Universität St.Gallen

Benutzeranleitung DELINEA Portal (SSC) Rev. 1.2

St.Gallen, 24. September 2024

Inhaltsverzeichnis

1 Einleitung

Vorbemerkung:

Diese Anleitung erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit. In der Anfangsphase werden laufend Aktualisierungen vorgenommen. Wir geben uns Mühe nur die für die Nutzung nötigsten Begriffe und Tätigkeiten zu erläutern. Sie können uns gerne Ihre Rückmeldungen diesbezüglich an die untenstehende Mailadresse weiterleiten.

Mit dieser Anleitung erhalten Sie Informationen zur PAM-Lösung der Universität St.Gallen. Erklärt werden die grundlegenden Funktionen und die Bedienung vom eingesetzten Werkzeug, dem Delinea Secret Server Cloud (Abkürzung: SSC). Diese Anleitung erklärt, wie Sie mit Hilfe vom SSC einen Fernzugriff auf ein System der Universität St.Gallen durchführen (Remote Access: RAS) und Secrets (Informationen, wie Anmeldenamen und Passwörter) verwalten können.

Jeder Zugriff setzt selbstverständlich die dafür notwendigen Berechtigungen voraus. Wenn Sie Hilfe benötigen, wenden Sie sich bitte an Ihre zuständige Ansprechperson oder senden Sie ein E-Mail (Angabe von: Kontoname, Vermerk "PAMSOLUS", Ihrer Mobilnummer und Erreichbarkeit) an: BusinessPlatform@unisg.ch.

Das Delinea Portal ist der zentrale Einstiegspunkt für den RAS-Verbindungen und die Verwaltung von Secrets. Es ersetzt die bisher verwendete Applikation «pwdb.unisg.ch».

1.1 RAS

Unter RAS versteht man einen Dienst, der eine Verbindung zu einem Zielsystem ermöglicht (z.B. RPD, SSH, …). RAS benutzt für die Anmeldung Secrets, die im SSC gespeichert sind. Grundsätzlich wird für den Systemzugriff ein lokales Systemkonto verwendet.

Das Delinea Portal ermöglicht es, sich über RAS mit den Systemen zu verbinden, ohne das Passwort des Zielsystems zu wissen. Diese Verbindungen werden gesichert und der Service steht auch ohne VPN-Nutzung zur Verfügung.

1.2 Secrets

Secrets sind Geheimnisse, die mit vertraulichen Informationen wie Benutzernamen, Passwörtern und allenfalls weiteren sicherheitsrelevanten Informationen.
Der Zugriff auf ein Secret erfolgt nach dem Prinzip der minimalen Rechtevergabe. Benutzer*innen werden nur Secrets angezeigt, wenn mindestens Leseberechtigungen vorhanden sind.

1.3 Secret Vorlagen

Secret Vorlagen legen fest, welche Attribute und Parameter in einem Secret vorausgesetzt und/oder freiwillig sind. Basierend auf diesen Vorlagen kann auch das Verhalten und die erlaubten Funktionen für ein Geheimnis gesteuert werden.

Zudem können über das Delinea Portal Secrets (analog PWDB) verwaltet werden.
Die Berechtigungen für die Secrets sind nach dem Prinzip der minimalen Rechtevergabe nur für die bestimmte Personen erteilt.

2 Erste Schritte

2.1 Benutzerkonto

Für Erstanmeldung befolgen Sie bitte die Schritte wie sie im zugestellten E-Mail aufgeführt sind. Die privilegierten [PAB|PAE|PAN]-Konten* ist ausschliesslich für die Verwendung im Zusammenhang mit dem Delinea Portal vorgesehen. Nach der erfolgreichen Konto-Einrichtung** (My Account (microsoft.com) können Sie sich am Delinea Portal (s.u.) anmelden. Die Aktivierung von MFA und die Kennwortänderung sind zwingend.

* PAB (Business User); PAE (External User); PAN (Named User)

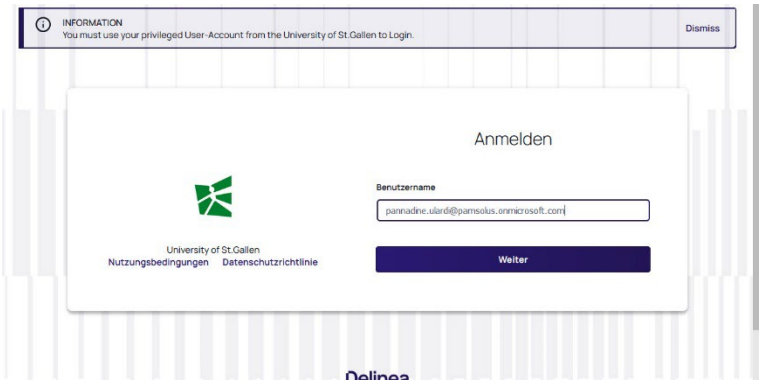
** siehe Microsoft Kontoregistrierung und Informationen anzeigen

2.2 Portal Login

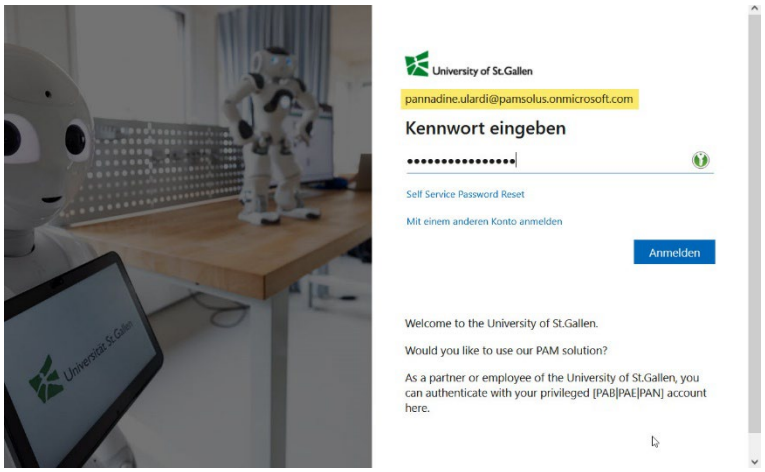
Um sich beim DELINEA Portal (https://pamsolus.delinea.app/)anzumelden (Authentifizierung) verwenden Sie ihr PAMSOLUS Microsoft-Konto mit MFA!

Wenn Sie unsicher sind oder Hilfe benötigen, wenden Sie sich bitte per E-Mail und unter Angabe von: Kontoname, Vermerk "PAMSOLUS", Ihrer Mobilnummer und Erreichbarkeit an unseren Servicedesk: "BusinessPlatform@unisg.ch".

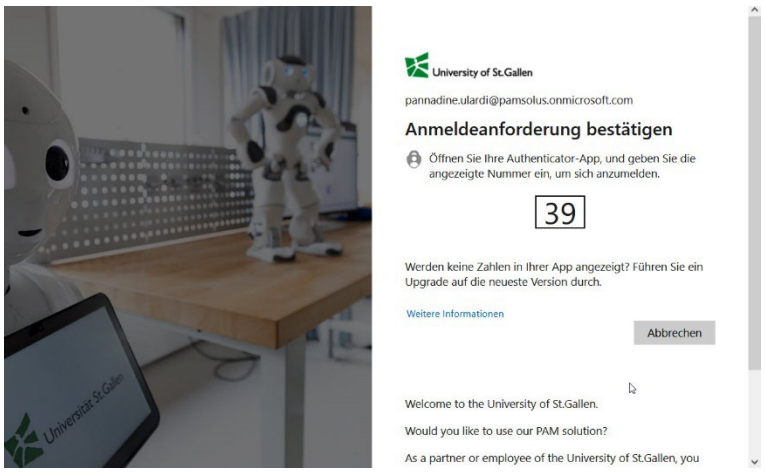
Benutzername eingeben.



Es erfolgt die automatische Weiterleitung zum Authentifizierungsportal von Microsoft. Bitte geben Sie Ihr Kennwort ein. Zukünftig werden wir auch die kennwortlose Anmeldung anbieten, wissen aber noch nicht, wann dass der Fall sein wird.

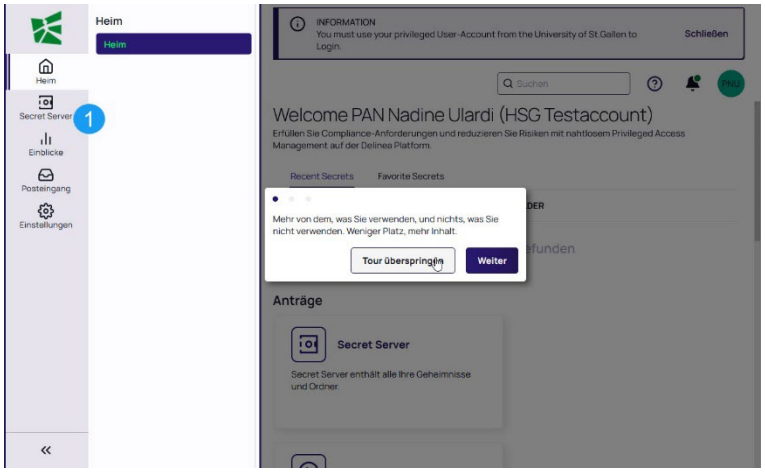


Wurde das Kennwort erfolgreich verifiziert, werden Sie aufgefordert in der Microsoft Authenticator App einen 2 Faktor einzugeben, hier z.B. einen 2-stelligen Code einzugeben.

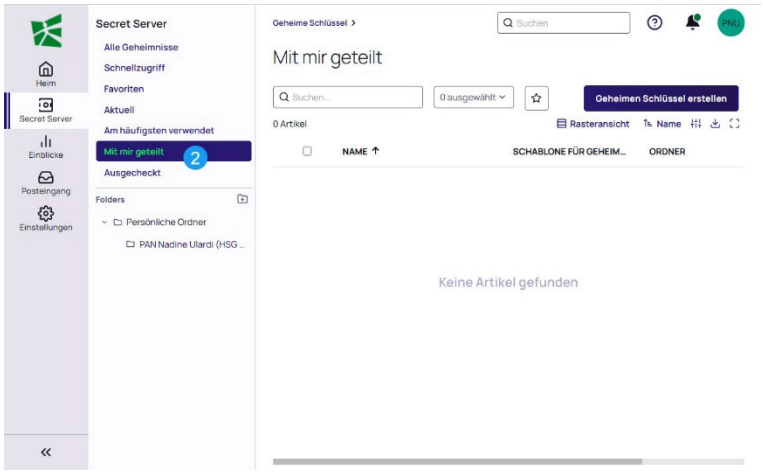


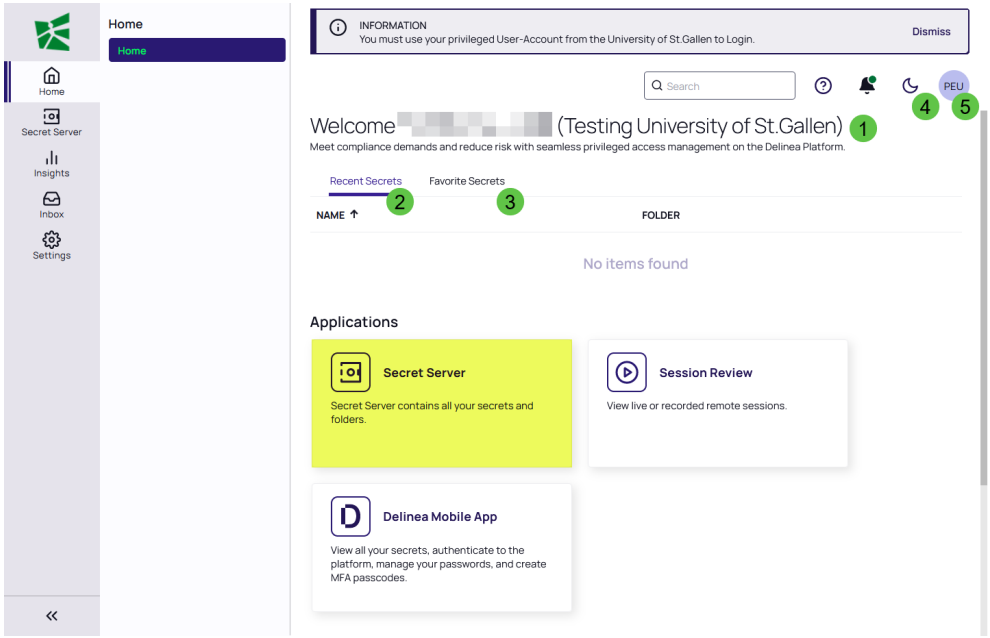
Ist das ebenfalls erfolgreich, können Sie das DELINEA Portal (mit den Ihnen zugeteilten Berechtigungen, Authorisierung) benutzen.

Der wichtigste Menu-Punkt wird "Secret Server" (1) sein.



Unter dem Menu Punkt (2) sehen Sie alle Secrets auf die Sie mindestens Lesezugriff haben.

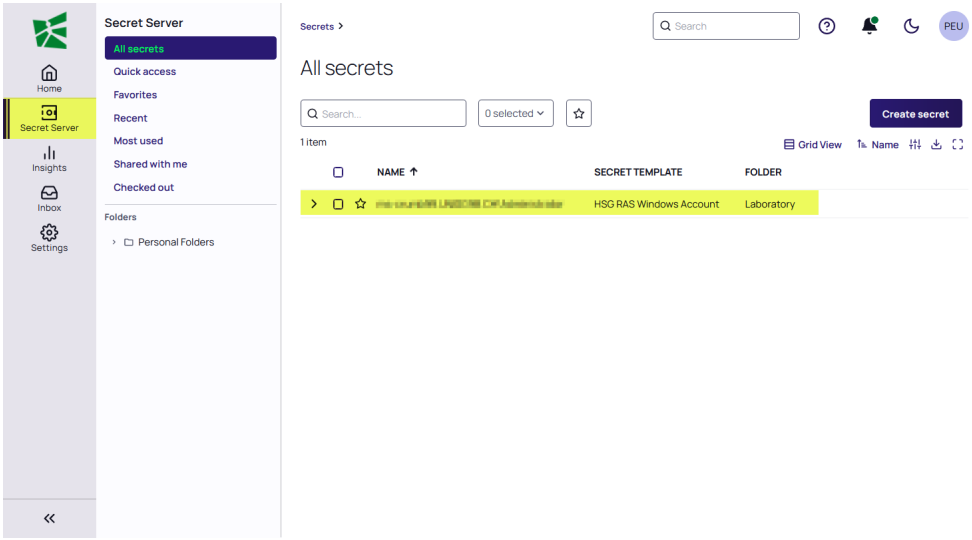




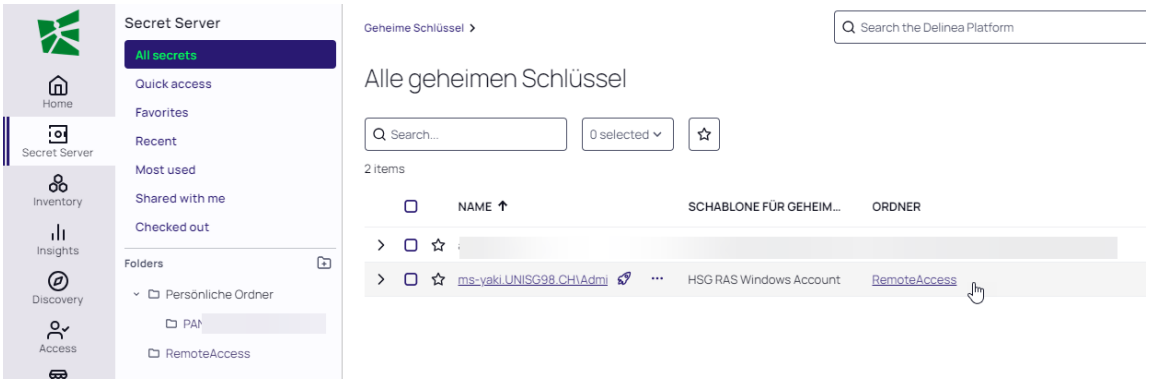
Auf der Home-Anzeige werden Ihr Anmeldename (1), die zuletzt verwendeten Secrets (2) und Ihre Lesezeichen (3) angezeigt. Das Mondsymbol (4) erlaubt es zur dunklen Anzeige zu wechseln und unter dem Punkt (5) können Sie sich wieder abmelden und Kontoinformationen anzeigen lassen.

2.3 Secrets finden (suchen)

Die Secrets sind über die Hauptnavigation –> Secret Server zugänglich. Die Anzahl der sichtbaren Secrets hängt von Ihren Berechtigungen ab. Die Anzeige können Sie gemäss Ihren Vorlieben anpassen.



Tipp: Verwenden Sie die **Suche,** um ein Secret zu finden!



Benutzer*innen können einen persönlichen Ordner mit exklusivem Zugriff nutzen.
Im persönlichen Ordner dürfen KEINE privaten Secrets gespeichert werden. Erlaubt sind ausschliesslich persönliche, geschäftliche Secrets. Teilen Sie diese Secrets mit niemandem. Es gibt keinen Support für persönliche Ordner.

2.4 Secret erstellen

Für den Namen und den Speicherort eines Secret empfehlen wir Folgendes:

- Gute Namen verwenden. Goldene Regel s.u.
- Immer vorher absprechen mit Teamkollegen.
- Secret-Ordner sinnvoll auswählen und Berechtigungen korrekt setzen. Ausser in wenigen Ausnahmen werden diese vererbt!

Verwendung von Präfix/Schlüsselwort (Empfehlung)
[APP|WEB|CERT|SRV|USR|...]_[Admin|User|Support|...]_[Kurze, prägnante und SUCHBARE Beschreibung)

Beispiele:

WEB Admin ADOBE
APP Admin Glutz Access
WEB Support MVPS SoftwareOne
SRV ADFS Service Production
PRIV User PCIHans.Muster
WEB User PERI-01078 (NETIO 4)
CERT LDAPS Active Directory Production

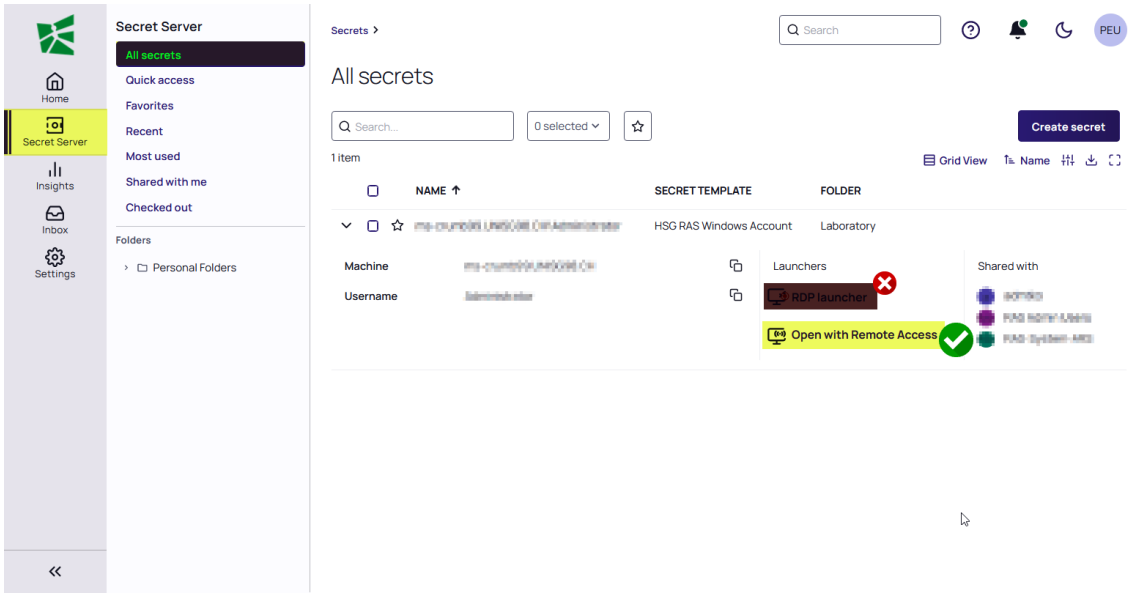
Wenn Unsicherheiten bezüglich Namen oder Speicherort bestehen, zögern Sie nicht das Team Secret Server zu kontaktieren.

2.5 Remote Access

SSC stellt verschiedene Launcher für den Remote Access auf ein System zur Verfügung. Der klassische RDP-Launcher (Windows RDP) wird künftig seitens HSG-IT nicht mehr unterstützt, daher wird er hier nicht beschrieben.

2.5.1 Remote Access Launcher (Webbrowser)

Die Remotesitzung startet im Webbrowser. Es wird keine Installation benötigt.



2.5.2 Remote Access Launcher (Connection Manager)

Der Connection Manager von Delinea erlaubt direkte Serververbindungen ohne das Delinea Portal. Er muss auf dem Client installiert werden. Dieses Werkzeug kann für häufige und gleichzeitige RAS-Verbindungen eingesetzt werden.

Bild wird noch eingefügt

2.5.3 Putty launcher (SSH)

Mit dem Putty launcher kann man sich per SSH mit Systemen verbinden, wenn Putty auf dem Client installiert ist, von dem aus man die Verbindung herstellen will.

Bild wird noch eingefügt

2.5.4 Weblauncher

Bild wird noch eingefügt

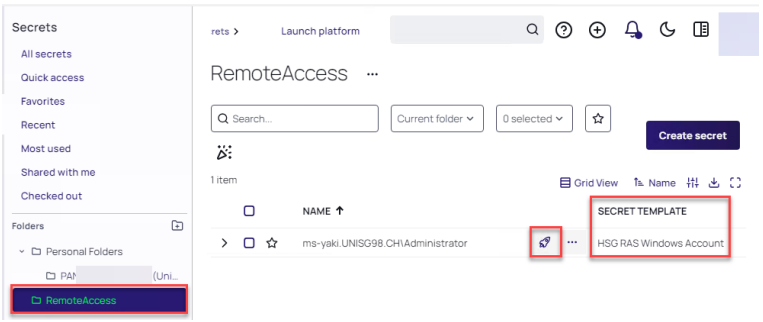
Weitere Launcher werden in Zukunft bei Bedarf implementiert.

2.5.5 Verbindung auf das System per Webbrowser Launcher

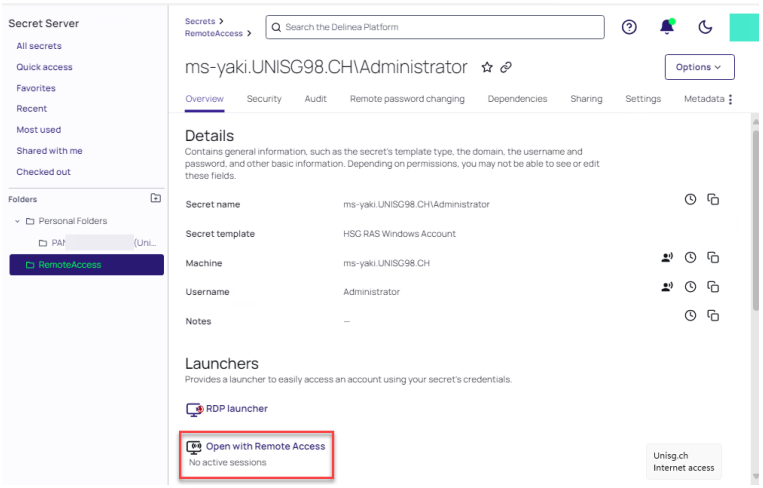
Suchen und identifizieren Sie das Secret, dass Sie für die Herstellung der Verbindung benötigen. Wenn ein Secret ein Launcher-Symbol (Rakete) hat, bedeutet dies, dass Sie einen Remotezugriff mit diesem Secret herstellen können. Der Launcher ist in diversen Anzeigen zu sehen. Das verwendete Secret Template «HSG RAS Windows Account» deutet auf ein Secret hin, das für Windows Systeme für den RAS-Zugang benutzt werden kann.

Der Ordner «Remote Access» ist der Speicherort für alle Secrets, die für den Fernzugriff auf Systeme erforderlich sind.

Listenansicht des Secret Ordners:



Oder über das geöffnete Secret:



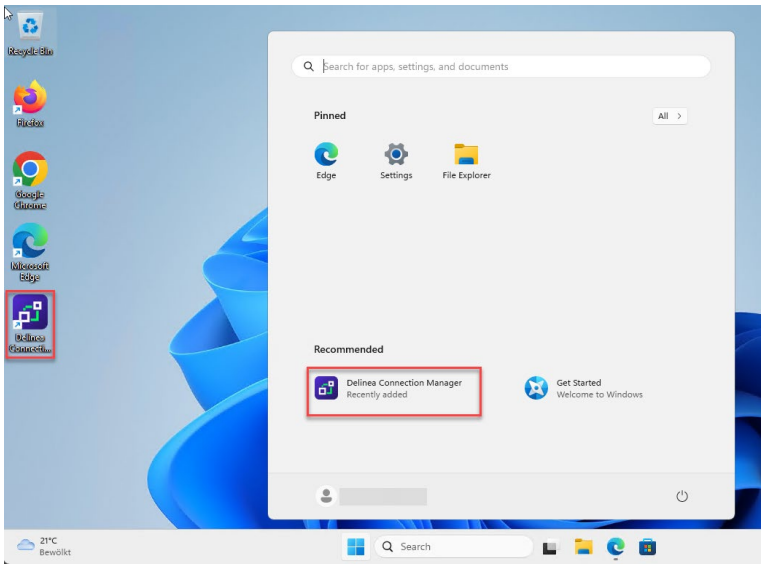
Weitere Funktionen stehen ihnen über das Delinea Menu zur Verfügung. Trennen Sie Ihre Verbindung über das Delinea Menü «D» - **Disconnect**.

2.5.6 Connection Manager

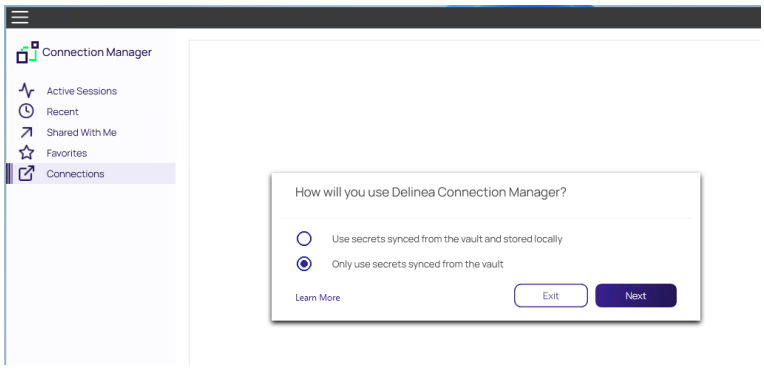
Mit dem Connection Manager kann man sich mit dem System verbinden, ohne einen Webbrowser zu verwenden. Das Gerät, das die Systemverbindung aufbauen will, muss den Connection Manager installiert haben.

Der Connection Manager kann unter dem folgenden Link heruntergeladen und installiert werden: https://delinea.center/cmgr/link/ConnectionManagerWinDownload

Öffnen Sie die installierte Applikation «Connection Manager».



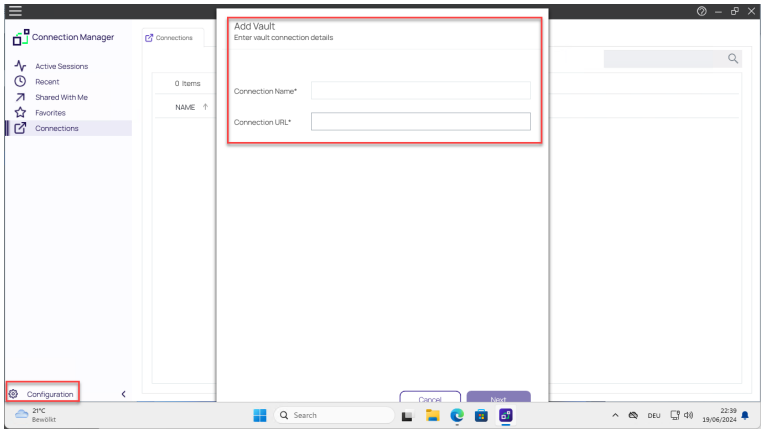
Wählen Sie «Only use secrets synced from the vault».



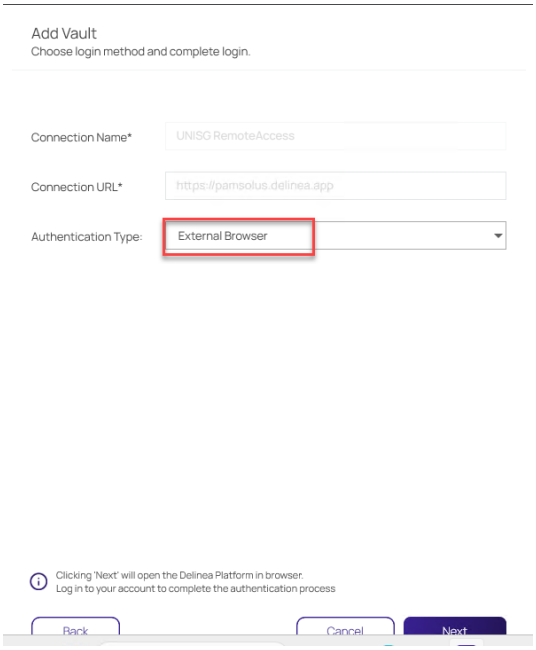
Bei der ersten Nutzung muss eine Verbindung zum Secret Server hergestellt werden. Falls diese Aufforderung aus Versehen geschlossen wird, wird man über Configuration – Delinea Vaults wieder zu ihr gelangen.

Geben Sie der Verbindung einen Namen, z.B. UNISG RemoteAccess

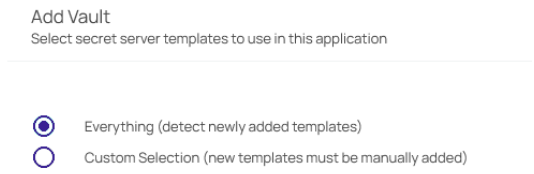
Geben Sie die URL ein: https://pamsolus.delinea.app



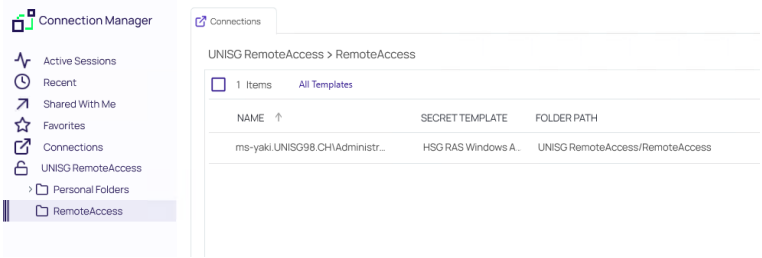
Wählen Sie «External Browser» - Next und folgen Sie dem Anmeldeprozess.



Übernehmen Sie die Standardeinstellung.



Ein Doppelklick auf das Secret im Connection Manager stellt eine Verbindung zum System her.



3 Anhang

3.1 Microsoft Kontoregistrierung und Informationen anzeigen

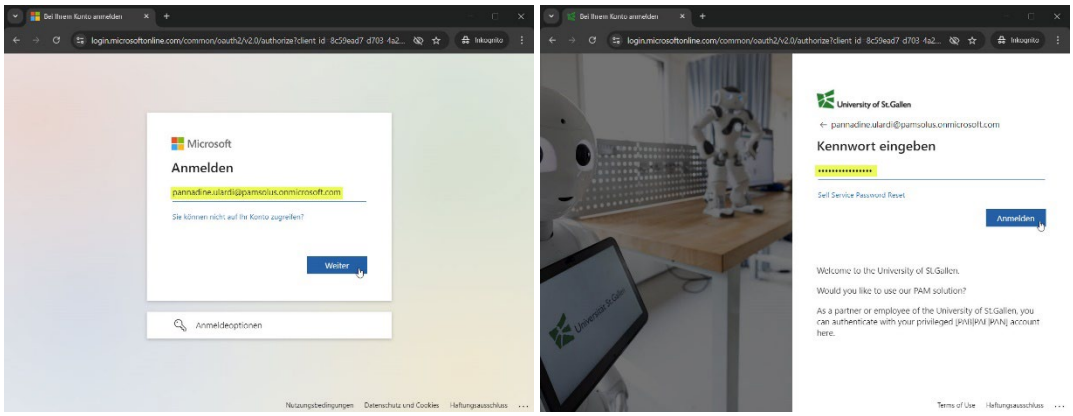
Nach dem Erhalt der Kontoinformationen zum PAMSOLUS-Account müssen sie vor der Benutzung die Registrierung durchführen.

In der folgenden Anleitung sind sinngemäss die dazu notwendigen Schritte aufgeführt. Beachten sie bitte, dass je nach Betriebssystem/Browser die Darstellung etwas anders sein kann. Es ist auch möglich, dass sich die Verfahren leicht ändern.

Wenn Sie unsicher sind oder Hilfe benötigen, wenden Sie sich bitte per E-Mail und unter Angabe von: Kontoname, Vermerk "PAMSOLUS", Ihrer Mobilnummer und Erreichbarkeit an unseren Servicedesk: "BusinessPlatform@unisg.ch".

Registrierung: Webbrowser öffnen und URL: https://https://myaccount.microsoft.com/ eingeben.

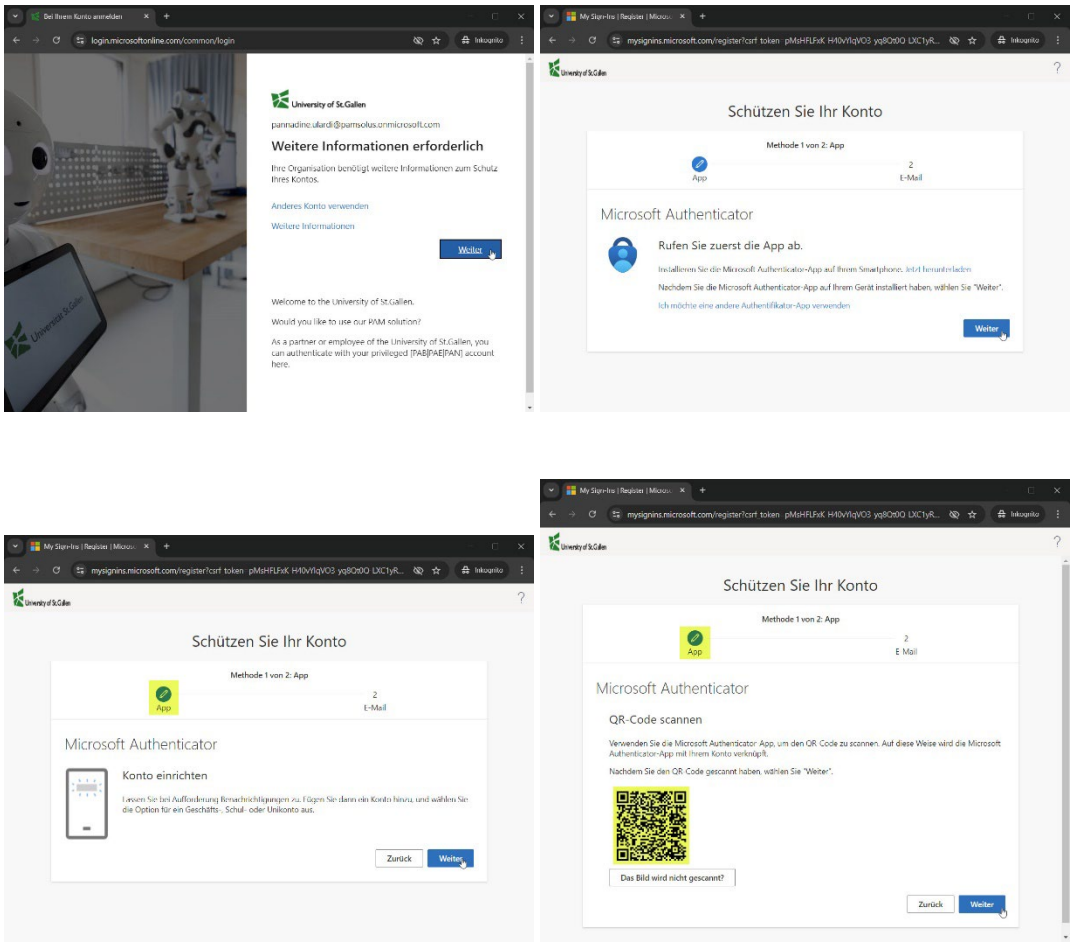
Bei aufgeführten Kontonamen handelt es sich um ein internes Testkonto, dann stellvertretend für Ihr persönliches Konto steht.



Achten Sie bitte darauf, dass im 2. Fenster das Logo der Universität St.Gallen mit dem entsprechenden Text erscheint.

Falls Sie nicht sicher sind, ob Sie sich auf der korrekten Seite sind, brechen Sie bitte den Vorgang ab und melden Sie sich bei uns.

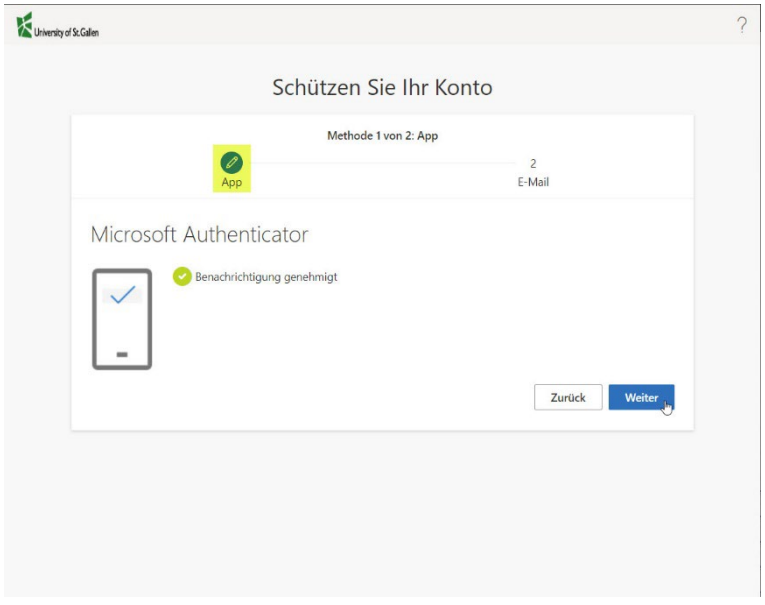
Wurde das Initialkennwort korrekt eingegeben, werden Sie aufgefordert weiter sicherheitsrelevante Informationen zu registrieren:



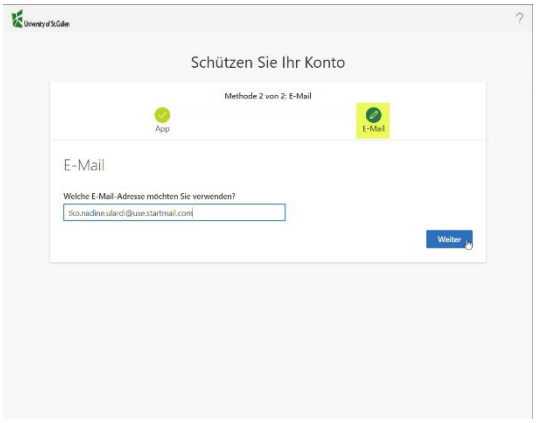
In der Microsoft Authenticator App können sie mit dem "+"-Zeichen ein neues "Geschäfts- oder Schulkonto hinzufügen.

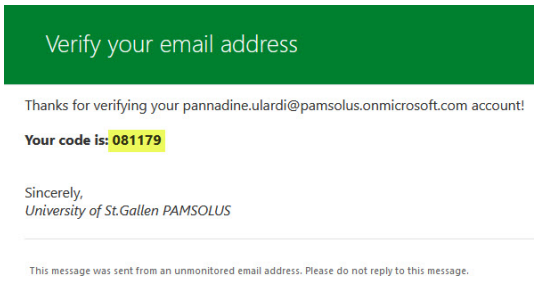
Scannen Sie den angezeigten Code.

Ist das Konto in der App eingerichtet, werden Sie aufgefordert einen 2-stelligen Nummerncode einzugeben. Ist das erfolgreich, ist der erste Teil angeschlossen und Sie sehen die folgende Meldung:

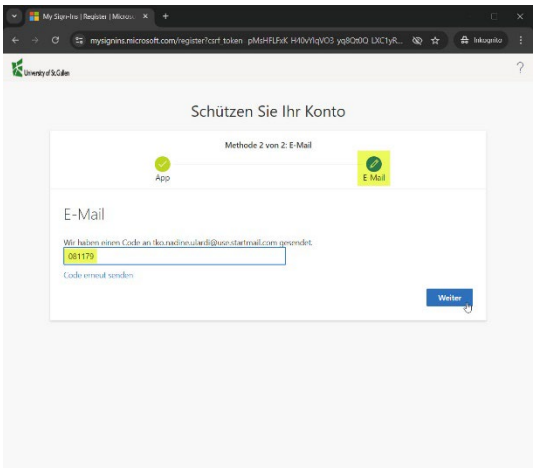


Geben Sie als zweites eine gültige für Sie lesbare E-Mail-Adresse an, um den Verifikationscode zu erhalten.

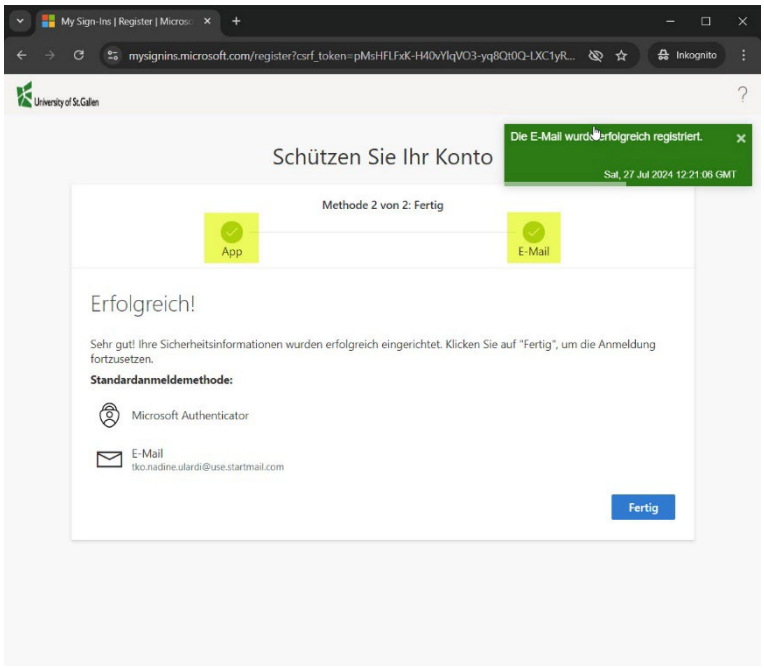




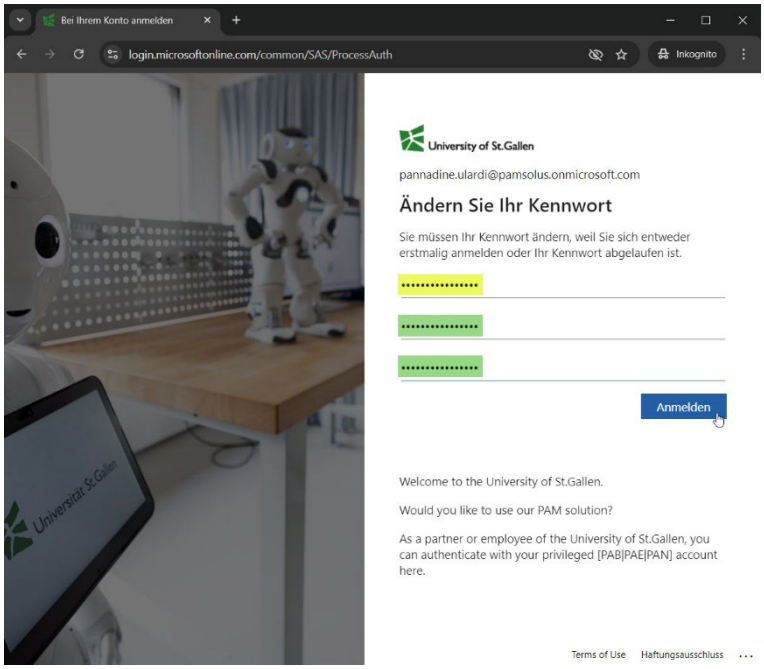
Den Code geben Sie im folgenden Fenster ein.



Haben Sie 2 Methoden erfolgreich registriert, erhalten Sie eine Erfolgsmeldung und müssen nur noch den letzten Schritt (Kennwortänderung) durchführen.

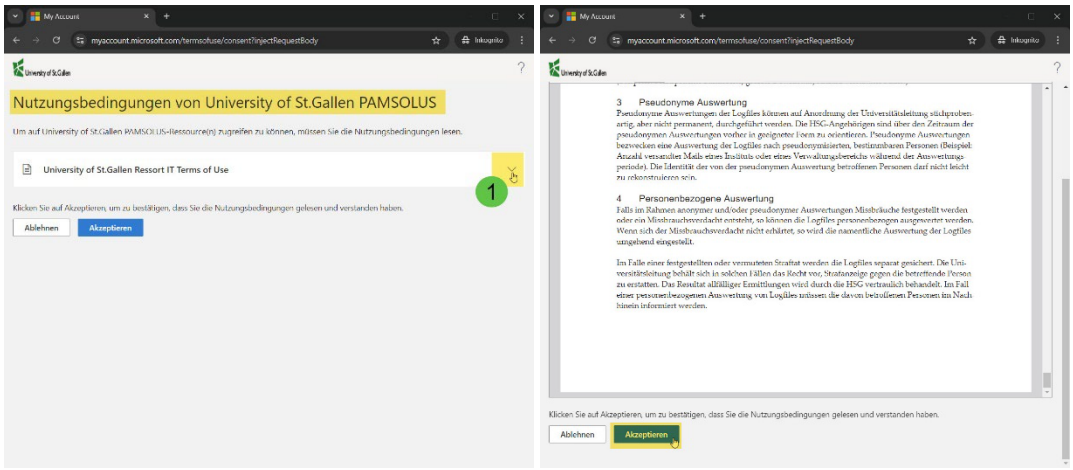


Bitte geben Sie dazu im folgenden Fenster das Initialkennwort (gelb) und ein neues nur Ihnen bekanntes Kennwort (grün) ein.



Entspricht dann Kennwort unseren Vorgaben (https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy#microsoft-entra-password-policies), werden sie automatisch weitergeleitet.

Lesen Sie bitte unsere Nutzungsbedingungen (1) und akzeptieren Sie diese. Andernfalls dürfen Sie Ihr Konto nicht benutzen.



Sie haben nun Zugriff zu Ihrem PAMSOLUS-Konto.