

Create authentication flow with mandatory 2FA with OTP or WebAuthn #14988

✓ Answered by claudioweiler claudioweiler asked this question in Q&A



claudioweiler on Oct 19, 2022



















edited

Hi,

KeyCloak comes with default browser authentication flow with OTP 2FA Conditional flow configured (Forms - Auth-otp-form - Conditional). If this flow is changed to Required , then OTP will be mandatory, and user must configure one on login if he do not have one configured yet.

How to add an additional WebAuthn Authenticator execution as alternative to OTP, but continue with mandatory 2FA?

I tried to add WebAuthn Authenticator in same level of OTP, and changed both to "Alternative", this works since user has one of them configured, but to new users the authentication fails with log KC-SERVICE0013: Failed authentication: org.keycloak.authentication.AuthenticationFlowException .

Browser Com FIDO2				Novo Copiar Excluir Edit Flow Adicionar execução Adicionar fluxo			
Tipo		Condição					
 	Cookie			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Ações
 	Kerberos			<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED	Ações
 	Identity Provider Redirector			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Ações
 	Browser Forms			<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL Ações
	 	Username Password Form		<input checked="" type="radio"/> REQUIRED			Ações
	 	Browser 2FA		<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	<input type="radio"/> CONDITIONAL Ações
		 	Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED		Ações
		 	OTP Form	<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Ações
		 	WebAuthn Authenticator	<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED	Ações

I'm trying to understand the execution Condition - User Configured , I'm think that the gotcha lives there. But all test that I make fails miserably: or authentication fails, or OTP is always required without the link to use another method.

↑ 2 



Answered by claudioweiler on Oct 19, 2022

Hi!

I think I found a way to this. Added this flow below Username Password Form :

Require 2FA - required

[View full answer](#) ↓

6 comments · 15 replies

Oldest

Newest

Top



claudioweiler on Oct 19, 2022 Author

Hi!

I think I found a way to this. Added this flow below Username Password Form :

- Browser 2FA: required
- Authenticate: alternative
 - Condition - User Configured: required
 - OTP Form: alternative
 - WebAuthn Authentication: alternative
- Register: alternative
 - OTP Form: required



Some tests, looks OK.

If someone can points any problem with this, or have a better way, please share.

✓ Marked as answer ↑ 1 😊

10 replies

[Show 5 previous replies](#)



claudioweiler on Oct 31, 2022 Author

edited ▼

It looks good [@darius-m](#), thanks!

It's simpler.

If you post this flow as an answer, I will mark it as accepted.



ashish1099 on Mar 28, 2023

works absolutely fine.

Thanks for writing this down



dblas on Apr 5, 2023

Hello,

Well done.

What if the user forgot his mandatory OTP and would like to use the alternative one that is to say Webauthn?

In my case, kc 21.0.2, your solution doesn't work that way.

When selecting "another way" in the passwordless context, a panel pops up to present alternatives: password OR webauthn.

But, in the case where alternatives are OTP Form OR Webauthn it's always OTP form that shows up.

Curious, isn't it?

Is it a 21.0.2 bug or is there something missing in a *.ftl?

⋮	▼ Authenticate Authentication with whatever 2FA	Alternative	+	▼	✎	🗑
⋮	WebAuthn Authenticator	Alternative				🗑
⋮	OTP Form	Alternative				🗑
⋮	▼ Register Register with OTP	Alternative	+	▼	✎	🗑
⋮	OTP Form	Required				🗑

Thank you,

db



darius-m on Apr 6, 2023

Does the user have an OTP configured in their account, but not an WebAuthn token? If so, not having the option to select a different way to authenticate is the expected behavior, since in that case the second factor could be enforced (and would thus be expected). Being able to select WebAuthn as the alternative (for configuration) after the correct password is entered, without entering a valid OTP code, would be a security issue since 2FA would not be correctly enforced.

The reason why the flow I've mentioned before makes any sense is because for the first user login, they do not have any second factor configured, and allowing the user to login with a single factor is the only reasonable approach; however, after one of the second factors has been configured, using it becomes mandatory. The user can access their account console to configure alternative 2FA options at any point, if they are able to log in into their account.



claudioweiler on Apr 10, 2023 Author

Hi [@dblas](#)!

What if the user forgot his mandatory OTP and would like to use the alternative one that is to say Webauthn?

This flow is designed to work exactly this way. As [@darius-m](#) sad above, the user just had to have both 2FA methods configured, and select "another way", remembering that the main method can be changed by the user in his account page.

In my case, kc 21.0.2, your solution doesn't work that way.

When selecting "another way" in the passwordless context, a panel pops up to present alternatives: password OR webauthn.

...

Curious, isn't it?

Is it a 21.0.2 bug or is there something missing in a *.ftl?

Hum... I can't test this in KC 21.

But this flow isn't designed for **passwordless** authentication. Maybe I'm missing something here...

But, in the case where alternatives are OTP Form OR Webauthn it's always OTP form that shows up.

As explained above user must have both methods configured and the user can change the primary method on his account page (old keycloak theme, AFAIK on new keycloak.v2 theme this isn't possible).

If "another way" do not appears to the user, them is possible that the user do not have webauthn configured.



Write a reply

Answer selected by **claudioweiler**



jbman on Apr 5, 2023

I filed a similar question. The difference is, that both second factors should be enforced to be configured: [#19548](#)
Doesn't seem to be possible out-of-the-box.



1



4 replies



dblas on Apr 5, 2023

edited ▾

Someone seems to have done [it](#) but he doesn't remember (or doesn't want to remember) how he did it.
db



darius-m on Apr 6, 2023

Configuring additional 2FA options can be enforced (at least partially) through required actions. When the user logs in, they have to go through some operations, like configuring OTP / WebAuthn, agreeing to terms and conditions, etc.. If an action should be assigned to a user when they are first created, default required actions can be used, where the action is automatically assigned to new users.

Making sure that the user has both 2FA factors configured is, however, not achievable through default required actions alone (as these only apply to new users, so if the user logs in and then removes the 2FA option through their account console, the required actions is not re-assigned). If you need this, you can probably use an SPI (i.e., a plugin) to check if the 2FA options are configured whenever the user logs in.



jberman on Apr 6, 2023

Required actions work, if every user should be enforced to use 2FA. But in case of step-up authentication, a client decides that some operation needs 2FA. The second factor (or two of them - one for recovery) needs to be setup only for users who trigger this client operation.

I think the 2FA authenticators Webauthn, OTP Form and Recovery Codes should be configurable to enforce setup even if alternative in the flow.



darius-m on Apr 6, 2023

Yes, I also see the merit of having an option to enforce setting up multiple second factor methods. Maybe a simple checkbox in the flow interface, or the required actions tab, that checks the if the 2FA option is enabled at every login would suffice. However, I do not know how complex the implementation would be, since I would assume that the flow logic would have to check what 2FA methods there are, and how to not interfere with the other flows (i.e., allow the user to login using only their password if no 2FA option is available, but otherwise enforce 2FA). As far as I can tell, this is not an option out of the box, but it may be a good feature request.



Write a reply



dblas on Apr 5, 2023

Question was discussed, amongst other things, 4 years ago, [here](#).

Doesn't seem to have been implemented so far.

It's a pity,

db



1



1

0 replies

Write a reply



eggynap on Jul 6, 2023

This works nicely enough for me. I've configured OTP, WebAuthn, and Recovery Codes all as alternatives. I've required recovery code registration as a default required action in the realm, and in our case, administrators will need to assign OTP or WebAuthn as a required action for new users. This shouldn't be a problem in our case. Thanks for the ideas!



1



0 replies

Write a reply



PRD-1 on Apr 11

edited ▾

I want to develop a user authentication flow and need guidance on setting it up correctly. Currently, my process requires users to log in with a username and password, followed by a TAN (Transaction Authentication Number) sent to their email for further verification. I want to implement an optional feature where users can choose to register for a Web Authenticator instead of receiving a TAN. When a user opts for the Web Authenticator, the TAN verification step should automatically be skipped.

However, I'm encountering problems with the configuration:

When OTP and TAN are set as alternatives: The system fails to bypass the TAN step for users who are registered with the Web Authenticator, which it should ideally do. But it is also Bypassing the OTP step for registered Users with Web Authenticators.

When I set OTP as required and TAN as an alternative: If the user has neither method configured, the system either forces them to register upon login (which we want to avoid), or it fails to function correctly (i.e., does not authenticate them at all).

I need the Web Authenticator to be a voluntary, non-mandatory option that, when used, eliminates the need for TAN verification. How can I configure the system to:

Allow users to choose the Web Authenticator without making it mandatory?

Ensure that choosing the Web Authenticator bypasses the TAN step?

Avoid forcing users to register for any method as a prerequisite for login if they have not already set up an authentication method?



0 replies



andrewmeyer on Apr 11

the workflow I was trying to accomplish was to "prefer" webauthn over OTP for users that have both set up. the solution was to, as an admin, drag webauthn over OTP on the user's credential page - very unfortunate that this is not something the user can do, but I can probably count on one hand the number of users that would prefer this.



1 reply



claudioweiler on Apr 11 Author

If my memory isn't joking me, old v1 account console template had this. Maybe some great soul can help on guides to tweaking current template with a custom page or something like this.



Category

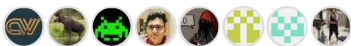


Q&A

Labels

None yet

8 participants



Events



claudioweiler Marked an Answer 2y