2-Faktoren-Authentisierung (2FA/MFA)

# **Abacus Access**

Vorbereitung, Installation & Verwendung

April 2020/sko

Diese Unterlagen sind urheberrechtlich geschützt.

Insbesondere das Recht, die Unterlagen mittels irgendeines Mediums (grafisch, technisch, elektronisch und/oder digital, einschliesslich Fotokopie und Download) ganz oder teilweise zu vervielfältigen, vorzutragen, zu verbreiten, zu bearbeiten, zu übersetzen, zu übertragen oder zu speichern, liegt ausschliesslich bei Abacus Research AG.

Jede Verwertung in den genannten oder in anderen als den gesetzlich zugelassenen Fällen, namentlich jede kommerzielle Nutzung, bedarf der vorherigen schriftlichen Einwilligung von Abacus Research AG.

Die gewerbsmässige Verletzung der Urheberrechte kann gemäss Art. 67 Abs. 2 URG bestraft werden.

Copyright © 2020 by Abacus Research AG, CH-9300 Wittenbach-St.Gallen

# Inhaltsverzeichnis

1	Abacus Access App	3
1.1	Komponenten	3
	1.1.1 Anfragen (Startseite)	. 3
	1.1.1.1 Abgelaurene Antragen	3
	1.1.2 Scaliner	
	1.1.4 Benutzerkonten	. 5
	1.1.5 Über	. 7
	1.1.6 Generelle Einstellungen	. 7
2	Access App Login aktivieren	8
2.1	Einstellungen im Abacus Configurator	8
~ ~	2.1.1 Offline-Modus	. 9
2.2	Einstellungen in der Benutzerverwaltung.	12
	2.2.2 Aktivierung pro Benutzer	12
	2.2.2.1 MFA mit der nächsten Anmeldung aktivieren	13
	2.2.2.2 Benutzer darf MFA selbst verwalten	13
3	Access Onboarding Prozess	14
3.1	Beispiel-Ablauf	14
3.2	Installation Abacus Access App	14
3.3	Erstmalige Anmeldung und Registrierung	14
4	Log-In mit Abacus Access	20
4.1	Ablauf	20
4.2	Ablauf im Browser	21
	4.2.1 Anmeldedaten	21
	4.2.2 2FA / Hinweis auf Abacus Access	21
4.3	4.2.3 Timeout	22 22
	4.3.1 QR-Code	23
	4.3.2 Länge des Zeichencodes definieren	24
5	Verwaltung Access App in Benutzerverwaltung	26
5.1	Authentisierung	26
5.2	Verwendetes Gerät	26
5.3	Gerät löschen	27
5.4		21
6	Einstellungsmöglichkeiten (Kombinationen)	28
6.1	Abacus Configurator	28
6.2	Benutzerverwaltung	28
0.5		23
7	Ablosung SuisselD / MobileID	30
7.1	Login mit Benutzername & Passwort	30
	7.1.1 Generelle MFA-Aktivierung	30
	7.1.3 MFA zwingend	31
7.2	Nur externe Authentisierung	31
7.3	Abacus Configurator	32
1.4 75	LOG-IN MOZESS	33 34
7.6	Arbeitsablauf Ablösung SuisselD/MobileID	35
8	Checkliste generell	40

## Wunsch & Umsetzung

Abacus bietet aktuell standardmässig die 2-Faktoren-Authentisierung (2FA) über SuisseID und Mobile ID an (Stand 04.2020). Kunden wünschten schon lange, dass eine 2FA-Lösung ins ERP integriert wird, ohne Abhängigkeit von einem externen Anbieter.

Es sollte also eine Multi-Faktor-Authentisierung zum ERP hinzugefügt werden, welche diesen Punkten Rechnung trägt. Die Benutzbarkeit sowie die Betreibbarkeit sind wichtige Kriterien.

Mit der Entwicklung der Abacus Access App (Access) wurde zum jetzigen Zeitpunkt (Stand 04.2020) der erste Teil erfolgreich umgesetzt.

So verfügen wir nun über eine Authenticator-App, die ab den folgenden Versionen für die Multi-Faktor-Authentisierung (2FA) verwendet werden kann:

- Version 2020 15.02.2020 Release Version
- Version 2019 15.03.2020 Servicepack
- Version 2018 15.04.2020 Servicepack

Die neue Mobile-App wird also schrittweise ab Februar 2020 für die Versionen 2018 – 2020 bereitgestellt (genaue Auslieferungstermine siehe oben).

Mit "Abacus Access" wird zudem nicht nur die 2-Faktor-Authentisierung von Abacus direkt angeboten, die App wird in einer späteren, zweiten Phase auch für Transaktionsfreigaben genutzt werden können.

Die Stärken dieser eigenen App von Abacus:

- Eigene Lösung und dadurch volle Integration im Abacus Umfeld
- Erhöhte Sicherheit durch Einsatz eines 2-Faktors
- Der 2-Faktor wird auch bei Einsatz eines externen Logins verwendet
- Einfaches und sicheres Onboarding
- Kunde erhält neben der erhöhten Sicherheit dadurch einen wesentlichen Mehrnutzen

## 1 Abacus Access App

Die Abacus Access App steht für Android und iOS zur Verfügung und kann entsprechend über den Google Play Store oder über den App Store heruntergeladen werden. Die App ist kostenlos.

### 1.1 Komponenten

Im Folgenden werden die einzelnen Bereiche der Abacus Access App beschrieben.

#### 1.1.1 Anfragen (Startseite)

Beim Öffnen der App steht man auf der "Anfragen" Seite. Steht kein Log-In Vorgang an, so wird hier nichts angezeigt.

Ansonsten wird hier die Log-In Anfrage angezeigt. Anfragen werden automatisch angezeigt, falls eine Anfrage erfolgt und die Ansicht offen ist.

Mit einem Swipe nach unten kann die Ansicht auch manuell aktualisiert werden.



#### 1.1.1.1 Abgelaufene Anfragen

Der Log-In Prozess läuft in einen Timeout, wenn die Anfrage in der App nicht innert 1 Minute bestätigt wird.

Diese Änfragen sind nun in der App pendent. Will man diese Anfragen löschen, so können diese mit einem Swipe nach links oder rechts einfach gelöscht werden.

Natürlich kann eine solche Anfrage auch einfach erlaubt oder abgelehnt werden, was aber dazu führt, dass dies im Verlauf protokolliert wird. Wird die Anfrage hingegen gelöscht (Swipe), so erfolgt kein Eintrag.

=	Anfragen
Â	Anmeldung bei abavm68576-3117.ext.abatest.ch <sup>kollers</sup>
Ê	Anmeldung bei abavm68576-3117.ext.abatest.ch <sub>kollers</sub>
ıng bei 8576-31	17.ext.abatest.ch
	Swipe

### 1.1.2 Scanner

Über das Foto-Icon wird der Scanner gestartet.



#### 1.1.3 Menü

Über das 🧮 Icon wird das Menü geöffnet.

#### 1.1.4 Benutzerkonten

Hier wird der/die entsprechende/n Benutzer pro Installation angezeigt.



Mit dem Anwählen eines Kontos gelangt man in die Übersicht, bzw. die Verlaufs-Ansicht.

<	kollers	
Ihr Verlauf		
Anmeldung be abavm68576- Abgelehnt vor w	ei -3117.ext.abatest.ch reniger als einer Minute	¢
Anmeldung be abavm68576- Erlaubt vor 13 M	ei 3117.ext.abatest.ch linuten	~
Anmeldung be abavm68576- Erlaubt vor ~1 S	ei 3117.ext.abatest.ch tunde	~
Anmeldung be abavm68576- Erlaubt vor 2 Str	ei 3117.ext.abatest.ch unden	Ş
Anmeldung be abavm68576- Abgelehnt vor 2	ei 3117.ext.abatest.ch Stunden	Ş
Anmeldung be abavm68576- Erlaubt vor 2 Ste	ei 3117.ext.abatest.ch unden	~

Hier werden alle empfangenen Anfragen, inkl. der Information von welcher Installation, angezeigt und auch, ob diese abgelehnt oder erlaubt wurden.

Über das Papierkorb-Icon kann das angezeigte Benutzerkonto getrennt werden.



### 1.1.5 Über

Informationen zur Version der App und der hinterlegten Datenbank.

<	Über	
	Abacus Access	
	Abacus Access	
	Ê	
	Applikation Version 1.0.3, Build 24	
	Datenbank	
	Version 1	

### 1.1.6 Generelle Einstellungen

Die Einstellungen bezüglich Log-In werden im Abacus Configurator und in der Benutzerverwaltung gemacht. Die entsprechenden Informationen dazu finden sich im jeweiligen Kapitel.

Je nach Kombination dieser Einstellungen ergeben sich die Log-In-Kombinationen gemäss Tabelle unter 6.3.

### 2.1 Einstellungen im Abacus Configurator

In den Authentifizierungskontextrichtlinien können unter Rules die Regeln entsprechend angepasst werden.

Abacus Konfigurator [Scope = DefaultScope]	ope]							-		×
Datei Dienst Einstellungen										
Start Stop Registrieren Standard Deregistrie	ren Aktualisie	ren Speichern	Load Balancin	g DBConfig	AbaSysInf	중 Scope	Remote Debugging	Cloud Server	(?) Hilfe	
Dienste	Aktuo		- DofoultS							
Dienst-Einstellungen	Aktue	iei Scope	- Delaulo	Lope						
Ports	Authent	.ifizierungsko	ntextrichtlinie	in	-			D		
Proxy-Einstellungen	Default	Policy	DOME.		d	efault		0		
Service-URL	Internet	Policy			ir	nternet				
Aktualisierungen										
Webserver										
External Webserver	Hir	ızufügen	Umben	nenen	Entfe	rnen				
Service Monitoring	Rules									
c-tree Mandanten Konvertierung					NAME					
c-tree Verschlüsselung	Rule 1									
Speicherzuweisung										
Administrator zurücksetzen										
LDAP										
SAML 2.0 / OpenID Connect										
Authentifizierungskontextklassen										
Authentifizierungskontextrichtlinien										
Authentifizierung										
Vertrauenswürdige CAs										
Webserver Zertifikate										
Portal										
index.html										
AbaSystemProperties										
Mandant kopieren										
Scope erstellen / löschen										
OpenFolders										
EB-Commserver										
	Hir	ızufügen	Editiere	n 🔓	Umbenne	nen	Entfernen			
V 2020.9999 TESTVERSION   ABACUS	Research	AG (17)   CI	D 15.02.2020	https://	localhost:4	0001				

In der gewünschten Regel kann im Bereich "MultiFactorAuth" nun aus den folgenden Optionen gewählt werden:

- Opportunistic (angepasst)
- Mandatory (zwingend)
- Off (nicht aktiv)



Damit im folgenden Schritt 2FA in der Benutzerverwaltung aktiviert werden kann, muss "Opportunistic" oder "Mandatory" ausgewählt werden. Bei "Opportunistic" wird die Entscheidung, ob 2FA verwendet wird, offengelassen. Bei "Mandatory" ist es hingegen zwingend, dass 2FA vom Benutzer eingerichtet (Onboarding) und verwendet (Log-In) wird.

## i

Weitere Informationen, wie sich diese Einstellungen auf den Log-In Prozess auswirken, finden sie im Kapitel 6.

Die getroffene Wahl wird mit OK bestätigt. Wichtig ist, dass die Regel danach gespeichert wird.

🔅 Abacus Konfigurator [Scope = DefaultSco	pe] – 🗆	×
Datei Dienst Einstellungen	$\frown$	
Start Stop Registrieren Standard Deregistrieren	en Aktuartieren Speichern Load alancing DBConfig AbaSysInfo Scope Remote Debugging Cloud Server Hilfe	
Dienste	Aktueor Scope = FefaultScope	
Dienst-Einstellungen	Authentifizierungskontextrichtlinien	
Ports	NAME ID	
Proxy-Einstellungen	Default Policy default	
Service-URL	Internet Policy internet	
Aktualisierungen		
Webserver		
External Webserver	Hinzurugen Ombennenen Entremen	
Service Monitoring	Rules	
c-tree Mandanten Konvertierung	NAME	
c-tree Verschlüsselung	Rule 1	
Speicherzuweisung		
Administrator zurücksetzen		
LDAP		
SAML 2.0 / OpenID Connect		
Authentifizierungskontextklassen		
Authentifizierungskontextrichtlinien		

#### 2.1.1 Offline-Modus

Sollte es aus verschiedenen Gründen nicht möglich sein eine Installation von extern zugänglich zu machen, so kann das Onboarding und der Log-In auch "offline" erfolgen.

# 

Damit eine "Offline"-Registrierung (Onboarding) des Geräts funktioniert, muss im Abacus Configurator entsprechend zuerst die Einstellung vorgenommen werden, da es ansonsten zu einem Fehler kommt.

$\oslash$
Entschuldigung.
Das hat nicht geklappt.

Im Abacus Configurator wird dazu unter Authentifizierung entsprechend der Key "Defines if by default a fallback to offline based multi-factor authentication" eingefügt und auf "true" gestellt.

Abacus Konfigurator [Scope = De	faultScope]	– 🗆 X	
Datei Dienst Finstellungen			
mm m		~ ~ @	
Start Stap Bagistrianan Standard Bar	VIII VIII III III III VIII VIII VIII V	Debugging Claud Server Hilfs	
Dienete	gistreren Akualisieren Spechern Luau balancing boconnig Auasysimo Scope Renor	e Debugging Cloud Server Time	
Dienste Dienst Einstellungen	Aktueller Scope = DefaultScope		
Dienst-Einstellungen	KEY	VALUE	
Poits	Multi-factor authentication enabled true		
Proxy-Einstellungen			
Service-URL			
Aktualisierungen	Property-Vorlage	×	
Webserver	KEY	VALUE	
External Webserver	Gültigkeitsdauer Access-Token	600	
Service Monitoring	Passwort zurücksetzen erlauben	true	
c-tree Mandanten Konvertierung	Zeitlimit Single Sign-on bei Inaktivität	1800	
c-tree Verschlüsselung	Max. Guitigkeitsdauer vom Single Sign-on	36000	
Speicherzuweisung	Defines if by default a fallback to offline based multi-factor authentication	false	
Administrator zurücksetzen	Defines the number of digits an OCRA code (signature) must have 1 - 9	8	
LDAP		-	
SAML 2.0 / OpenID Connect			
Authentifizierungskontextklassen			
Authentifizierungskontextrichtli			
Authentifizierung			
Vertrauenswürdige CAs			
Webserver Zertifikate			
Portal			
index html			
AbeSusternDresstics	Hinzufü	igen Abbrechen	
AbaSystemProperties			
Mandant Konieren			
20			
211			
		205 <b>205</b>	A 20
		~ VF	
ard Deregistrieren Aktualis	sieren Speichern Load Balancing DBConfig AbaSysInfo	Scope Remote Debugging Clo	ud Server Hilfe
Aktuallar S	cono - DofaultScono		
Aktuellel S	cope – Delaulocope		
	KEY	VALUE	
Multi-factor aut	hentication enabled true		
Defines if by de	efault a fallback to offline based multi-fac		
Donnoo n by de	line		

Daraufhin erfolgt der Log-In wie gewohnt.

	Abacus ERP	Login	
Benutzername			
kollers			
Passwort			
•••••	•		
		Anmel	den

Im nächsten Schritt wird ein QR-Code angezeigt, der mit der Access App gescannt wird, woraufhin in der Access App ein Zahlencode angezeigt wird.



Nach der Eingabe des Zahlencodes ist das Onboarding abgeschlossen und der Benutzer wird im Abacus eingeloggt.

	Abacus ERP Login	Business Software
Anmeldung bei abavm76362-3056.abatest.ch 35946321	Benutzerkonto schützen	« Zur Anmeldung ing mit Abacus Access Weiter

In der Benutzerverwaltung wird bei einem Benutzer, der das Onboarding offline durchgeführt hat, im Gegensatz zum Online-Onboarding, ein anderer Eintrag für das verbundene Gerät angezeigt, der auf die entsprechende Onboarding-Methode hinweist.

981 Benutzerverwaltung - ABACUS-DEMO [7777]									
Datei Bearbeiten Ansicht Extras Fenster ?									
ତୁ• 🗒 ⅔ ⊗•∣ ୦ 🖳 C		Programm							
Hierarchie Policy 📼 📼 ×	kollers Maske Alle Einstellungen ATK-Benutzer (Standard) v Alles	zuklappen							
Policies Aktiv	Benutzer darf MF-A selbst verwalten	4							
1 2 3 4 5 6 7 8 9 Benutzerkategorien v									
✓ ☐ Root	AUTHENTISIERUNG								
V 🗋 Admin									
🧏 VVMP	EXTERNE AUTHENTISIERUNG MULTI-FAKTOR-AUTHENTISIERUNG	_							
🤰 VVPP									
👤 kollers	AKTIV HOST BENUTZERID OPENID DISPLAYNA GERATENAME ERSTELLT ZÜLETZTE	JENUIZI							
Administrator	TADECUS ACCESS - Omine 16.02.2020 13:50 16.02.2020	) 13:50							
A EBusinessService									
🏂 System	Hinzufügen Editieren Entfernen Domänen Benutzer Zuordnung Entfernen								
SystemSwiss21									

## 2.2 Einstellungen in der Benutzerverwaltung

#### 2.2.1 Generelle Aktivierung

In der Benutzerverwaltung muss 2FA/MFA ebenfalls aktiviert werden. Hierzu wird in den Login Einstellungen das Flag "Multi-Faktor-Authentisierung aktiv" gesetzt.

	_							
♦ 981 Benutzerverwaltung - ABACUS-DEMO [7777]								
2atei Bearbeiten Ansicht Extras Fenster 2								
ତୁ∽ 💾 🖗 ⊗ ×   ୦. 🖳 (	C & & &	) 🔅 🔳						
Hierarchie Policy 🗗 🗖 🗠	Root			Macka	Allo Einstellungen Benutzerket	agoria (Standard)		
Policies Aktiv			Score Login Einstellur	ngen		×		
1 2 3 4 5 6 7 8 9 Benutzerkategorien 🗸		V	MUI TI-FAKTO	R-AUTHENTISIERUNG				
✓ ☐ Root	ID	3eb95610 of24						
v 🛅 Admin	Name	Root	Multi-Faktor-Au	thentisierung aktiv	<b>~</b>	/ /		
🧕 VMM	Schutzstufe	8 ^			43	-		
🧏 VVP			ALLGEMEINE	BENUIZERKONTO EINSTEI	LUNGEN			
및 Dash	ZUGRIFF AUF ABAV	ISION	Ablaufzeit der F	Passwörter	30   ‡	Tage		

### 2.2.2 Aktivierung pro Benutzer

Nun kann pro Benutzer folgendes gewählt werden:

- MFA mit der nächsten Anmeldung aktivieren
- Benutzer darf MFA selbst verwalten

× C Root	AMOLYIOM DELIGISE	Сазн манада	Saao Dalinital (nian)
✓ ☐ Admin	Secure Mail Benutzer	Visumsbenutzer (0/30)	Visumsbenutzer2 (0/20)
🧕 VMM	AbaMonitor Benutzer	ViewOnly Benutzer	DBX Benutzer
A VVP	ODBC Benutzer		
1 Dash			
👤 kollers	LOGIN DATEN		
Administrator	Passwort mit der nächsten Anmeldung ändern	Passwort ändern	
🏂 System	Passwort nicht veränderbar	Link zum Erfassen einer externen Authentisierung verser	nden
🔈 SystemSwiss21	Passwort läuft nicht ab		
	Passwort zurücksetzen erlauben		
	Nur mit externer Authentisierung einloggen		
	Benutzer darf "angemeldet bleiben"		$\triangleright$
	Benutzerkonto inaktiv		
	MFA mit der nächsten Anmeldung aktivieren		
1	Benutzer darf MFA selber verwalten	LDAP Konfiguration	
1			

#### 2.2.2.1 MFA mit der nächsten Anmeldung aktivieren

Dies aktiviert für den Benutzer die 2-Faktoren-Authentisierung. Bei der nächsten Anmeldung ist 2FA für diesen Benutzer zwingend. Das heisst, beim ersten Log-In nach der Aktivierung erfolgt das Onboarding und danach der Log-In mit Abacus Access.

#### 2.2.2.2 Benutzer darf MFA selbst verwalten

Dies lässt zu, dass der Benutzer seine Mehr-Faktor-Authentisierung in der Account-App selbst verwaltet.

Wird die Funktion/Button "Trennen" verwendet (in der Account-App), so führt dies aktuell (02.2020) dazu, dass der Administrator danach "MFA mit der nächsten Anmeldung aktivieren" auf diesem Benutzer erneut aktivieren muss, da sich der Benutzer sonst nicht mehr einloggen kann.

<b>ABA</b> Business	CUS Software Profil Passwort Verbindungen -	
V H je Si	<b>'erbundene Applikationen</b> alten Sie ein Auge darauf, welchen Applikationen und Diensten Sie die Erlaubnis gegeben haben me, die Sie nicht mehr benötigen oder denen Sie nicht mehr trauen. ie haben die folgenden Applikationen verbunden:	, in Ihrem Namen auf das Abacus zuzugreifen. Entfernen Sie
	> Abacus Access	Letzte Aktivität 14.02.2020, 08:58:19
Zukünftig w	vird es den Benutzer selbst möglich sein, ihre Verbind	dung zu trennen.

### 1

Weitere Informationen, wie sich diese Einstellungen auf den Log-In Prozess auswirken, finden sie im Kapitel 6.

## **3 Access Onboarding Prozess**

Damit die 2FA verwendet werden kann, müssen vorgängig einige Einstellungen im Abacus Configurator (siehe Kapitel 2.1), sowie der Benutzerverwaltung (siehe Kapitel 2.2) vorgenommen werden.

## 3.1 Beispiel-Ablauf

Folgend wird ein Beispiel angegeben, wie das Onboarding zu erfolgen hat. In diesem Beispiel wird davon ausgegangen, dass sich der Benutzer mit Benutzername und Passwort einloggt.

### 3.2 Installation Abacus Access App

Nun muss auf dem gewünschten Gerät noch die Abacus Access App installiert werden. Diese ist für Android und iOS verfügbar.



### 3.3 Erstmalige Anmeldung und Registrierung

Sind die Vorbereitungen soweit abgeschlossen, kann sich der Benutzer wie gewohnt mit seinem Benutzernamen und Passwort anmelden.

🎄 AbaClient localhost			- 🗆 X
	Abacus ERP Login	Business Software	
	Bitte anmelden für Abacus		
	Benutzername		
	kollers		
	Passwort		
	Passwort vergessen?	Anmelden	
		Deutsch 🔺	

Das Onboarding und der spätere Log-In können auch "offline" erfolgen, dazu mehr im Kapitel 2.1.1.

Nach erfolgreicher Eingabe erscheint das neue 2FA-Onboarding-Fenster.



Nun muss auf dem Gerät die Abacus Access App gestartet werden

 $\mathbf{\hat{\cdot}}$ 

Über das Foto-Icon wird der Scanner gestartet.

13:44 • • • • • 46 🛋	
Anfragen	j1 j2 selap trank
e haben im Moment keine Anfragen.	
	AbaClard Istalheat
	ABACUS
	202 let ref
	Erhöhen Sie die Sicherheit von ährem Benutzerkonto indem
	Sie bullstaator Authensierung antoieren. Sie richten dies mit 2 Schritten ein:
	1. Installieren Sie Abacus Access für Android oder IOS.
	Google Play
	2. Offnen Sie die App Abacus Access und scannen Sie de nachfolgenden QII. Code.

Wurde der QR-Code korrekt erkannt, erfolgt die Abfrage, ob das Benutzerkonto mit diesem Gerät geschützt werden soll.

Nachdem dies mit "Fortfahren" bestätigt wurde, erfolgt bei erfolgreicher Verifizierung eine entsprechende Bestätigung.

	<b>13:36</b>
÷	×
Ihr Benutzerkonto auf	
mit diesem Gerät schützen?	
	$\mathbf{v}$
Fortfahren 🗸	
	Alles klar.
Abbrechen X	Die Einrichtung ist beendet.

Im Log-In Browser wird ebenfalls eine entsprechende Meldung ausgegeben. Drückt man im Browser auf "Weiter", so verschwindet die Bestätigung in der App ebenfalls.

Abacus ERP Login	Business Software	
Benutzerkonto schützen	« Zur Anmeldung	
Gratulation! Multifaktor-Authentisierung wurde eingerichtet.	mit Abacus Access Weiter	
	Deutsch 🔺	
In der Abacus Access App gel	angt man über das Syn	nbol 📃 in das Hauptmenü.

Im "Benutzerkonto" ist nun ein entsprechender Eintrag mit Benutzernamen (Bsp. "kollers") und Installationsname (Service-URL) vorhanden.

13:44		•11 4G 💷	13:4	14	📲 4G 💷
Abacus Access			<	Benutzerkonten	
			÷	<b>kollers</b> abavm68576-3117.ext.abatest.ch	
•	Benutzerkonten				
	Über				

Im Browser kann nun mit einem Klick auf "Weiter" der Log-In Prozess fortgesetzt werden.

Abacus ERP Login	Business Software
Benutzerkonto schützen	« Zur Anmeldung
Gratulation! Multifaktor-Authentisie wurde eingerichtet.	rung mit Abacus Access
	Deutsch 🔺

Hierdurch wird ein Vorgang ausgelöst, der zum einen im Log-In Browser anzeigt, dass der Log-In mit der Abacus Access App bestätigt werden muss...

Abacus ERP Login		13:54 -7 ☴ Anfr	•⊪ 4G 📼
		Anmeldung bei abavm68576-311 kollers	7.ext.abatest.ch
Mit Abacus Access bestätigen	« Zur Anmeldung		
Bitte bestätigen Sie diesen Login mit de auf ihrem Smartphone.	er App Abacus Access		
9.8			
Abacus Access zeigt Ihnen keine Login- statt dessen den QR-Code mit Abacus /	Anfrage? Sie können Access scannen.		
	Deutsch 🔺		D

... und zum anderen wird in der Abacus Access App eine entsprechende Anfrage angezeigt.

Mit der Bestätigung der Anfrage wird in der App der entsprechende Installations-Name angezeigt, und die Anmeldung kann erlaubt oder abgelehnt werden.



Sobald diese Meldung erlaubt wurde, wird man im Abacus angemeldet. Der Onboarding Prozess ist somit abgeschlossen und der Benutzer wird im Abacus eingeloggt.

# 4 Log-In mit Abacus Access

Nachdem die Abacus Access App initial eingerichtet werden musste (Onboarding), gestaltet sich der zukünftige Login sehr einfach.

### 4.1 Ablauf

1. Log-In mit Benutzername & Passwort	2. Hinweis auf die 2FA wird angezeigt
AbaClient abavm68376-3117.ext.abatest.ch	♦ AbaClient abovn98576-317.oc. abotects Ab
3. In der Abacus Access App wird die Anfrage angezeigt.          14:42-7       •1146         Mnfragen         Anfragen         Anmeldung bei abavm68576-3117.ext.abatest.ch kollers	4. Mit "Erlauben" wird der Log-In Prozess abgeschlossen, Abacus startet.
	Anmeldung bei abavm68576-3117.ext.abatest.ch Erlauben

### 4.2 Ablauf im Browser

Im Folgenden sind die einzelnen Schritte aus Sicht des Log-In Browsers beschrieben.

#### 4.2.1 Anmeldedaten

Der Login-Prozess startet mit der Eingabe von Benutzername & Passwort.

🎲 AbaClient abavm68576-3117.ext.abatest.ch	-	×
Business Software		
Abacus ERP Login Benutzername		
kollers		
Passwort		
Anmelden		
Deutsch	1 🔺	

#### 4.2.2 2FA / Hinweis auf Abacus Access

Nach der Eingabe dieser Daten erscheint der Hinweis auf die Verwendung der 2FA, bzw. die Aufforderung, den Log-In in der Abacus Access App zu bestätigen.

鐌 AbaClient abavmé	88576-3117.ext.abatest.ch	-	×
	Business Software		
	Mit Abacus Access bestätigen « Zur Anmeldung		
	Bitte bestätigen Sie diesen Login mit der App Abacus Access auf ihrem Smartphone.		
	Abacus Access zeigt ihnen keine Login-Anfrage? Sie können statt dessen den QR-Code mit Abacus Access scannen.		
	Deutsch +		

#### 4.2.3 Timeout

Wird die Anfrage nicht innerhalb 1 Minute bestätigt, so läuft die Anfrage in einen Timeout, was im Browser entsprechend angezeigt wird.

🍓 AbaClient abavm6	8576-3117.ext.abatest.ch		_	$\times$
	Business Software			
	Mit Abacus Access bestätigen «Zur Anmeldu	ng		
	$\bigcirc$			
	Verzeihung! Die Bestätigung wurde bis jetzt nicht erhalten. Bitte gehen Sie zurück zur Anmeldeseite und versuchen es erneut.			
	Deuts	ich 🔺		

Mit "<<Zur Anmeldung" gelangt man zurück zur Startseite (Eingabe Benutzername & Passwort) und kann den Log-In Prozess so erneut starten.

### 4.3 Offline-Login

Der Log-In Prozess startet wie gewohnt.

	Abacus ERP	Login
Benutzername		
kollers		
Passwort		
		Anmelden

#### 4.3.1 QR-Code

Wird nun keine Anfrage in der Abacus Access App empfangen (z.B. weil der Server nicht erreichbar ist), kann der Link "QR-Code mit Abacus Access scannen" angeklickt werden.



Daraufhin wird im Browser folgendes angezeigt:



Nun wird über die Abacus Access App dieser QR-Code gescannt, woraufhin ein Zahlencode ausgegeben wird.



### **i**

Sollte es grundsätzlich so sein, dass auf diese Installation "offline" zugegriffen wird/werden muss, so kann im QR-Code Fenster das entsprechende Flag gesetzt werden. Auf diese Weise wird beim nächsten Log-In automatisch ein QR-Code generiert, ohne dass dafür vorgängig der Link angeklickt werden muss.

#### 4.3.2 Länge des Zeichencodes definieren

Per Default wird ein 8-stelliger Zahlencode für das Offline-Log-In ausgegeben. Dies kann über den Abacus Configurator, unter Authentifizierung, angepasst werden.

Authentifizierungskontextklassen Authentifizierungskontextrichtlinien
Authentifizierung
Vertrauenswürdige CAs
Webserver Zertifikate
Portal
index.html
AbaSystemProperties
Mandant kopieren
Scope erstellen / löschen
Scope erstellen / löschen OpenFolders

Hier wird über "Hinzufügen" ein neuer Key hinzugefügt.

Der Key "Defines the number of digits an OCRA code (signature) must have 1 - 9" wird hinzugefügt.

🔅 Property-Vorlage			$\times$
KEY		VALUE	
Gültigkeitsdauer Access-Token	600		
Passwort zurücksetzen erlauben	true		
Zeitlimit Single Sign-on bei Inaktivität	1800		
Max. Gültigkeitsdauer vom Single Sign-on	36000		
Multi-factor authentication enabled	false		
Defines if by default a fallback to offline based multi-factor authentication	false		
Defines the number of digits an OCRA code (signature) must have 1 - 9	8		
Hinzufi	ügen <sub>(Im)</sub>	Abbrechen	

Danach kann der "Value" entsprechend angepasst werden (1-9 Zeichen).



Nach dem Speichern, bzw. beim nächsten Offline-Log-In, wird in diesem Beispiel nur noch ein 4-stelliger Zahlencode generiert.



## **5** Verwaltung Access App in Benutzerverwaltung

### 5.1 Authentisierung

Nachdem sich ein Benutzer das erste Mal erfolgreich mit 2FA angemeldet hat, wird in seinem Profil in der Benutzerverwaltung, unter Authentisierung, das mit dem Konto verknüpfte Gerät angezeigt.

981 Benutzerverwaltung - ABACUS-DEMO [7777]	
Datei Bearbeiten Ansicht Extras Fenster 2	
🕞 • 🖪 🦩 🛞 •   ۹ 🗐	은 🤽 🔅 🗄 🐟 🔳 🔂
Hierarchie Policy 📼 🖚 🛪	Kollers Maske Alle Einstellungen ATK-Benutzer (Standard) V Alles zuklappen
Policies Aktiv 1 (2) (3 (6) (2) (3 (6) Benutzerkategorien ~ ~ Root ~ Admin <u>\$</u> VVMP <u>\$</u> VVPP <u>1</u> Dash <u>1</u> kollers <u>4</u> kollers	Nur mit externer Authentisierung einloggen     Benutzer danf "angemeldet bleiben"     Benutzer danf "angemeldet bleiben"     Benutzer danf MFA mit der nächsten Anmeldung aktivieren     Benutzer danf MFA selber verwalten     LDAP Konfiguration
	EXTERNE AUTHENTISIERUNG         MULTI-FAKTOR-AUTHENTISIERUNG           AKTIV         HOST         BENUTZER ID         OPENID DISPLAYNA         GERÄTENAME         ERSTELLT         ZULEIZT BENUTZT         IPhone         10.02.2020 08.47         10.02.2020 08.57           Hitzufügen         Exitemen         Doménéne Benutzer Zuordnung         Enternen         Enternen         Enternen

### 5.2 Verwendetes Gerät

Hier wird der Gerätename (iPhone/Android), der Timestamp der ersten Anmeldung und der Timestamp der letzten Verwendung angezeigt.

MULTI-FAKTOR-AUTHENTISIERUNG		
GERÄTENAME	ERSTELLT	ZULETZT BENUTZT
iPhone	10.02.2020 08:47	10.02.2020 08:57
Entfernen		

Der Gerätename wird beim Registrieren automatisch gesetzt und kann nicht manuell bearbeitet, bzw. umbenannt werden.

Pro Installation, bzw. Benutzer kann nur ein (1) Gerät hinterlegt werden. Es ist also nicht möglich, 2FA auf verschiedenen Geräten für dieselbe Installation/Benutzer zu aktivieren.

## 5.3 Gerät löschen

Es kann aus unterschiedlichen Gründen notwendig sein, ein hinterlegtes Gerät zu löschen. Dies erfolgt ebenfalls in der Benutzerverwaltung.

MULTI-FAKTOR-AUTHENTISI	ERUNG		
GERÄTENAME	ERSTELLT	ZULETZT BENUTZT	
iPhone	10.02.2020 08:47	10.02.2020 09:51	
Entfernen			>

🔅 Frage	×
Wollen sie das Gerät "iPhone" wirklich entfernen?	
Ja	

### 5.4 Erneutes hinterlegen eines Gerätes

Es besteht keine Möglichkeit, ein Gerät direkt in der Benutzerverwaltung zu hinterlegen. Soll sich ein Benutzer in Zukunft wieder mit 2FA anmelden können, so muss entsprechend das Flag gesetzt werden, dass der Benutzer beim nächsten Log-In Prozess 2FA aktivieren muss.

MFA mit der nächsten Anmeldung aktivieren	
Demokana da KMCA selles menekan	

## 6 Einstellungsmöglichkeiten (Kombinationen)

Wie bereits gesehen, muss für die Verwendung der 2FA zum einen die Einstellung im Abacus Configurator, wie auch in der Benutzerverwaltung erfolgen.

## 6.1 Abacus Configurator



### 6.2 Benutzerverwaltung

<ul> <li>981 Benutzerverwaltung - ABACUS-DEMO</li> <li>Datei Bearbeiten Ansicht Extras Fe</li> </ul>	10 [7777]	
<u></u> • <u></u> <i>₹</i> ⊗ •   Q		
Hierarchie Policy	🖙 🗖 × Root	Macka Alla Einstellungen Benutzerketegerie (Standard)
Policies Aktiv		V Login Einstellungen X
1 2 3 4 5 6 7 8 9 Benutzerkate	egorien V	MULTI-FAKTOR-AUTHENTISIERUNG
✓ ☐ Root	ID 3eb95610	10 5/24
✓ ☐ Admin	Name Root	Multi-Faktor-Authentisierung aktiv
🧟 VMM	Schutzstufe 8	
🤽 VVP		ALLGEMEINE BENUTZERKONTO EINSTELLUNGEN
👤 Dash		Ablaufzait dar Basswätter
l	200RIT AUT ADAVISION	
× C Boot	AMOLVION DELIGIZEL	_ Сазл маладел Саас Белисен (V/40)
Admin	Secure Mail Benutzer	Visumsbenutzer (0/30) Visumsbenutzer2 (0/20)
🧏 VMM	AbaMonitor Benutzer	ViewOnly Benutzer
🧏 VVP	ODBC Benutzer	
1 Dash		
kollers	LOGIN DATEN	
Automistrator EBusinessService	Passwort mit der nächsten Anmeldung ändern	Passwort ändern
🏂 System	Passwort nicht veränderbar	Link zum Erfassen einer externen Authentisierung versenden
🎄 SystemSwiss21	Passwort läuft nicht ab	
	Passwort zurücksetzen erlauben	
	Nur mit externer Authentisierung einloggen	
	Benutzer darf "angemeldet bleiben"	The second secon
	Benutzerkonto inaktiv	
	MFA mit der nächsten Anmeldung aktivieren	
	Benutzer darf MFA selber verwalten	LDAP Konfiguration

Je nachdem wie diese Kombinationen eingestellt werden, ergibt sich ein anderes Verhalten beim Log-In. Nachfolgend eine Übersicht, welche Kombination aus diesen Einstellungen zu welchem Verhalten führt.

Abacus Access

# 6.3 Einstellungen auf Benutzer und Login Policy

Benutzer/Login Policy	Opportunistic	Mandatory	Off
Keine MFA Flags	Normaler Login möglich	Zugriff verweigert	Normaler Login möglich
MFA mit der nächsten Anmeldung aktivieren	Onboarding erfolgt Bei neuer Anmeldung erfolgt MFA-Abfrage.	Onboarding erfolgt Bei neuer Anmeldung erfolgt MFA-Abfrage.	Normaler Login möglich Kein MFA Onboarding
Benutzer darf MFA selber verwalten	Normaler Login möglich Kein MFA Onboarding	Onboarding erfolgt Bei neuer Anmeldung erfolgt MFA-Abfrage.	Normaler Login möglich
Beide MFA Flags aktiv	Onboarding erfolgt Bei neuer Anmeldung erfolgt MFA-Abfrage.	Onboarding erfolgt Bei neuer Anmeldung erfolgt MFA-Abfrage.	Normaler Login möglich Kein MFA Onboarding

## 7 Ablösung SuisselD / MobileID

Falls ein oder mehrere Benutzer aktuell die SuisselD oder MobileID verwenden, so ist dies in der Benutzerverwaltung ersichtlich.

981 Benutzerverwaltung - ABACUS-DEMO [7777]	
Datei Bearbeiten Ansicht Extras Fenster ?	
🝺 • 💾 🖗 🛞 •   ۹ 🖴 🕂 🤞	🕸 🔒 🔅 🔳 🔎 🚺 🏷
Hierarchie Policy 🖾 📼 ×	× kollers
Policies Aktiv	
1 2 3 4 5 6 7 8 9 Benutzerkategorien v	Y EXTERNE AUTHENTISIERUNG
V 🗋 Root	
V 🗋 Admin	AKTIV HOST BENUTZER ID OPENID DISPLAYNA
🧕 VVMP	✓ suisseid-prod 1234-5678-9012-3456
🧏 VVPP	
👤 Dash	Hinzufügen Editieren Entfernen Domänen Benutzer Zuordnung
👤 kollers	

### 7.1 Login mit Benutzername & Passwort

Damit sich nach der Ablösung der SuisseID/MobileID die User einloggen können, muss der Log-In mit Benutzername & Passwort für die User entsprechend möglich sein und in der Benutzerverwaltung entsprechend eingerichtet werden.

#### 7.1.1 Generelle MFA-Aktivierung

In der Benutzerverwaltung muss 2FA/MFA zuerst generell aktiviert werden um es danach für einzelne User aktivieren zu können. Hierzu wird in den Login Einstellungen das Flag "Multi-Faktor-Authentisierung aktiv" gesetzt.

♦ 981 Benutzerverwaltung - ABACUS-DEMO [7777]       Datei Bearbeiten Ansicht Extras Fenster 2       • • • • • • • • • • • • • • • • • • •		) * E	] 😡 🔞 🗖
Hierarchie Policy 🖙 🗖 🛛	Root		Alla Einstellungen Alla Einstellungen Benutzerkategoria (Standard)
Policies Aktiv 1 2 3 4 5 6 7 8 9 Benutzerkategorien v		V	MULTI-FAKTOR-AUTHENTISIERUNG
<ul> <li>✓ C Root</li> <li>✓ Admin</li> </ul>	ID Name	3eb95610.of24 Root	Multi-Faktor-Authentisierung aktiv
A VMM	Schutzstufe	8 🗘	
1 Dash	ZUGRIFF AUF ABAV	ISION	Ablaufzeit der Passwörter 30 🗘 Tage

### 7.1.2 MFA aktivieren

Ausserdem muss auf dem/den User/n die MFA-Flags gesetzt werden, damit nach der Ablösung von SuisseID/MobileID Abacus Access als neue 2FA aktiviert wird.

× C Root	AAOLVIION DEHICISE	Casii Manager	Saas Denurzei (0/40)
× Admin	Secure Mail Benutzer	Visumsbenutzer (0/30)	Visumsbenutzer2 (0/20)
A VMM	AbaMonitor Benutzer	ViewOnly Benutzer	DBX Benutzer
1 VVP	ODBC Benutzer		
1 Dash			
1 kollers	LOGIN DATEN		
<ul> <li>Administrator</li> <li>BusinessService</li> <li>System</li> <li>SystemSwiss21</li> </ul>	Passwort mit der nächsten Anmeldung ändern Passwort nicht veränderbar Passwort lauft nicht ab Passwort zurücksetzen erlauben Nur mit externer Authentisierung einloggen Benutzer dan <sup>®</sup> angemeldet bleiben <sup>®</sup>	Passwort ändem Link zum Erfassen einer externen Authentisierung verse	anden
	MFA mit der nachsten Anmeldung aktivieren	LDAP Konfiguration	

#### 7.1.3 MFA zwingend

Im Abacus Configurator sollte MFA ab diesem Zeitpunkt auf "zwingend" (Mandatory) gestellt werden. Weitere Informationen zu diesen Einstellungen sind unter 6.3 zu finden.

MultifFactorAuth —	
Opportunistic	
Mandatory	
Off	

### 7.2 Nur externe Authentisierung

Benutzer, die sich nur mit externer Authentisierung anmelden können, werden durch diese Ablösung aus Abacus/MyAbacus "ausgeschlossen", da sie nach der Ablösung der SuisselD keine Möglichkeit mehr haben, sich einzuloggen.

Passwort mit der nächsten Anmeldung ände	rn
Passwort nicht veränderbar	
Passwort läuft nicht ab	
Passwort zurücksetzen erlauben	
Nur mit externer Authentisierung einloggen	>
Benutzer darf "angemeldet bleiben"	
Benutzerkonto inaktiv	
MFA mit der nächsten Anmeldung aktivieren	I
Benutzer darf MFA selber verwalten	

Damit auch ein Login über Benutzername/Passwort möglich ist, muss auf diesen Benutzer das Flag "Nur externe Authentisierung einloggen" entfernt werden. Hierfür ist auch eine Massenanpassung in der Abacus Benutzerverwaltung verfügbar.

## 7.3 Abacus Configurator

Soll nun die SuisseID oder Mobile ID durch die Abacus Lösung, sprich Abacus Access, abgelöst werden, so kann dies relativ einfach über den Abacus Configurator gelöst werden.

Unter "SAML 2.0 / OpenID Connect" kann entsprechend das oder die Flags bei "SuisseID ablösen" bzw. "MobileID ablösen" gesetzt werden.

🔅 Abacus Konfigurator [Scope = De	efaultScope	=]						
Datei Dienst Einstellungen								
상상 상 습	£7	Ċ		盂		$\Box$	5	<u> </u>
Start Stop Registrieren Standard Der	registrieren	Aktualisieren	Speichern	Load Balancing	DBConfig	AbaSysInfo	Scope	Remote Debuggi
Dienste	Aktue	ller Scope	e = Defa	ultScope				
Dienst-Einstellungen								
Ports	Suis	selD ablose						
Proxy-Einstellungen		lieiD abiose	NAME					ID
Service-URL	Suissse	ld	INAME			Suissseld		
Aktualisierungen	Mobilelo	l				MobileId		
Webserver								
External Webserver								
Service Monitoring								
c-tree Mandanten Konvertierung								
c-tree Verschlüsselung								
Speicherzuweisung								
Administrator zurücksetzen								
LDAP	1							
SAML 2.0 / OpenID Connect	'							
Authentifizierungskontextklassen								
Authentifizierungskontextrichtli								

Danach muss diese Anpassung gespeichert werden.

## 7.4 Log-In Prozess

Loggt sich der Benutzer das nächste Mal mit SwissID ein, so ist das wie gewohnt möglich.

acus ERP Login	Business So
Bitte anmelden für Abacus	
Benutzername	Anmelden mit
	SuisselD
Passwort	
Anmelden	
	Deuts

Es folgt die Abfrage der E-Mail-Adresse, des Passworts und des SMS-Codes

suisseID	suisselD
<b>Login für Abacus ERP Login</b> Bitte geben Sie Ihr Passwort ein.	In wenigen Augenblicken erhalten Sie einen SMS-Code auf Ihr Handy.
E-Mail-Adresse	
sandro.koller@abacus.ch	Login für Abacus ERP Login
Passwort	Bitte geben Sie den SMS-Code ein.
	SMS-Code
Passwort anzeigen	804196
<ul> <li>▶ Neu registrieren</li> <li>₽ Passwort vergesen</li> </ul>	SMS-Code nochmals senden Bestätigen

Anstatt nun allerdings im Abacus angemeldet zu werden, erscheint die folgende Information:

Abacus ERP Login	Business Software
Anderen Login wählen	
Der Login über 'SuisselD' wird ausser Bitte wählen Sie einen alternativen Lo	Betrieb genommen. gin.
Sie können den Benutzernamen <b>kolle</b> Passwort auf der Anmeldeseite nutze	e <b>rs</b> mit dem zugehörigen n.
	Zur Anmeldung
Haben Sie Ihr Passwort vergessen? Sie zurücksetzen.	e können es hier
Pas	swort zurücksetzen
	Deutsch 🔺

Somit weiss der Benutzer, dass er sich zukünftig nicht mehr über SuisselD/MobileID einloggen kann.

### 7.5 Authentifizierungsmöglichkeit entfernen

Die Benutzer können somit weiterhin "versuchen" sich einzuloggen, solange diese Log-In Möglichkeit zur Verfügung steht. Es erfolgt keine Rückprüfung von Seiten Abacus, bzw. solange der Button "Anmelden mit SuisseID" zur Verfügung steht, können sich Benutzer damit versuchen anzumelden, was aber im letzten Schritt mit der zuvor genannten Meldung verhindert wird. Es ist also sinnvoll, diese Log-In Möglichkeit nach erfolgter Umstellung zu entfernen.

🔅 Abacus Konfigurator [Scope = Def	faultScope]							-		×
Datei Dienst Einstellungen										
중 중 중 🚳 💣	O     O		Æ		$\Box$		5	5	?	
Start Stop Registrieren Standard Dere	egistrieren Aktualisieren	Speichern Load	Balancing	DBConfig	AbaSysInf	o Scope	Remote Debugging	Cloud Server	Hilfe	
Dienste	Aktueller Scope	= DefaultSc	ope							
Dienst-Einstellungen	Authentifizierungsk	ontextklassen-								
Ports		NAME					ID			
Proxy-Einstellungen	Default				defau	lt				
Service-URL	Two-Factor				two-fa	actor				
Aktualisierungen										
Webserver										
External Webserver										
Service Monitoring										
c-tree Mandanten Konvertierung										
c-tree Verschlüsselung	Hinzufügen	Umbenn	enen	Ent	fernen					
Speicherzuweisung	Authentifizierung									
Administrator zurücksetzen	✓ ADFS									
LDAP	<ul> <li>Benutzername</li> </ul>	/ Passwort								
SAML 2.0 / OpenID Connect	Google									
Authentifizierungskontextklassen	Mobile ID									
Authentifizierungskontextrichtli	SMS									
Authentifizierung	SuisselD	)								

## 7.6 Arbeitsablauf Ablösung SuisselD/MobileID

In diesen Arbeitsablauf wird von einer Standard Abacus Konfiguration ausgegangen. Es wird die Authentifizierungskontextrichtlinie "Internet Policy" verwendet.

### Arbeitsablauf SuisseID / Mobile ID Ablösen

- 1. Abacus Configurator Abacus Access erzwingen & Benutzername/Passwort aktivieren
- Sektion "Authentifizierungskontextrichtlinien"
- Internet Policy
- Rule 1 editieren

🔅 Abacus Konfigurator [Scope = DefaultS	icope] — 🗆	×					
Datei Dienst Einstellungen							
상상 산 방 수 산							
Start Stop Registrieren Standard Deregistri	eren Aktualisieren Speichern Load Balancing DBConfig AbaSysInfo Scope Remote Debugging Cloud Server Hilfe						
Dienste	Aktueller Scope = DefaultScope						
Dienst-Einstellungen							
Ports	NAME ID						
Proxy-Einstellungen	Default Policy default						
Service-URL	Internet Policy internet						
Aktualisierungen							
Webserver							
External Webserver Umbennenen Entfernen							
Service Monitoring	Rules						
c-tree Mandanten Konvertierung	NAME						
c-tree Verschlüsselung	Rule 1						
Speicherzuweisung							
Administrator zurücksetzen							
LDAP							
SAML 2.0 / OpenID Connect							
Authentifizierungskontextklassen							
Authentifizierungskontextrichtlinien							

- MultiFactorAuth auf "Mandatory" (zwingend) stellen
- Zusätzlich, falls nicht bereits erfolgt, Authentifizierungskontextklasse "Default" auswählen.
   Hierdurch wird der Log-In mit Benutzername & Passwort aktiviert.

🔅 Rule		×
Authentifizierungskontextklassen	- Clients	
🗹 Default	Alle anzeigen	
✓ Two-Factor	<ul> <li>Clients einschränken auf:</li> </ul>	
	- ULC	
MultifFactorAuth		
Opportunistic		
Mandatory	- Web	
0.44	AbaClocK Monitor	

#### Hinweis

Nach diesen zwei Arbeitsschritten ist ein Login über Benutzername & Passwort noch nicht möglich, da MFA in der Benutzerverwaltung noch nicht aktiviert wurde.

#### 2. Benutzerverwaltung - MFA global aktivieren

- Q981 -> Extras -> Login Einstellungen
- "Multi-Faktor-Authentisierung aktiv" Flag setzen

🔅 Login Einstellungen		×
MULTI-FAKTOR-AUTHENTISIERUNG		
Multi-Faktor-Authentisierung aktiv	×	

#### 🔔 Achtung

Ohne diesen Arbeitsschritt, können die MFA Flags auf dem Benutzer nicht manipuliert werden.

#### 3. Benutzerverwaltung – MFA auf dem/den Benutzer/n aktivieren

- "MFA mit der nächsten Anmeldung aktivieren" Flag setzen Bewirkt, dass beim nächsten Log-In des entsprechenden Users die Aufforderung zur Registrierung (Onboarding) mit Abacus Access erfolgt.
- "Benutzer darf MFA selbst verwalten" Flag setzen

MFA mit der nächsten Anmeldung aktivieren

Benutzer darf MFA selbst verwalten

 Massenanpassung – Soll MFA f
ür mehrere oder alle Benutzer aktiviert werden, kann dies auch 
über die Massenanpassung erfolgen.

#### Massenanpassung

- Benutzerverwaltung (Q981)
- Bearbeiten -> Massenanpassung -> Login Daten -> Multi-Faktor-Authentisierung

Massenanpassung	
1. Massenanpassung von - c ···	Massenanpassung von Auswahl der Daten, welche global mutiert werden sollen
	Login Daten

Massenanpassung	
1. Massenanpassung von 2. Login Daten	Benutzer selektieren Selektieren Sie alle Benutzer denen Sie die Einstellung "MFA mit der nächsten Anmeldung aktivieren / Benutzer darf MFA selbst verwalten" selektieren / deselektieren möchten.
	MULTI-FAKTOR-AUTHENTISIERUNG MFA mit der nächsten Anmeldung aktivieren Benutzer darf MFA selbst verwalten Bestehender Faktor deaktivieren
	1 2 3 4 5 6 2 8 9 > Root > ESS Root

- 4. Benutzerverwaltung "Nur mit ext. Authentisierung einloggen" entfernen
- Flag auf dem User entfernen, falls noch gesetzt



 Soll dies bei mehreren oder allen Usern entfernt werden, besteht auch hier die Möglichkeit der Massenanpassung

Q981 -> Bearbeiten -> Massenanpassung -> Login Daten -> Nur mit externer Authentisierung einloggen

Massenanpassung	Maske Alle Einstellungen ATK-Benutzer (Standard)
1. Massenanpassung von	Massenanpassung von Auswahl der Daten, welche global mutiert werden sollen
	Login Daten

Massenanpassung	— D	×
1. Massenanpassung von 2. Login Daten	Benutzer selektieren Selektieren Sie alle Benutzer denen Sie die Einstellung "Nur mit externer Authentisierung einloggen" selektieren deselektieren möchten.	/
	NUR MIT EXTERNER AUTHENTISIERUNG EINLOGGEN	-
	Root       Administrator       Kollers       Super1       ESS Root	



Dieser Flag wurde auf SaaS-Benutzern standardmässig gesetzt. Diese Standardeinstellung wurde mittlerweile aufgehoben, dennoch können viele User diese Einstellung noch aktiv haben.

- 5. Abacus Configurator SuisseID /Mobile ID ablösen aktivieren
- Sektion "SAML 2.0 / OpenID Connect"



Flag bei SuisseID und/oder MobileID setzen

Aktueller Scope = DefaultScope
SuisselD ablösen
MobileID ablösen



Nach dem Setzen der Flags ist immer noch ein Log-In über den jeweiligen IdP möglich. Dem Benutzer wird am Ende des Log-In Prozesses nun allerdings ein Text angezeigt, dass er eine andere Log-In Methode wählen muss (z.B. Benutzername & Passwort).

Abacus ERP Login	Business Software	
Anderen Login wählen		
Der Login über 'SuisselD' wird ausse Bitte wählen Sie einen alternativen L	r Betrieb genommen. ogin.	
Sie können den Benutzernamen <b>kollers</b> mit dem zugehörigen Passwort auf der Anmeldeseite nutzen.		
	Zur Anmeldung	
Haben Sie Ihr Passwort vergessen? S zurücksetzen.	ie können es hier	
Pa	isswort zurücksetzen	
	Deutsch 🔺	

Ein Starten von Abacus ist nicht möglich.

- 6. Abacus Configurator SuisselD /MobileID als Log-In Möglichkeit entfernen
- Sektion "Authentifizierungskontextklassen"
- Authentifizierungskontextklasse "Two-Factor" auswählen
- Flag/s bei SuisseID/MobileID entfernen

🔅 Abacus Konfigurator [Scope = DefaultScope]					
Datei Dienst Einstellungen					
Start Stop Registrieren Standard Deregistrieren	Aktualisieren Speichern Load Balancing DBConfig AbaSysInfo Scope Remote Debugging Cloud Server Hilfe				
Dienste	Aktueller Scope = DefaultScope				
Dienst-Einstellungen	Authentifizierungskontextklassen				
Ports	NAME				
Proxy-Einstellungen	Default	default			
Service-URL	Two-Factor	two-factor			
Aktualisierungen					
Webserver					
External Webserver					
Service Monitoring					
c-tree Mandanten Konvertierung	Hinzufügen IImbennenen Entfermen				
c-tree Verschlüsselung					
Speicherzuweisung					
Administrator zurücksetzen					
LDAP					
SAML 2.0 / OpenID Connect	SuisselD				
Authentifizierungskontextklassen	$\smile$				



#### Hinweis

Nach dem Entfernen des/der Flags stehen diese Log-In Methoden nicht mehr zur Verfügung, bzw. der User kann diese beim Log-In Prozess nicht mehr auswählen.

## 8 Checkliste generell

Was muss vorhanden sein, bzw. welche Einstellungen sind notwendig, um 2FA zu verwenden.

#### Checkliste

- Download/Einrichten der Abacus Access App (siehe Kapitel 1)
- Einstellung im Abacus Configurator vornehmen (siehe Kapitel 2.1)
- Abacus-Installation extern erreichbar? Online-/Offline-Modus (siehe Kapitel 2.1.1)
- Einstellungen in der Benutzerverwaltung Generell/Benutzer (siehe Kapitel 2.2)
- Erstmalige Anmeldung/Aktivierung pro User Onboarding (siehe Kapitel 3)
- □ Ist eine abzulösende Log-In Methode/IdP vorhanden (siehe Kapitel 7)?