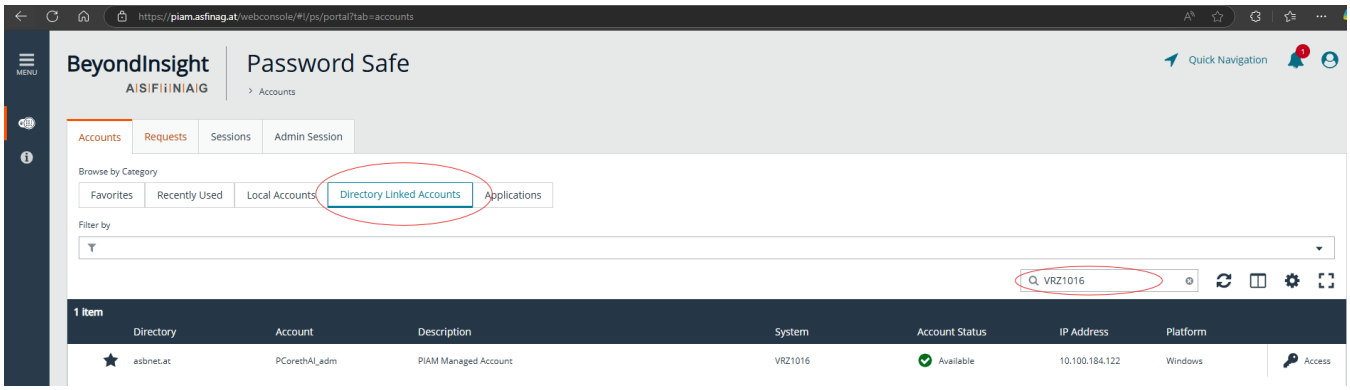
4.3 Favoriten

In der PIAM-Benutzeroberfläche werden grundsätzlich alle Systeme angezeigt. Abhängig von den Benutzerrechten, kann eine Remote Verbindung zum Zielsystem aufgebaut werden. Mit Hilfe der Favoriten Funktion kann eine persönliche Server Liste erstellt werden.

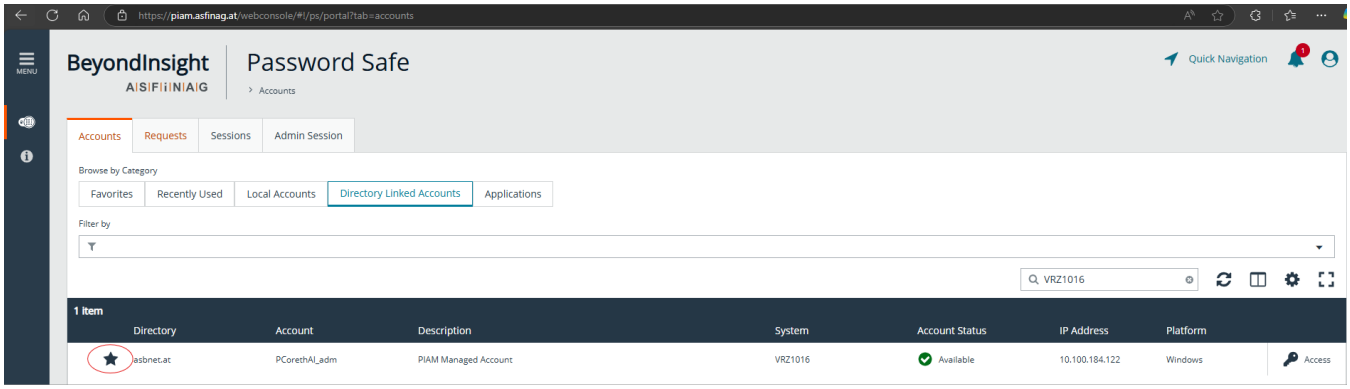
Als Erstes öffnen Sie mit „**Domain Linked Accounts**“ die Liste aller verfügbaren Systeme.



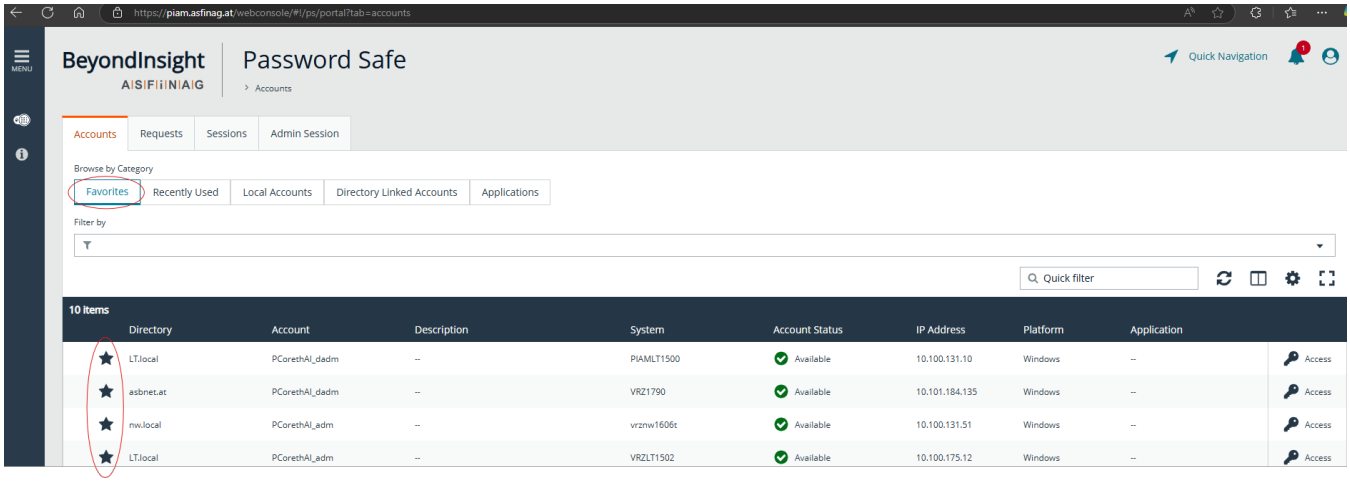
Durch Eintippen des Hostnamens kann nun das gewünschte System gesucht werden.



Mit dem Sternsymbol kann das gewünschte System zu den Favoriten hinzugefügt werden.

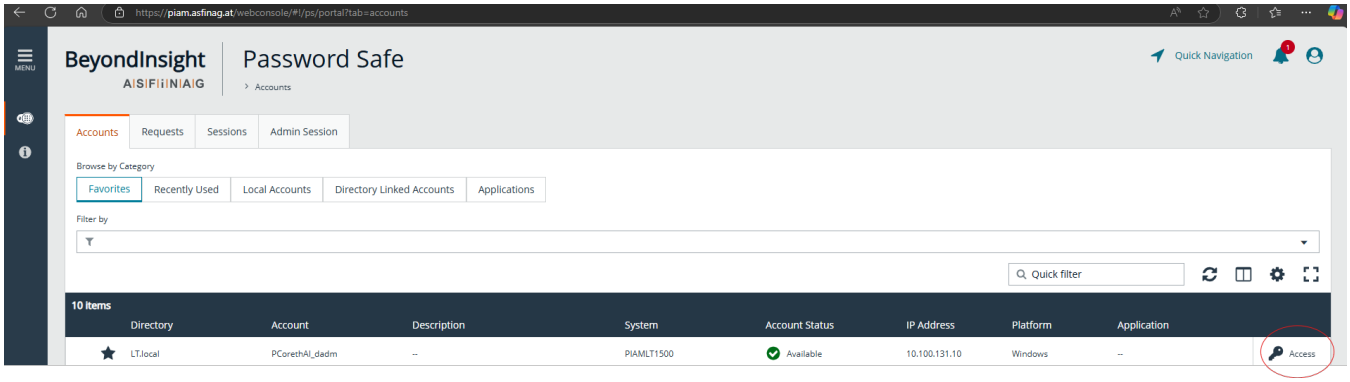


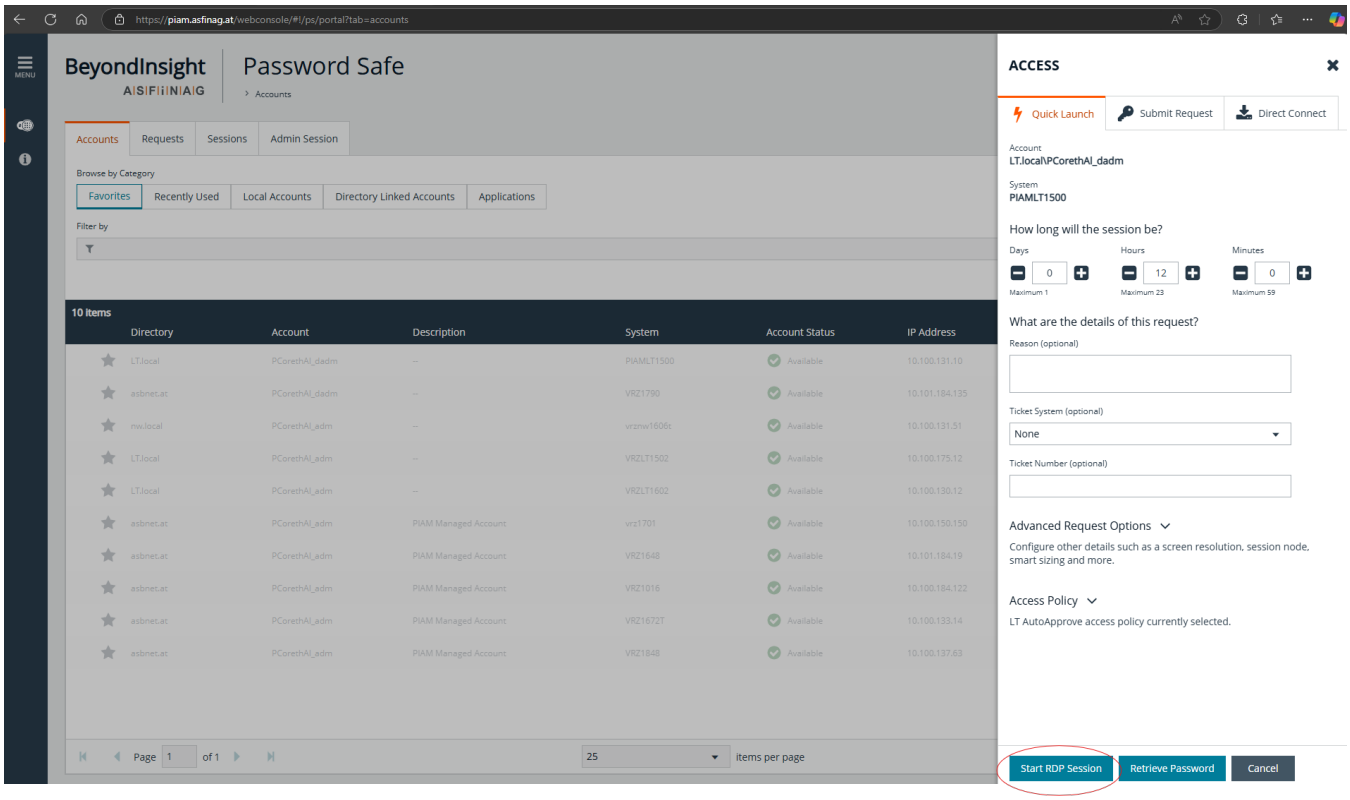
Die ausgewählten Server werden nun unter „Favorites“ angezeigt.



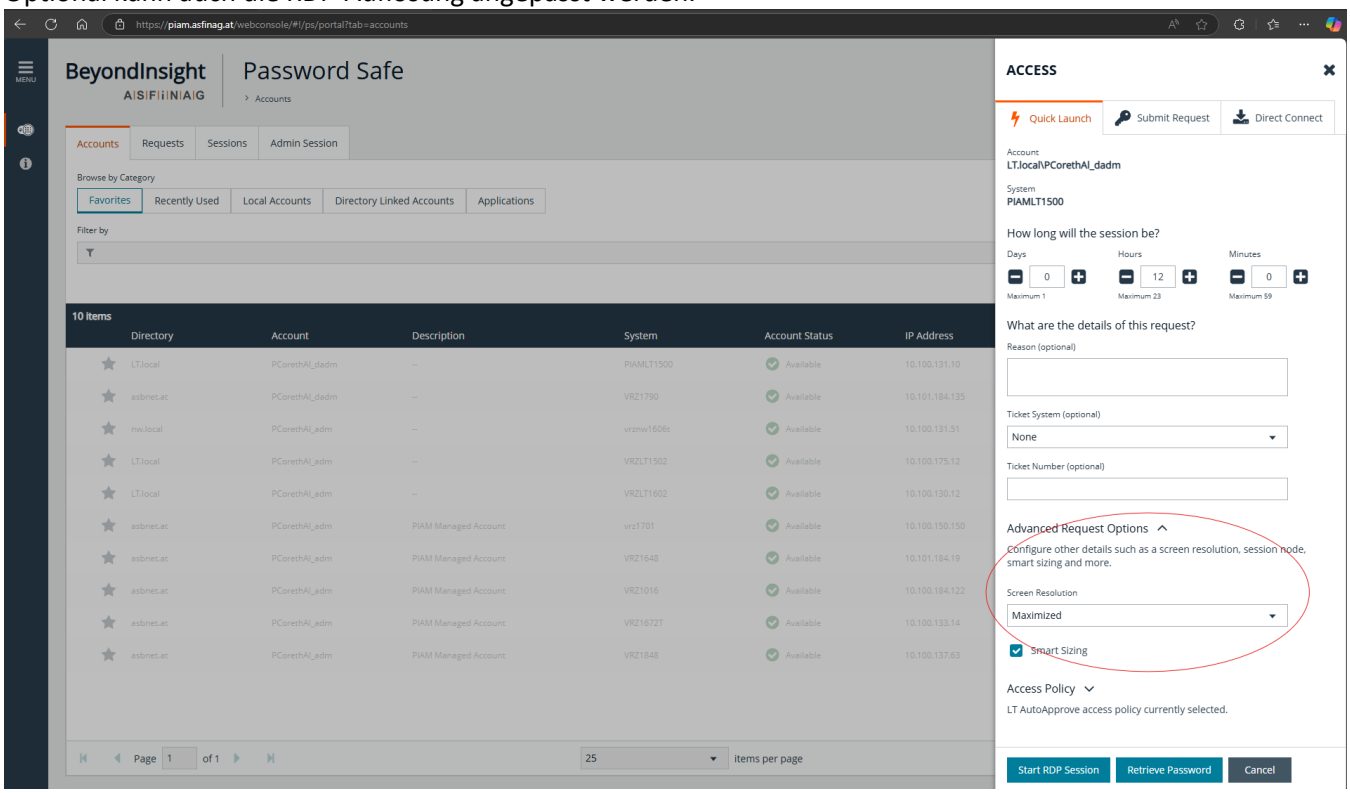
4.4 Öffnen einer RDP-Session zum Zielsystem

Abhängig von den Benutzerrechten wird eine Remote-Verbindung durch Klick auf das Access Symbol / Start RDP Session aufgebaut.

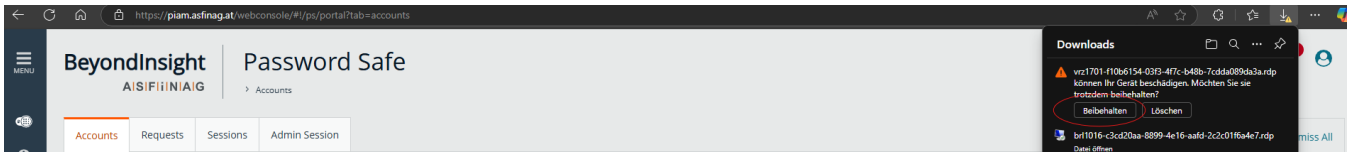




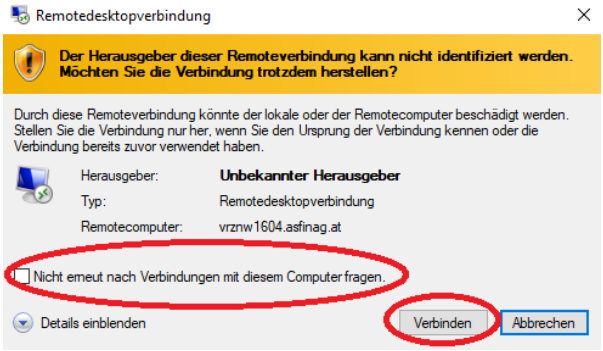
Optional kann auch die RDP-Auflösung angepasst werden.



Je nachdem, welcher Browser verwendet wird, müssen Pop-Up-Fenster erlaubt werden.



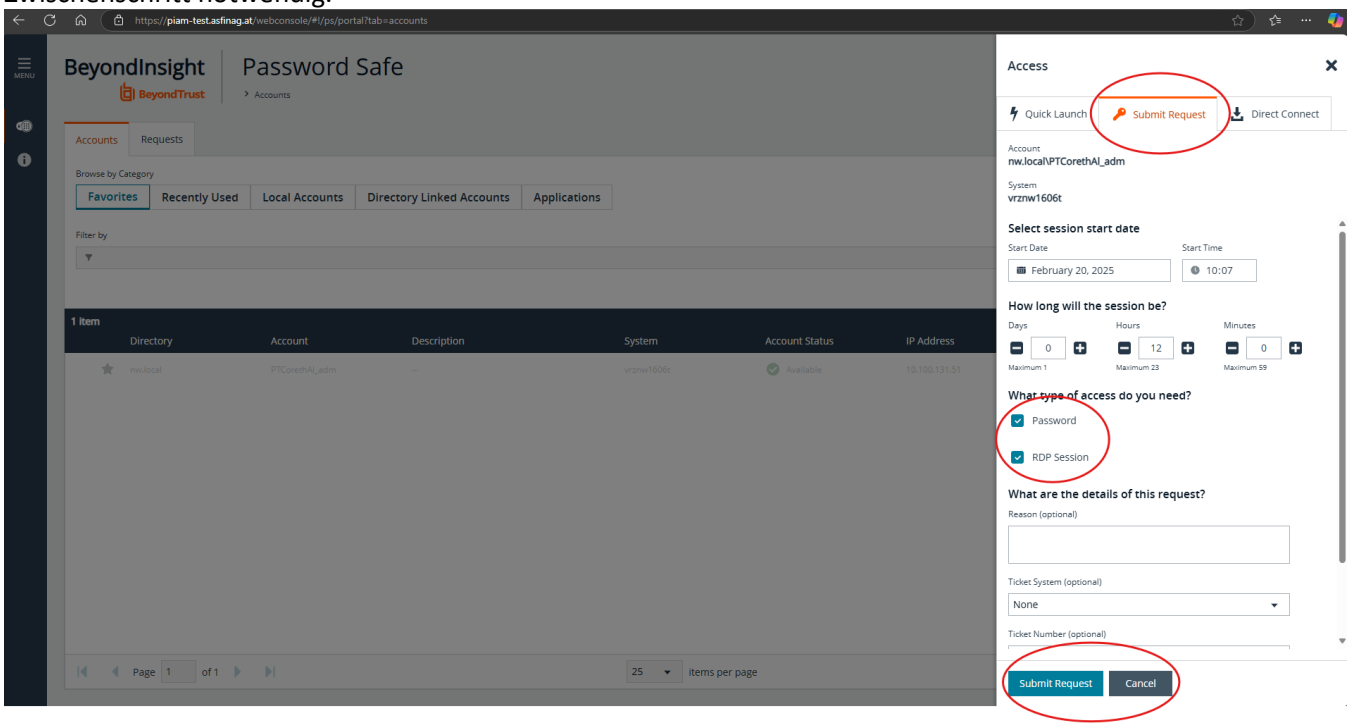
Abhängig von den verwendeten Sicherheitseinstellungen des Betriebssystems muss das Öffnen der RDP-Datei mit „Verbinden“ bestätigt werden.



Sie werden automatisch am Zielsystem (SSO) angemeldet.

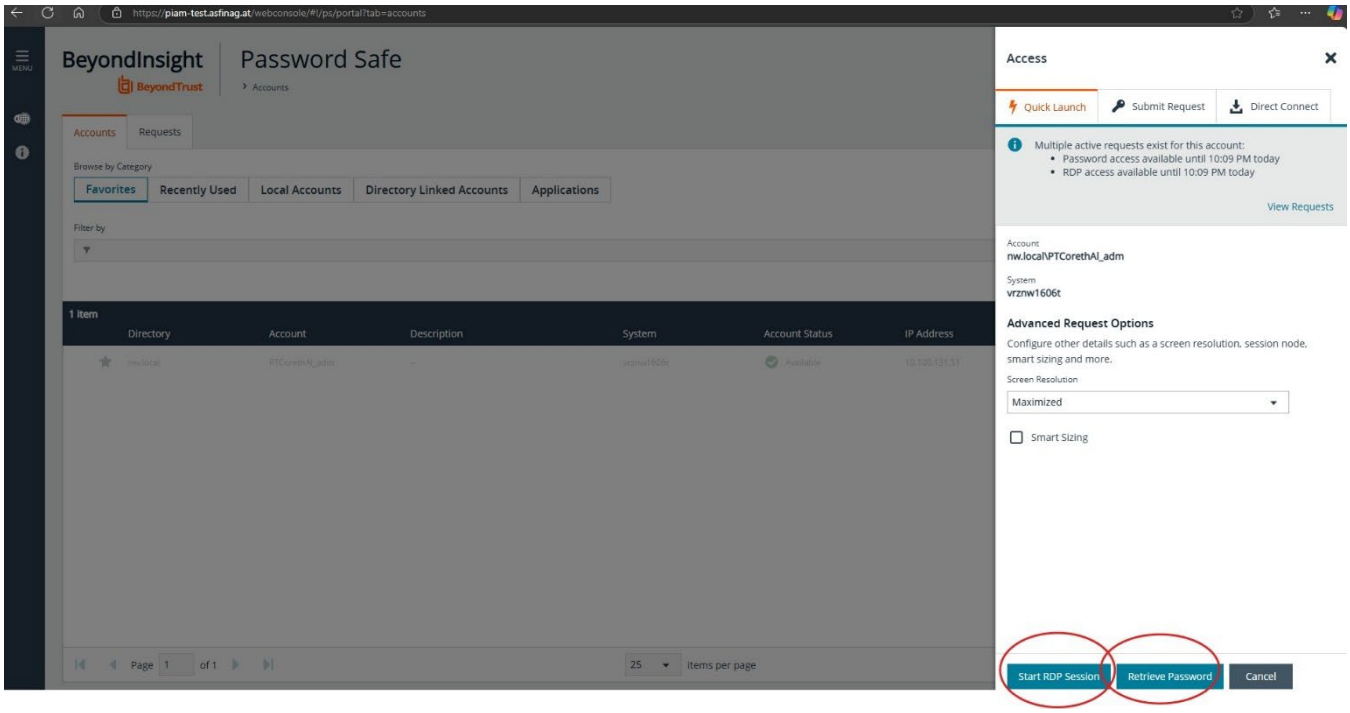
4.5 Öffnen einer RDP-Session und gleichzeitiges Auslesen des aktuellen Passworts

Um eine RDP-Session starten zu können und das Auslesen des aktuellen Passworts zu aktivieren ist folgender Zwischenschritt notwendig.



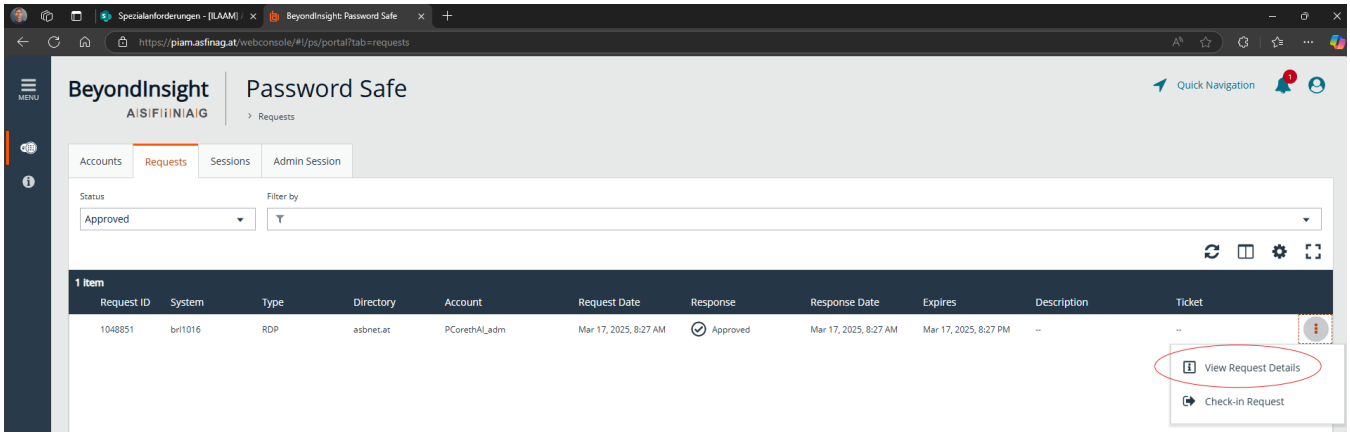
Achtung: Sollte bereits eine RDP-Session gestartet worden sein, muss das Häkchen bei „RDP-Session“ entfernt werden!

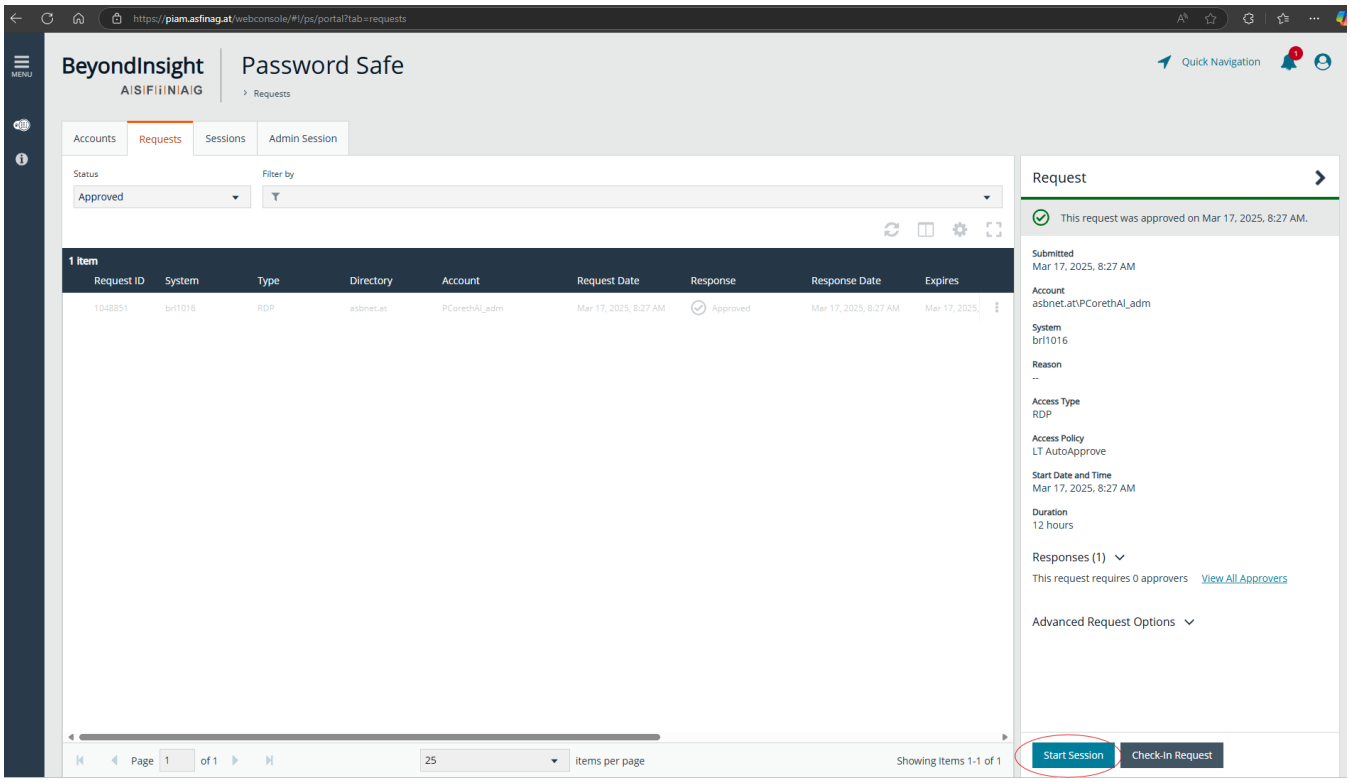
Nun kann eine RDP-Session gestartet und das Passwort ausgelesen werden:



4.6 Wiederverbinden einer RDP-Session bzw. erneutes Auslesen des aktuellen Passworts

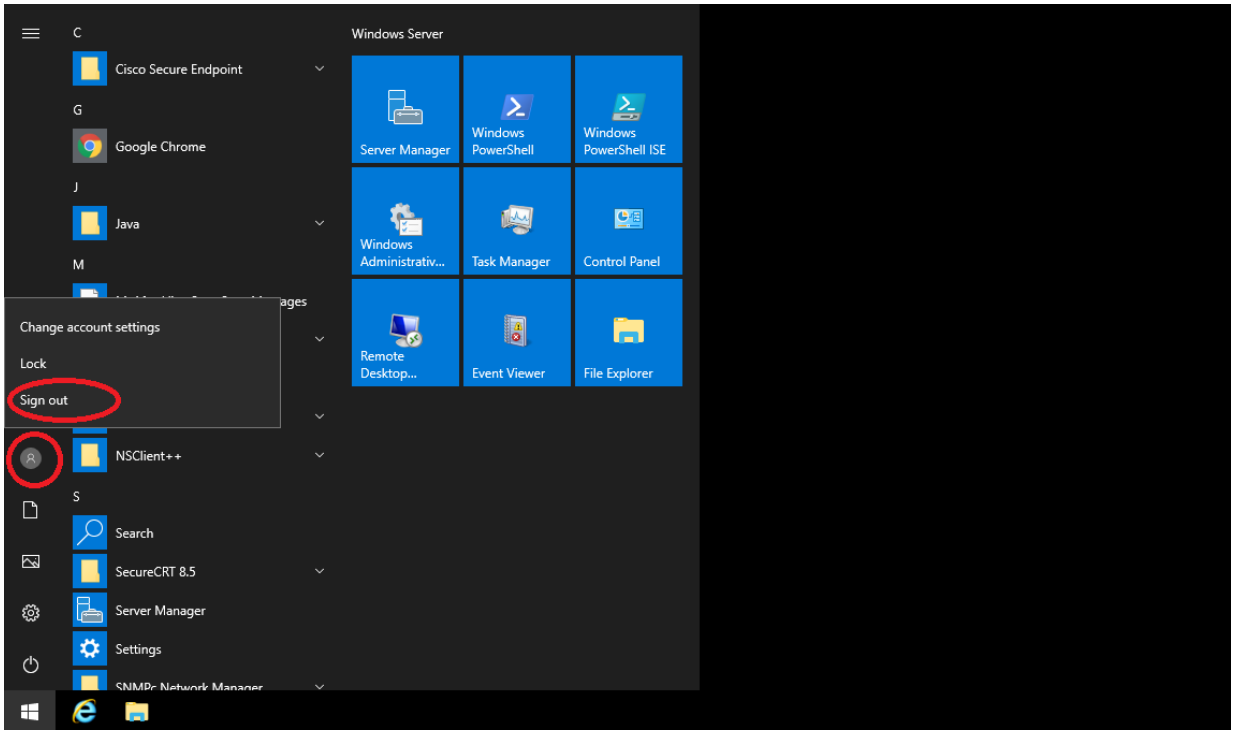
Um eine beendete RDP-Verbindung erneut zu verbinden, muss der aktuelle Request verwendet werden.





4.7 Beenden einer RDP-Session zum Zielsystem

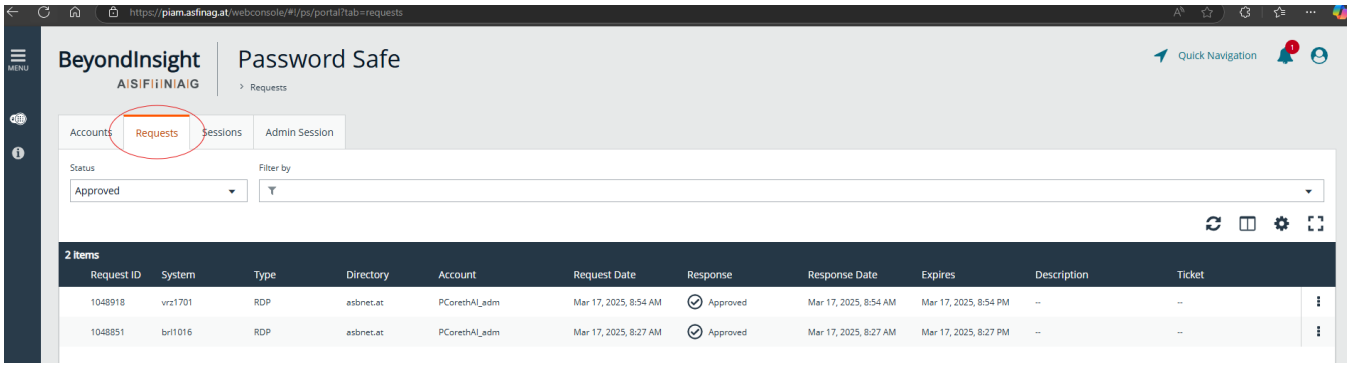
Aus Sicherheitsgründen ist es notwendig, alle bestehenden RDP-Sessions nach Abschluss der Administrationstätigkeiten wieder mit „Sign out“ zu beenden. „Getrennte“ RDP-Sessions mit geöffneten Programmen, führen fast immer zu einer Sperre des Benutzeraccounts!



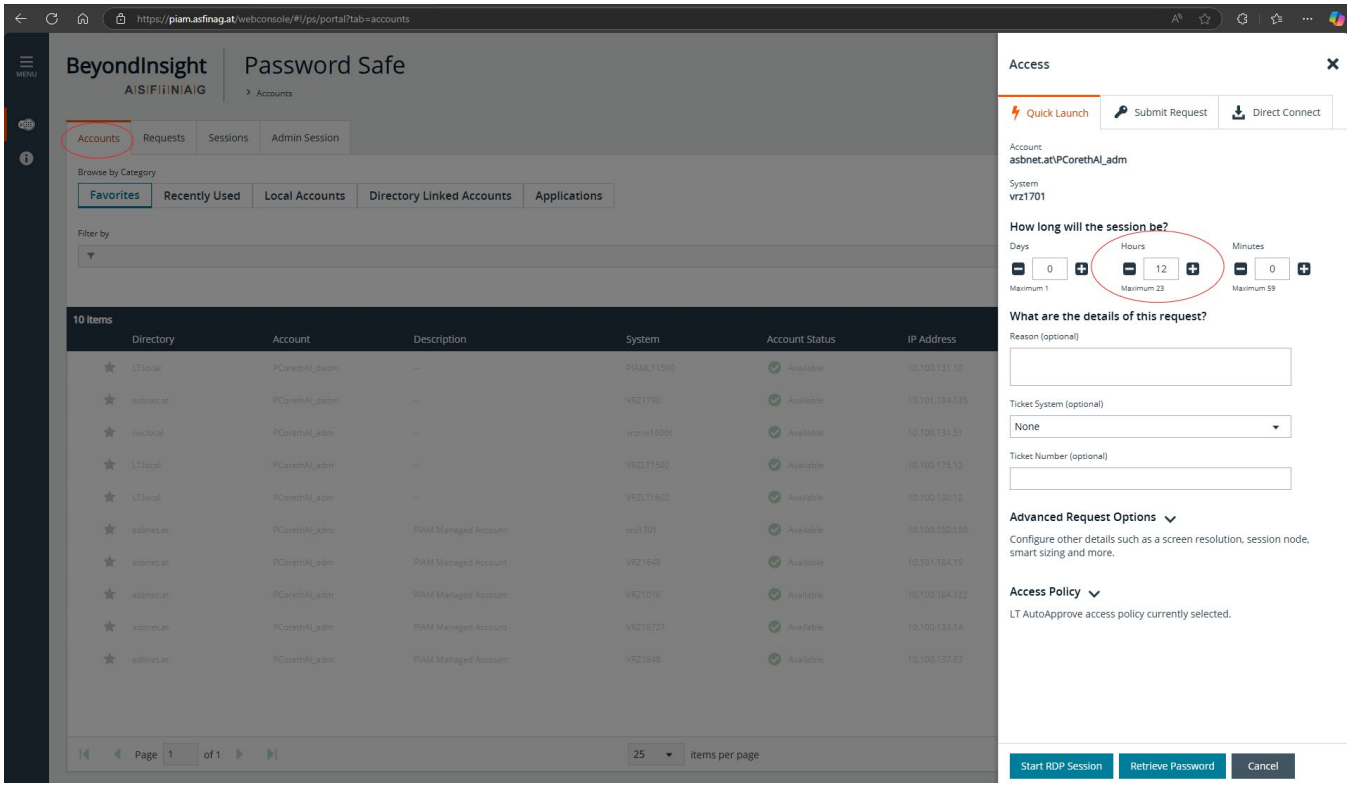
4.8 Requests anzeigen bzw. Requests mit bis zu 23 Stunden Laufzeit anfordern

Das Öffnen einer RDP/SSH-Verbindung bzw. das Auslesen eines Passwortes stellt im PIAM-System einen Request dar. Ein Standard-Request hat eine Gültigkeit von 12 Stunden. Nach Ablauf des Requests werden Kennwörter der verwendeten Accounts vom PIAM-System geändert.

Eine Liste der aktiven Requests sowie Ablaufzeit kann wie folgt abgefragt werden:



Der Request kann wie folgt bis auf eine Dauer von 23 Stunden geöffnet werden.



5 Fehlerbehebung

5.1 Browser

Die ASFINAG hat keinen Einfluss auf den installierten Browser sowie Browser Einstellungen unserer Partner und Dienstleister. Aus diesem Grund raten wir bei Problemen einen anderen Browser zu verwenden, um mögliche Inkompatibilitäten bzw. fehlerhafte Browser Einstellungen auszuschließen.
Weitere Lösungen für erfahrene Benutzer:

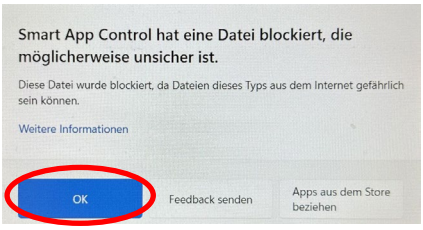
- Löschen des Browser Cache
- Zurücksetzen der Browsereinstellungen auf Default Werte

5.2 Pop-Up Blocker

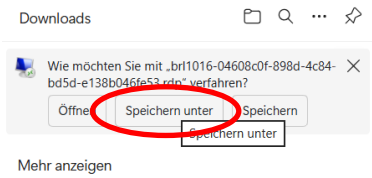
Pop-Up Fenster der PIAM-Webseite dürfen vom Browser nicht blockiert werden. Bei Verwendung eines Pop-Up Blockers ist eine Ausnahme für die PIAM-Webseite einzurichten.

5.3 Smart App Control blockiert RDP-Dateien

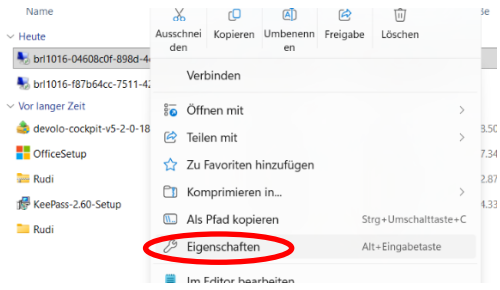
Bei bestimmten Installationen von Windows 11 verhindert Smart App Control den Download von RDP-Dateien.

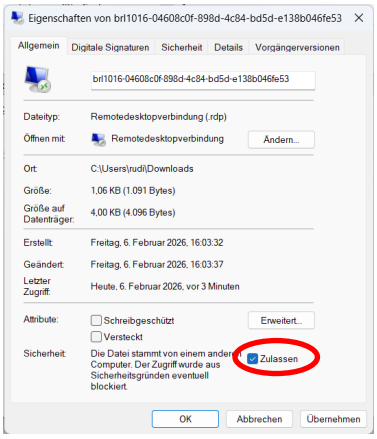


Aus diesem Grund muss die RDP-Datei zuerst gespeichert werden.



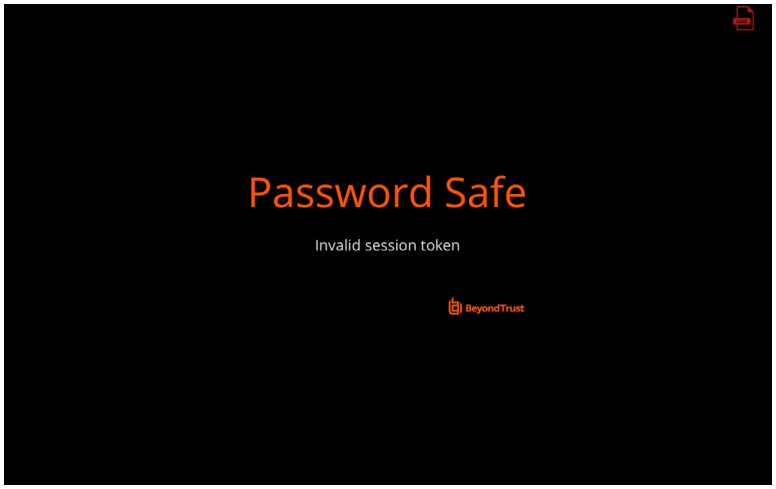
Danach können die Eigenschaften der RDP Datei wie folgt angepasst werden.





Nach der Anpassung kann die Datei geöffnet werden.

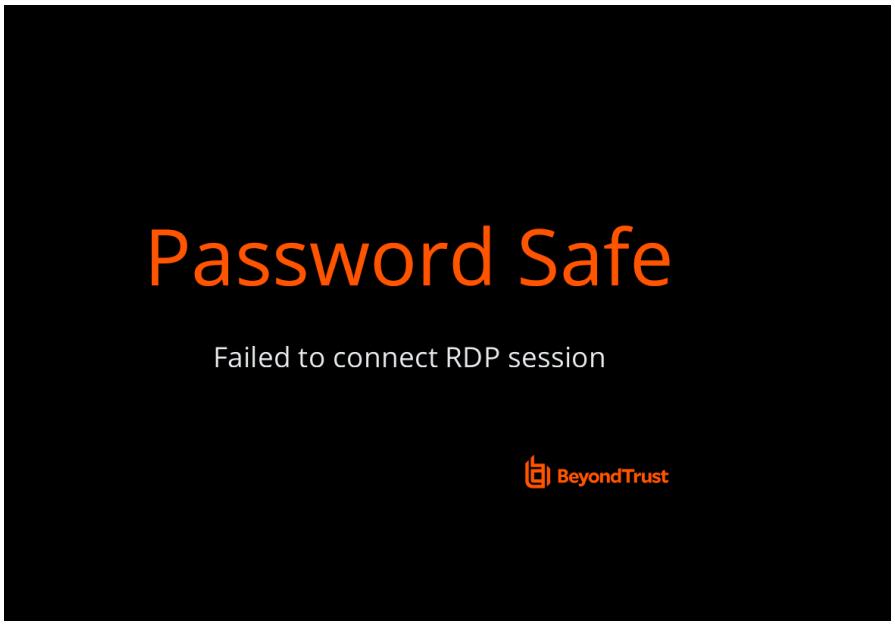
5.4 Fehlermeldung: „Invalid Session Token“



Eine Anmeldung auf dem Zielserver ist nicht möglich. Dieser Fehler tritt vermutlich aufgrund fehlender Berechtigungen auf Zielserver auf. Bitte klären Sie mit dem Technischen Support, ob ihr PIAM-Benutzer die notwendigen Rechte besitzt.

Externe Mitarbeiter können fehlende Berechtigungen über ihren ASFiNAG Ansprechpartner anfordern. ASFiNAG Mitarbeiter können fehlende Rechte direkt unter https://meinshop.asfinag.at anfordern.

5.5 Fehlermeldung „Failed to Connect RDP Session“

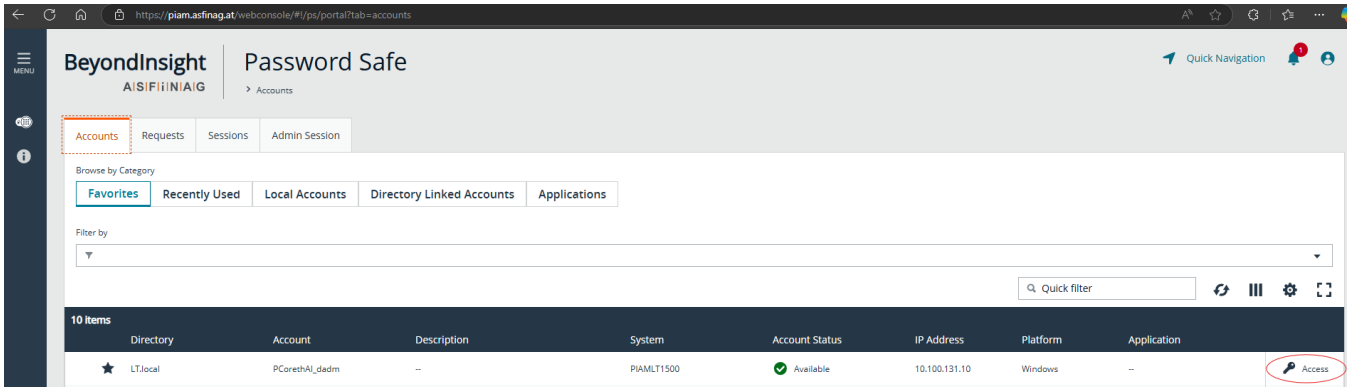


Diese Meldung deutet auf einen Fehler am Zielserver oder eines Anmeldeproblems am Zielserver hin. Dieser ist eventuell ausgeschalten oder auf Grund eines technischen Problems nicht erreichbar. Bitte klären Sie mit dem Technischen Support den Status des Zielservers ab, als auch ob die erforderlichen Zugriffsberechtigungen für diesen Server vorhanden sind.

5.6 Fehlermeldung: „Failed to authenticate due to one or more factors”

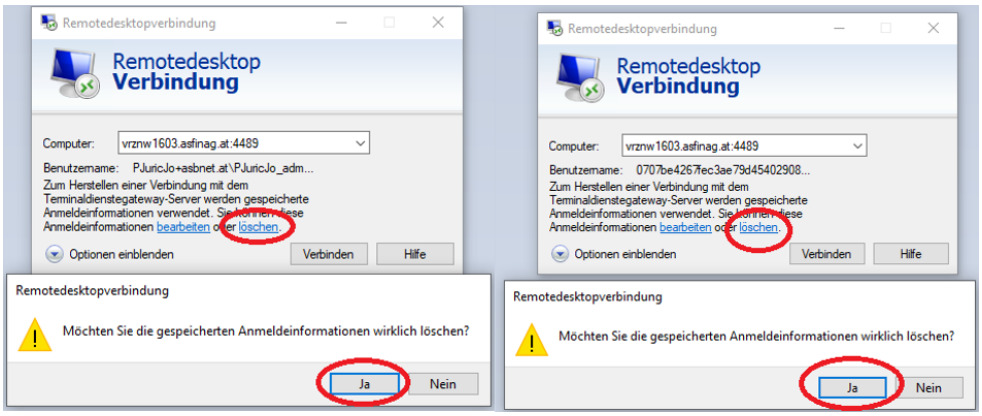
Nach dem Öffnen der RDP-Session über das PIAM Webinterface wird die Fehlermeldung „**Failed to authenticate due to one or more factors**” angezeigt.

Wichtig: Bitte beachten Sie, dass eine RDP-Session immer über den Button „Access“ gestartet werden muss!



Sollte der Fehler weiterbestehen, deutet dies meist auf eine fehlerhafte Konfiguration des Remotedesktop-Programms von Windows bzw. einem Fehler im Benutzer Profil des Client Rechners.

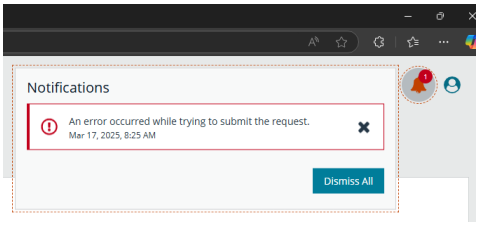
Als Erstes überprüfen Sie bitte, ob beim Windows Remotedesktop Programm Anmeldeinformationen für die Computer: piam.asfinag.at, vrznw1603.asfinag.at, vrznw1604.asfinag.at, brlnw1603.asfinag.at oder brlnw1604.asfinag.at gespeichert wurden. Wenn dies der Fall ist, bitte die Anmeldeinformation löschen und den Verbindungsaufbau erneut testen.



Sollte der Fehler weiterhin bestehen, kann der Fehler auch durch Löschen des Windows User Profiles behoben werden. Dieser Schritt sollte nur von erfahrenen Benutzern durchgeführt werden.

Um einen Datenverlust zu vermeiden, ist vor dem Löschen des Benutzerprofils ein Backup zu erstellen. Bei Firmen PCs nehmen sie bitte Kontakt mit Ihrer IT-Abteilung auf, um die weitere Vorgehensweise abzustimmen.

5.7 Fehlermeldung: „An error occurred while trying to submit the Request"



Dieser Fehler tritt auf, wenn eine beendete RDP-Session erneut über „Accounts" geöffnet wird. Der korrekte Weg, um eine Verbindung wieder zu verbinden ist unter Punkt 4.6 beschrieben.

5.8 https://piam.asfinag.at kann im Browser nicht geöffnet werden

Diese Meldung deutet auf einen Fehler bei der DNS-Auflösung von piam.asfinag.at auf dem Client hin. Die DNS-Auflösung kann mit folgendem Befehl auf Windows Rechnern überprüft werden:

nslookup piam.asfinag.at

Das Ergebnis muss wie folgt aussehen:

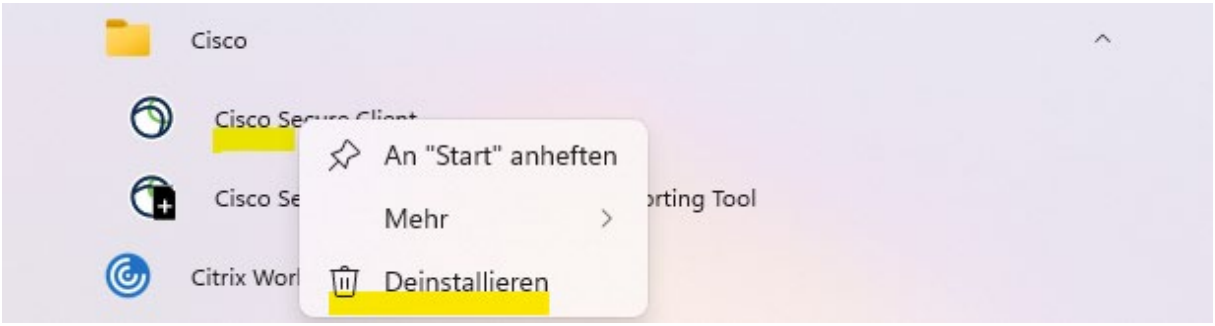
Name: piam.asfinag.at
Address: 10.100.131.253

Sollte der Befehl keine Antwort liefern, handelt es sich um einen DNS-Problem auf dem Client. Häufig blockiert eine Firewall im Clientnetzwerk DNS-Antworten mit privaten IP-Adressen 10.x.x.x. Diese sind aber für die Funktion von PIAM zwingend notwendig.

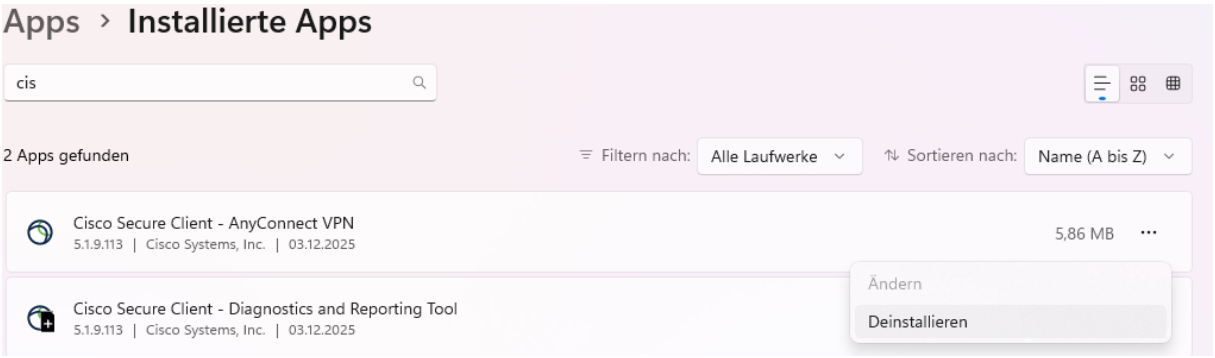
5.9 Deinstallation Cisco AnyConnect

Es wird empfohlen, den Cisco AnyConnect Client zu deinstallieren, da es bei einem Parallelbetrieb mit dem Palo Alto GlobalProtect VPN-Client zu Verbindungs- oder Routingkonflikten kommen kann. Bitte verwenden Sie ausschließlich den Palo Alto GlobalProtect Client.

Im Start Menu kann dieser deinstalliert werden.



Deinstallieren Sie folgende Cisco Apps.



6 Fehlermeldungen und Technischer Support

Störungen und Fehler am PIAM-System können per Telefon bzw. Mail an den ASFINAG MSG Service Desk gemeldet werden.

E-Mail Support: **support@asfinag.at**
Telefon Support: +43 50 108 – 99999 und die „2“
Erreichbarkeit: 24x7

Durch Angabe der folgenden Informationen kann die Entstörung beschleunigt werden, da bereits einige Fehler durch gezielte Checks ausgeschlossen werden können.

PIAM-Benutzeraccount	z.B.: Pext_MusterMa
Zielserver	z.B.: VRZLT1500

7 Anhang

7.1 Abkürzungen und Begriffsbestimmungen

Abk. / Begriff	Bedeutung
PIAM	**P**rivileged **I**dentity & **A**ccess **M**anagement
MSG	ASFiNAG Maut Service GmbH
RDP	MS Remote Desktop Protocol

7.2 Historie

Freigabe-Version	**Gültig ab**	**Erstellt von** Ges/Abt./Name	**Änderungsgrund**
1.0	14.04.2018	MSG/SE/ACO	
1.1	04.12.2018	MSG/SE/ACO	VPN Firewall Tausch remote.cnas.at → rfw.cnas.at
1.2	08.01.2019	MSG/SE/ACO	Kapitel Fehlerbehebung hinzugefügt
1.3	04.09.2019	MSG/SE/ACO	Favoriten Funktion, Beenden einer RDP Session, Request Verwaltung, Fehlerbehebung erweitert
1.4	18.08.2020	MSG/SM/ACO	Punkt 5.5 Fehlermeldung: „Failed to authenticate due to one or more factors" hinzugefügt.
1.5	14.09.2020	MSG/SM/ACO	VPN Firewall Link geändert rfw.cnas.at
1.6	25.09.2020	MSG/SM/ACO	Fehlermeldungen überarbeitet
1.7	23.05.2022	MSG/SM/ACO	piam.asfinag.at und node Auswahl angepasst
1.8	05.08.2022	MSG/SM/JJR	Screenshots, Node-Namen und Texte aktualisiert
1.9	14.03.2025	MSG/SM/ACO	Screenshots, Texte angepasst, weitere Punkte hinzugefügt
2.0	20.03.2025	MSG/SM/ACO	Screenshots, Texte angepasst, weitere Punkte hinzugefügt
2.1	03.02.2026	MSG/SM/ACO	Paloalto GlobalProtect