



Universität St.Gallen

DELINEA Portal mit Secret Server Cloud (SSC)

St.Gallen, 15. August 2024
Thomas Köppel
Turgay Demirci



From insight to impact.



Was ist denn das überhaupt?

Es geht um die Ablösung von «pwdb.unisg.ch», dem aktuellen «Kennwortspeicher».

Im Rahmen eines Projekts (s.r.) haben wir eine Lösung gesucht, die es erlaubt die Verfügbarkeit und vor allem die Funktionalität eines solchen Services zu erweitern.

Eine erste Erweiterung wird der sichere (administrative) und ortsunabhängige Fernzugriff auf unsere Systeme und Services sein.

SSC = **S**ecret **S**erver **C**loud

Number	SFEPIC0001031
Enabler	<input checked="" type="checkbox"/>
State	Implementation
Approval	Approved
* Priority	2 - High
Department	IT-BS
Watch list	 
Short description	Secret Server: Funktionserweiterung und sicherer Remote-Zugriff
Description	<p>Initiales Basic Setup und Deployment (Cloud => Ersatz OnPrem Instanz) Authentifizierung AAD, MFA Struktur und Gruppierungen, Migration Utility, Berechtigungskonzept, Globale & Standort Secrets, Password Rotation Usecase: Konfiguration von 3 Launchern (RDP, SSH, Web) Usecase: Discovery PAM & Service Accounts Usecase: RAS Remote Access Services für externen Zugriff</p> <p>Die Datenschutzabklärung für eine Migration in die Cloud wurde bereits mit einem pos. Ergebnis durchgeführt: https://servicedesk.unisg.ch/form/2183679149a567=8</p>
Primary goal	Technologie/Digitalisierung/Innovation
* Service	Secret Server IT Backend Services
* Portfolio	IT Sounding
Assignment group	IT BS SRV Infrastruktur
Assigned to	Thomas Köppel

Der neue Service kann ausschliesslich mit einem persönlichen, privilegierten Konto (Microsoft Account) aus dem «PAMSOLUS» Tenant verwendet werden.

PAM = **P**riviliged**A**ccount**M**anagment
SOL = **S**OLution
US = **U**niversity of **S**t.**G**allen

Agenda

1. Geheimnisse (**Secrets**) *
2. Demonstration (Login, pers. Ordner, allg. Ordner) *
3. Fernzugriff (**PRA** – **P**rivileged **R**emote **A**ccess) **
4. Demonstration (**RDP**-, **SSH**-Launch) **
5. Projektverlauf (Secret Migration, System-Onboarding) *
6. Q&A für Grundsatzfragen ***

* TKO

** TDE

*** Beide

1. Geheimnisse (Secrets) –
psssst.

Auch Männer können ein
Geheimnis für sich behalten
– vorausgesetzt man erzählt
es Ihnen nicht.



Was ist ein Secret im SSC?

- Ein Secret basiert im SSC immer auf einem Template.
- Ein Template gibt vor welche Informationen in einem Secret gespeichert werden können oder müssen.
- Wir verwenden ausschliesslich für die HSG angepasste Templates (Kopien der Originale). Diese werden auch bei Aktualisierungen nicht verändert.
- Der Name eines Secrets ist wichtig zum Finden. Verwendet wenn immer möglich die Suche, um auf Secrets zuzugreifen.
- Im Bild seht ihr ein Such-Beispiel.

Secrets >

All secrets

Q PAB 1 Active 0 selected ☆ ⚙

2 items

	NAME ↑ 2	SECRET TEMPLATE 3	FOLDER
> ☆	PAB Emma Acronis Test Secret	Web Password	Acronis
> ☆	PAB Emma Testaccount	HSG Active Directory Account	Acronis 4

Welches Template soll ich verwenden?

- Sucht bitte jeweils ein entsprechendes Template für die Erstellung eines Secrets aus.
- Der Name eines Templates (1, 2, .. 3 ..) sollte für die korrekte Auswahl «ausreichen». Wir haben versucht die aktuelle und voraussichtliche Anforderung / Verwendung an ein Secret bestmöglich abzubilden.
- Die Verwendung eines Templates kann je nach Ordner eingeschränkt sein.
- Wenn ihr ein Secret erstellt, werden alle möglichen oder erforderlichen Felder angezeigt.
- Die «4» wird nur für PRA (Windows RDP) verwendet!


Secret templates

Templates			Character sets	Password requirements	Launchers	Audit
<input type="text" value="Q Search"/>			Enabled ▾			🔍
10 items						
SECRET TEMPLATES ↑	TOTAL SECRETS	ENABLED				
HSG Active Directory Account 1	2	✓				
HSG Active Directory Service Account 2	2	✓				
HSG Application User (Website Login)	2	✓				
HSG Certificate	1	✓				
HSG Credit Card	0	✓				
HSG Encryption Key	0	✓				
HSG Entra ID User Account 3	1	✓				
HSG Local User	1	✓				
HSG RAS Windows Account 4	35	✓				
HSG Unix Account (Privileged Account SSH Key Rotation)	2	✓				


Secret Management? Teil 1

- Im persönlichen Ordner könnt ihr fast «tun und lassen», was ihr wollt. Es gibt jedoch 3 Regeln:
 - 1) Verwaltet Secrets nur zur persönlichen, geschäftlichen Verwendung.
 - 2) Teilt diese Secrets mit niemandem.
 - 3) Deaktiviert nicht mehr verwendete Secrets.
- Persönliche Ordner werden von uns nicht unterstützt.
- Jede Person ist die einzige Person, die auf diese Secrets Zugriff hat.
- Meldet euch bitte mit dem privilegierten Konto an (<https://pamsolus.delinea.app/>).



 University of St.Gallen
paeemma.ulardi@pamsolus.onmicrosoft.com

Kennwort eingeben

.....| 

[Self Service Password Reset](#)

[Mit einem anderen Konto anmelden](#)

Anmelden

Welcome to the University of St.Gallen.

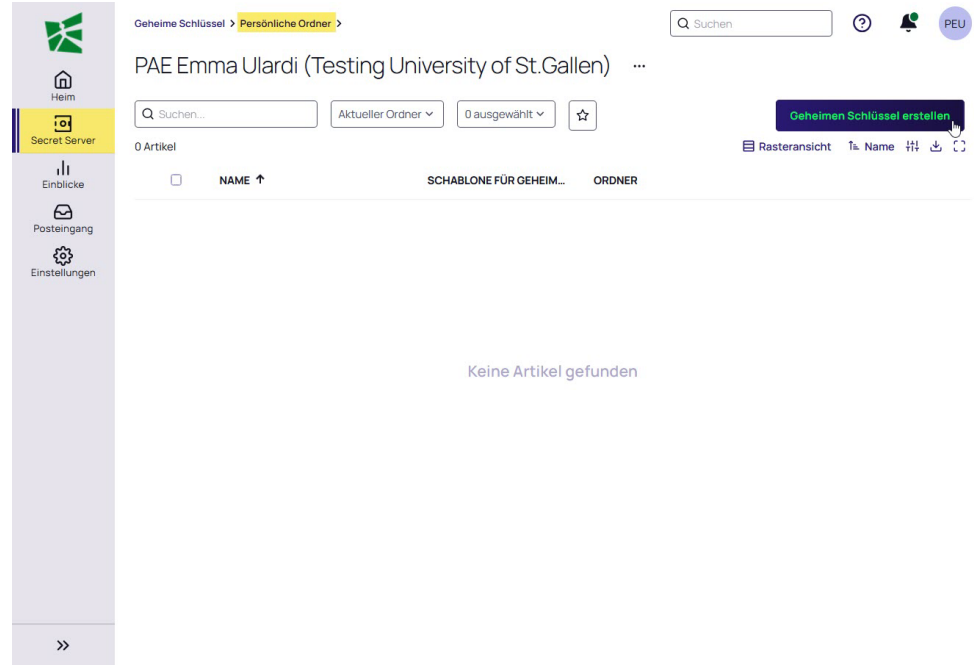
Would you like to use our PAM solution?

As a partner or employee of the University of St.Gallen, you can authenticate with your privileged [PAB|PAE|PAN] account here.

[Terms of Use](#) ...

Secret Management? Teil 2

- Im persönlichen Ordner kann ein Secret erstellt werden.
- Klickt dazu auf den pers. Ordner und wählt «Geheimen Schlüssel erstellen».
- Ihr könnt nun das gewünschte Template für ein neues Secret auswählen und die gewünschten Einträge vornehmen.



Secret Management? Teil 3

- 1: Template
 - 2: Ordner
 - 3: Name des Secrets
 - 4: URL
 - 5: Benutzername
 - 6: Kennwort (kann auch generiert werden)
 - 7: Hinweise
- Beim Kennwortfeld werden Informationen zur Kennwortbeschaffenheit angegeben. Je nach Template kann dies restriktiv sein.
 - Nach dem Anlegen des Secrets steht dieses im Ordner zur Verwendung bereit.

Neuen geheimen Schlüssel erstellen

Dieser Ordner ist nur für geheime Schlüssel im Zusammenhang mit Ihrer Arbeit vorgesehen. Speichern Sie in diesem Ordner keine persönlichen geheimen Schlüssel, die nicht im Zusammenhang mit Ihrer Arbeit stehen, wie z. B. Ihr Online-Banking-Kennwort.

Schablone für geheime Schlüssel: HSG Application User (Website Login) **Ändern** 1

Persönliche Ordner/PAE Emma Ulardi (Testing University of St.Gallen) 2

WEB Support Portal MVPS SoftwareOne 3

4

5

6 Generiere

7

Kennwort sollte enthalten:

- ✓ Mindestens 12 Zeichen.
- ✓ Mindestens 1 Lower case letters (a-z)
- ✓ Mindestens 1 Symbols (Symbols)
- ✓ !@#\$%^&*()
- ✓ Mindestens 1 Numbers (0-9)
- ✓ 1234567890
- ✓ Mindestens 1 Upper case letters (A-Z)
- ✓ ABCDEFGHIJKLMNOPQRSTUVWXYZ

Kennwort sollte nicht enthalten:

- ✓ Wörterbucheinträge
- ✓ Sequenzen aufeinanderfolgender Zeichen wie 'abc' oder '123'
- ✓ Raumbezogene Muster wie '12345678' oder 'qwertyuiop'
- ✓ Benutzername

Abbrechen Geheime Schlüssel erstellen

Secret Management? Teil 4

UNISG What folder permissions exist for groups?

[View report](#)

Permissions

Schedule

Audit

218 items

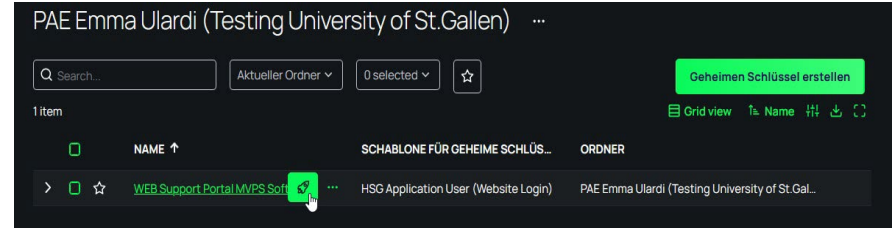
FOLDER PATH	INHERIT PERMISSIONS	GROUP	
\AD	No	AD-Anonym-Edit	
\AD	No	AD-Anonym-View	
\AD	No	AD-Service-Edit	
\AD	No	AD-Service-View	View
\AD	No	AD-Test-Edit	View
\AD	No	AD-Test-View	View
\AD	No	Secret Admin Users	View/Add Secret/Edit/Owner
\AD\Anonym	No	AD-Anonym-Edit	View/Add Secret/Edit
\AD\Anonym	No	AD-Anonym-View	View
\AD\Anonym	No	Secret Admin Users	View/Add Secret/Edit/Owner
\AD\Service	No	AD-Service-Edit	View/Add Secret/Edit
\AD\Service	No	AD-Service-View	View
\AD\Service	No	Secret Admin Users	View/Add Secret/Edit/Owner



- Die Zugriffsberechtigungen können für jedes Secret einzeln, in Gruppen oder pro Ordner (mit Vererbung) eingestellt werden.
- In Zukunft werden wir mit den Berechtigungen restriktiver umgehen (müssen) um den «zero trust» und «least priviledge» -Ansatz besser umsetzen zu können.
- Je nach Situation (Gruppen (s.B.), Teams, Verantwortlichkeiten, ...) wird festgelegt, wie die Berechtigungen eingestellt werden sollen. Dies betrifft nicht nur neue sondern vor Allem auch bestehende, zu migrierende Secrets.

The «Launcher» Story

- Je nach Template sind unterschiedliche Launcher verfügbar.
- Für das dargestellte Secret ist es ein WEB-Launcher. Dies ist Template basiert.
- Ein Klick auf das Raketensymbol und los geht's.
- Damit ihr den Benutzernamen und das Kennwort nicht abtippen und oder kopieren müssen, stellt DELINEA Browser Plugins für's autom. Einfügen zur Verfügung. Das müsst ihr jedoch selbst einrichten ([Installing Browser Extensions \(delinea.com\)](https://delinea.com)).



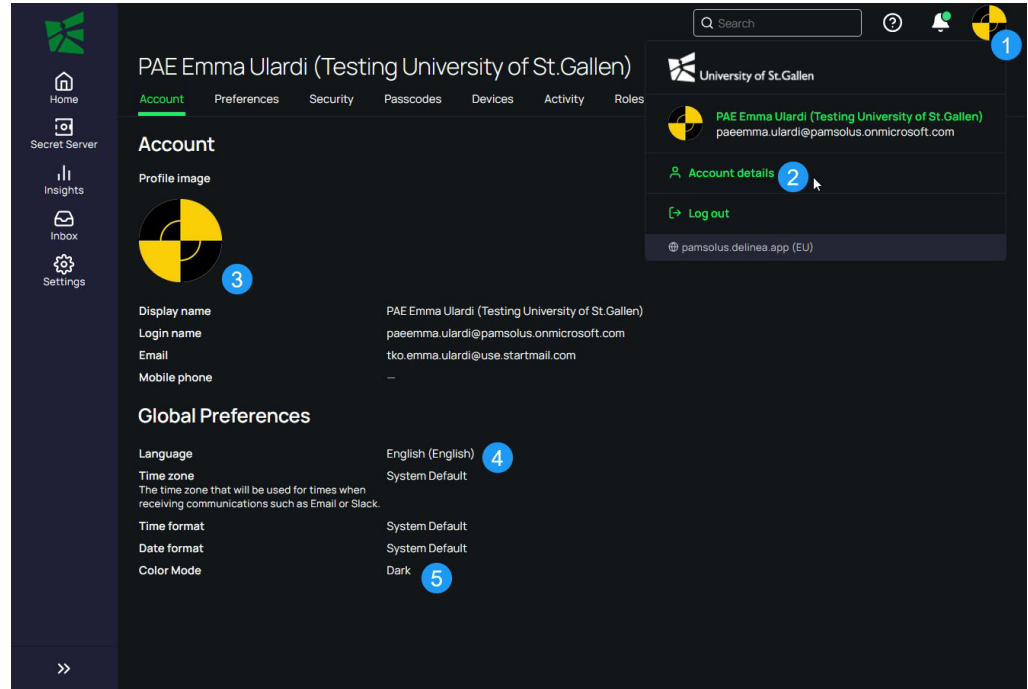
Secret templates

Templates	Character sets	Password requirements	Launchers	Audit
<input type="text" value="Search"/> <input type="button" value="Enabled"/>				
5 items				
NAME ↑	STATE			
Powershell Launcher	Enabled			
PuTTY	Enabled			
Remote Desktop	Enabled			
SQL Server Launcher	Enabled			
Website Login	Enabled			

Persönliche Einstellungen

- Sie können persönliche Profil-Einstellungen vornehmen.

- 1: Aufklappen
- 2: Kontoeinstellungen
- 3: Bild ändern
- 4: Sprache anpassen
- 5: Farbmodus wechseln



2. Demonstration

DELINEA Portal



Anpassungen

- Die aktuelle Konfiguration wurde nach bestem Wissen und Gewissen erstellt – und ist sicher nicht perfekt, aber nah dran!
- Gerne nehmen wir eure Rückmeldungen, Anregungen, Verbesserungsvorschläge, ... entgegen.
- Bitte einfach eine E-Mail an «BusinessPlattform» mit dem Vermerk «Rückmeldung SSC» senden und schon bald stehts im Backlog.



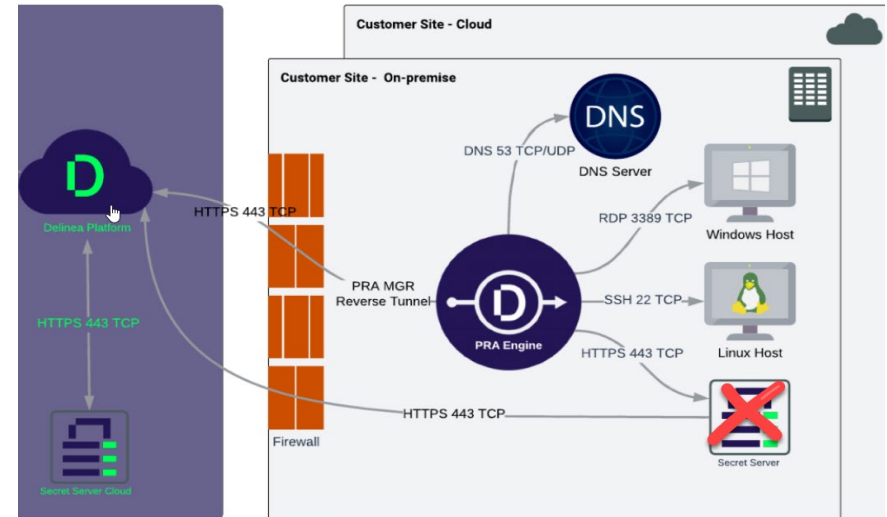
3. Fernzugriff – neu definiert.

Sicherheit und Verfügbarkeit
hat eine sehr hohe Priorität
und gewinnt zunehmend an
Bedeutung.



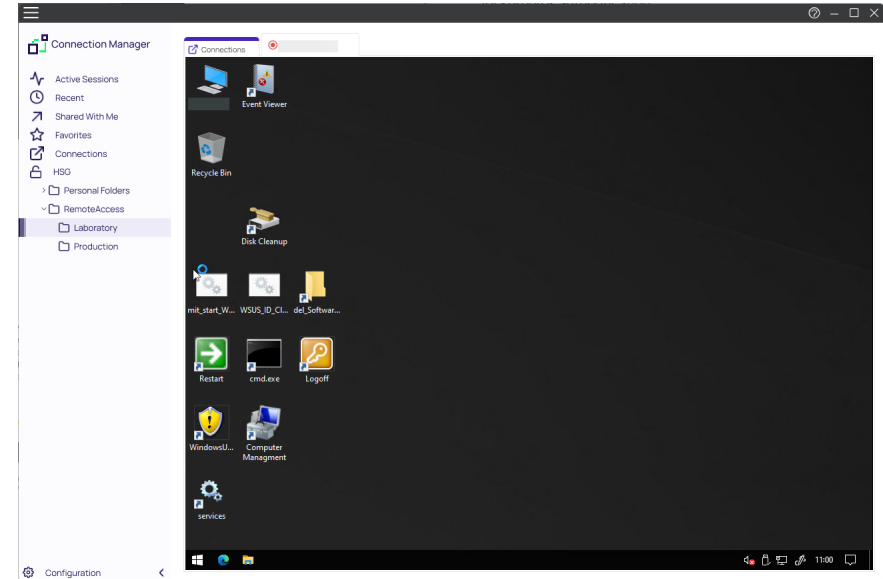
Was ist PRA?

- Privilege Remote Access (PRA)
 - Ermöglicht nahtlosen Zugriff auf Remote-Rechner, ohne dass VPN* benötigt wird.
 - Zugänge erfolgen, ohne dass sensible Teile der Anmeldeinformation für den Endbenutzer sichtbar ist.
 - RDP, SSH, Delinea Connection Manager und Web-Browser*
- Zugang
 - SSC-Portal (<https://pamsolus.delinea.app/>)
 - Delinea Connection Manager



PRA-Verbindungsmöglichkeiten und Funktionen

- Check-Out/In-Funktion (Prävention Sessionübernahme)
- Mit Fernzugriff öffnen (Open with Remote Access)
Remote Access über Webbrowser, keine Installation
- RDP-Startprogramm (RDP-Launcher)
Protocol Handler notwendig
- Delinea Connection Manager
Tool mit integriertem Passwortmanager und Remote Access.
[Installationsanleitung](#) (Kapitel 2.4.6 Connection Manager)
- PuTTY-Startprogramm (PuTTY-Launcher)
PuTTY Installation auf dem Client notwendig.



4. Demonstration

Remote Access Launcher
Connection Manager

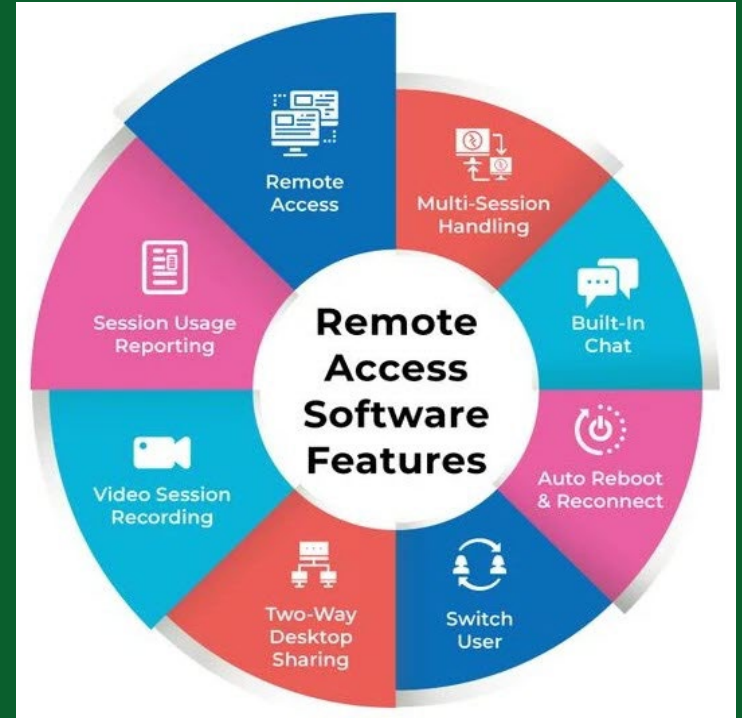


5. Projektverlauf

System-Onboarding (PRA)
Secret Migration



5.1 System Onboarding



Ca. 80 PRA-Systeme sind im SSC integriert.

- Jedes Team, bestehend aus Verantwortlichen, Stellvertreterinnen, ext. Supportern, ... werden pro System definiert/für den Zugriff berechtigt (view). Ein Report zur Kontrolle kann angefordert werden.
- Personen, die sich erfolgreich am Portal angemeldet haben, haben auch Zugriff auf die entsprechenden Secrets, bzw. Systeme.
- Aus Lizenzgründen verwalten wir nur wirklich notwendige Benutzerkonten. Bei Bedarf bitte melden. Bei Wegfall unbedingt melden!
- Vorrang haben Active Directory integrierte Systeme.
- Systeme mit SSH-Zugriff können ebenfalls ab sofort integriert werden. Bitte Termin vereinbaren.

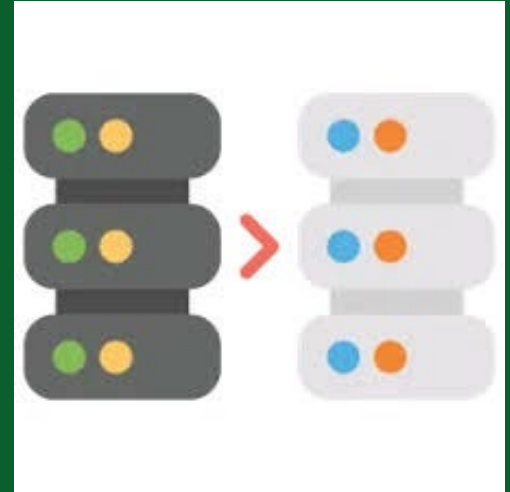


5.2 Secret Migration ?!

Start nach dieser Präsentation!

Der Service «pwdb.unisg.ch» wird auf «Read-Only» umgestellt.

Break Glass Accounts sind ausgeschlossen!



Tipps.

- Gute Namen verwenden. Goldene Regel s.u.
- Persönliche Ordner zuerst bearbeiten.
- Immer vorher absprechen mit Teamkollegen.
- Secret-Ordner sinnvoll auswählen und Berechtigungen korrekt setzen.
- Nach Neuerstellung im SSC die alten Secrets in «pwdb.unisg.ch» deaktivieren.

Verwendung von Präfix/Schlüsselwort (Empfehlung)

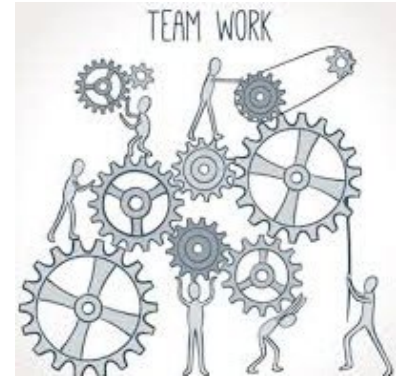
[**APP|WEB|CERT|SRV|...**][**Admin|User|Support|...**][Kurze, prägnante und SUCHBARE Beschreibung)

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

Leider kein Automatismus.

- Die Secret Templates in «pwdb.unisg.ch» waren mal «gut», erfüllen aber heutige Anforderungen nicht mehr.
 - Die Namen der Templates und persönlicher Ordner haben sich geändert.
 - Die Ordnerstruktur wurde (vor)-angepasst.
 - Viele der bestehenden Secrets entsprechen nicht (mehr) unseren Vorgaben (z.B. Kennwortlänge für Service-Accounts).
 - Nicht mehr verwendete Secrets wurden nicht deaktiviert. => Es kann «aufgeräumt» werden.
 - Copy & Paste «geht» mit 2 Browserfenstern.
-
- Unterstützung gibt's bei **Thomas K. und Turgay D.** Bitte meldet euch bei Bedarf möglichst bald (Ferien TKO ab 23.8. – 18.9.24). Wir haben uns für kommende Woche extra Zeit dafür reserviert.



Migrationsabschluss.

- Nach einem Monat (bis 20. Sept. 2024) sollten alle noch benötigten Secrets migriert sein.
- Der Service «pwdb.unisg.ch» wird zu dem Datum hoffentlich ausser Betrieb genommen (Wartung abgelaufen).
- Das Benutzerhandbuch ist zu finden unter: [rit-download.unisg.ch - /ssc/](https://rit-download.unisg.ch/-/ssc/). Dieses wird laufend aktualisiert. Orientiert euch bitte an der höchsten Versionsnummer.



Fragen?

Feedback?

Anregungen?



Vielen Dank.

Köppel Thomas

System Engineer IT-BS

+41 71 224 2651

thomas.koeppel@unisg.ch

Demirci Turgay

System Engineer IT-BS

+41 71 224 2467

turgay.demirci@unisg.ch

Sponsor Städler Kurt

Leiter SC

+41 71 224 3039

kurt.staedler@unisg.ch



Universität St. Gallen (HSG)

Dufourstrasse 50

9000 St. Gallen

unisg.ch

Akkreditierungen

