

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.

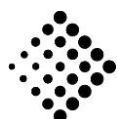
Jede Verwertung in den genannten oder in anderen als den gesetzlich zugelassenen Fällen, namentlich jede kommerzielle Nutzung, bedarf der vorherigen schriftlichen Einwilligung von Abacus Research AG.

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	Abgelaufene Anfragen.....	3
1.1.2	Scanner	4
1.1.3	Menü.....	5
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
2.2.1	Generelle Aktivierung	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
4.2.3	Timeout.....	22
4.3	Offline-Login	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	Erneutes hinterlegen eines Gerätes.....	27
6	Einstellungsmöglichkeiten (Kombinationen)	28
6.1	Abacus Configurator	28
6.2	Benutzerverwaltung	28
6.3	Einstellungen auf Benutzer und Login Policy.....	29
7	Ablösung SuisseID / MobileID	30
7.1	Login mit Benutzername & Passwort.....	30
7.1.1	Generelle MFA-Aktivierung	30
7.1.2	MFA aktivieren	30
7.1.3	MFA zwingend.....	31
7.2	Nur externe Authentisierung	31
7.3	Abacus Configurator	32
7.4	Log-In Prozess	33
7.5	Authentifizierungsmöglichkeit entfernen	34
7.6	Arbeitsablauf Ablösung SuisseID/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 Betriebbarkeit 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:

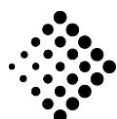
- Version 2020 – 15.02.2020 Release Version
- Version 2019 – 15.03.2020 Servicepack
- Version 2018 – 15.04.2020 Servicepack

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

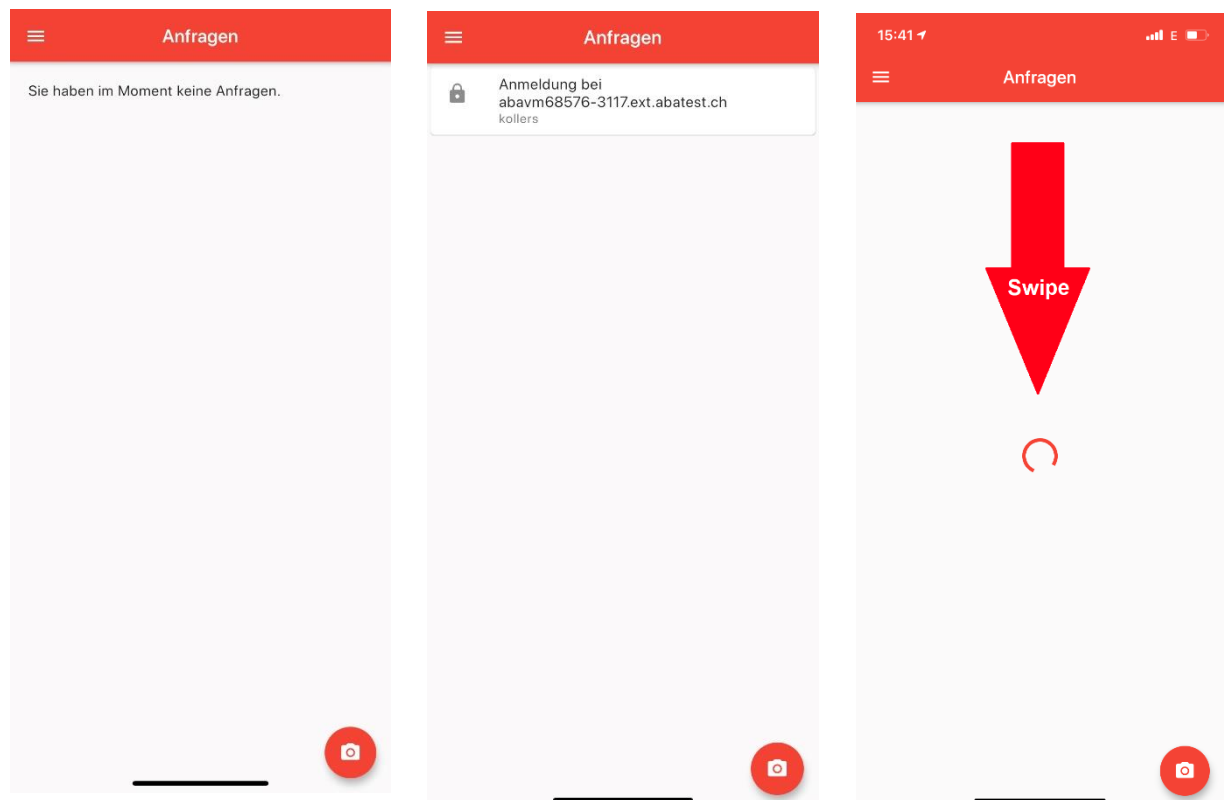
Im Folgenden werden die einzelnen Bereiche der Abacus Access App beschrieben.

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.

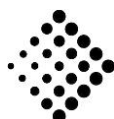
Mit einem Swipe nach unten kann die Ansicht auch manuell aktualisiert werden.



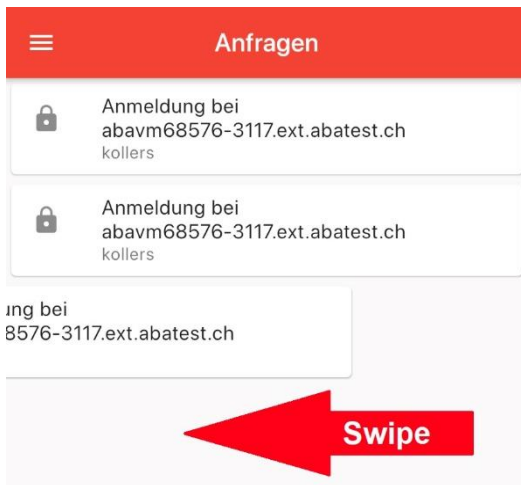
1.1.1.1 Abgelaufene Anfragen

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

Diese Anfragen 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.




1.1.2 Scanner

Über das Foto-Icon wird der Scanner gestartet.

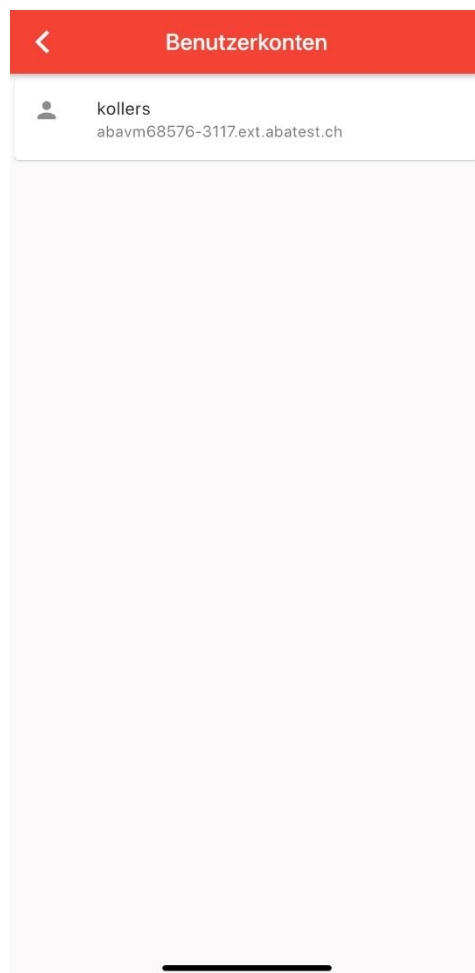


1.1.3 Menü

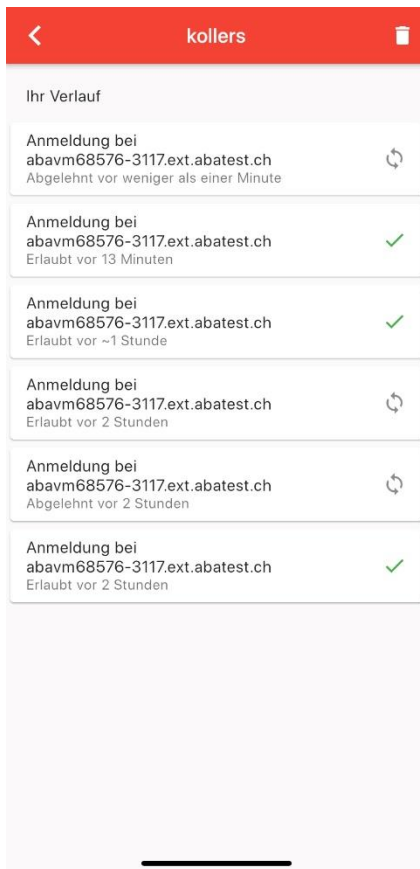
Über das  Icon wird das Menü geöffnet.

1.1.4 Benutzerkonten

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

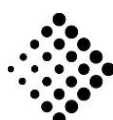
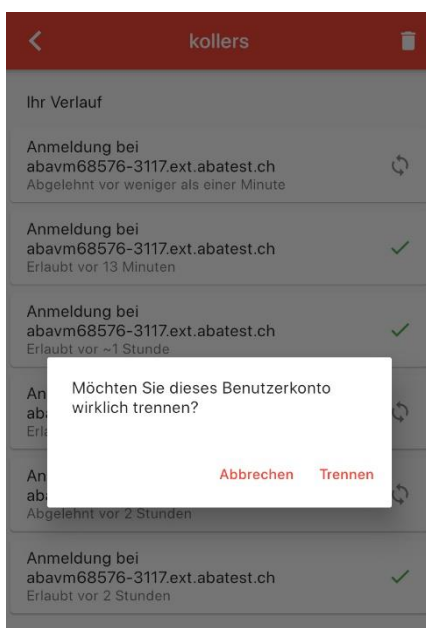


Mit dem Anwählen eines Kontos gelangt man in die Übersicht, bzw. die Verlaufs-Ansicht.



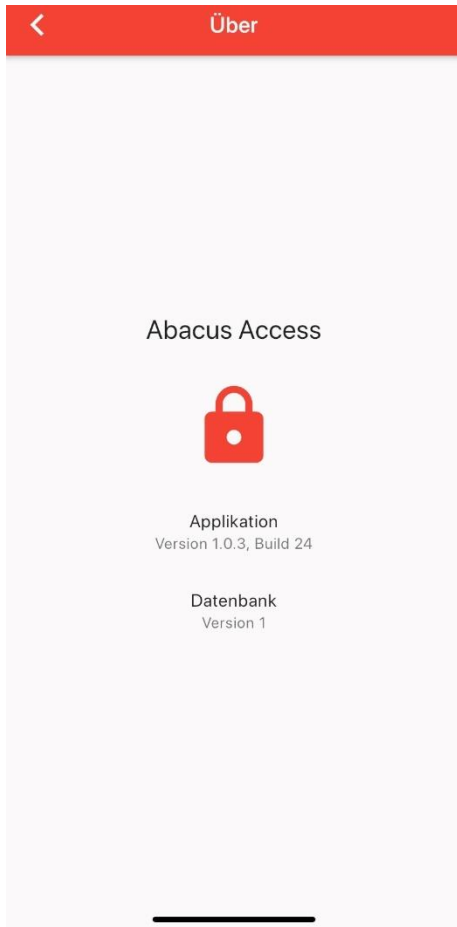
Hier werden alle empfangenen Anfragen, inkl. der Information von welcher Installation, angezeigt und auch, ob diese abgelehnt oder erlaubt wurden.

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



1.1.5 Über

Informationen zur Version der App und der hinterlegten Datenbank.



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.

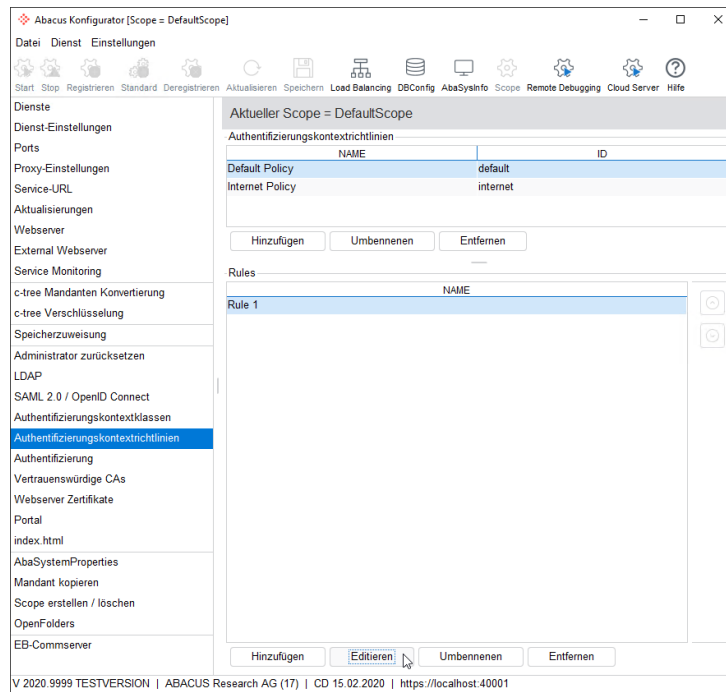
Je nach Kombination dieser Einstellungen ergeben sich die Log-In-Kombinationen gemäss Tabelle unter 6.3.



2 Access App Login aktivieren

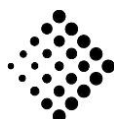
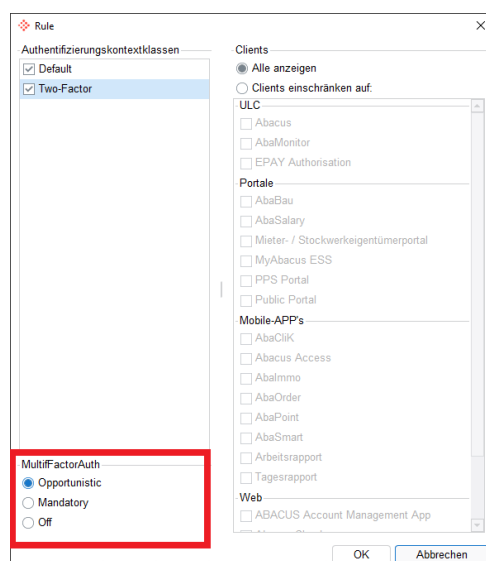
2.1 Einstellungen im Abacus Configurator

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



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

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

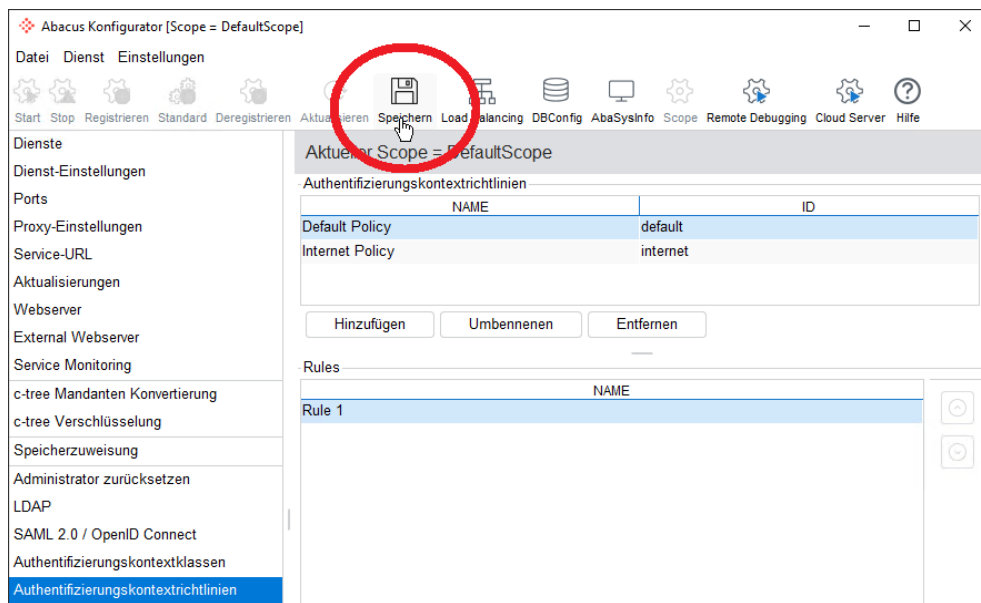


Damit im folgenden Schritt 2FA in der Benutzerverwaltung aktiviert werden kann, muss "Opportunistic" oder "Mandatory" ausgewählt werden. Bei "Opportunistic" wird die Entscheidung, ob 2FA verwendet wird, offengelassen. Bei "Mandatory" ist es hingegen zwingend, dass 2FA vom Benutzer eingerichtet (Onboarding)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



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.

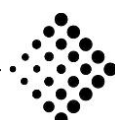
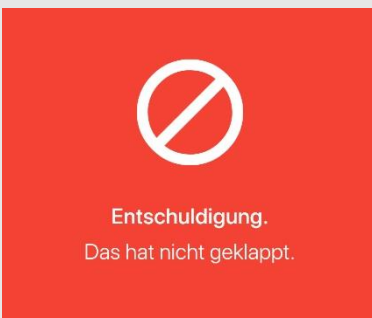


2.1.1 Offline-Modus

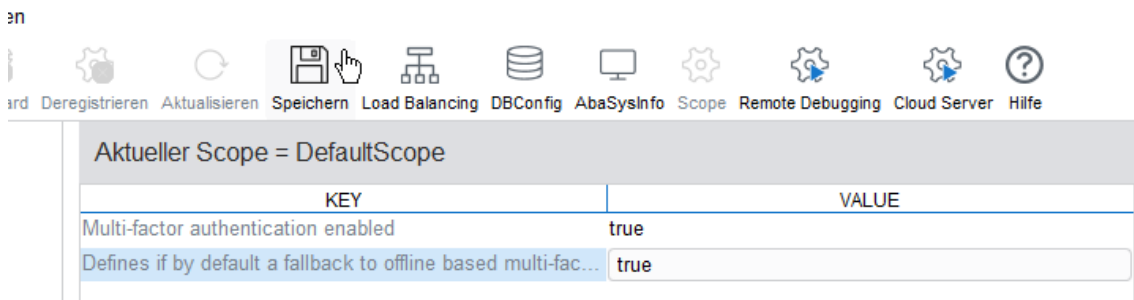
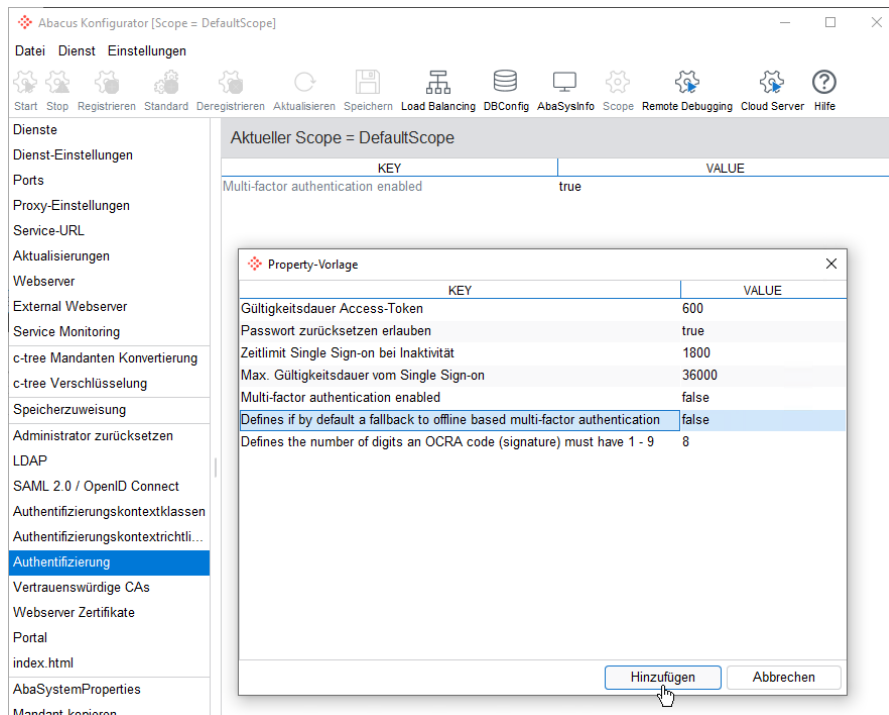
Sollte es aus verschiedenen Gründen nicht möglich sein eine Installation von extern zugänglich zu machen, so kann das Onboarding und der Log-In auch "offline" erfolgen.



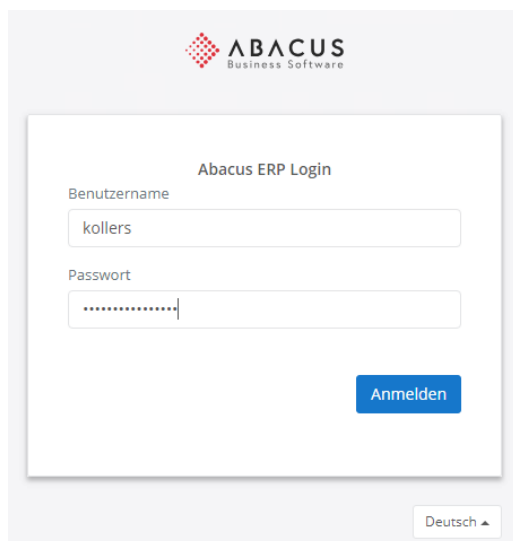
Damit eine "Offline"-Registrierung (Onboarding) des Geräts funktioniert, muss im Abacus Configurator entsprechend zuerst die Einstellung vorgenommen werden, da es ansonsten zu einem Fehler kommt.



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.



Daraufhin erfolgt der Log-In wie gewohnt.

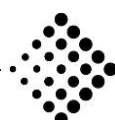


Im nächsten Schritt wird ein QR-Code angezeigt, der mit der Access App gescannt wird, woraufhin in der Access App ein Zahlencode angezeigt wird.

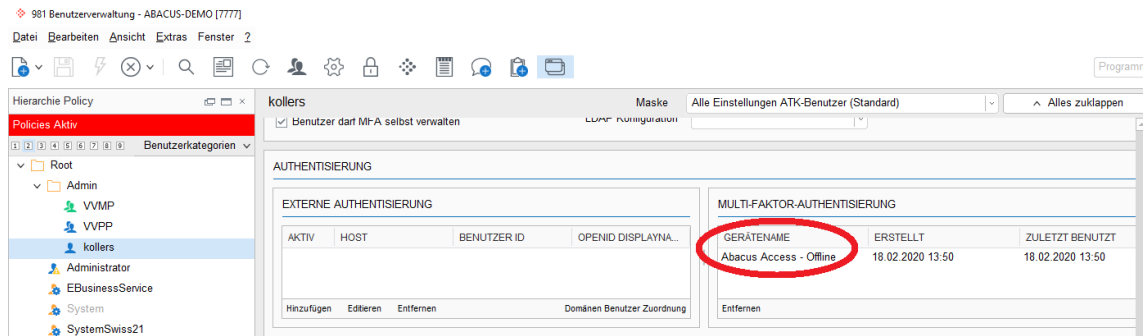
The image shows two parts of the Abacus ERP Login process. On the left is a screenshot of the 'Benutzerkonto schützen' (Protect user account) page. It features the Abacus Business Software logo and instructions to activate Multifactor-Authentication. Step 1 shows download links for Google Play and the App Store. Step 2 shows a large QR code. Step 3 shows a text input field for a 'Zahlencode' (numeric code) and a 'Weiter' (Next) button. On the right is a red confirmation dialog with the text: 'Ihr Benutzerkonto auf abavm76362-3056.abatest.ch mit diesem Gerät schützen?' (Protect your user account on abavm76362-3056.abatest.ch with this device?). It has two buttons: 'Fortfahren' (Continue) with a checkmark and 'Abbrechen' (Cancel) with an X.

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

The image shows two parts of the Abacus ERP Login process. On the left is a green confirmation screen with the text: 'Anmeldung bei abavm76362-3056.abatest.ch' and a large numeric code '35946321'. On the right is a screenshot of the 'Benutzerkonto schützen' page after successful activation. It features a padlock icon and the message: 'Gratulation! Multifaktor-Authentisierung mit Abacus Access wurde eingerichtet.' (Congratulations! Multifactor authentication with Abacus Access has been set up.). A 'Weiter' (Next) button is visible at the bottom.



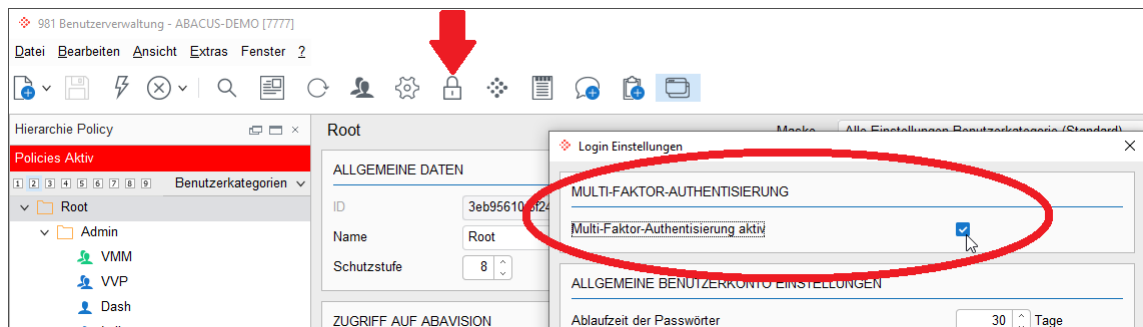
In der Benutzerverwaltung wird bei einem Benutzer, der das Onboarding offline durchgeführt hat, im Gegensatz zum Online-Onboarding, ein anderer Eintrag für das verbundene Gerät angezeigt, der auf die entsprechende Onboarding-Methode hinweist.



2.2 Einstellungen in der Benutzerverwaltung

2.2.1 Generelle Aktivierung

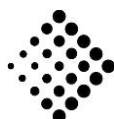
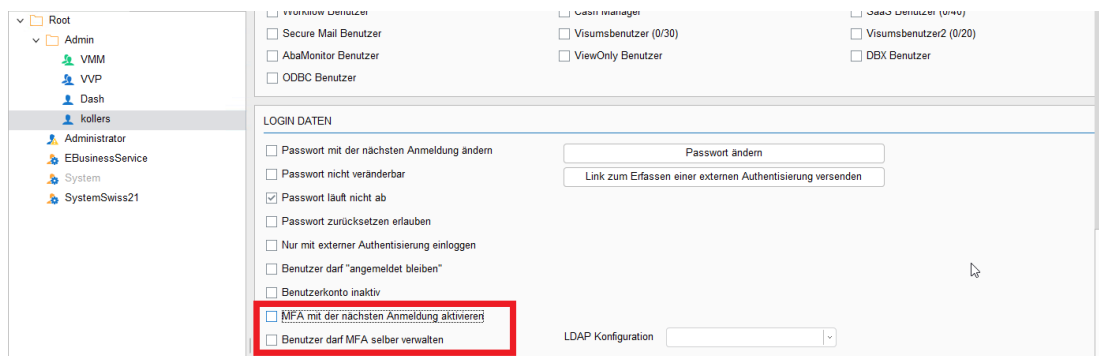
In der Benutzerverwaltung muss 2FA/MFA ebenfalls aktiviert werden. Hierzu wird in den Login Einstellungen das Flag "Multi-Faktor-Authentisierung aktiv" gesetzt.



2.2.2 Aktivierung pro Benutzer

Nun kann pro Benutzer folgendes gewählt werden:

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



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.

 **ABACUS** Profil Passwort Verbindungen ▾

Verbundene Applikationen

Halten Sie ein Auge darauf, welchen Applikationen und Diensten Sie die Erlaubnis gegeben haben, in Ihrem Namen auf das Abacus zuzugreifen. Entfernen Sie jene, die Sie nicht mehr benötigen oder denen Sie nicht mehr trauen.

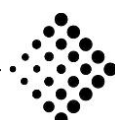
Sie haben die folgenden Applikationen verbunden:

Abacus Access	Letzte Aktivität 14.02.2020, 08:58:19	Trennen
-------------------------------	---------------------------------------	-------------------------

Zukünftig wird es den Benutzer selbst möglich sein, ihre Verbindung zu trennen.



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.



Pro Benutzer einer Installation kann nur ein (1) Gerät hinterlegt werden. Das heisst, es können zwar mehrere Abacus-Installationen und auch unterschiedliche Benutzer einer Installation pro Gerät hinterlegt werden, pro Benutzer auf einer Installation kann jedoch nur ein Gerät hinterlegt werden.

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

Abacus ERP Login

ABACUS
Business Software

Bitte anmelden für Abacus

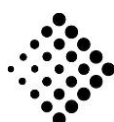
Benutzername
kollers

Passwort
.....

Passwort vergessen?

Anmelden

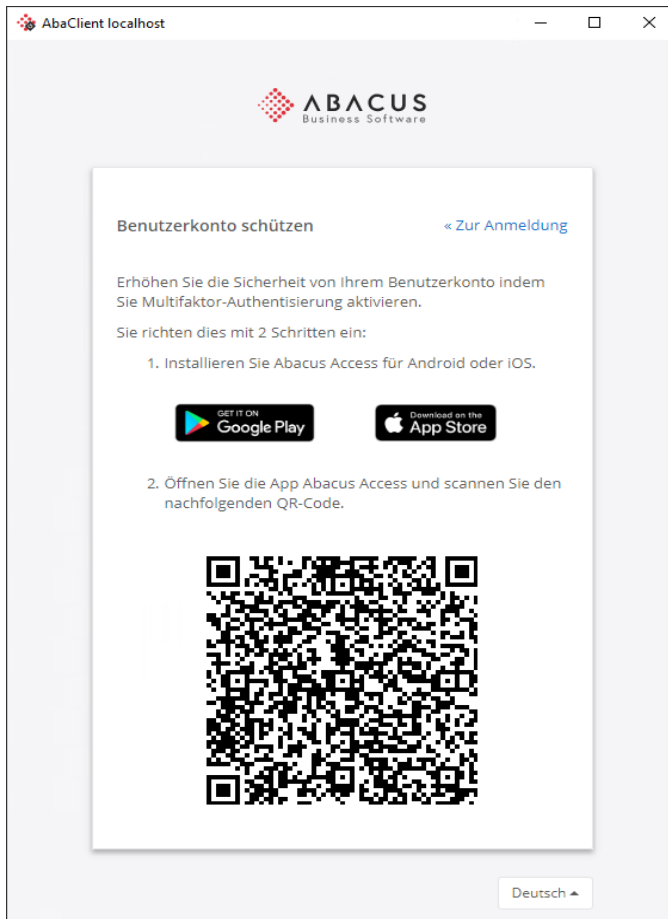
Deutsch ▾





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

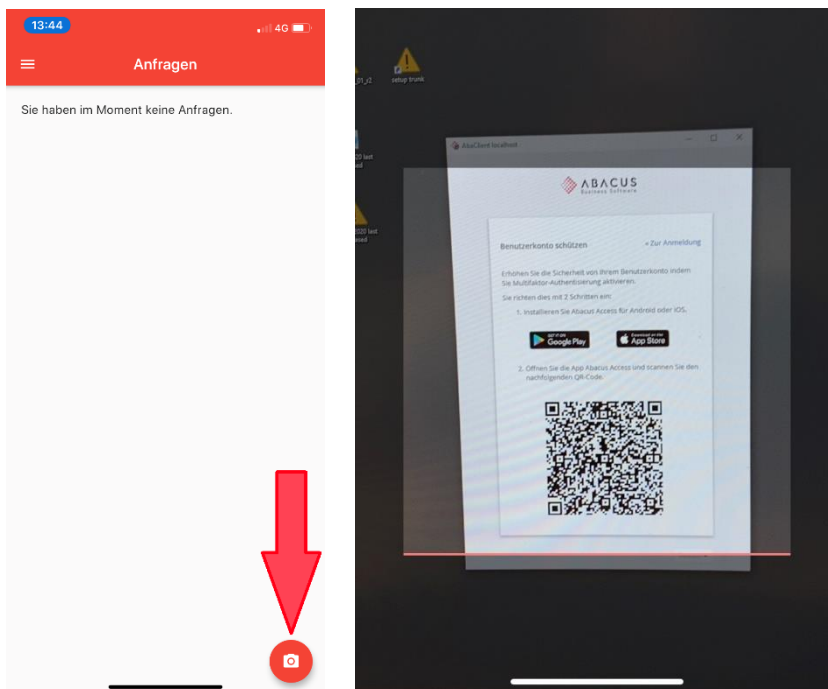
Nach erfolgreicher Eingabe erscheint das neue 2FA-Onboarding-Fenster.



Nun muss auf dem Gerät die Abacus Access App gestartet werden

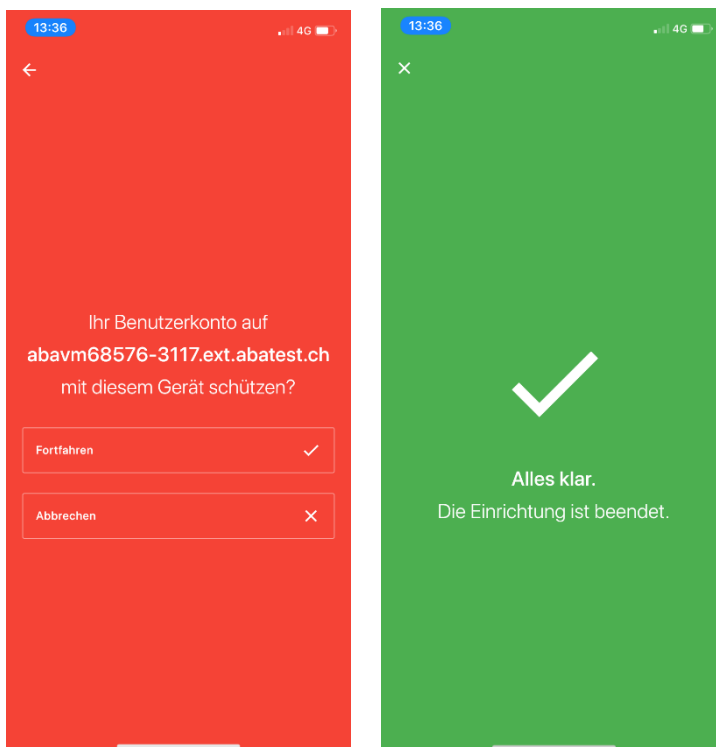


Über das Foto-Icon wird der Scanner gestartet.

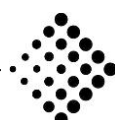


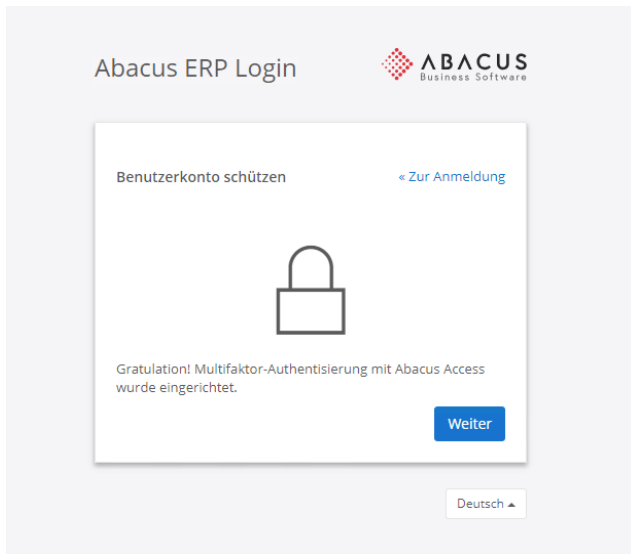
Wurde der QR-Code korrekt erkannt, erfolgt die Abfrage, ob das Benutzerkonto mit diesem Gerät geschützt werden soll.


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



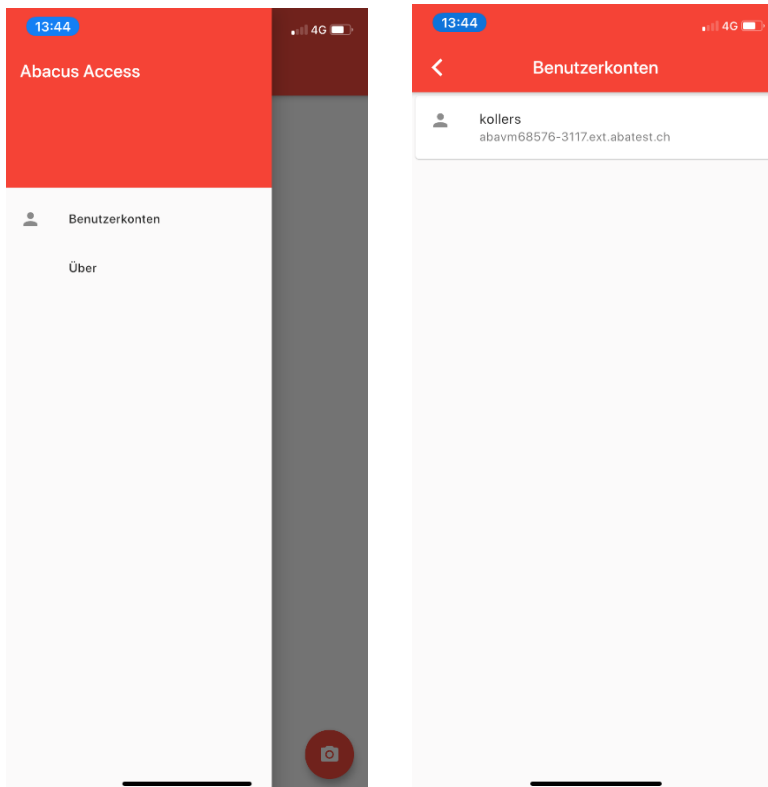
Im Log-In Browser wird ebenfalls eine entsprechende Meldung ausgegeben. Drückt man im Browser auf "Weiter", so verschwindet die Bestätigung in der App ebenfalls.



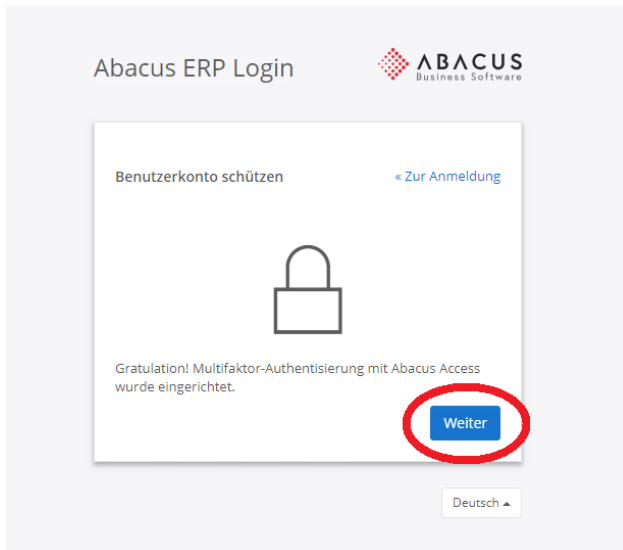


In der Abacus Access App gelangt man über das Symbol  in das Hauptmenü.

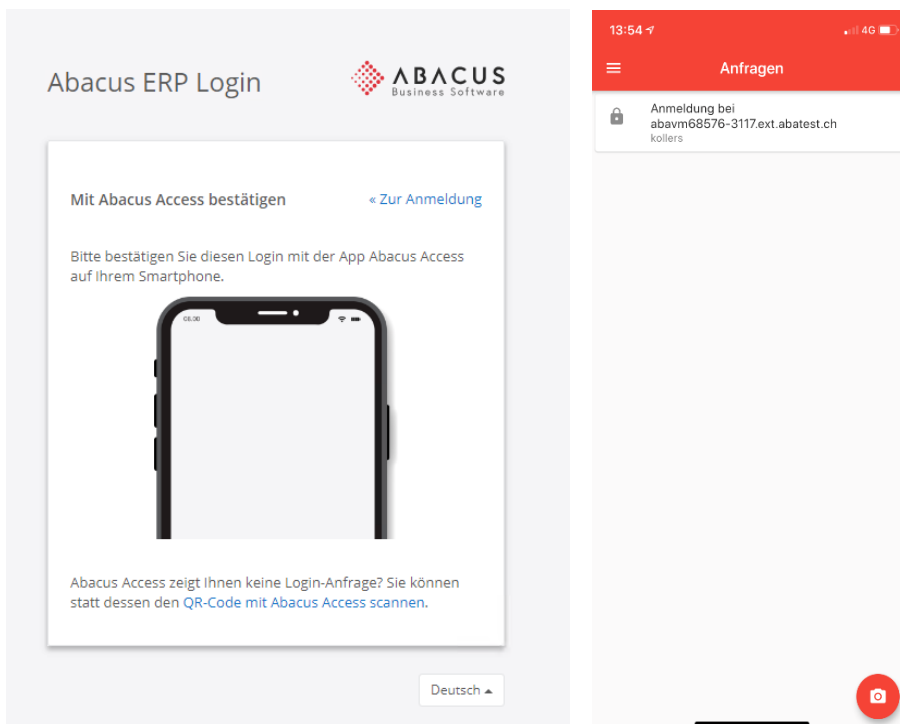
Im "Benutzerkonto" ist nun ein entsprechender Eintrag mit Benutzernamen (Bsp. "kollers") und Installationsname (Service-URL) vorhanden.



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



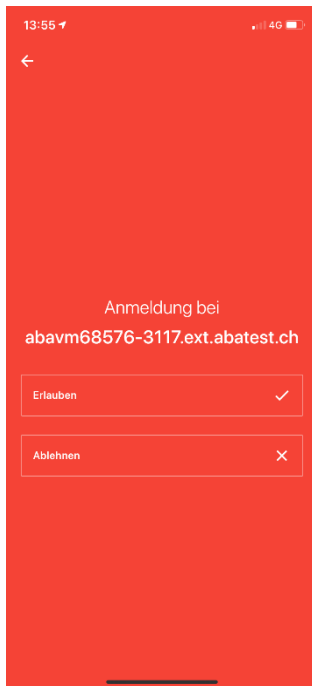
Hierdurch wird ein Vorgang ausgelöst, der zum einen im Log-In Browser anzeigt, dass der Log-In mit der Abacus Access App bestätigt werden muss...



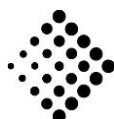
...und zum anderen wird in der Abacus Access App eine entsprechende Anfrage angezeigt.

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





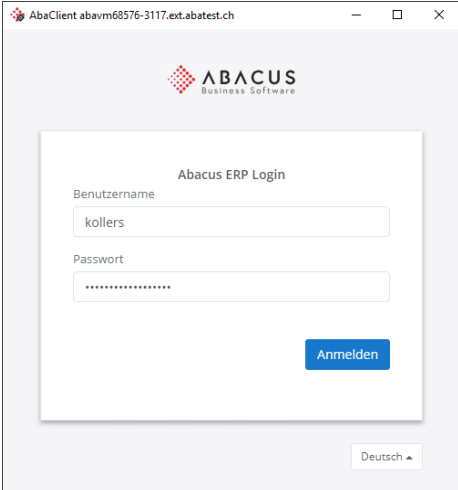


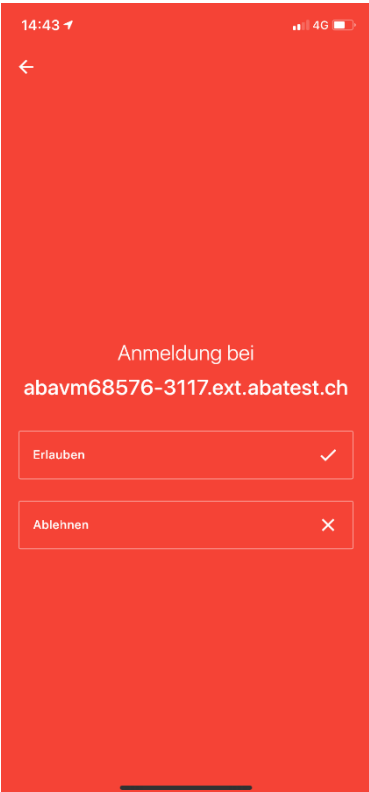
Sobald diese Meldung erlaubt wurde, wird man im Abacus angemeldet.
Der Onboarding Prozess ist somit abgeschlossen und der Benutzer wird im Abacus eingeloggt.

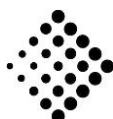


4 Log-In mit Abacus Access

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

4.1 Ablauf

<p>1. Log-In mit Benutzername & Passwort</p> 	<p>2. Hinweis auf die 2FA wird angezeigt</p> 
<p>3. In der Abacus Access App wird die Anfrage angezeigt.</p> 	<p>4. Mit "Erlauben" wird der Log-In Prozess abgeschlossen, Abacus startet.</p> 

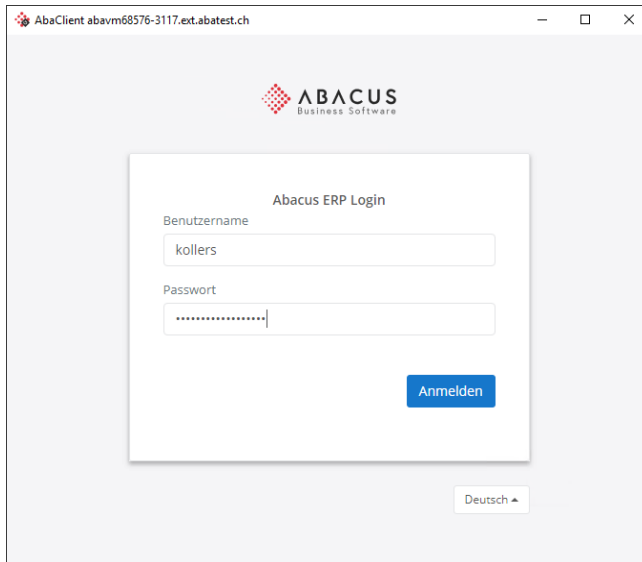


4.2 Ablauf im Browser

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

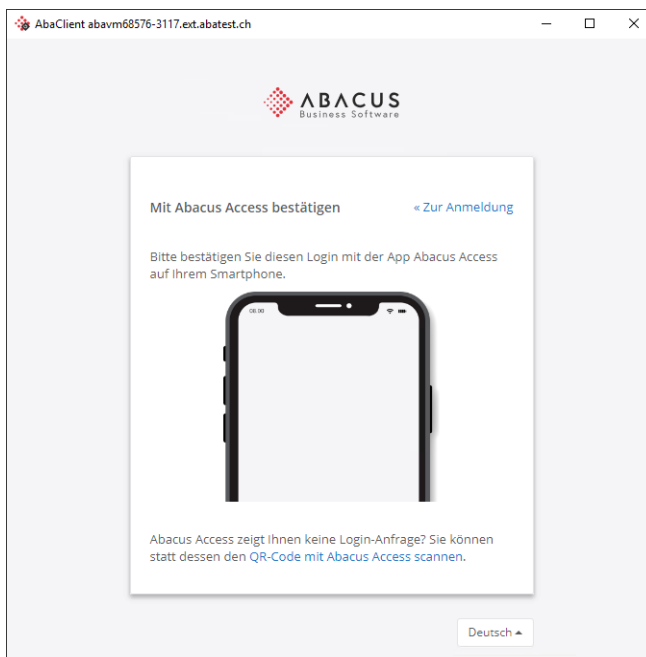
4.2.1 Anmeldedaten

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



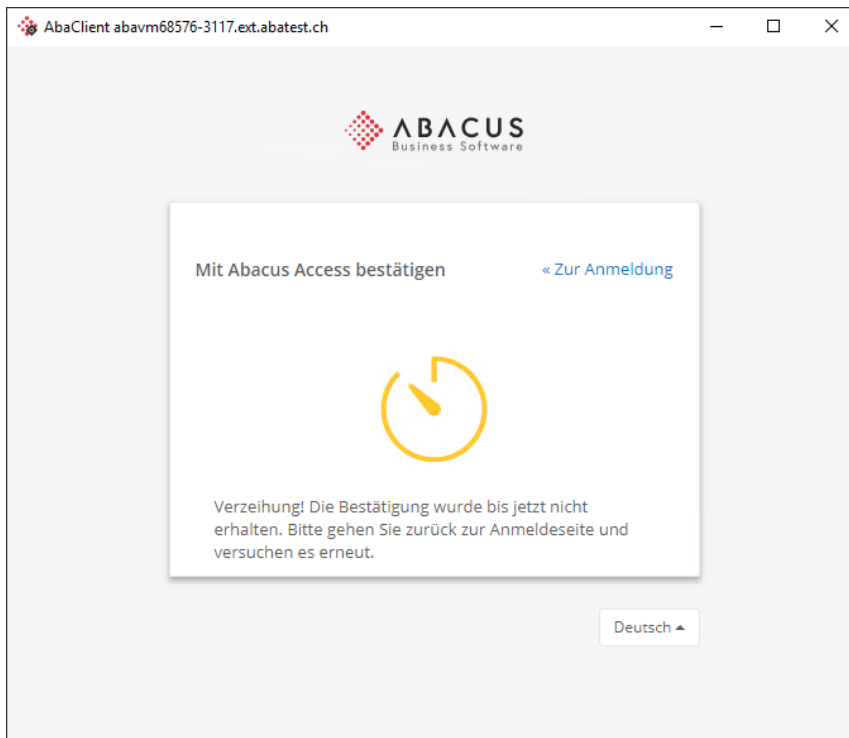
4.2.2 2FA / Hinweis auf Abacus Access

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.



4.2.3 Timeout

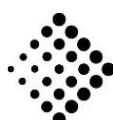
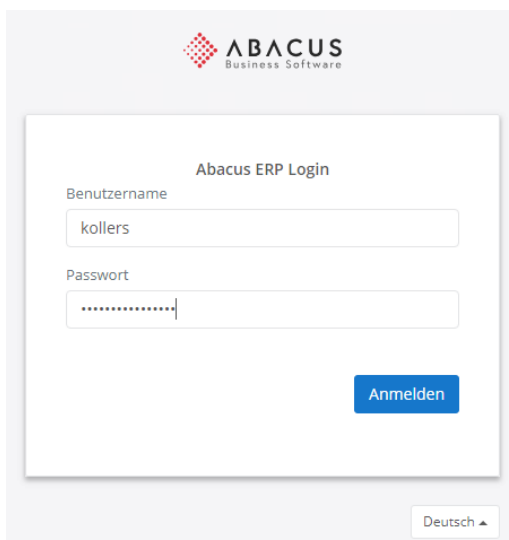
Wird die Anfrage nicht innerhalb 1 Minute bestätigt, so läuft die Anfrage in einen Timeout, was im Browser entsprechend angezeigt wird.



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

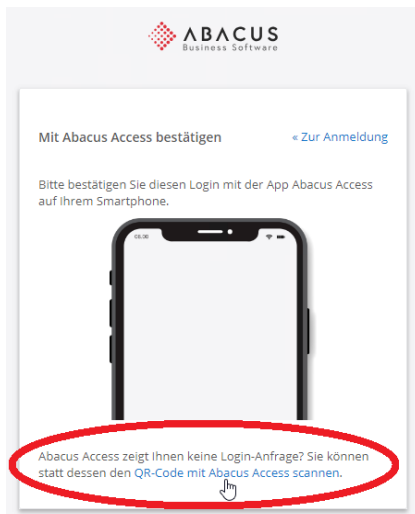
4.3 Offline-Login

Der Log-In Prozess startet wie gewohnt.

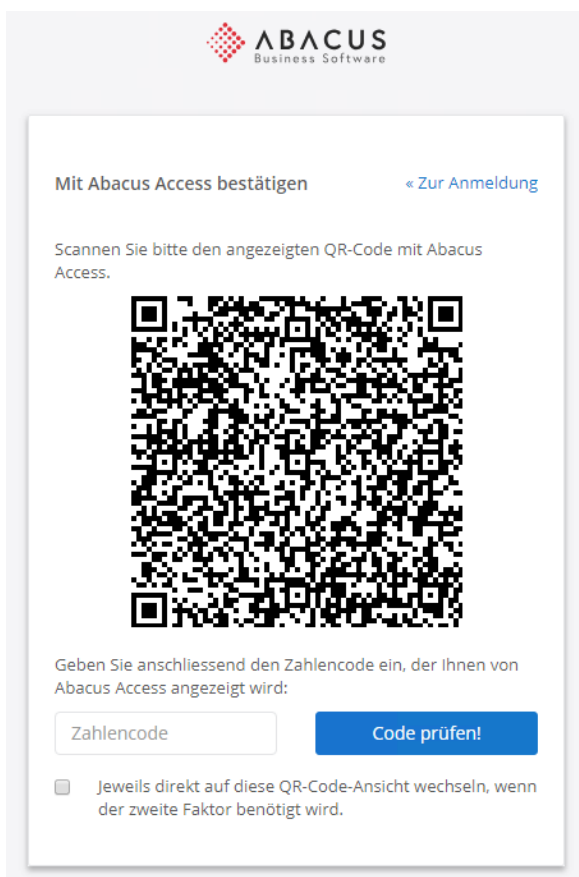


4.3.1 QR-Code

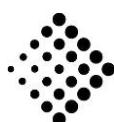
Wird nun keine Anfrage in der Abacus Access App empfangen (z.B. weil der Server nicht erreichbar ist), kann der Link "QR-Code mit Abacus Access scannen" angeklickt werden.

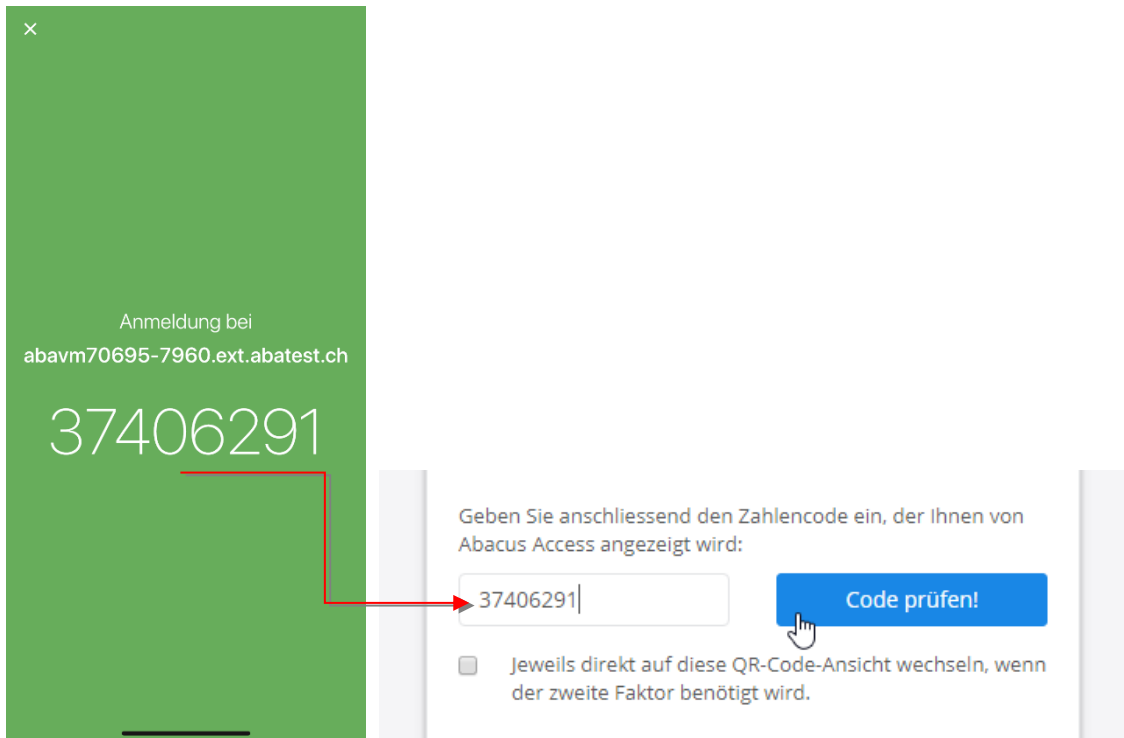


Daraufhin wird im Browser folgendes angezeigt:



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

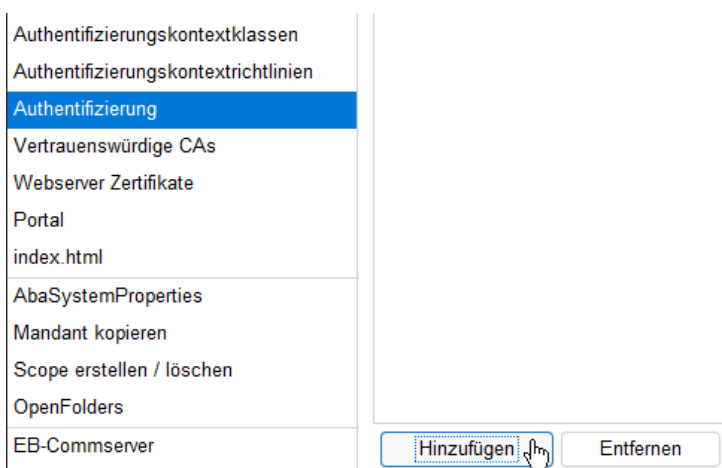




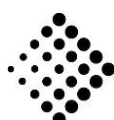
Sollte es grundsätzlich so sein, dass auf diese Installation "offline" zugegriffen wird/werden muss, so kann im QR-Code Fenster das entsprechende Flag gesetzt werden. Auf diese Weise wird beim nächsten Log-In automatisch ein QR-Code generiert, ohne dass dafür vorgängig der Link angeklickt werden muss.

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.



Hier wird über "Hinzufügen" ein neuer Key hinzugefügt.



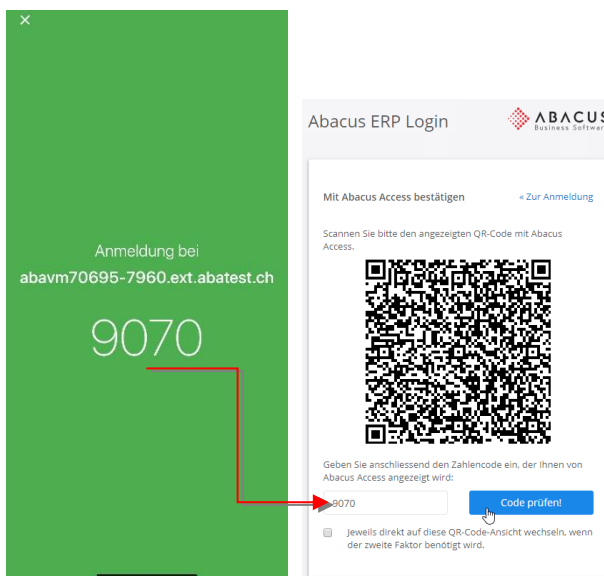
Der Key "Defines the number of digits an OCRA code (signature) must have 1 – 9" wird hinzugefügt.

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

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

KEY	VALUE
Multi-factor authentication enabled	true
Defines the number of digits an OCRA code (signature)	4

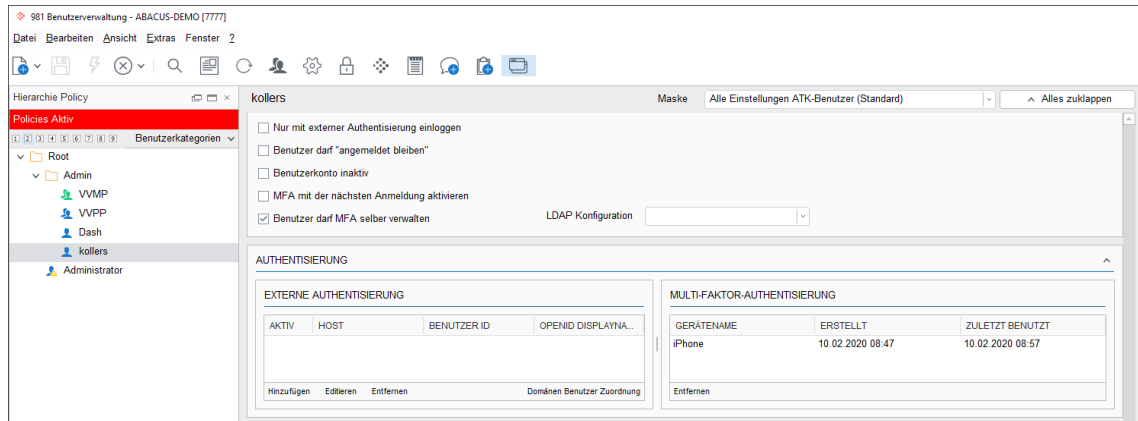
Nach dem Speichern, bzw. beim nächsten Offline-Log-In, wird in diesem Beispiel nur noch ein 4-stelliger Zahlencode generiert.



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.



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-AUTHENTISIERUNG		
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 Nein

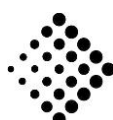
5.4 Erneutes hinterlegen eines Gerätes

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.

Benutzerkonto inaktiv

MFA mit der nächsten Anmeldung aktivieren

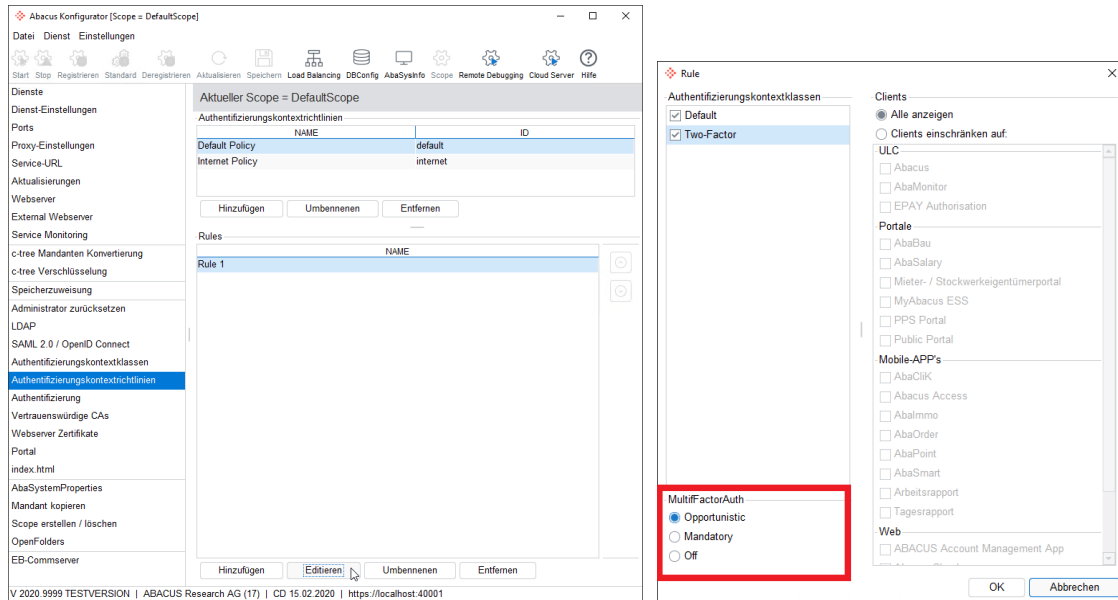
Benutzer darf MFA selbst konfigurieren



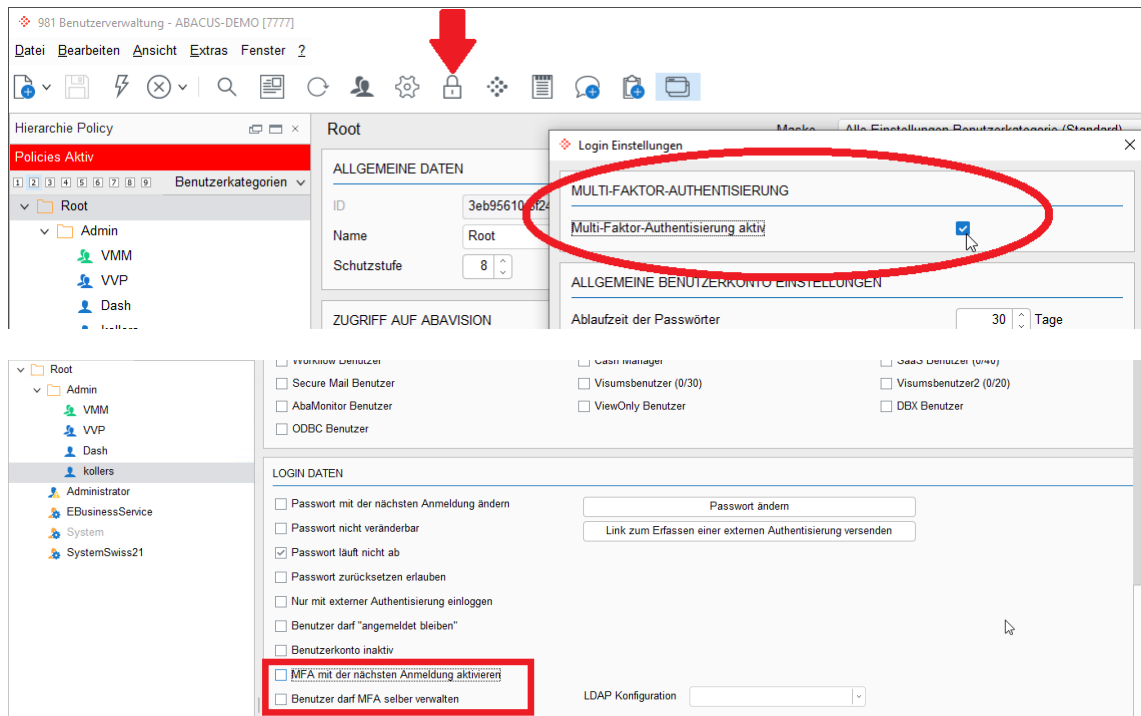
6 Einstellungsmöglichkeiten (Kombinationen)

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

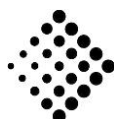
6.1 Abacus Configurator



6.2 Benutzerverwaltung

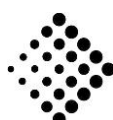


Je nachdem wie diese Kombinationen eingestellt werden, ergibt sich ein anderes Verhalten beim Log-In. Nachfolgend eine Übersicht, welche Kombination aus diesen Einstellungen zu welchem Verhalten führt.



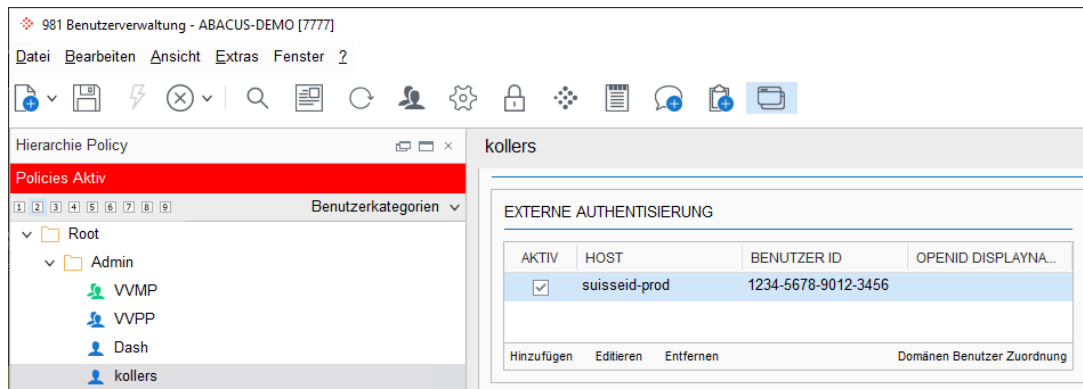
6.3 Einstellungen auf Benutzer und Login Policy

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 SuisseID / MobileID

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

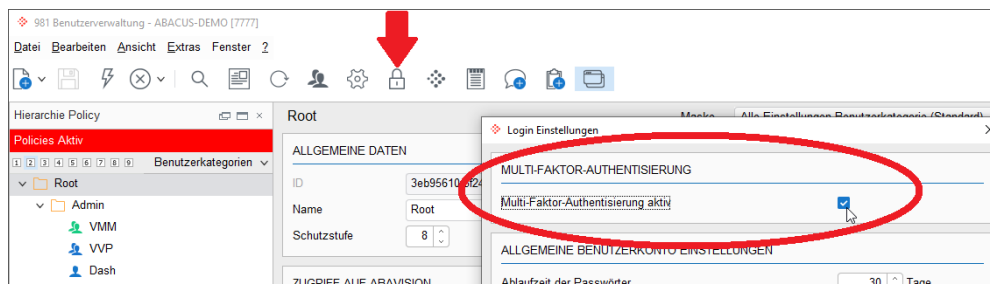


7.1 Login mit Benutzername & Passwort

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

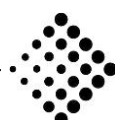
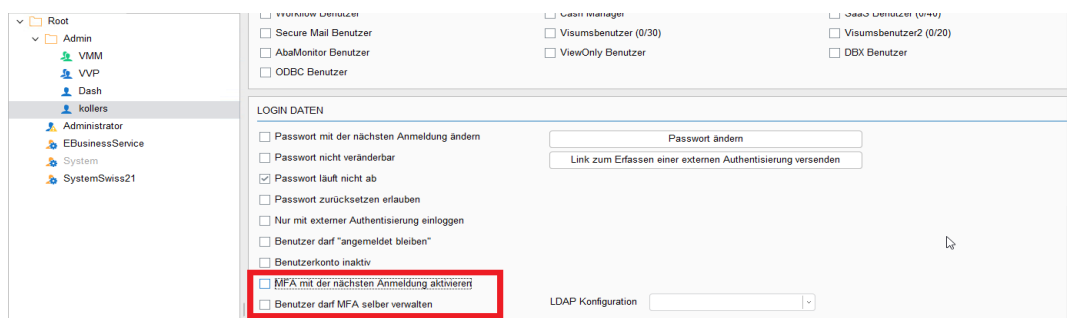
7.1.1 Generelle MFA-Aktivierung

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.



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.



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.

MultifactorAuth

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 SuisseID keine Möglichkeit mehr haben, sich einzuloggen.

LOGIN DATEN

Passwort mit der nächsten Anmeldung ändern

Passwort nicht veränderbar

Passwort läuft nicht ab

Passwort zurücksetzen erlauben

Nur mit externer Authentisierung einloggen

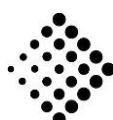
Benutzer darf "angemeldet bleiben"

Benutzerkonto inaktiv

MFA mit der nächsten Anmeldung aktivieren

Benutzer darf MFA selber verwalten

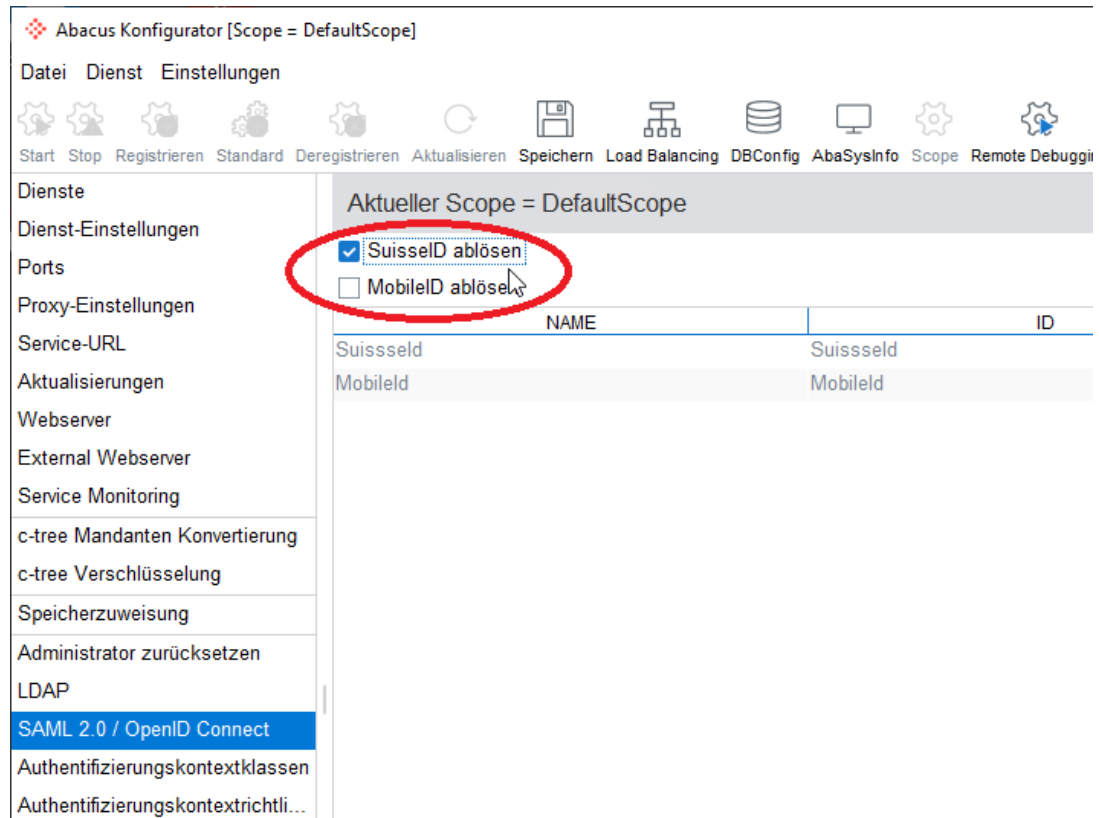
Damit auch ein Login über Benutzername/Passwort möglich ist, muss auf diesen Benutzer das Flag "Nur externe Authentisierung einloggen" entfernt werden. Hierfür ist auch eine Massenanpassung in der Abacus Benutzerverwaltung verfügbar.



7.3 Abacus Configurator

Soll nun die SuisselD 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 "SuisselD ablösen" bzw. "MobileID ablösen" gesetzt werden.



Abacus Konfigurator [Scope = DefaultScope]

Datei Dienst Einstellungen

Start Stop Registrieren Standard Deregistrieren Aktualisieren Speichern Load Balancing DBConfig AbaSysInfo Scope Remote Debuggi

Dienste

Dienst-Einstellungen

Ports

Proxy-Einstellungen

Service-URL

Aktualisierungen

Webserver

External Webserver

Service Monitoring

c-tree Mandanten Konvertierung

c-tree Verschlüsselung

Speicherzuweisung

Administrator zurücksetzen

LDAP

SAML 2.0 / OpenID Connect

Authentifizierungskontextklassen

Authentifizierungskontextrichtli...

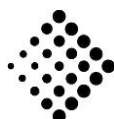
Aktueller Scope = DefaultScope

SuisselD ablösen

MobileID ablösen

NAME	ID
SuisselD	SuisselD
MobileID	MobileID

Danach muss diese Anpassung gespeichert werden.



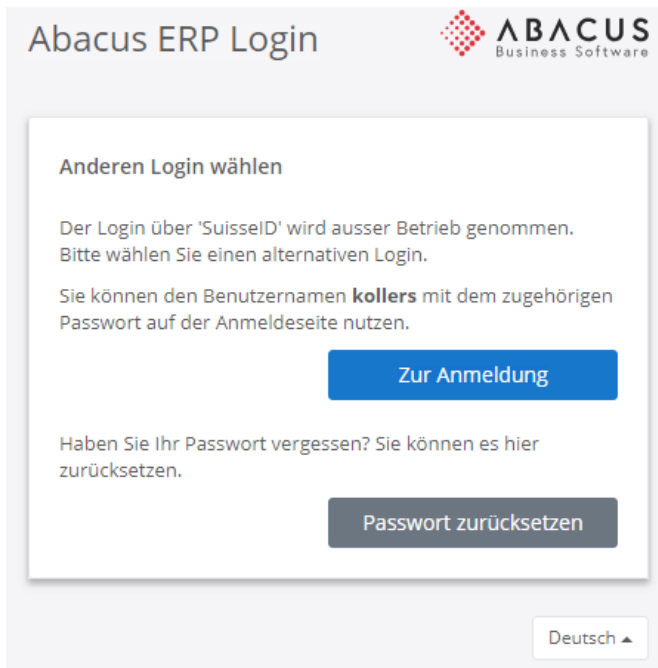
7.4 Log-In Prozess

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

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



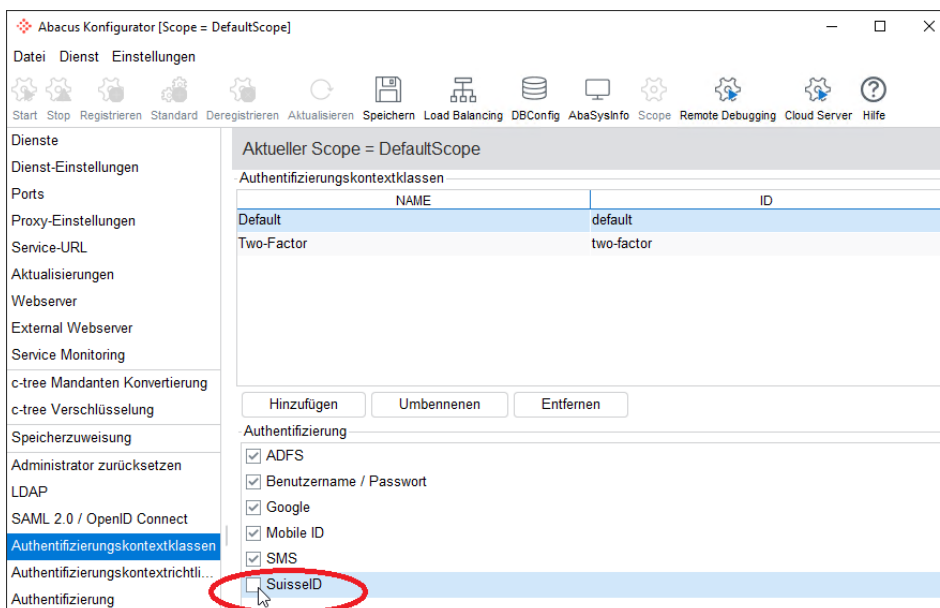
Anstatt nun allerdings im Abacus angemeldet zu werden, erscheint die folgende Information:



Somit weiss der Benutzer, dass er sich zukünftig nicht mehr über SuisseID/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.



7.6 Arbeitsablauf Ablösung SuisseID/MobileID

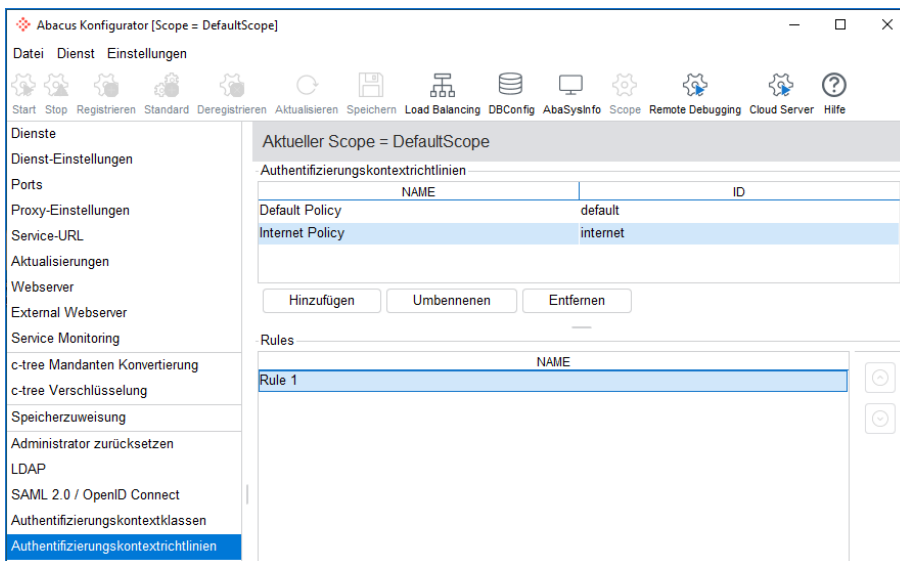
In diesen Arbeitsablauf wird von einer Standard Abacus Konfiguration ausgegangen. Es wird die Authentifizierungskontextrichtlinie "Internet Policy" verwendet.



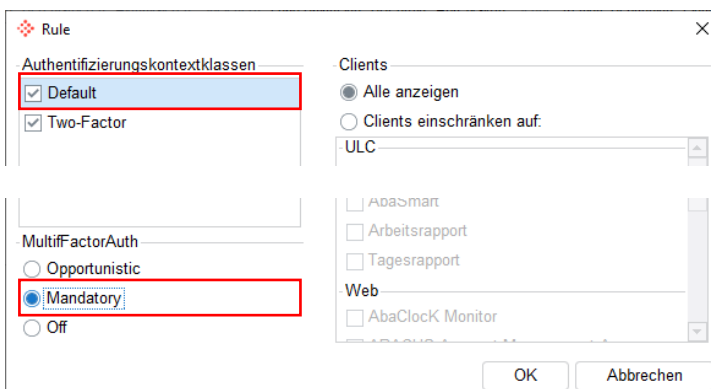
Arbeitsablauf SuisseID / Mobile ID Ablösen

1. Abacus Configurator – Abacus Access erzwingen & Benutzername/Passwort aktivieren

- Sektion "Authentifizierungskontextrichtlinien"
- Internet Policy
- Rule 1 editieren

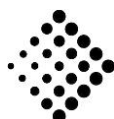


- MultiFactorAuth auf "Mandatory" (zwingend) stellen
- Zusätzlich, falls nicht bereits erfolgt, Authentifizierungskontextklasse "Default" auswählen. Hierdurch wird der Log-In mit Benutzername & Passwort aktiviert.



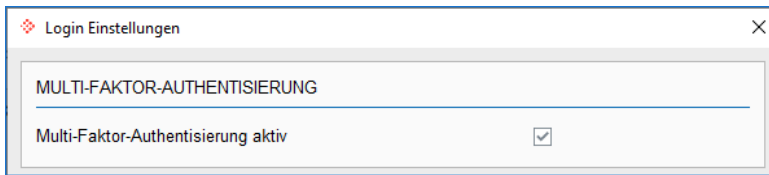
Hinweis

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

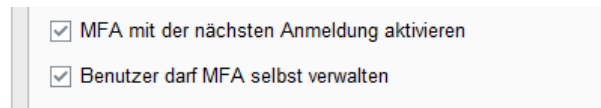


Achtung

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

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

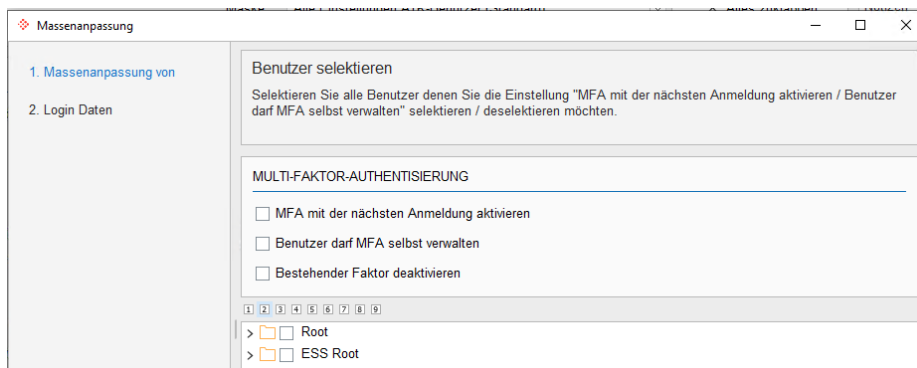
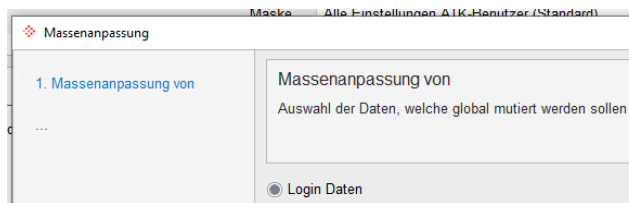
- "MFA mit der nächsten Anmeldung aktivieren" Flag setzen – Bewirkt, dass beim nächsten Log-In des entsprechenden Users die Aufforderung zur Registrierung (Onboarding) mit Abacus Access erfolgt.
- "Benutzer darf MFA selbst verwalten" Flag setzen



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

Massenanpassung

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



4. Benutzerverwaltung – "Nur mit ext. Authentisierung einloggen" entfernen

- Flag auf dem User entfernen, falls noch gesetzt

LOGIN DATEN

- Passwort mit der nächsten Anmeldung ändern
- Passwort nicht veränderbar
- Passwort läuft nicht ab
- Passwort zurücksetzen erlauben
- Nur mit externer Authentisierung einloggen
- Benutzer darf "angemeldet bleiben"

- 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

Masken: Alle Einstellungen AIK-Benutzer (Standard)

Massenanpassung

1. Massenanpassung von

...

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 "Nur mit externer Authentisierung einloggen" selektieren / deselektieren möchten.

NUR MIT EXTERNER AUTHENTISIERUNG EINLOGGEN

Nur mit externer Authentisierung einloggen

1 2 3 4 5 6 7 8 9

- Root
 - Administrator
 - kollers
 - Super1
- > ESS Root



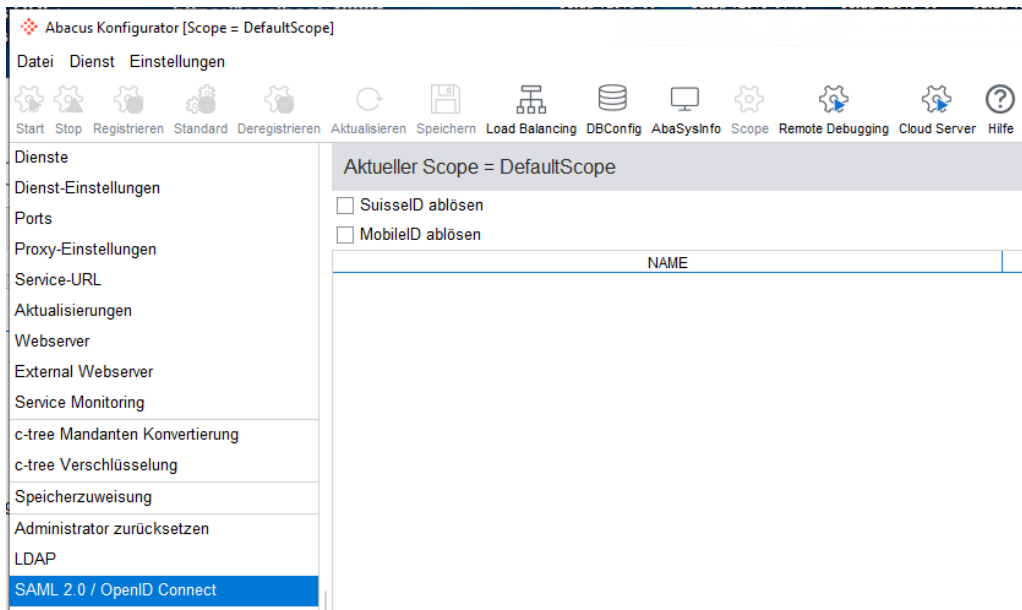
Hinweis

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

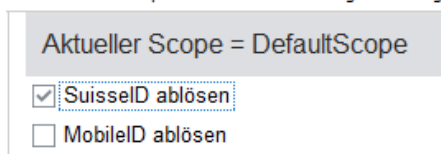


5. Abacus Configurator – SuisselD /Mobile ID ablösen aktivieren

- Sektion "SAML 2.0 / OpenID Connect"

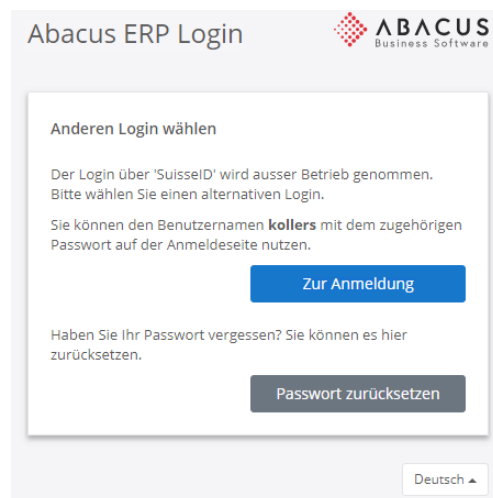


- Flag bei SuisselD und/oder MobileID setzen

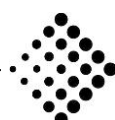


Hinweis

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).

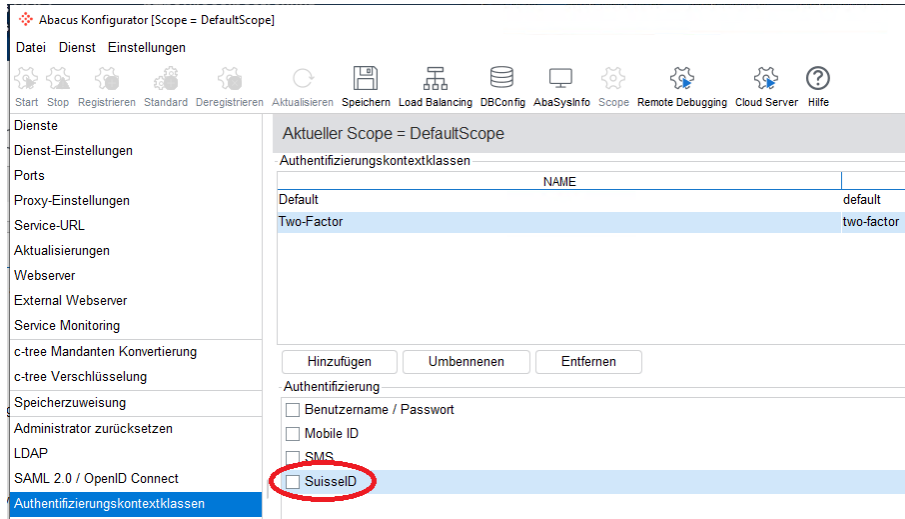


Ein Starten von Abacus ist nicht möglich.



6. Abacus Configurator – SuisseID /MobileID als Log-In Möglichkeit entfernen

- Sektion "Authentifizierungskontextklassen"
- Authentifizierungskontextklasse "Two-Factor" auswählen
- Flag/s bei SuisseID/MobileID entfernen



Abacus Konfigurator [Scope = DefaultScope]

Start Stop Registrieren Standard Deregistrieren Aktualisieren Speichern Load Balancing DBConfig AbaSysInfo Scope Remote Debugging Cloud Server Hilfe

Dienste

Dienst-Einstellungen

Ports

Proxy-Einstellungen

Service-URL

Aktualisierungen

Webserver

External Webserver

Service Monitoring

c-tree Mandanten Konvertierung

c-tree Verschlüsselung

Speicherzuweisung

Administrator zurücksetzen

LDAP

SAML 2.0 / OpenID Connect

Authentifizierungskontextklassen

Aktueller Scope = DefaultScope

Authentifizierungskontextklassen

NAME	
Default	default
Two-Factor	two-factor

Hinzufügen Umbenennen Entfernen

Authentifizierung

Benutzername / Passwort

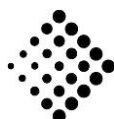
Mobile ID

SMS

SuisseID

**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)?

