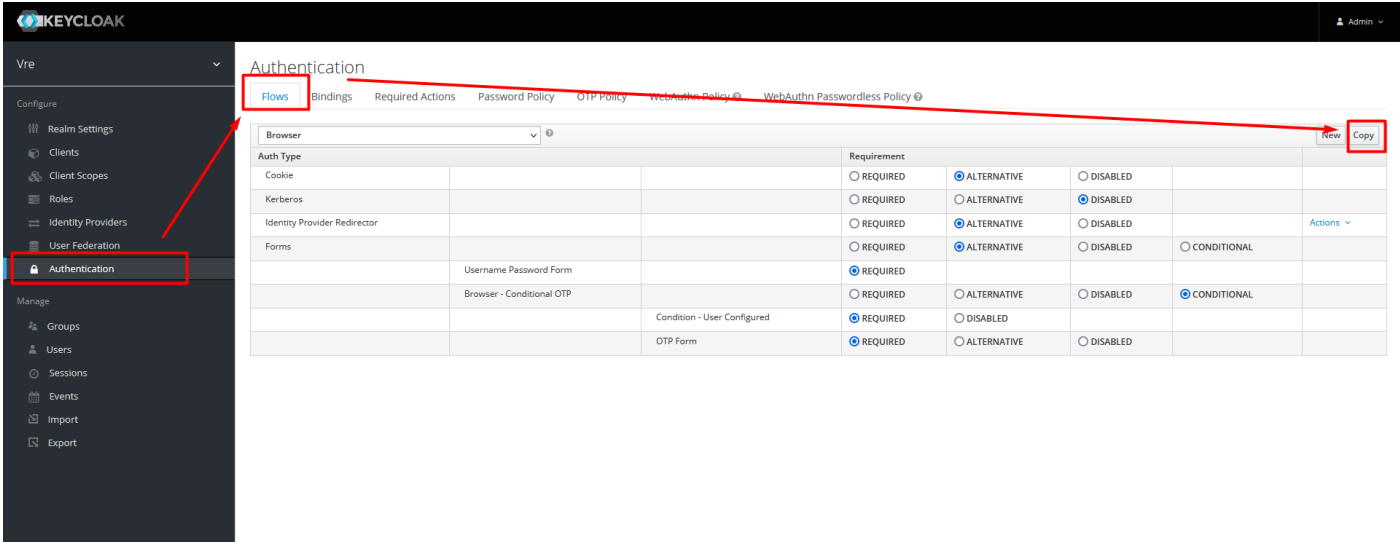# Overview:

This page is to document how to add the script into the workflow to do the customized authentication

Step:

1. The authentication flow will based on browser setup. So create a copy of the browser authentication flow and named as the `Browser with Attribute Enforcement`

2. In the forth row `Browser With Attribute Enforcement Forms`, select `Action -> Add execution` to add new authentication check.
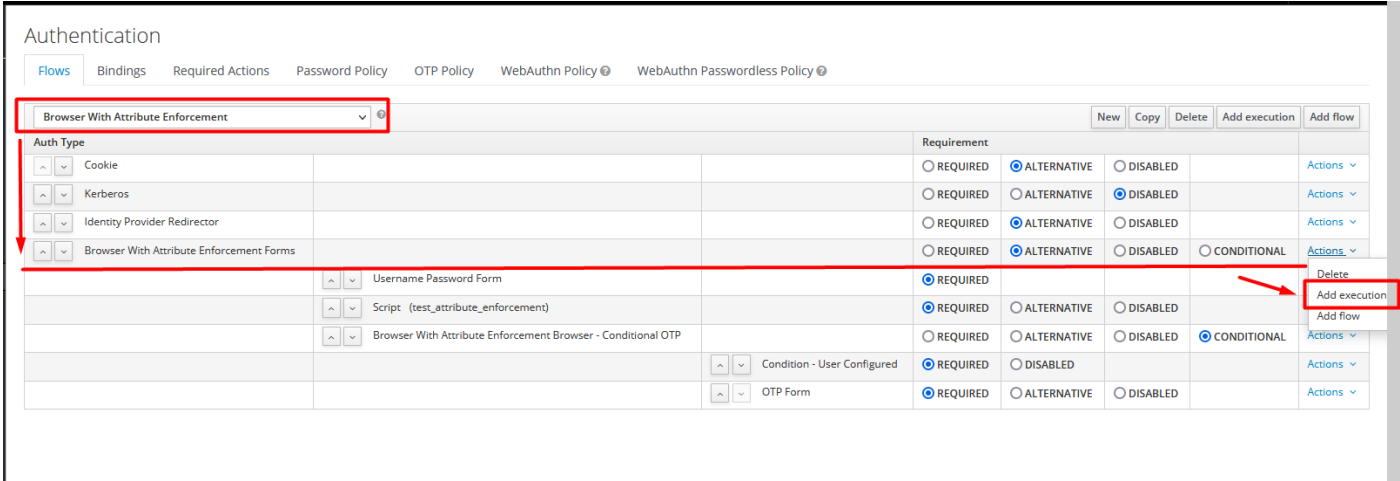
3. For the new execution, select script for customized logic

Create Authenticator Execution

Flows	Bindings	Required Actions	Password Policy	OTP Policy	WebAuthn Policy ❔	WebAuthn Passwordless Policy ❔

Provider ❔ Script ▾

```
OTP
OTP Form
Password
Password Form
Require Group
Reset OTP
Reset Password
Review Profile
Script
Send Reset Email
Username Form
Username Password Challenge
Username Password Form
Username Password Form For Identity Provider Reauthentication
Username Validation
Verify Existing Account By Email
WebAuthn Authenticator
WebAuthn Passwordless Authenticator
X509/Validate Username
X509/Validate Username Form
```

then move the script execution after validating the password

Authentication

Flows	Bindings	Required Actions	Password Policy	OTP Policy	WebAuthn Policy ❔	WebAuthn Passwordless Policy ❔	CIBA Policy

Browser With Attribute Enforcement ▾ ❔   New | Copy | Delete | Edit Flow | Add execution | Add flow

Auth Type			Requirement			
Cookie			◯ REQUIRED	⦿ ALTERNATIVE	◯ DISABLED		Actions ⌄
Kerberos			◯ REQUIRED	◯ ALTERNATIVE	⦿ DISABLED		Actions ⌄
Identity Provider Redirector			◯ REQUIRED	⦿ ALTERNATIVE	◯ DISABLED		Actions ⌄
Browser With Attribute Enforcement Forms ❔			◯ REQUIRED	⦿ ALTERNATIVE	◯ DISABLED	◯ CONDITIONAL	Actions ⌄
	Username Password Form		⦿ REQUIRED				Actions ⌄
	Script (test_attribute_enforcement)		⦿ REQUIRED	◯ ALTERNATIVE	◯ DISABLED		Actions ⌄
	Browser With Attribute Enforcement Browser - Conditional OTP ❔		◯ REQUIRED	◯ ALTERNATIVE	◯ DISABLED	⦿ CONDITIONAL	Actions ⌄
		Condition - User Configured	⦿ REQUIRED	◯ DISABLED			Actions ⌄
		OTP Form	⦿ REQUIRED	◯ ALTERNATIVE	◯ DISABLED		Actions ⌄

4. Following script is to check if user attribute has `status=disable`. If so, the user will be blocked to login. Note here with the script, the authentication can also check user group/roles.

```
/*
 * Template for JavaScript based authenticator's.
 * See
org.keycloak.authentication.authenticators.browser.ScriptBasedAuthenticatorFactory
 */

// import enum for error lookup
AuthenticationFlowError =
Java.type("org.keycloak.authentication.AuthenticationFlowError");

/**
 * An example authenticate function.
 *
 * The following variables are available for convenience:
 * user - current user {@see org.keycloak.models.UserModel}
 * realm - current realm {@see org.keycloak.models.RealmModel}
 * session - current KeycloakSession {@see org.keycloak.models.KeycloakSession}
 * httpRequest - current HttpRequest {@see org.jboss.resteasy.spi.HttpRequest}
 * script - current script {@see org.keycloak.models.ScriptModel}
```

```
 * authenticationSession - current authentication session {@see
org.keycloak.sessions.AuthenticationSessionModel}
 * LOG - current logger {@see org.jboss.logging.Logger}
 *
 * You one can extract current http request headers via:
 * httpRequest.getHttpHeaders().getHeaderString("Forwarded")
 *
 * @param context {@see org.keycloak.authentication.AuthenticationFlowContext}
 */
function authenticate(context) {

    var username = user ? user.username : "anonymous";
    // LOG.info(script.name + " trace auth for: " + username);

    var authShouldFail = false;

    // fetch the user attribute to see if user has `status=disable`
    var attributes = user.getAttributes()
    user.set
    for (var att in attributes){

        // block login
        if(att==="status" && attributes[att][0]==="disabled"){
            context.failure(AuthenticationFlowError.USER_DISABLED);
            return;
        }

    }

    context.success();
}
```

5. And remember to check the `REQUIRED` option

Authentication

Flows   Bindings   Required Actions   Password Policy   OTP Policy   WebAuthn Policy ❓   WebAuthn Passwordless Policy ❓

| Browser With Attribute Enforcement | | | | New | Copy | Delete | Add execution | Add flow |

Auth Type			Requirement				
Cookie			○ REQUIRED	● ALTERNATIVE	○ DISABLED		Actions ⌄
Kerberos			○ REQUIRED	○ ALTERNATIVE	● DISABLED		Actions ⌄
Identity Provider Redirector			○ REQUIRED	● ALTERNATIVE	○ DISABLED		Actions ⌄
Browser With Attribute Enforcement Forms			○ REQUIRED	● ALTERNATIVE	○ DISABLED	○ CONDITIONAL	Actions ⌄
	Username Password Form		● REQUIRED				Actions ⌄
	Script (test_attribute_enforcement)		● REQUIRED	○ ALTERNATIVE	○ DISABLED		Actions ⌄
	Browser With Attribute Enforcement Browser - Conditional OTP		○ REQUIRED	○ ALTERNATIVE	○ DISABLED	● CONDITIONAL	Actions ⌄
		Condition - User Configured	● REQUIRED	○ DISABLED			Actions ⌄
		OTP Form	● REQUIRED	○ ALTERNATIVE	○ DISABLED		Actions ⌄

6. Switching the tab to `Binds`, change the browser flow to what we create in step 1`Browser with Attribute Enforcement`.

New flow created in step 1