Property	Type	Default	Description
additionalRoles	String		Array of additional role names to add to the principal role when the user is authenticated via OIDC Provider. These roles are merged with any roles obtained from the ID Token (via *rolesClaim*) or from the UserInfo endpoint. Duplicate roles are not added twice. Example: *["ExtraRole1", "ExtraRole2"]*.
configUrl	String	-	URL for the OP configuration document. If not specified, the URL is automatically constructed from the issuer ID using the process defined in OpenID Connect Discovery. However, some non-standard OPs may have their configuration document at a different location. This property allows configuring such non-standard OPs.
issuerConfigFile	String	-	Path to the configuration file of the issuer, if the issuer config cannot be loaded from the */.well-known/openid-configuration* URL. This is only intended to be used for partial providers, where only the JWKS URL is available in the issuer config.
validIssPattern	Regex	-	A regex pattern to use to validate the *iss* claim in the ID Token. If unspecified, a valid *iss* ID Token claim must be exactly equal to the issuer value, which is the standard OpenID Connect specification behavior. The standard behavior can be overridden for non-standard IdP implementations using this configuration attribute. If specified, the regex is matched against the *entire iss* value (see *java.util.regex.Matcher.matches()* method).
pkceMethod	String	S256	The supported code challenge method. When enabled, the authenticator will use Proof Key for Code Exchange (PKCE) to protect the authorization code flow against authorization code interception attacks. It will generate a code verifier and a code challenge, and add the code challenge together with the method to the authorization request. When exchanging the authorization code for an access token, the authenticator will send the verifier and the OP will then verify the code challenge. If plain or S256 is specified, the value overrides the provider supported methods. If none is specified, PKCE is not used. If not specified, it defaults to the supported provider methods preferring the standard S256 method.
extraAuthEndpointParams	String	-	Extra parameters added to the query string of the OP's Authorization Endpoint URL. The value is an object with keys being the parameter names and value being the parameter values.
tokenEndpointAuthMethod	String	-	Explicitly specified authentication method for the OP's Token Endpoint. Normally the authenticator will use *client_secret_basic* if the OP configuration includes a client secret, and *none* if it does not. This property, however, allows overriding that logic and forcing a specific authentication method. For the description of the authentication methods see Client Authentication. Note that, currently, *client_secret_jwt* and *private_key_jwt* methods are not supported.
jwksUri	URL	-	URL for the JSON Web Key Set. If not specified, the URL will be read from */.well-known/openid-configuration* URL OpenID Connect Discovery. However, some non-standard OPs may have their configuration document at a different location. This property allows configuring such non-standard OPs.
endpointHttpConnectTimeout	Integer	5000	HTTP connection timeout (in milliseconds) for the OP endpoints.
endpointHttpReadTimeout	Integer	5000	HTTP read timeout (in milliseconds) for the OP endpoints.
configHttpConnectTimeout	Integer	5000	HTTP timeout (in milliseconds) for connecting to the OP configuration document URL (see configUrl property).
configHttpReadTimeout	Integer	5000	HTTP timeout (in milliseconds) for loading the OP configuration document (see configUrl property).
jwksHttpConnectTimeout	Integer	5000	HTTP timeout (in milliseconds) for connecting to the OP JWKS URL (see jwks_uri property in OpenID Provider Metadata).
jwksHttpReadTimeout	Integer	5000	HTTP timeout (in milliseconds) for loading the OP JWKS (see jwks_uri property in OpenID Provider Metadata).

disabled	boolean	false	If true, the OP is ignored and not loaded from the providers configuration file.
configRetryTimeout	Integer	10000	Time to wait (in milliseconds) before another attempt to configure a failed OP is made. It is only relevant if optional is set to true.
maxAge	Integer	-1	Allowable elapsed time (in seconds) since the user was last actively authenticated by the OP. If set to a value >= 0, it will be used as the authentication request parameter "max_age". A value of 0 means that the user must always be re-authenticated.
userInfoCheckEnabled	boolean	false	If true, the OpenID Connect UserInfo endpoint is called to update the user roles which are not already included in the ID Token.
defaultAdminKcIdpHint	String	-	Default value for the *kc_idp_hint* query parameter when logging in from admin pages using given Keycloak IdP and no *kc_idp_hint* parameter is present in the request. If not set, no default *kc_idp_hint* is applied.