Abstract

This guide consists of information for securing applications and services using Red Hat Single Sign-On 7.6
Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE ........................................... 6

CHAPTER 1. PLANNING FOR SECURING APPLICATIONS AND SERVICES ........................................... 7
1.1. CLIENT ADAPTERS .......................... 7
1.2. SUPPORTED PLATFORMS ......................... 7
   1.2.1. OpenID Connect .......................... 7
       1.2.1.1. Java ............................. 7
       1.2.1.2. JavaScript (client-side) ......... 7
       1.2.1.3. Node.js (server-side) ......... 7
   1.2.2. SAML ..................................... 7
       1.2.2.1. Java ............................. 7
       1.2.2.2. Apache HTTP Server ......... 7
1.3. SUPPORTED PROTOCOLS .......................... 8
   1.3.1. OpenID Connect .......................... 8
   1.3.2. SAML 2.0 ..................................... 8
   1.3.3. OpenID Connect vs. SAML ............... 8
1.4. TERMINOLOGY ................................. 9
1.5. BASIC STEPS TO SECURE APPLICATIONS AND SERVICES ........................................... 9

CHAPTER 2. USING OPENID CONNECT TO SECURE APPLICATIONS AND SERVICES ........................................... 11
2.1. JAVA ADAPTERS .......................... 11
   2.1.1. Java adapter configuration ....................... 11
   2.1.2. JBoss EAP adapter ......................... 15
   2.1.3. Installing JBOSS EAP adapters from a ZIP file ............. 16
       2.1.3.1. JBoss SSO .......................... 17
       2.1.3.2. Securing a WAR ..................... 17
       2.1.3.3. Securing WARs via adapter subsystem ............. 18
       2.1.3.4. Security domain ...................... 19
   2.1.4. Installing JBoss EAP 7 adapters from an RPM ............. 19
   2.1.5. Installing JBoss EAP 6 adapters from an RPM ............. 20
   2.1.6. Spring Boot adapter ......................... 21
       2.1.6.1. Installing the Spring Boot adapter ............. 21
       2.1.6.2. Configuring the Spring Boot Adapter ............. 22
   2.1.7. Java servlet filter adapter ....................... 23
   2.1.8. Security Context .......................... 24
   2.1.9. Error handling ............................. 24
   2.1.10. Logout ..................................... 25
   2.1.11. Parameters forwarding ....................... 25
   2.1.12. Client authentication ....................... 27
       2.1.12.1. Client ID and Client Secret ............. 27
       2.1.12.2. Client authentication with Signed JWT ............. 27
   2.1.13. Multi Tenancy ............................. 28
       2.1.14.1. Stateless token store ............. 29
       2.1.14.2. Relative URI optimization ............. 30
       2.1.14.3. Admin URL configuration ............. 30
       2.1.14.4. Registration of application nodes ............. 31
       2.1.14.5. Refresh token in each request ............. 31
   2.2. JAVASCRIPT ADAPTER .......................... 32
   2.2.1. Session Status iframe ....................... 35
   2.2.2. Implicit and hybrid flow ....................... 35
2.2.3. Hybrid Apps with Cordova
2.2.4. Custom Adapters
2.2.5. Earlier Browsers
2.2.6. Modern Browsers with Tracking Protection
  2.2.6.1. Browsers with "SameSite=Lax by Default" Policy
  2.2.6.2. Browsers with Blocked Third-Party Cookies
2.2.7. JavaScript Adapter Reference
  2.2.7.1. Constructor
  2.2.7.2. Properties
  2.2.7.3. Methods
  2.2.7.4. Callback Events
2.3. NODE.JS ADAPTER
  2.3.1. Installation
  2.3.2. Usage
  2.3.3. Installing middleware
  2.3.4. Configuration for proxies
  2.3.5. Checking authentication
  2.3.6. Protecting resources
  2.3.7. Additional URLs
  2.3.8. Complete example
2.4. OTHER OPENID CONNECT LIBRARIES
  2.4.1. Endpoints
    2.4.1.1. Authorization endpoint
    2.4.1.2. Token endpoint
    2.4.1.3. Userinfo endpoint
    2.4.1.4. Logout endpoint
    2.4.1.5. Certificate endpoint
    2.4.1.6. Introspection endpoint
    2.4.1.7. Dynamic Client Registration endpoint
    2.4.1.8. Token Revocation endpoint
    2.4.1.9. Device Authorization endpoint
    2.4.1.10. Backchannel Authentication endpoint
  2.4.2. Validating access tokens
  2.4.3. Flows
    2.4.3.1. Authorization code
    2.4.3.2. Implicit
    2.4.3.3. Resource Owner Password Credentials
      2.4.3.3.1. Example using CURL
    2.4.3.4. Client credentials
    2.4.3.5. Device Authorization Grant
    2.4.3.6. Client Initiated Backchannel Authentication Grant
  2.4.4. Redirect URIs
2.5. FINANCIAL-GRADE API (FAPI) SUPPORT
  2.5.1. FAPI client profiles
  2.5.2. Open Banking Brasil Financial-grade API Security Profile
  2.5.3. TLS considerations

CHAPTER 3. USING SAML TO SECURE APPLICATIONS AND SERVICES

3.1. JAVA ADAPTERS
  3.1.1. General Adapter Config
    3.1.1.1. SP element
    3.1.1.2. Service Provider keys and key elements
      3.1.1.2.1. KeyStore element

2
3.1.1. Key PEMS
3.1.1.3. SP PrincipalNameMapping element
3.1.1.4. RoleIdentifiers element
3.1.1.5. RoleMappingsProvider element
  3.1.1.5.1. Properties Based role mappings provider
  3.1.1.5.2. Adding your own role mappings provider
3.1.1.6. IDP Element
3.1.1.7. IDP AllowedClockSkew sub element
3.1.1.8. IDP SingleSignOnService sub element
3.1.1.9. IDP SingleLogoutService sub element
3.1.1.10. IDP Keys sub element
3.1.1.11. IDP HttpClient sub element
3.1.2. JBoss EAP adapter
3.1.3. Installing adapters from a ZIP file
  3.1.3.1. JBoss SSO
  3.1.3.2. Setting SameSite value for JSESSIONID cookie
3.1.4. Installing JBoss EAP 7 Adapters from an RPM
3.1.5. Installing JBoss EAP 6 Adapters from an RPM
  3.1.5.1. Securing a WAR
  3.1.5.2. Securing WARs using the Red Hat Single Sign-On SAML Subsystem
3.1.6. Java Servlet filter adapter
3.1.7. Registering with an Identity Provider
3.1.8. Logout
  3.1.8.1. Logout in clustered environment
  3.1.8.2. Logout in cross-site scenario
3.1.9. Obtaining assertion attributes
3.1.10. Error Handling
3.1.11. Troubleshooting
3.1.12. Multi Tenancy
3.2. MOD_AUTH_MELLON APACHE HTTPD MODULE
  3.2.1. Configuring mod_auth_mellon with Red Hat Single Sign-On
    3.2.1.1. Installing the packages
    3.2.1.2. Creating a configuration directory for Apache SAML
    3.2.1.3. Configuring the Mellon Service Provider
  3.2.2. Setting the SameSite value for the cookie used by mod_auth_mellon
    3.2.2.1. Creating the Service Provider metadata
    3.2.2.2. Adding the Mellon Service Provider to the Red Hat Single Sign-On Identity Provider
      3.2.2.2.1. Adding the Mellon Service Provider as a client of the realm
      3.2.2.2.2. Adding the Mellon SP client
      3.2.2.2.3. Editing the Mellon SP client
      3.2.2.2.4. Retrieving the Identity Provider metadata

CHAPTER 4. CONFIGURING A DOCKER REGISTRY TO USE RED HAT SINGLE SIGN-ON
  4.1. DOCKER REGISTRY CONFIGURATION FILE INSTALLATION
  4.2. DOCKER REGISTRY ENVIRONMENT VARIABLE OVERRIDE INSTALLATION
  4.3. DOCKER COMPOSE YAML FILE

CHAPTER 5. USING THE CLIENT REGISTRATION SERVICE
  5.1. AUTHENTICATION
    5.1.1. Bearer token
    5.1.2. Initial Access Token
    5.1.3. Registration Access Token
  5.2. RED HAT SINGLE SIGN-ON REPRESENTATIONS
MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright’s message.
CHAPTER 1. PLANNING FOR SECURING APPLICATIONS AND SERVICES

Red Hat Single Sign-On supports both OpenID Connect (an extension to OAuth 2.0) and SAML 2.0. When securing clients and services the first thing you need to decide is which of the two you are going to use. If you want you can also choose to secure some with OpenID Connect and others with SAML.

To secure clients and services you are also going to need an adapter or library for the protocol you’ve selected. Red Hat Single Sign-On comes with its own adapters for selected platforms, but it is also possible to use generic OpenID Connect Relying Party and SAML Service Provider libraries.

1.1. CLIENT ADAPTERS

Red Hat Single Sign-On client adapters are libraries that make it very easy to secure applications and services with Red Hat Single Sign-On. We call them adapters rather than libraries as they provide a tight integration to the underlying platform and framework. This makes our adapters easy to use and they require less boilerplate code than what is typically required by a library.

1.2. SUPPORTED PLATFORMS

Red Hat Single Sign-On enables you to protect applications running on different platforms and using different technology stacks using OpenID Connect and SAML protocols.

1.2.1. OpenID Connect

1.2.1.1. Java
- JBoss EAP
- Servlet Filter
- Spring Boot

1.2.1.2. JavaScript (client-side)
- JavaScript

1.2.1.3. Node.js (server-side)
- Node.js

1.2.2. SAML

1.2.2.1. Java
- JBoss EAP
- Servlet filter

1.2.2.2. Apache HTTP Server
- mod_auth_mellon
1.3. SUPPORTED PROTOCOLS

Red Hat Single Sign-On supports both OpenID Connect and SAML protocols.

1.3.1. OpenID Connect

OpenID Connect (OIDC) is an authentication protocol that is an extension of OAuth 2.0. While OAuth 2.0 is only a framework for building authorization protocols and is mainly incomplete, OIDC is a full-fledged authentication and authorization protocol. OIDC also makes heavy use of the Json Web Token (JWT) set of standards. These standards define an identity token JSON format and ways to digitally sign and encrypt that data in a compact and web-friendly way.

There are really two types of use cases when using OIDC. The first is an application that asks the Red Hat Single Sign-On server to authenticate a user for them. After a successful login, the application will receive an identity token and an access token. The identity token contains information about the user such as username, email, and other profile information. The access token is digitally signed by the realm and contains access information (like user role mappings) that the application can use to determine what resources the user is allowed to access on the application.

The second type of use cases is that of a client that wants to gain access to remote services. In this case, the client asks Red Hat Single Sign-On to obtain an access token it can use to invoke on other remote services on behalf of the user. Red Hat Single Sign-On authenticates the user then asks the user for consent to grant access to the client requesting it. The client then receives the access token. This access token is digitally signed by the realm. The client can make REST invocations on remote services using this access token. The REST service extracts the access token, verifies the signature of the token, then decides based on access information within the token whether or not to process the request.

1.3.2. SAML 2.0

SAML 2.0 is a similar specification to OIDC but a lot older and more mature. It has its roots in SOAP and the plethora of WS-* specifications so it tends to be a bit more verbose than OIDC. SAML 2.0 is primarily an authentication protocol that works by exchanging XML documents between the authentication server and the application. XML signatures and encryption are used to verify requests and responses.

In Red Hat Single Sign-On SAML serves two types of use cases: browser applications and REST invocations.

There are really two types of use cases when using SAML. The first is an application that asks the Red Hat Single Sign-On server to authenticate a user for them. After a successful login, the application will receive an XML document that contains something called a SAML assertion that specifies various attributes about the user. This XML document is digitally signed by the realm and contains access information (like user role mappings) that the application can use to determine what resources the user is allowed to access on the application.

The second type of use cases is that of a client that wants to gain access to remote services. In this case, the client asks Red Hat Single Sign-On to obtain a SAML assertion it can use to invoke on other remote services on behalf of the user.

1.3.3. OpenID Connect vs. SAML

Choosing between OpenID Connect and SAML is not just a matter of using a newer protocol (OIDC) instead of the older more mature protocol (SAML).

In most cases Red Hat Single Sign-On recommends using OIDC.
SAML tends to be a bit more verbose than OIDC.

Beyond verbosity of exchanged data, if you compare the specifications you’ll find that OIDC was designed to work with the web while SAML was retrofitted to work on top of the web. For example, OIDC is also more suited for HTML5/JavaScript applications because it is easier to implement on the client side than SAML. As tokens are in the JSON format, they are easier to consume by JavaScript. You will also find several nice features that make implementing security in your web applications easier. For example, check out the iframe trick that the specification uses to easily determine if a user is still logged in or not.

SAML has its uses though. As you see the OIDC specifications evolve you see they implement more and more features that SAML has had for years. What we often see is that people pick SAML over OIDC because of the perception that it is more mature and also because they already have existing applications that are secured with it.

1.4. TERMINOLOGY

These terms are used in this guide:

- **Clients** are entities that interact with Red Hat Single Sign-On to authenticate users and obtain tokens. Most often, clients are applications and services acting on behalf of users that provide a single sign-on experience to their users and access other services using the tokens issued by the server. Clients can also be entities only interested in obtaining tokens and acting on their own behalf for accessing other services.

- **Applications** include a wide range of applications that work for specific platforms for each protocol

- **Client adapters** are libraries that make it easy to secure applications and services with Red Hat Single Sign-On. They provide a tight integration to the underlying platform and framework.

- **Creating a client** and **registering a client** are the same action. **Creating a Client** is the term used to create a client by using the Admin Console. **Registering a client** is the term used to register a client by using the Red Hat Single Sign-On Client Registration Service.

- **A service account** is a type of client that is able to obtain tokens on its own behalf.

1.5. BASIC STEPS TO SECURE APPLICATIONS AND SERVICES

These are the basic steps for securing an application or a service in Red Hat Single Sign-On.

1. Configure a client using one of these options:
   - A Red Hat Single Sign-On adapter
   - A generic OpenID connect or SAML library

2. Register a client using one of these options:
   - The Red Hat Single Sign-On Admin Console
   - The client registration service
   - The CLI
This guide provides the detailed instructions for these steps. Related information exists in the Server Administration Guide. That guide provides instructions for using Admin Console to create a client. Creating a client is the same task as registering a client using the Red Hat Single Sign-On Client Registration Service.
CHAPTER 2. USING OPENID CONNECT TO SECURE APPLICATIONS AND SERVICES

This section describes how you can secure applications and services with OpenID Connect using either Red Hat Single Sign-On adapters or generic OpenID Connect Relying Party libraries.

2.1. JAVA ADAPTERS

Red Hat Single Sign-On comes with a range of different adapters for Java application. Selecting the correct adapter depends on the target platform.

All Java adapters share a set of common configuration options described in the Java Adapters Config chapter.

2.1.1. Java adapter configuration

Each Java adapter supported by Red Hat Single Sign-On can be configured by a simple JSON file. This is what one might look like:

```json
{
    "realm" : "demo",
    "resource" : "customer-portal",
    "realm-public-key" : "MIGfMA0GCSqGSIb3D...31LwIDAQAB",
    "auth-server-url" : "https://localhost:8443/auth",
    "ssl-required" : "external",
    "use-resource-role-mappings" : false,
    "enable-cors" : true,
    "cors-max-age" : 1000,
    "cors-allowed-methods" : "POST, PUT, DELETE, GET",
    "cors-exposed-headers" : "WWW-Authenticate, My-custom-exposed-Header",
    "bearer-only" : false,
    "enable-basic-auth" : false,
    "expose-token" : true,
    "verify-token-audience" : true,
    "credentials" : {
        "secret" : "234234-234234-234234"
    },
    "connection-pool-size" : 20,
    "socket-timeout-millis" : 5000,
    "connection-timeout-millis" : 6000,
    "connection-ttl-millis" : 500,
    "disable-trust-manager" : false,
    "allow-any-hostname" : false,
    "truststore" : "path/to/truststore.jks",
    "truststore-password" : "geheim",
    "client-keystore" : "path/to/client-keystore.jks",
    "client-keystore-password" : "geheim",
    "client-key-password" : "geheim",
    "token-minimum-time-to-live" : 10,
    "min-time-between-jwks-requests" : 10,
    "public-key-cache-ttl" : 86400,
    "redirect-rewrite-rules" : {
```
You can use ${...} enclosure for system property replacement. For example, \$\{jboss.server.config.dir\} would be replaced by /path/to/Red Hat Single Sign-On. Replacement of environment variables is also supported via the env prefix, for example \$\{env.MY_ENVIRONMENT_VARIABLE\}.

The initial config file can be obtained from the admin console. This can be done by opening the admin console, select Clients from the menu and clicking on the corresponding client. Once the page for the client is opened click on the Installation tab and select Keycloak OIDC JSON.

Here is a description of each configuration option:

### realm
Name of the realm. This is **REQUIRED**.

### resource
The client-id of the application. Each application has a client-id that is used to identify the application. This is **REQUIRED**.

### realm-public-key
PEM format of the realm public key. You can obtain this from the Admin Console. This is **OPTIONAL** and it’s not recommended to set it. If not set, the adapter will download this from Red Hat Single Sign-On and it will always re-download it when needed (eg. Red Hat Single Sign-On rotates its keys). However if realm-public-key is set, then adapter will never download new keys from Red Hat Single Sign-On, so when Red Hat Single Sign-On rotate it’s keys, adapter will break.

### auth-server-url
The base URL of the Red Hat Single Sign-On server. All other Red Hat Single Sign-On pages and REST service endpoints are derived from this. It is usually of the form https://host:port/auth. This is **REQUIRED**.

### ssl-required
Ensures that all communication to and from the Red Hat Single Sign-On server is over HTTPS. In production this should be set to all. This is **OPTIONAL**. The default value is external meaning that HTTPS is required by default for external requests. Valid values are 'all', 'external' and 'none'.

### confidential-port
The confidential port used by the Red Hat Single Sign-On server for secure connections over SSL/TLS. This is **OPTIONAL**. The default value is 8443.

### use-resource-role-mappings
If set to true, the adapter will look inside the token for application level role mappings for the user. If false, it will look at the realm level for user role mappings. This is **OPTIONAL**. The default value is false.

### public-client
If set to true, the adapter will not send credentials for the client to Red Hat Single Sign-On. This is **OPTIONAL**. The default value is false.

### enable-cors
This enables CORS support. It will handle CORS preflight requests. It will also look into the access token to determine valid origins. This is **OPTIONAL**. The default value is false.

### cors-max-age
If CORS is enabled, this sets the value of the Access-Control-Max-Age header. This is **OPTIONAL**. If not set, this header is not returned in CORS responses.
cors-allowed-methods
If CORS is enabled, this sets the value of the Access-Control-Allow-Methods header. This should be a comma-separated string. This is OPTIONAL. If not set, this header is not returned in CORS responses.

cors-allowed-headers
If CORS is enabled, this sets the value of the Access-Control-Allow-Headers header. This should be a comma-separated string. This is OPTIONAL. If not set, this header is not returned in CORS responses.

cors-exposed-headers
If CORS is enabled, this sets the value of the Access-Control-Expose-Headers header. This should be a comma-separated string. This is OPTIONAL. If not set, this header is not returned in CORS responses.

bearer-only
This should be set to true for services. If enabled the adapter will not attempt to authenticate users, but only verify bearer tokens. This is OPTIONAL. The default value is false.

autodetect-bearer-only
This should be set to true if your application serves both a web application and web services (for example SOAP or REST). It allows you to redirect unauthenticated users of the web application to the Red Hat Single Sign-On login page, but send an HTTP 401 status code to unauthenticated SOAP or REST clients instead as they would not understand a redirect to the login page. Red Hat Single Sign-On auto-detects SOAP or REST clients based on typical headers like X-Requested-With, SOAPAction or Accept. The default value is false.

enable-basic-auth
This tells the adapter to also support basic authentication. If this option is enabled, then secret must also be provided. This is OPTIONAL. The default value is false.

expose-token
If true, an authenticated browser client (via a JavaScript HTTP invocation) can obtain the signed access token via the URL root/k_query_bearer_token. This is OPTIONAL. The default value is false.

credentials
Specify the credentials of the application. This is an object notation where the key is the credential type and the value is the value of the credential type. Currently password and jwt is supported. This is REQUIRED only for clients with 'Confidential' access type.

connection-pool-size
This config option defines how many connections to the Red Hat Single Sign-On server should be pooled. This is OPTIONAL. The default value is 20.

socket-timeout-millis
Timeout for socket waiting for data after establishing the connection in milliseconds. Maximum time of inactivity between two data packets. A timeout value of zero is interpreted as an infinite timeout. A negative value is interpreted as undefined (system default if applicable). The default value is -1. This is OPTIONAL.

connection-timeout-millis
Timeout for establishing the connection with the remote host in milliseconds. A timeout value of zero is interpreted as an infinite timeout. A negative value is interpreted as undefined (system default if applicable). The default value is -1. This is OPTIONAL.

connection-ttl-millis
Connection time-to-live for client in milliseconds. A value less than or equal to zero is interpreted as an infinite value. The default value is -1. This is OPTIONAL.

disable-trust-manager
If the Red Hat Single Sign-On server requires HTTPS and this config option is set to true you do not have to specify a truststore. This setting should only be used during development and never in production as it will disable verification of SSL certificates. This is OPTIONAL. The default value is false.

allow-any-hostname

If the Red Hat Single Sign-On server requires HTTPS and this config option is set to true the Red Hat Single Sign-On server’s certificate is validated via the truststore, but host name validation is not done. This setting should only be used during development and never in production as it will disable verification of SSL certificates. This setting may be useful in test environments This is OPTIONAL. The default value is false.

proxy-url

The URL for the HTTP proxy if one is used.

truststore

The value is the file path to a truststore file. If you prefix the path with classpath:, then the truststore will be obtained from the deployment’s classpath instead. Used for outgoing HTTPS communications to the Red Hat Single Sign-On server. Client making HTTPS requests need a way to verify the host of the server they are talking to. This is what the trustore does. The keystore contains one or more trusted host certificates or certificate authorities. You can create this truststore by extracting the public certificate of the Red Hat Single Sign-On server’s SSL keystore. This is REQUIRED unless ssl-required is none or disable-trust-manager is true.

truststore-password

Password for the truststore. This is REQUIRED if truststore is set and the truststore requires a password.

client-keystore

This is the file path to a keystore file. This keystore contains client certificate for two-way SSL when the adapter makes HTTPS requests to the Red Hat Single Sign-On server. This is OPTIONAL.

client-keystore-password

Password for the client keystore. This is REQUIRED if client-keystore is set.

client-key-password

Password for the client’s key. This is REQUIRED if client-keystore is set.

always-refresh-token

If true, the adapter will refresh token in every request. Warning – when enabled this will result in a request to Red Hat Single Sign-On for every request to your application.

register-node-at-startup

If true, then adapter will send registration request to Red Hat Single Sign-On. It’s false by default and useful only when application is clustered. See Application Clustering for details

register-node-period

Period for re-registration adapter to Red Hat Single Sign-On. Useful when application is clustered. See Application Clustering for details

token-store

Possible values are session and cookie. Default is session, which means that adapter stores account info in HTTP Session. Alternative cookie means storage of info in cookie. See Application Clustering for details

token-cookie-path

When using a cookie store, this option sets the path of the cookie used to store account info. If it’s a relative path, then it is assumed that the application is running in a context root, and is interpreted relative to that context root. If it’s an absolute path, then the absolute path is used to set the cookie path. Defaults to use paths relative to the context root.
principal-attribute
OpenID Connect ID Token attribute to populate the UserPrincipal name with. If token attribute is null, defaults to sub. Possible values are sub, preferred_username, email, name, nickname, given_name, family_name.

turn-off-change-session-id-on-login
The session id is changed by default on a successful login on some platforms to plug a security attack vector. Change this to true if you want to turn this off. This is OPTIONAL. The default value is false.

token-minimum-time-to-live
Amount of time, in seconds, to preemptively refresh an active access token with the Red Hat Single Sign-On server before it expires. This is especially useful when the access token is sent to another REST client where it could expire before being evaluated. This value should never exceed the realm’s access token lifespan. This is OPTIONAL. The default value is 0 seconds, so adapter will refresh access token just if it’s expired.

min-time-between-jwks-requests
Amount of time, in seconds, specifying minimum interval between two requests to Red Hat Single Sign-On to retrieve new public keys. It is 10 seconds by default. Adapter will always try to download new public key when it recognize token with unknown kid. However it won’t try it more than once per 10 seconds (by default). This is to avoid DoS when attacker sends lots of tokens with bad kid forcing adapter to send lots of requests to Red Hat Single Sign-On.

public-key-cache-ttl
Amount of time, in seconds, specifying maximum interval between two requests to Red Hat Single Sign-On to retrieve new public keys. It is 86400 seconds (1 day) by default. Adapter will always try to download new public key when it recognize token with unknown kid. If it recognize token with known kid, it will just use the public key downloaded previously. However at least once per this configured interval (1 day by default) will be new public key always downloaded even if the kid of token is already known.

ignore-oauth-query-parameter
Defaults to false, if set to true will turn off processing of the access_token query parameter for bearer token processing. Users will not be able to authenticate if they only pass in an access_token

redirect-rewrite-rules
If needed, specify the Redirect URI rewrite rule. This is an object notation where the key is the regular expression to which the Redirect URI is to be matched and the value is the replacement String. $ character can be used for backreferences in the replacement String.

verify-token-audience
If set to true, then during authentication with the bearer token, the adapter will verify whether the token contains this client name (resource) as an audience. The option is especially useful for services, which primarily serve requests authenticated by the bearer token. This is set to false by default, however for improved security, it is recommended to enable this. See Audience Support for more details about audience support.

2.1.2. JBoss EAP adapter
You can install this adapter from a ZIP file or from an RPM.

- Installing JBOSS EAP adapters from a ZIP file
- Installing JBoss EAP 7 Adapters from an RPM
- Installing JBoss EAP 6 Adapters from an RPM
2.1.3. Installing JBOSS EAP adapters from a ZIP file

To be able to secure WAR apps deployed on JBoss EAP, you must install and configure the Red Hat Single Sign-On adapter subsystem. You then have two options to secure your WARs.

- You can provide an adapter config file in your WAR and change the auth-method to KEYCLOAK within web.xml.

- Alternatively, you do not have to modify your WAR at all and you can secure it via the Red Hat Single Sign-On adapter subsystem configuration in the configuration file, such as standalone.xml.

Both methods are described in this section.

Adapters are available as a separate archive depending on what server version you are using.

Procedure

1. Install the adapter that applies to your application server from the Software Downloads site.
   
   • Install on JBoss EAP 7:
     
     $ cd $EAP_HOME
     $ unzip rh-sso-7.6.5-eap7-adapter.zip

     This ZIP archive contains JBoss Modules specific to the Red Hat Single Sign-On adapter. It also contains JBoss CLI scripts to configure the adapter subsystem.

2. To configure the adapter subsystem, execute the appropriate command.

   • Install on JBoss EAP 7.1 or newer if the server is not running.
     
     $ ./bin/jboss-cli.sh --file=bin/adapter-elytron-install-offline.cli

     NOTE
     
     The offline script is not available for JBoss EAP 6.4

   • Install on JBoss EAP 7.1 or newer if the server is running.
     
     $ ./bin/jboss-cli.sh -c --file=bin/adapter-elytron-install.cli

     NOTE
     
     It is possible to use the legacy non-Elytron adapter on JBoss EAP 7.1 or newer as well, meaning you can use adapter-install-offline.cli
NOTE

EAP supports OpenJDK 17 and Oracle JDK 17 since 7.4.CP7 and 7.4.CP8 respectively. Note that the new java version makes the elytron variant compulsory, so do not use the legacy adapter with JDK 17. Also, after running the adapter CLI file, execute the `enable-elytron-se17.cli` script provided by EAP. Both scripts are necessary to configure the elytron adapter and remove the incompatible EAP subsystems. For more details, see this Security Configuration Changes article.

- Install on JBoss EAP 6.4

  
  ```
  $ ./bin/jboss-cli.sh -c --file=bin/adapter-install.cli
  ```

2.1.3.1. JBoss SSO

JBoss EAP has built-in support for single sign-on for web applications deployed to the same JBoss EAP instance. This should not be enabled when using Red Hat Single Sign-On.

2.1.3.2. Securing a WAR

This section describes how to secure a WAR directly by adding configuration and editing files within your WAR package.

Procedure

1. Create a `keycloak.json` adapter configuration file within the `WEB-INF` directory of your WAR. The format of this configuration file is described in the Java adapter configuration section.

2. Set the `auth-method` to `KEYCLOAK` in `web.xml`.

3. Use standard servlet security to specify role-base constraints on your URLs. Here’s an example:

   ```xml
   <web-app xmlns="http://java.sun.com/xml/ns/javaee"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
                               http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd"
            version="3.0">

   <module-name>application</module-name>

   <security-constraint>
   <web-resource-collection>
    <web-resource-name>Admins</web-resource-name>
    <url-pattern>/admin/*</url-pattern>
   </web-resource-collection>
   <auth-constraint>
    <role-name>admin</role-name>
   </auth-constraint>
   <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
   </user-data-constraint>
   </security-constraint>

   </web-app>
   ```
2.1.3.3. Securing WARs via adapter subsystem

You do not have to modify your WAR to secure it with Red Hat Single Sign-On. Instead you can externally secure it via the Red Hat Single Sign-On Adapter Subsystem. While you don’t have to specify KEYCLOAK as an auth-method, you still have to define the security-constraints in web.xml. You do not, however, have to create a WEB-INF/keycloak.json file. The metadata is instead defined within server configuration (standalone.xml) in the Red Hat Single Sign-On subsystem definition.

```xml
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Customers</web-resource-name>
    <url-pattern>/customers/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>user</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>

<login-config>
  <auth-method>KEYCLOAK</auth-method>
  <realm-name>this is ignored currently</realm-name>
</login-config>

<security-role>
  <role-name>admin</role-name>
</security-role>
<security-role>
  <role-name>user</role-name>
</security-role>

<web-app>
  <extensions>
    <extension module="org.keycloak.keycloak-adapter-subsystem"/>
  </extensions>
</web-app>
```

The secure-deployment name attribute identifies the WAR you want to secure. Its value is the module-name defined in web.xml with .war appended. The rest of the configuration corresponds pretty much one to one with the keycloak.json configuration options defined in Java adapter configuration.

The exception is the credential element.
To make it easier for you, you can go to the Red Hat Single Sign-On Admin Console and go to the Client/Installation tab of the application this WAR is aligned with. It provides an example XML file you can cut and paste.

If you have multiple deployments secured by the same realm you can share the realm configuration in a separate element. For example:

```xml
<subsystem xmlns="urn:jboss:domain:keycloak:1.1">
  <realm name="demo">
    <auth-server-url>http://localhost:8080/auth</auth-server-url>
    <ssl-required>external</ssl-required>
  </realm>
  <secure-deployment name="customer-portal.war">
    <realm>demo</realm>
    <resource>customer-portal</resource>
    <credential name="secret">password</credential>
  </secure-deployment>
  <secure-deployment name="product-portal.war">
    <realm>demo</realm>
    <resource>product-portal</resource>
    <credential name="secret">password</credential>
  </secure-deployment>
  <secure-deployment name="database.war">
    <realm>demo</realm>
    <resource>database-service</resource>
    <bearer-only>true</bearer-only>
  </secure-deployment>
</subsystem>
```

2.1.3.4. Security domain

The security context is propagated to the EJB tier automatically.

2.1.4. Installing JBoss EAP 7 adapters from an RPM

**NOTE**

With Red Hat Enterprise Linux 7, the term channel was replaced with the term repository. In these instructions only the term repository is used.

**Prerequisites**

You must subscribe to the JBoss EAP 7.4 repository before you can install the JBoss EAP 7 adapters from an RPM.

- Ensure that your Red Hat Enterprise Linux system is registered to your account using Red Hat Subscription Manager. For more information see the Red Hat Subscription Management documentation.

- If you are already subscribed to another JBoss EAP repository, you must unsubscribe from that repository first.

  For Red Hat Enterprise Linux 6, 7: Using Red Hat Subscription Manager, subscribe to the JBoss EAP 7.4 repository using the following command. Replace `<RHEL_VERSION>` with either 6 or 7 depending on your Red Hat Enterprise Linux version.
$ sudo subscription-manager repos --enable=jb-eap-7-for-rhel-<RHEL_VERSION>-server-rpms

For Red Hat Enterprise Linux 8: Using Red Hat Subscription Manager, subscribe to the JBoss EAP 7.4 repository using the following command:

$ sudo subscription-manager repos --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms --enable=rhel-8-for-x86_64-baseos-rpms --enable=rhel-8-for-x86_64-appstream-rpms

Procedure

1. Install the JBoss EAP 7 adapters for OIDC based on your version of Red Hat Enterprise Linux.
   
   • Install on Red Hat Enterprise Linux 6, 7:
     
     $ sudo yum install eap7-keycloak-adapter-sso7_6
   
   • Install on Red Hat Enterprise Linux 8:
     
     $ sudo dnf install eap7-keycloak-adapter-sso7_6

   **NOTE**
   
   The default EAP_HOME path for the RPM installation is /opt/rh/eap7/root/usr/share/wildfly.

2. Run the installation script for the OIDC module.

   $ $EAP_HOME/bin/jboss-cli.sh -c --file=$EAP_HOME/bin/adapter-install.cli

Your installation is complete.

2.1.5. Installing JBoss EAP 6 adapters from an RPM

   **NOTE**
   
   With Red Hat Enterprise Linux 7, the term channel was replaced with the term repository. In these instructions only the term repository is used.

   You must subscribe to the JBoss EAP 6 repository before you can install the EAP 6 adapters from an RPM.

Prerequisites

- Ensure that your Red Hat Enterprise Linux system is registered to your account using Red Hat Subscription Manager. For more information see the Red Hat Subscription Management documentation.

- If you are already subscribed to another JBoss EAP repository, you must unsubscribe from that repository first.
Using Red Hat Subscription Manager, subscribe to the JBoss EAP 6 repository using the following command. Replace `<RHEL_VERSION>` with either 6 or 7 depending on your Red Hat Enterprise Linux version.

```
$ sudo subscription-manager repos --enable=jb-eap-6-for-rhel-<RHEL_VERSION>-server-rpms
```

**Procedure**

1. Install the EAP 6 adapters for OIDC using the following command:

```
$ sudo yum install keycloak-adapter-sso7_6-eap6
```

**NOTE**

The default EAP_HOME path for the RPM installation is 

2. Run the installation script for the OIDC module.

```
$ $EAP_HOME/bin/jboss-cli.sh -c --file=$EAP_HOME/bin/adapter-install.cli
```

Your installation is complete.

### 2.1.6. Spring Boot adapter

**NOTE**

The Spring Boot Adapter is deprecated and will not be included in the 8.0 and higher versions of RH-SSO. This adapter will be maintained during the lifecycle of RH-SSO 7.x. Users are urged to migrate to Spring Security to integrate their Spring Boot applications with RH-SSO.

#### 2.1.6.1. Installing the Spring Boot adapter

To be able to secure Spring Boot apps you must add the Keycloak Spring Boot adapter JAR to your app. You then have to provide some extra configuration via normal Spring Boot configuration (`application.properties`).

The Keycloak Spring Boot adapter takes advantage of Spring Boot’s autoconfiguration so all you need to do is add this adapter Keycloak Spring Boot starter to your project.

**Procedure**

1. To add the starter to your project using Maven, add the following to your dependencies:

```xml
<dependency>
  <groupId>org.keycloak</groupId>
  <artifactId>keycloak-spring-boot-starter</artifactId>
</dependency>
```

2. Add the Adapter BOM dependency:
Currently the following embedded containers are supported and do not require any extra dependencies if using the Starter:

- Tomcat
- Undertow
- Jetty

### 2.1.6.2. Configuring the Spring Boot Adapter

Use the procedure to configure your Spring Boot app to use Red Hat Single Sign-On.

**Procedure**

1. Instead of a `keycloak.json` file, you configure the realm for the Spring Boot adapter via the normal Spring Boot configuration. For example:

```xml
<dependencyManagement>
  <dependencies>
    <dependency>
      <groupId>org.keycloak.bom</groupId>
      <artifactId>keycloak-adapter-bom</artifactId>
      <version>18.0.9.redhat-00001</version>
      <type>pom</type>
      <scope>import</scope>
    </dependency>
  </dependencies>
</dependencyManagement>
```

You can disable the Keycloak Spring Boot Adapter (for example in tests) by setting `keycloak.enabled = false`.

2. To configure a Policy Enforcer, unlike `keycloak.json`, use `policy-enforcer-config` instead of just `policy-enforcer`.

3. Specify the Jakarta EE security config that would normally go in the `web.xml`.

   The Spring Boot Adapter will set the `login-method` to `KEYCLOAK` and configure the `security-constraints` at startup time. Here’s an example configuration:

```xml
keycloak.securityConstraints[0].authRoles[0] = admin
keycloak.securityConstraints[0].authRoles[1] = user
keycloak.securityConstraints[0].securityCollections[0].name = insecure stuff
keycloak.securityConstraints[0].securityCollections[0].patterns[0] = /insecure

keycloak.securityConstraints[1].authRoles[0] = admin
keycloak.securityConstraints[1].securityCollections[0].name = admin stuff
keycloak.securityConstraints[1].securityCollections[0].patterns[0] = /admin
```
2.1.7. Java servlet filter adapter

If you are deploying your Java Servlet application on a platform where there is no Red Hat Single Sign-On adapter you opt to use the servlet filter adapter. This adapter works a bit differently than the other adapters. You do not define security constraints in web.xml. Instead you define a filter mapping using the Red Hat Single Sign-On servlet filter adapter to secure the url patterns you want to secure.

WARNING

Backchannel logout works a bit differently than the standard adapters. Instead of invalidating the HTTP session it marks the session id as logged out. There's no standard way to invalidate an HTTP session based on a session id.

```xml
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="3.0">
  <module-name>application</module-name>

  <filter>
    <filter-name>Keycloak Filter</filter-name>
    <filter-class>org.keycloak.adapters.servlet.KeycloakOIDCFilter</filter-class>
  </filter>

  <filter-mapping>
    <filter-name>Keycloak Filter</filter-name>
    <url-pattern>/keycloak/*</url-pattern>
    <url-pattern>/protected/*</url-pattern>
  </filter-mapping>
</web-app>
```

In the snippet above there are two url-patterns. /protected/* are the files we want protected, while the /keycloak/* url-pattern handles callbacks from the Red Hat Single Sign-On server.

If you need to exclude some paths beneath the configured url-patterns you can use the Filter init-param keycloak.config.skipPattern to configure a regular expression that describes a path-pattern for which the keycloak filter should immediately delegate to the filter-chain. By default no skipPattern is
Patterns are matched against the requestURI without the context-path. Given the context-path /myapp a request for /myapp/index.html will be matched with /index.html against the skip pattern.

```xml
<init-param>
  <param-name>keycloak.config.skipPattern</param-name>
  <param-value>^/(path1|path2|path3).*</param-value>
</init-param>
```

Note that you should configure your client in the Red Hat Single Sign-On Admin Console with an Admin URL that points to a secured section covered by the filter’s url-pattern.

The Admin URL will make callbacks to the Admin URL to do things like backchannel logout. So, the Admin URL in this example should be `http[s]://hostname/{context-root}/keycloak`.

If you need to customize the session ID mapper, you can configure the fully qualified name of the class in the Filter init-param keycloak.config.idMapper. Session ID mapper is a mapper that is used to map user IDs and session IDs. By default org.keycloak.adapters.spi.InMemorySessionIdMapper is configured.

```xml
<init-param>
  <param-name>keycloak.config.idMapper</param-name>
  <param-value>org.keycloak.adapters.spi.InMemorySessionIdMapper</param-value>
</init-param>
```

The Red Hat Single Sign-On filter has the same configuration parameters as the other adapters except you must define them as filter init params instead of context params.

To use this filter, include this maven artifact in your WAR poms:

```xml
<dependency>
  <groupId>org.keycloak</groupId>
  <artifactId>keycloak-servlet-filter-adapter</artifactId>
  <version>18.0.9.redhat-00001</version>
</dependency>
```

### 2.1.8. Security Context

The KeycloakSecurityContext interface is available if you need to access to the tokens directly. This could be useful if you want to retrieve additional details from the token (such as user profile information) or you want to invoke a RESTful service that is protected by Red Hat Single Sign-On.

In servlet environments it is available in secured invocations as an attribute in HttpServletRequest:

```java
httpServletRequest.getAttribute(KeycloakSecurityContext.class.getName());
```

Or, it is available in insecure requests in the HttpSession:

```java
httpServletRequest.getSession().getAttribute(KeycloakSecurityContext.class.getName());
```

### 2.1.9. Error handling
Red Hat Single Sign-On has some error handling facilities for servlet based client adapters. When an error is encountered in authentication, Red Hat Single Sign-On will call `HttpServletResponse.sendError()`. You can set up an error-page within your `web.xml` file to handle the error however you want. Red Hat Single Sign-On can throw 400, 401, 403, and 500 errors.

```xml
<error-page>
  <error-code>403</error-code>
  <location>/ErrorHandler</location>
</error-page>
```

Red Hat Single Sign-On also sets a `HttpServletRequest` attribute that you can retrieve. The attribute name is `org.keycloak.adapters.spi.AuthenticationError`, which should be casted to `org.keycloak.adapters.OIDCAuthenticationError`.

For example:

```java
import org.keycloak.adapters.OIDCAuthenticationError;
import org.keycloak.adapters.OIDCAuthenticationError.Reason;
...
OIDCAuthenticationError error = (OIDCAuthenticationError) httpServletRequest.getAttribute("org.keycloak.adapters.spi.AuthenticationError");
Reason reason = error.getReason();
System.out.println(reason.name());
```

### 2.1.10. Logout

You can log out of a web application in multiple ways. For Jakarta EE servlet containers, you can call `HttpServletRequest.logout()`. For other browser applications, you can redirect the browser to `http://auth-server/auth realms/{realm-name}/protocol/openid-connect/logout`, which logs the user out if that user has an SSO session with his browser. The actual logout is done once the user confirms the logout. You can optionally include parameters such as `id_token_hint`, `post_logout_redirect_uri`, `client_id` and others as described in the OpenID Connect RP-Initiated Logout. As a result, that logout does not need to be explicitly confirmed by the user if you include the `id_token_hint` parameter. After logout, the user will be automatically redirected to the specified `post_logout_redirect_uri` as long as it is provided. Note that you need to include either the `client_id` or `id_token_hint` parameter in case that `post_logout_redirect_uri` is included.

If you want to avoid logging out of an external identity provider as part of the logout process, you can supply the parameter `initiating_idp`, with the value being the identity (alias) of the identity provider in question. This parameter is useful when the logout endpoint is invoked as part of single logout initiated by the external identity provider. The parameter `initiating_idp` is the supported parameter of the Red Hat Single Sign-On logout endpoint in addition to the parameters described in the RP-Initiated Logout specification.

When using the `HttpServletRequest.logout()` option the adapter executes a back-channel POST call against the Red Hat Single Sign-On server passing the refresh token. If the method is executed from an unprotected page (a page that does not check for a valid token) the refresh token can be unavailable and, in that case, the adapter skips the call. For this reason, using a protected page to execute `HttpServletRequest.logout()` is recommended so that current tokens are always taken into account and an interaction with the Red Hat Single Sign-On server is performed if needed.

### 2.1.11. Parameters forwarding
The Red Hat Single Sign-On initial authorization endpoint request has support for various parameters. Most of the parameters are described in the [OIDC specification](#). Some parameters are added automatically by the adapter based on the adapter configuration. However, there are also a few parameters that can be added on a per-invocation basis. When you open the secured application URI, the particular parameter will be forwarded to the Red Hat Single Sign-On authorization endpoint.

For example, if you request an offline token, then you can open the secured application URI with the `scope` parameter like:

```plaintext
http://myappserver/mysecuredapp?scope=offline_access
```

and the parameter `scope=offline_access` will be automatically forwarded to the Red Hat Single Sign-On authorization endpoint.

The supported parameters are:

- **scope** - Use a space-delimited list of scopes. A space-delimited list typically references Client scopes defined on particular client. Note that the scope `openid` will be always added to the list of scopes by the adapter. For example, if you enter the scope options `address phone`, then the request to Red Hat Single Sign-On will contain the scope parameter `scope=openid address phone`.

- **prompt** - Red Hat Single Sign-On supports these settings:
  - `login` - SSO will be ignored and the Red Hat Single Sign-On login page will be always shown, even if the user is already authenticated.
  - `consent` - Applicable only for the clients with Consent Required. If it is used, the Consent page will always be displayed, even if the user previously granted consent to this client.
  - `none` - The login page will never be shown; instead the user will be redirected to the application, with an error if the user is not yet authenticated. This setting allows you to create a filter/interceptor on the application side and show a custom error page to the user. See more details in the specification.

- **max_age** - Used only if a user is already authenticated. Specifies maximum permitted time for the authentication to persist, measured from when the user authenticated. If user is authenticated longer than `maxAge`, the SSO is ignored and he must re-authenticate.

- **login_hint** - Used to pre-fill the username/email field on the login form.

- **kc_idp_hint** - Used to tell Red Hat Single Sign-On to skip showing login page and automatically redirect to specified identity provider instead. More info in the [Identity Provider documentation](#).

Most of the parameters are described in the [OIDC specification](#). The only exception is parameter `kc_idp_hint`, which is specific to Red Hat Single Sign-On and contains the name of the identity provider to automatically use. For more information see the [Identity Brokering](#) section in the Server Administration Guide.
2.1.12. Client authentication

When a confidential OIDC client needs to send a backchannel request (for example, to exchange code for the token, or to refresh the token) it needs to authenticate against the Red Hat Single Sign-On server. By default, there are three ways to authenticate the client: client ID and client secret, client authentication with signed JWT, or client authentication with signed JWT using client secret.

2.1.12.1. Client ID and Client Secret

This is the traditional method described in the OAuth2 specification. The client has a secret, which needs to be known to both the adapter (application) and the Red Hat Single Sign-On server. You can generate the secret for a particular client in the Red Hat Single Sign-On Admin Console, and then paste this secret into the `keycloak.json` file on the application side:

```json
"credentials": {
  "secret": "19666a4f-32dd-4049-b082-684c74115f28"
}
```

2.1.12.2. Client authentication with Signed JWT

This is based on the RFC7523 specification. It works this way:

- The client must have the private key and certificate. For Red Hat Single Sign-On this is available through the traditional `keystore` file, which is either available on the client application’s classpath or somewhere on the file system.

- Once the client application is started, it allows to download its public key in JWKS format using a URL such as `http://myhost.com/myapp/k_jwks`, assuming that `http://myhost.com/myapp` is the base URL of your client application. This URL can be used by Red Hat Single Sign-On (see below).

- During authentication, the client generates a JWT token and signs it with its private key and sends it to Red Hat Single Sign-On in the particular backchannel request (for example, code-to-token request) in the `client_assertion` parameter.

- Red Hat Single Sign-On must have the public key or certificate of the client so that it can verify the signature on JWT. In Red Hat Single Sign-On you need to configure client credentials for your client. First you need to choose Signed JWT as the method of authenticating your client in the tab Credentials in the Admin Console. Then you can choose to either in the tab Keys:

  - Configure the JWKS URL where Red Hat Single Sign-On can download the client’s public keys. This can be a URL such as `http://myhost.com/myapp/k_jwks` (see details above). This
option is the most flexible, since the client can rotate its keys anytime and Red Hat Single Sign-On then always downloads new keys when needed without needing to change the configuration. More accurately, Red Hat Single Sign-On downloads new keys when it sees the token signed by an unknown kid (Key ID).

- Upload the client’s public key or certificate, either in PEM format, in JWK format, or from the keystore. With this option, the public key is hardcoded and must be changed when the client generates a new key pair. You can even generate your own keystore from the Red Hat Single Sign-On Admin Console if you don’t have your own available. For more details on how to set up the Red Hat Single Sign-On Admin Console, see the Server Administration Guide.

For set up on the adapter side you need to have something like this in your keycloak.json file:

```json
"credentials": {
  "jwt": {
    "client-keystore-file": "classpath:keystore-client.jks",
    "client-keystore-type": "JKS",
    "client-keystore-password": "storepass",
    "client-key-password": "keypass",
    "client-key-alias": "clientkey",
    "algorithm": "RS256",
    "token-expiration": 10
  }
}
```

With this configuration, the keystore file keystore-client.jks must be available on classpath in your WAR. If you do not use the prefix classpath: you can point to any file on the file system where the client application is running.

The algorithm field specifies the algorithm used for the Signed JWT and it defaults to RS256. This field should be in sync with the key pair. For example, the RS256 algorithm needs a RSA key pair while the ES256 algorithm requires an EC key pair. Please refer to Cryptographic Algorithms for Digital Signatures and MACs for more information.

### 2.1.13. Multi Tenancy

Multi Tenancy, in our context, means that a single target application (WAR) can be secured with multiple Red Hat Single Sign-On realms. The realms can be located on the same Red Hat Single Sign-On instance or on different instances.

In practice, this means that the application needs to have multiple keycloak.json adapter configuration files.

You could have multiple instances of your WAR with different adapter configuration files deployed to different context-paths. However, this may be inconvenient and you may also want to select the realm based on something else than context-path.

Red Hat Single Sign-On makes it possible to have a custom config resolver so you can choose what adapter config is used for each request.

To achieve this first you need to create an implementation of org.keycloak.adapters.KeycloakConfigResolver. For example:

```java
package example;
```
import org.keycloak.adapters.KeycloakConfigResolver;
import org.keycloak.adapters.KeycloakDeployment;
import org.keycloak.adapters.KeycloakDeploymentBuilder;

public class PathBasedKeycloakConfigResolver implements KeycloakConfigResolver {

    @Override
    public KeycloakDeployment resolve(OIDCHttpFacade.Request request) {
        if (path.startsWith("alternative")) {
            KeycloakDeployment deployment = cache.get(realm);
            if (null == deployment) {
                InputStream is = getClass().getResourceAsStream("/tenant1-keycloak.json");
                return KeycloakDeploymentBuilder.build(is);
            }
        } else {
            InputStream is = getClass().getResourceAsStream("/default-keycloak.json");
            return KeycloakDeploymentBuilder.build(is);
        }
    }
}

You also need to configure which KeycloakConfigResolver implementation to use with the
keycloak.config.resolver context-param in your web.xml:

```xml
<web-app>
    ...
    <context-param>
        <param-name>keycloak.config.resolver</param-name>
        <param-value>example.PathBasedKeycloakConfigResolver</param-value>
    </context-param>
<web-app>
```

2.14. Application clustering

This chapter is related to supporting clustered applications deployed to JBoss EAP.

There are a few options available depending on whether your application is:

- Stateless or stateful
- Distributable (replicated http session) or non-distributable
- Relying on sticky sessions provided by load balancer
- Hosted on same domain as Red Hat Single Sign-On

Dealing with clustering is not quite as simple as for a regular application. Mainly due to the fact that both
the browser and the server-side application sends requests to Red Hat Single Sign-On, so it’s not as
simple as enabling sticky sessions on your load balancer.

2.14.1. Stateless token store
By default, the web application secured by Red Hat Single Sign-On uses the HTTP session to store security context. This means that you either have to enable sticky sessions or replicate the HTTP session.

As an alternative to storing the security context in the HTTP session the adapter can be configured to store this in a cookie instead. This is useful if you want to make your application stateless or if you don’t want to store the security context in the HTTP session.

To use the cookie store for saving the security context, edit your applications `WEB-INF/keycloak.json` and add:

```
"token-store": "cookie"
```

**NOTE**

The default value for `token-store` is `session`, which stores the security context in the HTTP session.

One limitation of using the cookie store is that the whole security context is passed in the cookie for every HTTP request. This may impact performance.

Another small limitation is limited support for Single-Sign Out. It works without issues if you init servlet logout (HttpServletRequest.logout) from the application itself as the adapter will delete the KEYCLOAK_ADAPTER_STATE cookie. However, back-channel logout initialized from a different application isn’t propagated by Red Hat Single Sign-On to applications using cookie store. Hence it’s recommended to use a short value for the access token timeout (for example 1 minute).

**NOTE**

Some load balancers do not allow any configuration of the sticky session cookie name or contents, such as Amazon ALB. For these, it is recommended to set the `shouldAttachRoute` option to `false`.

### 2.1.14.2. Relative URI optimization

In deployment scenarios where Red Hat Single Sign-On and the application is hosted on the same domain (through a reverse proxy or load balancer) it can be convenient to use relative URI options in your client configuration.

With relative URIs the URI is resolved as relative to the URL used to access Red Hat Single Sign-On.

For example if the URL to your application is `https://acme.org/myapp` and the URL to Red Hat Single Sign-On is `https://acme.org/auth`, then you can use the redirect-uri `/myapp` instead of `https://acme.org/myapp`.

### 2.1.14.3. Admin URL configuration

Admin URL for a particular client can be configured in the Red Hat Single Sign-On Admin Console. It’s used by the Red Hat Single Sign-On server to send backend requests to the application for various tasks, like logout users or push revocation policies.

For example the way backchannel logout works is:

1. User sends logout request from one application
2. The application sends logout request to Red Hat Single Sign-On
3. The Red Hat Single Sign-On server invalidates the user session
4. The Red Hat Single Sign-On server then sends a backchannel request to application with an
admin url that are associated with the session
5. When an application receives the logout request it invalidates the corresponding HTTP session

If admin URL contains $\text{application.session.host}$ it will be replaced with the URL to the node
associated with the HTTP session.

### 2.1.14.4. Registration of application nodes

The previous section describes how Red Hat Single Sign-On can send logout request to node associated
with a specific HTTP session. However, in some cases admin may want to propagate admin tasks to all
registered cluster nodes, not just one of them. For example to push a new not before policy to the
application or to logout all users from the application.

In this case Red Hat Single Sign-On needs to be aware of all application cluster nodes, so it can send the
event to all of them. To achieve this, we support auto-discovery mechanism:

1. When a new application node joins the cluster, it sends a registration request to the Red Hat
   Single Sign-On server
2. The request may be re-sent to Red Hat Single Sign-On in configured periodic intervals
3. If the Red Hat Single Sign-On server doesn’t receive a re-registration request within a specified
timeout then it automatically unregisters the specific node
4. The node is also unregistered in Red Hat Single Sign-On when it sends an unregistration
   request, which is usually during node shutdown or application undeployment. This may not work
   properly for forced shutdown when undeployment listeners are not invoked, which results in the
   need for automatic unregistration

Sending startup registrations and periodic re-registration is disabled by default as it’s only required for
some clustered applications.

To enable the feature edit the WEB-INF/keycloak.json file for your application and add:

```
"register-node-at-startup": true,
"register-node-period": 600,
```

This means the adapter will send the registration request on startup and re-register every 10 minutes.

In the Red Hat Single Sign-On Admin Console you can specify the maximum node re-registration
timeout (should be larger than register-node-period from the adapter configuration). You can also
manually add and remove cluster nodes in through the Admin Console, which is useful if you don’t want
to rely on the automatic registration feature or if you want to remove stale application nodes in the
event your not using the automatic unregistration feature.

### 2.1.14.5. Refresh token in each request

By default the application adapter will only refresh the access token when it’s expired. However, you can
also configure the adapter to refresh the token on every request. This may have a performance impact
as your application will send more requests to the Red Hat Single Sign-On server.
To enable the feature edit the \texttt{WEB-INF/keycloak.json} file for your application and add:

\begin{verbatim}
"always-refresh-token": true
\end{verbatim}

\textbf{NOTE}

This may have a significant impact on performance. Only enable this feature if you can’t rely on backchannel messages to propagate logout and not before policies. Another thing to consider is that by default access tokens has a short expiration so even if logout is not propagated the token will expire within minutes of the logout.

\section*{2.2. JAVASCRIPT ADAPTER}

Red Hat Single Sign-On comes with a client-side JavaScript library that can be used to secure HTML5/JavaScript applications. The JavaScript adapter has built-in support for Cordova applications.

A good practice is to include the JavaScript adapter in your application using a package manager like NPM or Yarn. The \texttt{keycloak-js} package is available on the following locations:

- NPM: \url{https://www.npmjs.com/package/keycloak-js}
- Yarn: \url{https://yarnpkg.com/package/keycloak-js}

Alternatively, the library can be retrieved directly from the Red Hat Single Sign-On server at \url{/auth/js/keycloak.js} and is also distributed as a ZIP archive.

One important thing to note about using client-side applications is that the client has to be a public client as there is no secure way to store client credentials in a client-side application. This makes it very important to make sure the redirect URIs you have configured for the client are correct and as specific as possible.

To use the JavaScript adapter you must first create a client for your application in the Red Hat Single Sign-On Admin Console. Make sure \texttt{public} is selected for \texttt{Access Type}. You achieve this in Capability config by turning OFF client authentication toggle.

You also need to configure \texttt{Valid Redirect URIs} and \texttt{Web Origins}. Be as specific as possible as failing to do so may result in a security vulnerability.

Once the client is created click on the \texttt{Action} tab in the upper right corner and select \texttt{Download adapter config}. Select \texttt{Keycloak OIDC JSON} for \texttt{Format Option} then click \texttt{Download}. The downloaded \texttt{keycloak.json} file should be hosted on your web server at the same location as your HTML pages.

Alternatively, you can skip the configuration file and manually configure the adapter.

The following example shows how to initialize the JavaScript adapter:

\begin{verbatim}
<html>
<head>
  <script src="keycloak.js"></script>
</head>
<body>
  <script>
    function initKeycloak() {
      const options = {};
      const keycloak = new Keycloak();
      keycloak.init(options)
  
</script>
</body>
</html>
\end{verbatim}
If the `keycloak.json` file is in a different location you can specify it:

```javascript
const keycloak = new Keycloak('http://localhost:8080/myapp/keycloak.json');
```

Alternatively, you can pass in a JavaScript object with the required configuration instead:

```javascript
const keycloak = new Keycloak({
  url: 'http://keycloak-server$/auth',
  realm: 'myrealm',
  clientId: 'myapp'
});
```

By default to authenticate you need to call the `login` function. However, there are two options available to make the adapter automatically authenticate. You can pass `login-required` or `check-sso` to the `init` function. `login-required` will authenticate the client if the user is logged-in to Red Hat Single Sign-On or display the login page if not. `check-sso` will only authenticate the client if the user is already logged-in, if the user is not logged-in the browser will be redirected back to the application and remain unauthenticated.

You can configure a `silent check-sso` option. With this feature enabled, your browser won’t do a full redirect to the Red Hat Single Sign-On server and back to your application, but this action will be performed in a hidden iframe, so your application resources only need to be loaded and parsed once by the browser when the app is initialized and not again after the redirect back from Red Hat Single Sign-On to your app. This is particularly useful in case of SPAs (Single Page Applications).

To enable the `silent check-sso`, you have to provide a `silentCheckSsoRedirectUri` attribute in the `init` method. This URI needs to be a valid endpoint in the application (and of course it must be configured as a valid redirect for the client in the Red Hat Single Sign-On Admin Console):

```javascript
keycloak.init({
  onLoad: 'check-sso',
  silentCheckSsoRedirectUri: window.location.origin + '/silent-check-sso.html'
})
```

The page at the silent check-sso redirect uri is loaded in the iframe after successfully checking your authentication state and retrieving the tokens from the Red Hat Single Sign-On server. It has no other task than sending the received tokens to the main application and should only look like this:

```html
<html>
<body onload="initKeycloak()">
<!-- your page content goes here -->
</body>
</html>
```
WARNING

Silent check-sso functionality is limited in some modern browsers. Please see the Modern Browsers with Tracking Protection Section.

To enable login-required set onLoad to login-required and pass to the init method:

```javascript
keycloak.init({
    onLoad: 'login-required'
})
```

After the user is authenticated the application can make requests to RESTful services secured by Red Hat Single Sign-On by including the bearer token in the Authorization header. For example:

```javascript
const loadData = function () {
    const url = 'http://localhost:8080/restful-service';

    const req = new XMLHttpRequest();
    req.open('GET', url, true);
    req.setRequestHeader('Accept', 'application/json');
    req.setRequestHeader('Authorization', 'Bearer ' + keycloak.token);

    req.onreadystatechange = function () {
        if (req.readyState == 4) {
            if (req.status == 200) {
                alert('Success');
            } else if (req.status == 403) {
                alert('Forbidden');
            }
        }
    }

    req.send();
};
```

One thing to keep in mind is that the access token by default has a short life expiration so you may need to refresh the access token prior to sending the request. You can do this by the updateToken method. The updateToken method returns a promise which makes it easy to invoke the service only if the token was successfully refreshed and display an error to the user if it wasn’t. For example:

```javascript
parent.postMessage(location.href, location.origin)
```
2.2.1. Session Status iframe

By default, the JavaScript adapter creates a hidden iframe that is used to detect if a Single-Sign Out has occurred. This does not require any network traffic, instead the status is retrieved by looking at a special status cookie. This feature can be disabled by setting `checkLoginIframe: false` in the options passed to the `init` method.

You should not rely on looking at this cookie directly. Its format can change and it's also associated with the URL of the Red Hat Single Sign-On server, not your application.

```
keycloak.updateToken(30).then(function() {
    loadData();
}).catch(function() {
    alert('Failed to refresh token');
});
```

2.2.2. Implicit and hybrid flow

By default, the JavaScript adapter uses the Authorization Code flow.

With this flow the Red Hat Single Sign-On server returns an authorization code, not an authentication token, to the application. The JavaScript adapter exchanges the code for an access token and a refresh token after the browser is redirected back to the application.

Red Hat Single Sign-On also supports the Implicit flow where an access token is sent immediately after successful authentication with Red Hat Single Sign-On. This may have better performance than standard flow, as there is no additional request to exchange the code for tokens, but it has implications when the access token expires.

However, sending the access token in the URL fragment can be a security vulnerability. For example the token could be leaked through web server logs and or browser history.

To enable implicit flow, you need to enable the Implicit Flow Enabled flag for the client in the Red Hat Single Sign-On Admin Console. You also need to pass the parameter `flow` with value `implicit` to `init` method:

```
keycloak.init({
    flow: 'implicit'
})
```

One thing to note is that only an access token is provided and there is no refresh token. This means that once the access token has expired the application has to do the redirect to the Red Hat Single Sign-On again to obtain a new access token.

Red Hat Single Sign-On also supports the Hybrid flow.
This requires the client to have both the **Standard Flow Enabled** and **Implicit Flow Enabled** flags enabled in the admin console. The Red Hat Single Sign-On server will then send both the code and tokens to your application. The access token can be used immediately while the code can be exchanged for access and refresh tokens. Similar to the implicit flow, the hybrid flow is good for performance because the access token is available immediately. But, the token is still sent in the URL, and the security vulnerability mentioned earlier may still apply.

One advantage in the Hybrid flow is that the refresh token is made available to the application.

For the Hybrid flow, you need to pass the parameter `flow` with value `hybrid` to the `init` method:

```javascript
keycloak.init({
  flow: 'hybrid'
})
```

### 2.2.3. Hybrid Apps with Cordova

Keycloak support hybrid mobile apps developed with **Apache Cordova**. The JavaScript adapter has two modes for this: **cordova** and **cordova-native**:

The default is cordova, which the adapter will automatically select if no adapter type has been configured and `window.cordova` is present. When logging in, it will open an InApp Browser that lets the user interact with Red Hat Single Sign-On and afterwards returns to the app by redirecting to `http://localhost`. Because of this, you must whitelist this URL as a valid redirect-uri in the client configuration section of the Admin Console.

While this mode is easy to set up, it also has some disadvantages:

- The InApp-Browser is a browser embedded in the app and is not the phone’s default browser. Therefore it will have different settings and stored credentials will not be available.
- The InApp-Browser might also be slower, especially when rendering more complex themes.
- There are security concerns to consider, before using this mode, such as that it is possible for the app to gain access to the credentials of the user, as it has full control of the browser rendering the login page, so do not allow its use in apps you do not trust.

Use this example app to help you get started:

https://github.com/keycloak/keycloak/tree/master/examples/cordova

The alternative mode **cordova-native** takes a different approach. It opens the login page using the system’s browser. After the user has authenticated, the browser redirects back into the app using a special URL. From there, the Red Hat Single Sign-On adapter can finish the login by reading the code or token from the URL.

You can activate the native mode by passing the adapter type **cordova-native** to the `init` method:

```javascript
keycloak.init({
  adapter: 'cordova-native'
})
```

This adapter required two additional plugins:

- **cordova-plugin-browsertab**: allows the app to open webpages in the system’s browser
- **cordova-plugin-deeplinks**: allow the browser to redirect back to your app by special URLs
The technical details for linking to an app differ on each platform and special setup is needed. Please refer to the Android and iOS sections of the deeplinks plugin documentation for further instructions.

There are different kinds of links for opening apps: custom schemes (i.e. myapp://login or android-app://com.example.myapp/https/example.com/login) and Universal Links (iOS) / Deep Links (Android). While the former are easier to set up and tend to work more reliably, the later offer extra security as they are unique and only the owner of a domain can register them. Custom-URLs are deprecated on iOS. We recommend that you use universal links, combined with a fallback site with a custom-url link on it for best reliability.

Furthermore, we recommend the following steps to improve compatibility with the Keycloak Adapter:

- Universal Links on iOS seem to work more reliably with response-mode set to query
- To prevent Android from opening a new instance of your app on redirect add the following snippet to config.xml:

```xml
<preference name="AndroidLaunchMode" value="singleTask"/>
```

There is an example app that shows how to use the native-mode: https://github.com/keycloak/keycloak/tree/master/examples/cordova-native

### 2.2.4. Custom Adapters

Sometimes it’s necessary to run the JavaScript client in environments that are not supported by default (such as Capacitor). To make it possible to use the JavaScript client in these kind of unknown environments is possible to pass a custom adapter. For example a 3rd party library could provide such an adapter to make it possible to run the JavaScript client without issues:

```javascript
import Keycloak from 'keycloak-js';
import KeycloakCapacitorAdapter from 'keycloak-capacitor-adapter';

const keycloak = new Keycloak();
keycloak.init({
  adapter: KeycloakCapacitorAdapter,
});
```

This specific package does not exist, but it gives a pretty good example of how such an adapter could be passed into the client.

It’s also possible to make your own adapter, to do so you will have to implement the methods described in the KeycloakAdapter interface. For example the following TypeScript code ensures that all the methods are properly implemented:

```typescript
import Keycloak, { KeycloakAdapter } from 'keycloak-js';

// Implement the 'KeycloakAdapter' interface so that all required methods are guaranteed to be present.
const MyCustomAdapter: KeycloakAdapter = {
  login(options) {
    // Write your own implementation here.
  }

  // The other methods go here...
```
Naturally you can also do this without TypeScript by omitting the type information, but ensuring implementing the interface properly will then be left entirely up to you.

2.2.5. Earlier Browsers

The JavaScript adapter depends on Base64 (window.btoa and window.atob), HTML5 History API and optionally the Promise API. If you need to support browsers that do not have these available (for example, IE9) you need to add polyfillers.

Example polyfill libraries:

- Base64 - https://github.com/davidchambers/Base64.js
- HTML5 History - https://github.com/devote/HTML5-History-API
- Promise - https://github.com/stefanpenner/es6-promise

2.2.6. Modern Browsers with Tracking Protection

In the latest versions of some browsers various cookies policies are applied to prevent tracking of the users by third-parties, like SameSite in Chrome or completely blocked third-party cookies. It is expected that those policies will become even more restrictive and adopted by other browsers over time, eventually leading to cookies in third-party contexts to be completely unsupported and blocked by the browsers. The adapter features affected by this might get deprecated in the future.

Javascript adapter relies on third-party cookies for Session Status iframe, silent check-sso and partially also for regular (non-silent) check-sso. Those features have limited functionality or are completely disabled based on how the browser is restrictive regarding cookies. The adapter tries to detect this setting and reacts accordingly.

2.2.6.1. Browsers with “SameSite=Lax by Default” Policy

All features are supported if SSL / TLS connection is configured on the Red Hat Single Sign-On side as well as on the application side. Affected is for example Chrome starting with version 84.

2.2.6.2. Browsers with Blocked Third-Party Cookies

Session Status iframe is not supported and is automatically disabled if such browser behavior is detected by the JS adapter. This means the adapter cannot use session cookie for Single Sign-Out detection and have to rely purely on tokens. This implies that when user logs out in another window, the application using JavaScript adapter won’t be logged out until it tries to refresh the Access Token. Therefore, it is recommended to set Access Token Lifespan to relatively short time, so that the logout is detected rather sooner than later. Please see Session and Token Timeouts.

Silent check-sso is not supported and falls back to regular (non-silent) check-sso by default. This behaviour can be changed by setting silentCheckSsoFallback: false in the options passed to the init method. In this case, check-sso will be completely disabled if restrictive browser behavior is detected.
Regular check-sso is affected as well. Since Session Status iframe is unsupported, an additional redirect to Red Hat Single Sign-On has to be made when the adapter is initialized to check user’s login status. This is different from standard behavior when the iframe is used to tell whether the user is logged in, and the redirect is performed only when logged out.

An affected browser is for example Safari starting with version 13.1.

### 2.2.7. JavaScript Adapter Reference

#### 2.2.7.1. Constructor

```javascript
new Keycloak();
new Keycloak('http://localhost/keycloak.json');
```

#### 2.2.7.2. Properties

- **authenticated**
  - Is `true` if the user is authenticated, `false` otherwise.

- **token**
  - The base64 encoded token that can be sent in the `Authorization` header in requests to services.

- **tokenParsed**
  - The parsed token as a JavaScript object.

- **subject**
  - The user id.

- **idToken**
  - The base64 encoded ID token.

- **idTokenParsed**
  - The parsed id token as a JavaScript object.

- **realmAccess**
  - The realm roles associated with the token.

- **resourceAccess**
  - The resource roles associated with the token.

- **refreshToken**
  - The base64 encoded refresh token that can be used to retrieve a new token.

- **refreshTokenParsed**
  - The parsed refresh token as a JavaScript object.

- **timeSkew**
  - The estimated time difference between the browser time and the Red Hat Single Sign-On server in seconds. This value is just an estimation, but is accurate enough when determining if a token is expired or not.

- **responseMode**
  - Response mode passed in init (default value is fragment).

- **flow**
  - Flow passed in init.
adapter

 Allows you to override the way that redirects and other browser-related functions will be handled by the library. Available options:

- "default" - the library uses the browser api for redirects (this is the default)
- "cordova" - the library will try to use the InAppBrowser cordova plugin to load keycloak login/registration pages (this is used automatically when the library is working in a cordova ecosystem)
- "cordova-native" - the library tries to open the login and registration page using the phone’s system browser using the BrowserTabs cordova plugin. This requires extra setup for redirecting back to the app (see Section 2.2.3, "Hybrid Apps with Cordova")
- "custom" - allows you to implement a custom adapter (only for advanced use cases)

responseType

 Response type sent to Red Hat Single Sign-On with login requests. This is determined based on the flow value used during initialization, but can be overridden by setting this value.

2.2.7.3. Methods

init(options)

 Called to initialize the adapter.

Options is an Object, where:

- useNonce - Adds a cryptographic nonce to verify that the authentication response matches the request (default is true).
- onLoad - Specifies an action to do on load. Supported values are login-required or check-sso.
- silentCheckSsoRedirectUri - Set the redirect uri for silent authentication check if onLoad is set to 'check-sso'.
- silentCheckSsoFallback - Enables fall back to regular check-sso when silent check-sso is not supported by the browser (default is true).
- token - Set an initial value for the token.
- refreshToken - Set an initial value for the refresh token.
- idToken - Set an initial value for the id token (only together with token or refreshToken).
- scope - Set the default scope parameter to the Red Hat Single Sign-On login endpoint. Use a space-delimited list of scopes. Those typically reference Client scopes defined on a particular client. Note that the scope openid will always be added to the list of scopes by the adapter. For example, if you enter the scope options address phone, then the request to Red Hat Single Sign-On will contain the scope parameter scope=openid address phone. Note that the default scope specified here is overwritten if the login() options specify scope explicitly.
- timeSkew - Set an initial value for skew between local time and Red Hat Single Sign-On server in seconds (only together with token or refreshToken).
- checkLoginIframe - Set to enable/disable monitoring login state (default is true).
- \textbf{checkLoginIframeInterval} - Set the interval to check login state (default is 5 seconds).

- \textbf{responseMode} - Set the OpenID Connect response mode send to Red Hat Single Sign-On server at login request. Valid values are \texttt{query} or \texttt{fragment}. Default value is \texttt{fragment}, which means that after successful authentication will Red Hat Single Sign-On redirect to JavaScript application with OpenID Connect parameters added in URL fragment. This is generally safer and recommended over \texttt{query}.

- \textbf{flow} - Set the OpenID Connect flow. Valid values are \texttt{standard}, \texttt{implicit} or \texttt{hybrid}.

- \textbf{enableLogging} - Enables logging messages from Keycloak to the console (default is \texttt{false}).

- \textbf{pkceMethod} - The method for Proof Key Code Exchange (PKCE) to use. Configuring this value enables the PKCE mechanism. Available options:
  - \texttt{"S256"} - The SHA256 based PKCE method

- \textbf{messageReceiveTimeout} - Set a timeout in milliseconds for waiting for message responses from the Keycloak server. This is used, for example, when waiting for a message during 3rd party cookies check. The default value is 10000.

Returns a promise that resolves when initialization completes.

\textbf{login(options)}

Redirects to login form.

Options is an optional Object, where:

- \textbf{redirectUri} - Specifies the uri to redirect to after login.

- \textbf{prompt} - This parameter allows to slightly customize the login flow on the Red Hat Single Sign-On server side. For example enforce displaying the login screen in case of value \texttt{login}. See Parameters Forwarding Section for the details and all the possible values of the \texttt{prompt} parameter.

- \textbf{maxAge} - Used just if user is already authenticated. Specifies maximum time since the authentication of user happened. If user is already authenticated for longer time than \texttt{maxAge}, the SSO is ignored and he will need to re-authenticate again.

- \textbf{loginHint} - Used to pre-fill the username/email field on the login form.

- \textbf{scope} - Override the scope configured in \texttt{init} with a different value for this specific login.

- \textbf{idpHint} - Used to tell Red Hat Single Sign-On to skip showing the login page and automatically redirect to the specified identity provider instead. More info in the Identity Provider documentation.

- \textbf{acr} - Contains the information about acr claim, which will be sent inside \texttt{claims} parameter to the Red Hat Single Sign-On server. Typical usage is for step-up authentication. Example of use \{ \texttt{values: ["silver", "gold"], essential: true } \}. See OpenID Connect specification and Step-up authentication documentation for more details.

- \textbf{action} - If value is \texttt{register} then user is redirected to registration page, if the value is \texttt{UPDATE_PASSWORD} then the user will be redirected to the reset password page (if not authenticated will send user to login page first and redirect after authenticated), otherwise to login page.
locale - Sets the 'ui_locales' query param in compliance with section 3.1.2.1 of the OIDC 1.0 specification.

cordovaOptions - Specifies the arguments that are passed to the Cordova in-app-browser (if applicable). Options hidden and location are not affected by these arguments. All available options are defined at https://cordova.apache.org/docs/en/latest/reference/cordova-plugin-inappbrowser/. Example of use: { zoom: "no", hardwareback: "yes" };

createLoginUrl(options)

Returns the URL to login form.

Options is an optional Object, which supports same options as the function login.

logout(options)

Redirects to logout.

Options is an Object, where:

- redirectUri - Specifies the uri to redirect to after logout.

createLogoutUrl(options)

Returns the URL to log out the user.

Options is an Object, where:

- redirectUri - Specifies the uri to redirect to after logout.

register(options)

Redirects to registration form. Shortcut for login with option action = 'register'

Options are same as for the login method but 'action' is set to 'register'

createRegisterUrl(options)

Returns the url to registration page. Shortcut for createLoginUrl with option action = 'register'

Options are same as for the createLoginUrl method but 'action' is set to 'register'

accountManagement()

Redirects to the Account Management Console.

createAccountUrl(options)

Returns the URL to the Account Management Console.

Options is an Object, where:

- redirectUri - Specifies the uri to redirect to when redirecting back to the application.

hasRealmRole(role)

Returns true if the token has the given realm role.
hasResourceRole(role, resource)

Returns true if the token has the given role for the resource (resource is optional, if not specified clientId is used).

loadUserProfile()

Loads the users profile.

Returns a promise that resolves with the profile.

For example:

```javascript
keycloak.loadUserProfile()
.then(function(profile) {
    alert(JSON.stringify(profile, null, " "))
}).catch(function() {
    alert("Failed to load user profile");
});
```

isTokenExpired(minValidity)

Returns true if the token has less than minValidity seconds left before it expires (minValidity is optional, if not specified 0 is used).

updateToken(minValidity)

If the token expires within minValidity seconds (minValidity is optional, if not specified 5 is used) the token is refreshed. If -1 is passed as the minValidity, the token will be forcibly refreshed. If the session status iframe is enabled, the session status is also checked.

Returns a promise that resolves with a boolean indicating whether or not the token has been refreshed.

For example:

```javascript
keycloak.updateToken(5)
.then(function(refreshed) {
    if (refreshed) {
        alert('Token was successfully refreshed');
    } else {
        alert('Token is still valid');
    }
}).catch(function() {
    alert('Failed to refresh the token, or the session has expired');
});
```

clearToken()

Clear authentication state, including tokens. This can be useful if application has detected the session was expired, for example if updating token fails.

Invoking this results in onAuthLogout callback listener being invoked.

2.2.7.4. Callback Events
The adapter supports setting callback listeners for certain events. Keep in mind that these have to be set before the call to the `init` function.

For example:

```javascript
keycloak.onAuthSuccess = function() { alert('authenticated'); }
```

The available events are:

- **onReady(authenticated)** - Called when the adapter is initialized.
- **onAuthSuccess** - Called when a user is successfully authenticated.
- **onAuthError** - Called if there was an error during authentication.
- **onAuthRefreshSuccess** - Called when the token is refreshed.
- **onAuthRefreshError** - Called if there was an error while trying to refresh the token.
- **onAuthLogout** - Called if the user is logged out (will only be called if the session status iframe is enabled, or in Cordova mode).
- **onTokenExpired** - Called when the access token is expired. If a refresh token is available the token can be refreshed with `updateToken`, or in cases where it is not (that is, with implicit flow) you can redirect to the login screen to obtain a new access token.

### 2.3. NODE.JS ADAPTER

Red Hat Single Sign-On provides a Node.js adapter built on top of Connect to protect server-side JavaScript apps - the goal was to be flexible enough to integrate with frameworks like Express.js.

To use the Node.js adapter, first you must create a client for your application in the Red Hat Single Sign-On Admin Console. The adapter supports public, confidential, and bearer-only access type. Which one to choose depends on the use-case scenario.

Once the client is created click the **Installation** tab, select **Red Hat Single Sign-On OIDC JSON** for **Format Option**, and then click **Download**. The downloaded `keycloak.json` file should be at the root folder of your project.

#### 2.3.1. Installation

Assuming you’ve already installed Node.js, create a folder for your application:

```bash
mkdir myapp && cd myapp
```

Use `npm init` command to create a **package.json** for your application. Now add the Red Hat Single Sign-On connect adapter in the dependencies list:

```json
"dependencies": {
  "keycloak-connect": "file:keycloak-connect-18.0.6-redhat-00001.tgz"
}
```

#### 2.3.2. Usage
**Instantiate a Keycloak class**

The **Keycloak** class provides a central point for configuration and integration with your application. The simplest creation involves no arguments.

In the root directory of your project create a file called **server.js** and add the following code:

```javascript
const session = require('express-session');
const Keycloak = require('keycloak-connect');

const memoryStore = new session.MemoryStore();
const keycloak = new Keycloak({ store: memoryStore });
```

Install the **express-session** dependency:

```javascript
npm install express-session
```

To start the **server.js** script, add the following command in the 'scripts' section of the **package.json**:

```json
"scripts": {
  "test": "echo \"Error: no test specified\" & exit 1",
  "start": "node server.js"
},
```

Now we have the ability to run our server with following command:

```javascript
npm run start
```

By default, this will locate a file named **keycloak.json** alongside the main executable of your application, in our case on the root folder, to initialize keycloak-specific settings such as public key, realm name, various URLs.

In that case a Keycloak deployment is necessary to access Keycloak admin console.

Please visit links on how to deploy a Keycloak admin console with **Podman** or **Docker**

Now we are ready to obtain the **keycloak.json** file by visiting the Red Hat Single Sign-On Admin Console ➔ clients (left sidebar) ➔ choose your client ➔ Installation ➔ Format Option ➔ Keycloak OIDC JSON ➔ Download

Paste the downloaded file on the root folder of our project.

Instantiation with this method results in all of the reasonable defaults being used. As alternative, it’s also possible to provide a configuration object, rather than the **keycloak.json** file:

```javascript
const kcConfig = {
  clientId: 'myclient',
  bearerOnly: true,
  serverUrl: 'http://localhost:8080/auth',
  realm: 'myrealm',
  realmPublicKey: 'MIIBIjANB...' 
};

const keycloak = new Keycloak({ store: memoryStore }, kcConfig);
```
Applications can also redirect users to their preferred identity provider by using:

```javascript
const keycloak = new Keycloak({ store: memoryStore, idpHint: myIdP }, kcConfig);
```

### Configuring a web session store

If you want to use web sessions to manage server-side state for authentication, you need to initialize the `Keycloak(...)` with at least a `store` parameter, passing in the actual session store that `express-session` is using.

```javascript
const session = require('express-session');
const memoryStore = new session.MemoryStore();

// Configure session
app.use(
    session({
        secret: 'mySecret',
        resave: false,
        saveUninitialized: true,
        store: memoryStore,
    })
);

const keycloak = new Keycloak({ store: memoryStore });
```

### Passing a custom scope value

By default, the scope value `openid` is passed as a query parameter to Red Hat Single Sign-On’s login URL, but you can add an additional custom value:

```javascript
const keycloak = new Keycloak({ scope: 'offline_access' });
```

### 2.3.3. Installing middleware

Once instantiated, install the middleware into your connect-capable app:

In order to do so, first we have to install Express:

```javascript
npm install express
```

then require Express in our project as outlined below:

```javascript
const express = require('express');
const app = express();
```

and configure Keycloak middleware in Express, by adding at the code below:

```javascript
app.use( keycloak.middleware() );
```

Last but not least, let’s set up our server to listen for HTTP requests on port 3000 by adding the following code to `main.js`:
2.3.4. Configuration for proxies

If the application is running behind a proxy that terminates an SSL connection Express must be configured per the [express behind proxies](#) guide. Using an incorrect proxy configuration can result in invalid redirect URIs being generated.

Example configuration:

```javascript
const app = express();
app.set('trust proxy', true);
app.use(keycloak.middleware());
```

2.3.5. Checking authentication

To check that a user is authenticated before accessing a resource, simply use `keycloak.checkSso()`. It will only authenticate if the user is already logged-in. If the user is not logged-in, the browser will be redirected back to the originally-requested URL and remain unauthenticated:

```javascript
app.get('/check-sso', keycloak.checkSso(), checkSsoHandler);
```

2.3.6. Protecting resources

**Simple authentication**

To enforce that a user must be authenticated before accessing a resource, simply use a no-argument version of `keycloak.protect()`:

```javascript
app.get('/complain', keycloak.protect(), complaintHandler);
```

**Role-based authorization**

To secure a resource with an application role for the current app:

```javascript
app.get('/special', keycloak.protect('special'), specialHandler);
```

To secure a resource with an application role for a different app:

```javascript
app.get('/extra-special', keycloak.protect('other-app:special'), extraSpecialHandler);
```

To secure a resource with a realm role:

```javascript
app.get('/admin', keycloak.protect('realm:admin'), adminHandler);
```

**Resource-Based Authorization**
Resource-Based Authorization allows you to protect resources, and their specific methods/actions, based on a set of policies defined in Keycloak, thus externalizing authorization from your application. This is achieved by exposing a `keycloak.enforcer` method which you can use to protect resources.*

```javascript
app.get('/apis/me', keycloak.enforcer('user:profile'), userProfileHandler);
```

The `keycloak-enforcer` method operates in two modes, depending on the value of the `response_mode` configuration option.

```javascript
app.get('/apis/me', keycloak.enforcer('user:profile', {response_mode: 'token'}), userProfileHandler);
```

If `response_mode` is set to `token`, permissions are obtained from the server on behalf of the subject represented by the bearer token that was sent to your application. In this case, a new access token is issued by Keycloak with the permissions granted by the server. If the server did not respond with a token with the expected permissions, the request is denied. When using this mode, you should be able to obtain the token from the request as follows:

```javascript
app.get('/apis/me', keycloak.enforcer('user:profile', {response_mode: 'token'}), function (req, res) {
  const token = req.kauth.grant.access_token.content;
  const permissions = token.authorization ? token.authorization.permissions : undefined;
  // show user profile
});
```

Prefer this mode when your application is using sessions and you want to cache previous decisions from the server, as well as automatically handle refresh tokens. This mode is especially useful for applications acting as a client and resource server.

If `response_mode` is set to `permissions` (default mode), the server only returns the list of granted permissions, without issuing a new access token. In addition to not issuing a new token, this method exposes the permissions granted by the server through the `request` as follows:

```javascript
app.get('/apis/me', keycloak.enforcer('user:profile', {response_mode: 'permissions'}), function (req, res) {
  const permissions = req.permissions;
  // show user profile
});
```

Regardless of the `response_mode` in use, the `keycloak.enforcer` method will first try to check the permissions within the bearer token that was sent to your application. If the bearer token already carries the expected permissions, there is no need to interact with the server to obtain a decision. This is especially useful when your clients are capable of obtaining access tokens from the server with the expected permissions before accessing a protected resource, so they can use some capabilities provided by Keycloak Authorization Services such as incremental authorization and avoid additional requests to the server when `keycloak.enforcer` is enforcing access to the resource.

By default, the policy enforcer will use the `client_id` defined to the application (for instance, via `keycloak.json`) to reference a client in Keycloak that supports Keycloak Authorization Services. In this case, the client cannot be public given that it is actually a resource server.

If your application is acting as both a public client (frontend) and resource server (backend), you can use the following configuration to reference a different client in Keycloak with the policies that you want to enforce:

```javascript
app.get('/apis/me', keycloak.enforcer('user:profile', {client_id: 'your_client_id'}), userProfileHandler);
```
keycloak.enforcer('user:profile', {resource_server_id: 'my-apiserver'})

It is recommended to use distinct clients in Keycloak to represent your frontend and backend.

If the application you are protecting is enabled with Keycloak authorization services and you have defined client credentials in `keycloak.json`, you can push additional claims to the server and make them available to your policies in order to make decisions. For that, you can define a `claims` configuration option which expects a `function` that returns a JSON with the claims you want to push:

```javascript
app.get('/protected/resource', keycloak.enforcer(['resource:view', 'resource:write'],
    claims: function(request) {
        return {
            "http.uri": "/protected/resource",
            "user.agent": // get user agent from request
        }
    },
    function (req, res) {
        // access granted
    }),

For more details about how to configure Keycloak to protected your application resources, please take a look at the Authorization Services Guide.

Advanced authorization

To secure resources based on parts of the URL itself, assuming a role exists for each section:

```javascript
function protectBySection(token, request) {
    return token.hasRole(request.params.section);
}

app.get('/:section/:page', keycloak.protect(protectBySection), sectionHandler);
```

Advanced Login Configuration:

By default, all unauthorized requests will be redirected to the Red Hat Single Sign-On login page unless your client is bearer-only. However, a confidential or public client may host both browsable and API endpoints. To prevent redirects on unauthenticated API requests and instead return an HTTP 401, you can override the `redirectToLogin` function.

For example, this override checks if the URL contains `/api/` and disables login redirects:

```javascript
Keycloak.prototype.redirectToLogin = function(req) {
    const apiReqMatcher = //api/;
    return !apiReqMatcher.test(req.originalUrl || req.url);
};
```

2.3.7. Additional URLs

Explicit user-triggered logout

By default, the middleware catches calls to `/logout` to send the user through a Red Hat Single Sign-On-centric logout workflow. This can be changed by specifying a `logout` configuration parameter to the `middleware()` call:

```javascript
app.use(keycloak.middleware({ logout: '/logoff' }));
```
When the user-triggered logout is invoked a query parameter `redirect_url` can be passed:

```
https://example.com/logoff?
redirect_url=https%3A%2F%2Fexample.com%3A3000%2Flogged%2Fout
```

This parameter is then used as the redirect url of the OIDC logout endpoint and the user will be redirected to `https://example.com/logged/out`.

**Red Hat Single Sign-On Admin Callbacks**

Also, the middleware supports callbacks from the Red Hat Single Sign-On console to log out a single session or all sessions. By default, these type of admin callbacks occur relative to the root URL of `/` but can be changed by providing an `admin` parameter to the `middleware()` call:

```
app.use( keycloak.middleware( { admin: '/callbacks' } ));
```

### 2.3.8. Complete example

A complete example using the Node.js adapter usage can be found in Keycloak quickstarts for Node.js

### 2.4. OTHER OPENID CONNECT LIBRARIES

Red Hat Single Sign-On can be secured by supplied adapters that are usually easier to use and provide better integration with Red Hat Single Sign-On. However, if an adapter is not available for your programming language, framework, or platform you might opt to use a generic OpenID Connect Relying Party (RP) library instead. This chapter describes details specific to Red Hat Single Sign-On and does not contain specific protocol details. For more information see the OpenID Connect specifications and OAuth2 specification.

#### 2.4.1. Endpoints

The most important endpoint to understand is the `well-known` configuration endpoint. It lists endpoints and other configuration options relevant to the OpenID Connect implementation in Red Hat Single Sign-On. The endpoint is:

```
/realsms/{realm-name}/.well-known/openid-configuration
```

To obtain the full URL, add the base URL for Red Hat Single Sign-On and replace `{realm-name}` with the name of your realm. For example:

http://localhost:8080/auth/realms/master/.well-known/openid-configuration

Some RP libraries retrieve all required endpoints from this endpoint, but for others you might need to list the endpoints individually.

#### 2.4.1.1. Authorization endpoint

```
/realsms/{realm-name}/protocol/openid-connect/auth
```

The authorization endpoint performs authentication of the end-user. This is done by redirecting the user agent to this endpoint.

For more details see the Authorization Endpoint section in the OpenID Connect specification.
2.4.1.2. Token endpoint

/realms/{realm-name}/protocol/openid-connect/token

The token endpoint is used to obtain tokens. Tokens can either be obtained by exchanging an authorization code or by supplying credentials directly depending on what flow is used. The token endpoint is also used to obtain new access tokens when they expire.

For more details see the Token Endpoint section in the OpenID Connect specification.

2.4.1.3. Userinfo endpoint

/realms/{realm-name}/protocol/openid-connect/userinfo

The userinfo endpoint returns standard claims about the authenticated user, and is protected by a bearer token.

For more details see the Userinfo Endpoint section in the OpenID Connect specification.

2.4.1.4. Logout endpoint

/realms/{realm-name}/protocol/openid-connect/logout

The logout endpoint logs out the authenticated user.

The user agent can be redirected to the endpoint, in which case the active user session is logged out. Afterward the user agent is redirected back to the application.

The endpoint can also be invoked directly by the application. To invoke this endpoint directly the refresh token needs to be included as well as the credentials required to authenticate the client.

2.4.1.5. Certificate endpoint

/realms/{realm-name}/protocol/openid-connect/certs

The certificate endpoint returns the public keys enabled by the realm, encoded as a JSON Web Key (JWK). Depending on the realm settings there can be one or more keys enabled for verifying tokens.

For more information see the Server Administration Guide and the JSON Web Key specification.

2.4.1.6. Introspection endpoint

/realms/{realm-name}/protocol/openid-connect/token/introspect

The introspection endpoint is used to retrieve the active state of a token. In other words, you can use it to validate an access or refresh token. It can only be invoked by confidential clients.

For more details on how to invoke on this endpoint, see OAuth 2.0 Token Introspection specification.

2.4.1.7. Dynamic Client Registration endpoint

/realms/{realm-name}/clients-registrations/openid-connect
The dynamic client registration endpoint is used to dynamically register clients.

For more details see the Client Registration chapter and the OpenID Connect Dynamic Client Registration specification.

**2.4.1.8. Token Revocation endpoint**

```
/realms/{realm-name}/protocol/openid-connect/revoke
```

The token revocation endpoint is used to revoke tokens. Both refresh tokens and access tokens are supported by this endpoint.

For more details on how to invoke on this endpoint, see OAuth 2.0 Token Revocation specification.

**2.4.1.9. Device Authorization endpoint**

```
/realms/{realm-name}/protocol/openid-connect/auth/device
```

The device authorization endpoint is used to obtain a device code and a user code. It can be invoked by confidential or public clients.

For more details on how to invoke on this endpoint, see OAuth 2.0 Device Authorization Grant specification.

**2.4.1.10. Backchannel Authentication endpoint**

```
/realms/{realm-name}/protocol/openid-connect/ext/ciba/auth
```

The backchannel authentication endpoint is used to obtain an auth_req_id that identifies the authentication request made by the client. It can only be invoked by confidential clients.

For more details on how to invoke on this endpoint, see OpenID Connect Client Initiated Backchannel Authentication Flow specification.

Also please refer to other places of Red Hat Single Sign-On documentation like Client Initiated Backchannel Authentication Grant section of this guide and Client Initiated Backchannel Authentication Grant section of Server Administration Guide.

**2.4.2. Validating access tokens**

If you need to manually validate access tokens issued by Red Hat Single Sign-On you can invoke the Introspection Endpoint. The downside to this approach is that you have to make a network invocation to the Red Hat Single Sign-On server. This can be slow and possibly overload the server if you have too many validation requests going on at the same time. Red Hat Single Sign-On issued access tokens are JSON Web Tokens (JWT) digitally signed and encoded using JSON Web Signature (JWS). Because they are encoded in this way, this allows you to locally validate access tokens using the public key of the issuing realm. You can either hard code the realm’s public key in your validation code, or lookup and cache the public key using the certificate endpoint with the Key ID (KID) embedded within the JWS. Depending what language you code in, there are a multitude of third party libraries out there that can help you with JWS validation.

**2.4.3. Flows**
2.4.3.1. Authorization code

The Authorization Code flow redirects the user agent to Red Hat Single Sign-On. Once the user has successfully authenticated with Red Hat Single Sign-On an Authorization Code is created and the user agent is redirected back to the application. The application then uses the authorization code along with its credentials to obtain an Access Token, Refresh Token and ID Token from Red Hat Single Sign-On.

The flow is targeted towards web applications, but is also recommended for native applications, including mobile applications, where it is possible to embed a user agent.

For more details refer to the Authorization Code Flow in the OpenID Connect specification.

2.4.3.2. Implicit

The Implicit flow redirects works similarly to the Authorization Code flow, but instead of returning an Authorization Code the Access Token and ID Token is returned. This reduces the need for the extra invocation to exchange the Authorization Code for an Access Token. However, it does not include a Refresh Token. This results in the need to either permit Access Tokens with a long expiration, which is problematic as it’s very hard to invalidate these. Or requires a new redirect to obtain new Access Token once the initial Access Token has expired. The Implicit flow is useful if the application only wants to authenticate the user and deals with logout itself.

There’s also a Hybrid flow where both the Access Token and an Authorization Code is returned.

One thing to note is that both the Implicit flow and Hybrid flow has potential security risks as the Access Token may be leaked through web server logs and browser history. This is somewhat mitigated by using short expiration for Access Tokens.

For more details refer to the Implicit Flow in the OpenID Connect specification.

2.4.3.3. Resource Owner Password Credentials

Resource Owner Password Credentials, referred to as Direct Grant in Red Hat Single Sign-On, allows exchanging user credentials for tokens. It’s not recommended to use this flow unless you absolutely need to. Examples where this could be useful are legacy applications and command-line interfaces.

There are a number of limitations of using this flow, including:

- User credentials are exposed to the application
- Applications need login pages
- Application needs to be aware of the authentication scheme
- Changes to authentication flow requires changes to application
- No support for identity brokering or social login
- Flows are not supported (user self-registration, required actions, etc.)

For a client to be permitted to use the Resource Owner Password Credentials grant the client has to have the Direct Access Grants Enabled option enabled.

This flow is not included in OpenID Connect, but is a part of the OAuth 2.0 specification.

For more details refer to the Resource Owner Password Credentials Grant chapter in the OAuth 2.0 specification.
2.4.3.3.1. Example using CURL

The following example shows how to obtain an access token for a user in the realm master with username user and password password. The example is using the confidential client myclient:

```
curl \
-d "client_id=myclient" \
-d "client_secret=40cc097b-2a57-4c17-b36a-8fdf3fc2d578" \
-d "username=user" \
-d "password=password" \
"http://localhost:8080/auth/realms/master/protocol/openid-connect/token"
```

2.4.3.4. Client credentials

Client Credentials is used when clients (applications and services) wants to obtain access on behalf of themselves rather than on behalf of a user. This can for example be useful for background services that applies changes to the system in general rather than for a specific user.

Red Hat Single Sign-On provides support for clients to authenticate either with a secret or with public/private keys.

This flow is not included in OpenID Connect, but is a part of the OAuth 2.0 specification.

For more details refer to the Client Credentials Grant chapter in the OAuth 2.0 specification.

2.4.3.5. Device Authorization Grant

Device Authorization Grant is used by clients running on internet-connected devices that have limited input capabilities or lack a suitable browser. The application requests Red Hat Single Sign-On a device code and a user code. Red Hat Single Sign-On creates a device code and a user code. Red Hat Single Sign-On returns a response including the device code and the user code to the application. Then the application provides the user with the user code and the verification URI. The user accesses a verification URI to be authenticated by using another browser. The application repeatedly polls Red Hat Single Sign-On until Red Hat Single Sign-On completes the user authorization. If user authentication is complete, the application obtains the device code. Then the application uses the device code along with its credentials to obtain an Access Token, Refresh Token and ID Token from Red Hat Single Sign-On.

For more details refer to the OAuth 2.0 Device Authorization Grant specification.

2.4.3.6. Client Initiated Backchannel Authentication Grant

Client Initiated Backchannel Authentication Grant is used by clients who want to initiate the authentication flow by communicating with the OpenID Provider directly without redirect through the user’s browser like OAuth 2.0’s authorization code grant.

The client requests Red Hat Single Sign-On an auth_req_id that identifies the authentication request made by the client. Red Hat Single Sign-On creates the auth_req_id.

After receiving this auth_req_id, this client repeatedly needs to poll Red Hat Single Sign-On to obtain an Access Token, Refresh Token and ID Token from Red Hat Single Sign-On in return for the auth_req_id until the user is authenticated.

In case that client uses ping mode, it does not need to repeatedly poll the token endpoint, but it can wait for the notification sent by Red Hat Single Sign-On to the specified Client Notification Endpoint. The
Client Notification Endpoint can be configured in the Red Hat Single Sign-On Admin Console. The details of the contract for Client Notification Endpoint are described in the CIBA specification.

For more details refer to OpenID Connect Client Initiated Backchannel Authentication Flow specification.

Also please refer to other places of Red Hat Single Sign-On documentation like Backchannel Authentication Endpoint of this guide and Client Initiated Backchannel Authentication Grant section of Server Administration Guide. For the details about FAPI CIBA compliance, please refer to the FAPI section of this guide.

2.4.4. Redirect URIs

When using the redirect based flows it’s important to use valid redirect uris for your clients. The redirect uris should be as specific as possible. This especially applies to client-side (public clients) applications. Failing to do so could result in:

- Open redirects - this can allow attackers to create spoof links that looks like they are coming from your domain
- Unauthorized entry - when users are already authenticated with Red Hat Single Sign-On an attacker can use a public client where redirect uris have not be configured correctly to gain access by redirecting the user without the users knowledge

In production for web applications always use https for all redirect URIs. Do not allow redirects to http.

There’s also a few special redirect URIs:

http://localhost

This redirect URI is useful for native applications and allows the native application to create a web server on a random port that can be used to obtain the authorization code. This redirect uri allows any port.

urn:ietf:wg:oauth:2.0:oob

If its not possible to start a web server in the client (or a browser is not available) it is possible to use the special urn:ietf:wg:oauth:2.0:oob redirect uri. When this redirect uri is used Red Hat Single Sign-On displays a page with the code in the title and in a box on the page. The application can either detect that the browser title has changed, or the user can copy/paste the code manually to the application. With this redirect uri it is also possible for a user to use a different device to obtain a code to paste back to the application.

2.5. FINANCIAL-GRADE API (FAPI) SUPPORT

Red Hat Single Sign-On makes it easier for administrators to make sure that their clients are compliant with these specifications:

- Financial-grade API Security Profile 1.0 – Part 1: Baseline
- Financial-grade API Security Profile 1.0 – Part 2: Advanced
- Financial-grade API: Client Initiated Backchannel Authentication Profile (FAPI CIBA)

This compliance means that the Red Hat Single Sign-On server will verify the requirements for the authorization server, which are mentioned in the specifications. Red Hat Single Sign-On adapters do not have any specific support for the FAPI, hence the required validations on the client (application) side
may need to be still done manually or through some other third-party solutions.

2.5.1. FAPI client profiles

To make sure that your clients are FAPI compliant, you can configure Client Policies in your realm as described in the Server Administration Guide and link them to the global client profiles for FAPI support, which are automatically available in each realm. You can use either fapi-1-baseline or fapi-1-advanced profile based on which FAPI profile you need your clients to conform with.

In case you want to use Pushed Authorization Request (PAR), it is recommended that your client use both the fapi-1-baseline profile and fapi-1-advanced for PAR requests. Specifically, the fapi-1-baseline profile contains pkce-enforcer executor, which makes sure that client use PKCE with secured S256 algorithm. This is not required for FAPI Advanced clients unless they use PAR requests.

In case you want to use CIBA in a FAPI compliant way, make sure that your clients use both fapi-1-advanced and fapi-ciba client profiles. There is a need to use the fapi-1-advanced profile, or other client profile containing the requested executors, as the fapi-ciba profile contains just CIBA-specific executors. When enforcing the requirements of the FAPI CIBA specification, there is a need for more requirements, such as enforcement of confidential clients or certificate-bound access tokens.

2.5.2. Open Banking Brasil Financial-grade API Security Profile

Red Hat Single Sign-On is compliant with the Open Banking Brasil Financial-grade API Security Profile 1.0 Implementers Draft 2. This one is more strict in some requirements than the FAPI 1 Advanced specification and hence it may be needed to configure Client Policies in the more strict way to enforce some of the requirements. Especially:

- If your client does not use PAR, make sure that it uses encrypted OIDC request objects. This can be achieved by using a client profile with the secure-request-object executor configured with Encryption Required enabled.

- Make sure that for JWS, the client uses the PS256 algorithm. For JWE, the client should use the RSA-OAEP with A256GCM. This may need to be set in all the Client Settings where these algorithms are applicable.

2.5.3. TLS considerations

As confidential information is being exchanged, all interactions shall be encrypted with TLS (HTTPS). Moreover, there are some requirements in the FAPI specification for the cipher suites and TLS protocol versions used. To match these requirements, you can consider configure allowed ciphers. This configuration can be done in the KEYCLOAK_HOME/standalone/configuration/standalone-*.xml file in the Elytron subsystem. For example this element can be added under tls → server-ssl-contexts:

```xml
<server-ssl-context name="kcSSLContext" want-client-auth="true" protocols="TLSv1.2" \ key-manager="kcKeyManager" trust-manager="kcTrustManager" \ cipher-suite-filter="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_256_GCM_SHA384" protocols="TLSv1.2" />
```

The references to kcKeyManager and kcTrustManager refers to the corresponding Keystore and Truststore. See the documentation of Wildfly Elytron subsystem for more details and also other parts of Red Hat Single Sign-On documentation such as Network Setup Section or X.509 Authentication Section.
CHAPTER 3. USING SAML TO SECURE APPLICATIONS AND SERVICES

This section describes how you can secure applications and services with SAML using either Red Hat Single Sign-On client adapters or generic SAML provider libraries.

3.1. JAVA ADAPTERS

Red Hat Single Sign-On comes with a range of different adapters for Java application. Selecting the correct adapter depends on the target platform.

3.1.1. General Adapter Config

Each SAML client adapter supported by Red Hat Single Sign-On can be configured by a simple XML text file. This is what one might look like:

```xml
<keycloak-saml-adapter xmlns="urn:keycloak:saml:adapter"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:keycloak:saml:adapter
    https://www.keycloak.org/schema/keycloak_saml_adapter_1_10.xsd">
    <SP entityID="http://localhost:8081/sales-post-sig/"
        sslPolicy="EXTERNAL"
        nameIDPolicyFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
        logoutPage="/logout.jsp"
        forceAuthentication="false"
        isPassive="false"
        turnOffChangeSessionIdOnLogin="false"
        autodetectBearerOnly="false">
        <Keys>
            <Key signing="true">
                <KeyStore resource="/WEB-INF/keystore.jks" password="store123">
                    <PrivateKey alias="http://localhost:8080/sales-post-sig/" password="test123"/>
                </KeyStore>
            </Key/>
        </Keys>
        <PrincipalNameMapping policy="FROM_NAME_ID"/>
        <RoleIdentifiers>
            <Attribute name="Role"/>
        </RoleIdentifiers>
        <RoleMappingsProvider id="properties-based-role-mapper">
            <Property name="properties.resource.location" value="/WEB-INF/role-mappings.properties"/>
        </RoleMappingsProvider>
        <IDP entityID="idp"
            signaturesRequired="true">
            <SingleSignOnService requestBinding="POST"
                bindingUrl="http://localhost:8081/auth/realms/demo/protocol/saml"/>
            <SingleLogoutService requestBinding="POST"
                responseBinding="POST"
                postBindingUrl="http://localhost:8081/auth/realms/demo/protocol/saml"
                redirectBindingUrl="http://localhost:8081/auth/realms/demo/protocol/saml"/>
        </IDP>
    </SP>
</keycloak-saml-adapter>
```
Some of these configuration switches may be adapter specific and some are common across all adapters. For Java adapters you can use \${…} enclosure as System property replacement. For example \${jboss.server.config.dir}.

3.1.1.1. SP element

Here is the explanation of the SP element attributes:

```xml
<SP entityID="sp"
    sslPolicy="ssl"
    nameIDPolicyFormat="format"
    forceAuthentication="true"
    isPassive="false"
    keepDOMAssertion="true"
    autodetectBearerOnly="false">
    ...
</SP>
```

**entityID**

This is the identifier for this client. The IdP needs this value to determine who the client is that is communicating with it. This setting is **REQUIRED**.

**sslPolicy**

This is the SSL policy the adapter will enforce. Valid values are: **ALL**, **EXTERNAL**, and **NONE**. For **ALL**, all requests must come in via HTTPS. For **EXTERNAL**, only non-private IP addresses must come over the wire via HTTPS. For **NONE**, no requests are required to come over via HTTPS. This setting is **OPTIONAL**. Default value is **EXTERNAL**.

**nameIDPolicyFormat**

SAML clients can request a specific NameID Subject format. Fill in this value if you want a specific format. It must be a standard SAML format identifier: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`. This setting is **OPTIONAL**. By default, no special format is requested.

**forceAuthentication**

SAML clients can request that a user is re-authenticated even if they are already logged in at the IdP. Set this to `true` to enable. This setting is **OPTIONAL**. Default value is **false**.

**isPassive**

SAML clients can request that a user is never asked to authenticate even if they are not logged in at the IdP. Set this to `true` if you want this. Do not use together with **forceAuthentication** as they are opposite. This setting is **OPTIONAL**. Default value is **false**.

**turnOffChangeSessionIdOnLogin**
The session ID is changed by default on a successful login on some platforms to plug a security attack vector. Change this to `true` to disable this. It is recommended you do not turn it off. Default value is `false`.

**autodetectBearerOnly**

This should be set to `true` if your application serves both a web application and web services (for example SOAP or REST). It allows you to redirect unauthenticated users of the web application to the Red Hat Single Sign-On login page, but send an HTTP 401 status code to unauthenticated SOAP or REST clients instead as they would not understand a redirect to the login page. Red Hat Single Sign-On auto-detects SOAP or REST clients based on typical headers like `X-Requested-With`, `SOAPAction` or `Accept`. The default value is `false`.

**logoutPage**

This sets the page to display after logout. If the page is a full URL, such as `http://web.example.com/logout.html`, the user is redirected after logout to that page using the HTTP 302 status code. If a link without scheme part is specified, such as `/logout.jsp`, the page is displayed after logout, regardless of whether it lies in a protected area according to `security-constraint` declarations in web.xml, and the page is resolved relative to the deployment context root.

**keepDOMAssertion**

This attribute should be set to `true` to make the adapter store the DOM representation of the assertion in its original form inside the `SamlPrincipal` associated to the request. The assertion document can be retrieved using the method `getAssertionDocument` inside the principal. This is specially useful when re-playing a signed assertion. The returned document is the one that was generated parsing the SAML response received by the Red Hat Single Sign-On server. This setting is `OPTIONAL` and its default value is `false` (the document is not saved inside the principal).

### 3.1.1.2. Service Provider keys and key elements

If the IdP requires that the client application (or SP) sign all of its requests and/or if the IdP will encrypt assertions, you must define the keys used to do this. For client-signed documents you must define both the private and public key or certificate that is used to sign documents. For encryption, you only have to define the private key that is used to decrypt it.

There are two ways to describe your keys. They can be stored within a Java KeyStore or you can copy/paste the keys directly within `keycloak-saml.xml` in the PEM format.

```xml
<Keys>
  <Key signing="true">
    ...
  </Key>
</Keys>
```

The `Key` element has two optional attributes `signing` and `encryption`. When set to true these tell the adapter what the key will be used for. If both attributes are set to true, then the key will be used for both signing documents and decrypting encrypted assertions. You must set at least one of these attributes to true.

#### 3.1.1.2.1. KeyStore element

Within the `Key` element you can load your keys and certificates from a Java Keystore. This is declared within a `KeyStore` element.

```xml
<Keys>
  <Key signing="true">
    <KeyStore resource="/WEB-INF/keystore.jks" password="store123">
      ...
    </KeyStore>
  </Key>
</Keys>
```
Here are the XML config attributes that are defined with the `KeyStore` element.

**file**

File path to the key store. This option is **OPTIONAL**. The file or resource attribute must be set.

**resource**

WAR resource path to the KeyStore. This is a path used in method call to `ServletContext.getResourceAsStream()`. This option is **OPTIONAL**. The file or resource attribute must be set.

**password**

The password of the KeyStore. This option is **REQUIRED**.

If you are defining keys that the SP will use to sign document, you must also specify references to your private keys and certificates within the Java KeyStore. The `PrivateKey` and `Certificate` elements in the above example define an alias that points to the key or cert within the keystore. Keystores require an additional password to access private keys. In the `PrivateKey` element you must define this password within a `password` attribute.

### 3.1.1.2.2. Key PEMS

Within the `Key` element you declare your keys and certificates directly using the sub elements `PrivateKeyPem`, `PublicKeyPem`, and `CertificatePem`. The values contained in these elements must conform to the PEM key format. You usually use this option if you are generating keys using `openssl` or similar command line tool.

```xml
<Key signing="true">
   <PrivateKeyPem>
      2341251234AB31234==231BB998311222423522334
   </PrivateKeyPem>
   <CertificatePem>
      211111341251234AB31234==231BB998311222423522334
   </CertificatePem>
</Key>
</Keys>
```

### 3.1.1.3. SP PrincipalNameMapping element

This element is optional. When creating a Java Principal object that you obtain from methods such as `HttpServletRequest.getUserPrincipal()`, you can define what name is returned by the `Principal.getName()` method.

```xml
<SP ...>
   <PrincipalNameMapping policy="FROM_NAME_ID"/>
</SP>
```
The `policy` attribute defines the policy used to populate this value. The possible values for this attribute are:

**FROM_NAME_ID**
This policy just uses whatever the SAML subject value is. This is the default setting.

**FROM_ATTRIBUTE**
This will pull the value from one of the attributes declared in the SAML assertion received from the server. You'll need to specify the name of the SAML assertion attribute to use within the `attribute` XML attribute.

### 3.1.1.4. RoleIdentifiers element

The `RoleIdentifiers` element defines what SAML attributes within the assertion received from the user should be used as role identifiers within the Jakarta EE Security Context for the user.

```xml
<RoleIdentifiers>
    <Attribute name="Role"/>
    <Attribute name="member"/>
    <Attribute name="memberOf"/>
</RoleIdentifiers>
```

By default `Role` attribute values are converted to Jakarta EE roles. Some IdPs send roles using a `member` or `memberOf` attribute assertion. You can define one or more `Attribute` elements to specify which SAML attributes must be converted into roles.

### 3.1.1.5. RoleMappingsProvider element

The `RoleMappingsProvider` is an optional element that allows for the specification of the id and configuration of the `org.keycloak.adapters.saml.RoleMappingsProvider` SPI implementation that is to be used by the SAML adapter.

When Red Hat Single Sign-On is used as the IDP, it is possible to use the built in role mappers to map any roles before adding them to the SAML assertion. However, the SAML adapters can be used to send SAML requests to third party IDPs and in this case it might be necessary to map the roles extracted from the assertion into a different set of roles as required by the SP. The `RoleMappingsProvider` SPI allows for the configuration of pluggable role mappers that can be used to perform the necessary mappings.

The configuration of the provider looks as follows:

```xml
...<RoleIdentifiers>
    ...</RoleIdentifiers>
</RoleMappingsProvider>
<IDP>
    ...</IDP>
```
The `id` attribute identifies which of the installed providers is to be used. The `Property` sub-element can be used multiple times to specify configuration properties for the provider.

### 3.1.1.5.1. Properties Based role mappings provider

Red Hat Single Sign-On includes a `RoleMappingsProvider` implementation that performs the role mappings using a `properties` file. This provider is identified by the `id` `properties-based-role-mapper` and is implemented by the `org.keycloak.adapters.saml.PropertiesBasedRoleMapper` class.

This provider relies on two configuration properties that can be used to specify the location of the `properties` file that will be used. First, it checks if the `properties.file.location` property has been specified, using the configured value to locate the `properties` file in the filesystem. If the configured file is not located, the provider throws a `RuntimeException`. The following snippet shows an example of provider using the `properties.file.configuration` option to load the `roles.properties` file from the `/opt/mappers/` directory in the filesystem:

```xml
<RoleMappingsProvider id="properties-based-role-mapper">
  <Property name="properties.file.location" value="/opt/mappers/roles.properties"/>
</RoleMappingsProvider>
```

If the `properties.file.location` configuration has not been set, the provider checks the `properties.resource.location` property, using the configured value to load the `properties` file from the WAR resource. If this configuration property is also not present, the provider attempts to load the file from `/WEB-INF/role-mappings.properties` by default. Failure to load the file from the resource will result in the provider throwing a `RuntimeException`. The following snippet shows an example of provider using the `properties.resource.location` to load the `roles.properties` file from the application’s `/WEB-INF/conf/` directory:

```xml
<RoleMappingsProvider id="properties-based-role-mapper">
  <Property name="properties.resource.location" value="/WEB-INF/conf/roles.properties"/>
</RoleMappingsProvider>
```

The `properties` file can contain both roles and principals as keys, and a list of zero or more roles separated by comma as values. When invoked, the implementation iterates through the set of roles that were extracted from the assertion and checks, for each role, if a mapping exists. If the role maps to an empty role, it is discarded. If it maps to a set of one or more different roles, then these roles are set in the result set. If no mapping is found for the role then it is included as is in the result set.

Once the roles have been processed, the implementation checks if the principal extracted from the assertion contains an entry `properties` file. If a mapping for the principal exists, any roles listed as value are added to the result set. This allows the assignment of extra roles to a principal.

As an example, let’s assume the provider has been configured with the following properties file:

```properties
roleA=roleX,roleY
roleB=
kc_user=roleZ
```

If the principal `kc_user` is extracted from the assertion with roles `roleA`, `roleB` and `roleC`, the final set of roles assigned to the principal will be `roleC`, `roleX`, `roleY` and `roleZ` because `roleA` is being mapped into both `roleX` and `roleY`, `roleB` was mapped into an empty role - thus being discarded, `roleC` is used as is and finally an additional role was added to the `kc_user` principal (`roleZ`).
Note: to use spaces in role names for mappings, use unicode replacements for space. For example, incoming 'role A' would appear as:

```
role\u00200020A\u003d\u0020role\u0020X,\u0020role\u0020Y
```

### 3.1.1.5.2. Adding your own role mappings provider

To add a custom role mappings provider one simply needs to implement the `org.keycloak.adapters.saml.RoleMappingsProvider` SPI. For more details see the SAML Role Mappings SPI section in Server Developer Guide.

### 3.1.1.6. IDP Element

Everything in the IDP element describes the settings for the identity provider (authentication server) the SP is communicating with.

```
<IDP entityID=\"idp\"
    signaturesRequired=\"true\"
    signatureAlgorithm=\"RSA_SHA1\"
    signatureCanonicalizationMethod=\"http://www.w3.org/2001/10/xml-exc-c14n#\">
    ...
</IDP>
```

Here are the attribute config options you can specify within the IDP element declaration.

**entityID**

This is the issuer ID of the IDP. This setting is **REQUIRED**.

**signaturesRequired**

If set to **true**, the client adapter will sign every document it sends to the IDP. Also, the client will expect that the IDP will be signing any documents sent to it. This switch sets the default for all request and response types, but you will see later that you have some fine grain control over this. This setting is **OPTIONAL** and will default to **false**.

**signatureAlgorithm**

This is the signature algorithm that the IDP expects signed documents to use. Allowed values are: **RSA_SHA1**, **RSA_SHA256**, **RSA_SHA512**, and **DSA_SHA1**. This setting is **OPTIONAL** and defaults to **RSA_SHA256**.

**signatureCanonicalizationMethod**

This is the signature canonicalization method that the IDP expects signed documents to use. This setting is **OPTIONAL**. The default value is [http://www.w3.org/2001/10/xml-exc-c14n#](http://www.w3.org/2001/10/xml-exc-c14n#) and should be good for most IDPs.

**metadataUrl**

The URL used to retrieve the IDP metadata, currently this is only used to pick up signing and encryption keys periodically which allow cycling of these keys on the IDP without manual changes on the SP side.

### 3.1.1.7. IDP AllowedClockSkew sub element

The **AllowedClockSkew** optional sub element defines the allowed clock skew between IDP and SP. The default value is 0.

```
<AllowedClockSkew unit=\"MILLISECONDS\">3500</AllowedClockSkew>
```
It is possible to define the time unit attached to the value for this element. Allowed values are MICROSECONDS, MILLISECONDS, MINUTES, NANOSECONDS and SECONDS. This is OPTIONAL. The default value is SECONDS.

3.1.1.8. IDP SingleSignOnService sub element

The SingleSignOnService sub element defines the login SAML endpoint of the IDP. The client adapter will send requests to the IDP formatted via the settings within this element when it wants to login.

```xml
<SingleSignOnService
  signRequest="true"
  validateResponseSignature="true"
  requestBinding="post"
  bindingUrl="url"/>
```

Here are the config attributes you can define on this element:

**signRequest**
Should the client sign authn requests? This setting is OPTIONAL. Defaults to whatever the IDP signaturesRequired element value is.

**validateResponseSignature**
Should the client expect the IDP to sign the assertion response document sent back from an authn request? This setting OPTIONAL. Defaults to whatever the IDP signaturesRequired element value is.

**requestBinding**
This is the SAML binding type used for communicating with the IDP. This setting is OPTIONAL. The default value is POST, but you can set it to REDIRECT as well.

**responseBinding**
SAML allows the client to request what binding type it wants authn responses to use. The values of this can be POST or REDIRECT. This setting is OPTIONAL. The default is that the client will not request a specific binding type for responses.

**assertionConsumerServiceUrl**
URL of the assertion consumer service (ACS) where the IDP login service should send responses to. This setting is OPTIONAL. By default it is unset, relying on the configuration in the IdP. When set, it must end in /saml, for example http://sp.domain.com/my/endpoint/for/saml. The value of this property is sent in AssertionConsumerServiceURL attribute of SAML AuthnRequest message. This property is typically accompanied by the responseBinding attribute.

**bindingUrl**
This is the URL for the IDP login service that the client will send requests to. This setting is REQUIRED.

3.1.1.9. IDP SingleLogoutService sub element

The SingleLogoutService sub element defines the logout SAML endpoint of the IDP. The client adapter will send requests to the IDP formatted via the settings within this element when it wants to logout.

```xml
<SingleLogoutService
  validateRequestSignature="true"
  validateResponseSignature="true"
  signRequest="true"
  signResponse="true"
```
signRequest

Should the client sign logout requests it makes to the IDP? This setting is OPTIONAL. Defaults to whatever the IDP signaturesRequired element value is.

signResponse

Should the client sign logout responses it sends to the IDP requests? This setting is OPTIONAL. Defaults to whatever the IDP signaturesRequired element value is.

validateRequestSignature

Should the client expect signed logout request documents from the IDP? This setting is OPTIONAL. Defaults to whatever the IDP signaturesRequired element value is.

validateResponseSignature

Should the client expect signed logout response documents from the IDP? This setting is OPTIONAL. Defaults to whatever the IDP signaturesRequired element value is.

requestBinding

This is the SAML binding type used for communicating SAML requests to the IDP. This setting is OPTIONAL. The default value is POST, but you can set it to REDIRECT as well.

responseBinding

This is the SAML binding type used for communicating SAML responses to the IDP. The values of this can be POST or REDIRECT. This setting is OPTIONAL. The default value is POST, but you can set it to REDIRECT as well.

postBindingUrl

This is the URL for the IDP’s logout service when using the POST binding. This setting is REQUIRED if using the POST binding.

redirectBindingUrl

This is the URL for the IDP’s logout service when using the REDIRECT binding. This setting is REQUIRED if using the REDIRECT binding.

3.1.1.10. IDP Keys sub element

The Keys sub element of IDP is only used to define the certificate or public key to use to verify documents signed by the IDP. It is defined in the same way as the SP’s Keys element. But again, you only have to define one certificate or public key reference. Note that, if both IDP and SP are realized by Red Hat Single Sign-On server and adapter, respectively, there is no need to specify the keys for signature validation, see below.

It is possible to configure SP to obtain public keys for IDP signature validation from published certificates automatically, provided both SP and IDP are implemented by Red Hat Single Sign-On. This is done by removing all declarations of signature validation keys in Keys sub element. If the Keys sub element would then remain empty, it can be omitted completely. The keys are then automatically obtained by SP from SAML descriptor, location of which is derived from SAML endpoint URL specified in the IDP SingleSignOnService sub element. Settings of the HTTP client that is used for SAML descriptor retrieval usually needs no additional configuration, however it can be configured in the IDP HttpClient sub element.

It is also possible to specify multiple keys for signature verification. This is done by declaring multiple Key elements within Keys sub element that have signing attribute set to true. This is useful for example in situation when the IDP signing keys are rotated: There is usually a transition period when new SAML
protocol messages and assertions are signed with the new key but those signed by previous key should still be accepted.

It is not possible to configure Red Hat Single Sign-On to both obtain the keys for signature verification automatically and define additional static signature verification keys.

3.1.1.11. IDP HttpClient sub element

The HttpClient optional sub element defines the properties of HTTP client used for automatic obtaining of certificates containing public keys for IDP signature verification via SAML descriptor of the IDP when enabled.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<idp
  entityID="idp">
  ...
  <keys>
    <key signing="true">
      <keyStore resource="/WEB-INF/keystore.jks" password="store123">
        <certificate alias="demo"/>
      </keyStore>
    </key>
  </keys>
</idp>
```

3.1.11. IDP HttpClient sub element

The HttpClient optional sub element defines the properties of HTTP client used for automatic obtaining of certificates containing public keys for IDP signature verification via SAML descriptor of the IDP when enabled.

```xml
<httpclient
  connectionPoolSize="10"
  disableTrustManager="false"
  allowAnyHostname="false"
  clientKeystore="classpath:keystore.jks"
  clientKeystorePassword="pwd"
  truststore="classpath:truststore.jks"
  truststorePassword="pwd"
  proxyUrl="http://proxy/"
  socketTimeout="5000"
  connectionTimeout="6000"
  connectionTtl="500" />
```

connectionPoolSize

This config option defines how many connections to the Red Hat Single Sign-On server should be pooled. This is OPTIONAL. The default value is 10.

disableTrustManager

If the Red Hat Single Sign-On server requires HTTPS and this config option is set to true you do not have to specify a truststore. This setting should only be used during development and never in production as it will disable verification of SSL certificates. This is OPTIONAL. The default value is false.

allowAnyHostname

If the Red Hat Single Sign-On server requires HTTPS and this config option is set to true the Red Hat Single Sign-On server’s certificate is validated via the truststore, but host name validation is not done. This setting should only be used during development and never in production as it will partly disable verification of SSL certificates. This setting may be useful in test environments. This is OPTIONAL. The default value is false.

truststore

The value is the file path to a truststore file. If you prefix the path with classpath, then the truststore will be obtained from the deployment’s classpath instead. Used for outgoing HTTPS communications
to the Red Hat Single Sign-On server. Client making HTTPS requests need a way to verify the host of
the server they are talking to. This is what the trustore does. The keystore contains one or more
trusted host certificates or certificate authorities. You can create this truststore by extracting the
public certificate of the Red Hat Single Sign-On server’s SSL keystore. This is REQUIRED unless
disableTrustManager is true.

truststorePassword
Password for the truststore. This is REQUIRED if truststore is set and the truststore requires a
password.

clientKeystore
This is the file path to a keystore file. This keystore contains client certificate for two-way SSL when
the adapter makes HTTPS requests to the Red Hat Single Sign-On server. This is OPTIONAL.

clientKeystorePassword
Password for the client keystore and for the client’s key. This is REQUIRED if clientKeystore is set.

proxyUrl
URL to HTTP proxy to use for HTTP connections. This is OPTIONAL.

socketTimeout
Timeout for socket waiting for data after establishing the connection in milliseconds. Maximum time
of inactivity between two data packets. A timeout value of zero is interpreted as an infinite timeout. A
negative value is interpreted as undefined (system default if applicable). The default value is -1. This
is OPTIONAL.

collectionTimeout
Timeout for establishing the connection with the remote host in milliseconds. A timeout value of zero
is interpreted as an infinite timeout. A negative value is interpreted as undefined (system default if
applicable). The default value is -1. This is OPTIONAL.

collectionTtl
Connection time-to-live for client in milliseconds. A value less than or equal to zero is interpreted as
an infinite value. The default value is -1. This is OPTIONAL.

3.1.2. JBoss EAP adapter
To be able to secure WAR apps deployed on JBoss EAP, you must install and configure the Red Hat
Single Sign-On SAML Adapter Subsystem.

You then provide a keycloak config, /WEB-INF/keycloak-saml.xml file in your WAR and change the
auth-method to KEYCLOAK-SAML within web.xml.

You install the adapters by using a ZIP file or an RPM.

- Installing adapters from a ZIP file
- Installing JBoss EAP 7 Adapters from an RPM
- Installing JBoss EAP 6 Adapters from an RPM

3.1.3. Installing adapters from a ZIP file
Each adapter is a separate download on the Red Hat Single Sign-On download site.

Procedure
1. Install the adapter that applies to your application server from the Downloads site.
- Install on JBoss EAP 7.x:

  $ cd $EAP_HOME
  $ unzip rh-sso-saml-eap7-adapter.zip

- Install on JBoss EAP 6.x:

  $ cd $EAP_HOME
  $ unzip rh-sso-saml-eap6-adapter.zip

These ZIP files create new JBoss Modules specific to the JBoss EAP SAML Adapter within your JBoss EAP distribution.

2. Use a CLI script to enable the Red Hat Single Sign-On SAML Subsystem within your app server’s server configuration: `domain.xml` or `standalone.xml`. Start the server and run the script that applies to your application server.

- Use this command for JBoss EAP 7.1 or newer

  $ cd $JBOSS_HOME
  $ ./bin/jboss-cli.sh -c --file=bin/adapter-elytron-install-saml.cli

  **NOTE**
  
  EAP supports OpenJDK 17 and Oracle JDK 17 since 7.4.CP7 and 7.4.CP8 respectively. Note that the new java version makes the elytron variant compulsory, so do not use the legacy adapter with JDK 17. Also, after running the adapter CLI file, execute the `enable-elytron-se17.cli` script provided by EAP. Both scripts are necessary to configure the elytron adapter and remove the incompatible EAP subsystems. For more details, see this Security Configuration Changes article.

- Use this command for JBoss EAP 7.0 and EAP 6.4

  $ cd $JBOSS_HOME
  $ ./bin/jboss-cli.sh -c --file=bin/adapter-install-saml.cli

  **NOTE**
  
  It is possible to use the legacy non-Elytron adapter on JBoss EAP 7.1 or newer as well, meaning you can use `adapter-install-saml.cli` even on those versions. However, we recommend to use the newer Elytron adapter.

The script will add the extension, subsystem, and optional security-domain as described below.

```xml
<server xmlns="urn:jboss:domain:1.4">
  <extensions>
    <extension module="org.keycloak.keycloak-saml-adapter-subsystem"/>
    ...
  </extensions>
</server>
```
The **keycloak** security domain should be used with EJBs and other components when you need the security context created in the secured web tier to be propagated to the EJBs (other EE component) you are invoking. Otherwise this configuration is optional.

```xml
<server xmlns="urn:jboss:domain:1.4">
  <subsystem xmlns="urn:jboss:domain:security:1.2">
    <security-domains>
      <security-domain name="keycloak">
        <authentication>
          <login-module code="org.keycloak.adapters.jboss.KeycloakLoginModule" flag="required"/>
        </authentication>
      </security-domain>
    </security-domains>
  </subsystem>
</server>
```

The security context is propagated to the EJB tier automatically.

### 3.1.3.1. JBoss SSO

JBoss EAP has built-in support for single sign-on for web applications deployed to the same JBoss EAP instance. This should not be enabled when using Red Hat Single Sign-On.

### 3.1.3.2. Setting SameSite value for JSESSIONID cookie

Browsers are planning to set the default value for the **SameSite** attribute for cookies to **Lax**. This setting means that cookies will be sent to applications only if the request originates in the same domain. This behavior can affect the SAML POST binding which may become non-functional. To preserve full functionality of the SAML adapter, we recommend setting the **SameSite** value to **None** for the **JSESSIONID** cookie created by your container. Not doing so may result in resetting the container’s session with each request to Red Hat Single Sign-On.

**NOTE**

To avoid setting the **SameSite** attribute to **None**, consider switching to the REDIRECT binding if it is acceptable, or to OIDC protocol where this workaround is not necessary.

To set the **SameSite** value to **None** for the **JSESSIONID** cookie in Wildfly/EAP, add a file `undertow-handlers.conf` with the following content to the `WEB-INF` directory of your application.

```java
samesite-cookie(mode=None, cookie-pattern=JSESSIONID)
```

The support for this configuration is available in Wildfly from version 19.1.0.

### 3.1.4. Installing JBoss EAP 7 Adapters from an RPM
NOTE

With Red Hat Enterprise Linux 7, the term channel was replaced with the term repository. In these instructions only the term repository is used.

Prerequisites

You must subscribe to the JBoss EAP 7 repository before you can install the EAP 7 adapters from an RPM.

- Ensure that your Red Hat Enterprise Linux system is registered to your account using Red Hat Subscription Manager. For more information see the Red Hat Subscription Management documentation.

- If you are already subscribed to another JBoss EAP repository, you must unsubscribe from that repository first.

For Red Hat Enterprise Linux 6, 7: Using Red Hat Subscription Manager, subscribe to the JBoss EAP 7.4 repository using the following command. Replace <RHEL_VERSION> with either 6 or 7 depending on your Red Hat Enterprise Linux version.

```
$ sudo subscription-manager repos --enable=jb-eap-7-for-rhel-<RHEL_VERSION>-server-rpms
```

For Red Hat Enterprise Linux 8: Using Red Hat Subscription Manager, subscribe to the JBoss EAP 7.4 repository using the following command:

```
$ sudo subscription-manager repos --enable=jb-eap-7.4-for-rhel-8-x86_64-rpms --enable=rhel-8-for-x86_64-baseos-rpms --enable=rhel-8-for-x86_64-appstream-rpms
```

Procedure

1. Install the EAP 7 adapters for SAML based on your version of Red Hat Enterprise Linux.

   - Install on Red Hat Linux 7:

     ```
     $ sudo yum install eap7-keycloak-saml-adapter-sso7_6
     ```

   - Install on Red Hat Enterprise Linux 8:

     ```
     $ sudo dnf install eap7-keycloak-adapter-sso7_6
     ```

   NOTE

   The default EAP_HOME path for the RPM installation is /opt/rh/eap7/root/usr/share/wildfly.

2. Run the installation script for the SAML module:

   ```
   $ $EAP_HOME/bin/jboss-cli.sh -c --file=$EAP_HOME/bin/adapter-install-saml.cli
   ```

   Your installation is complete.
3.1.5. Installing JBoss EAP 6 Adapters from an RPM

NOTE
With Red Hat Enterprise Linux 7, the term channel was replaced with the term repository. In these instructions only the term repository is used.

Prerequisites
You must subscribe to the JBoss EAP 6 repository before you can install the EAP 6 adapters from an RPM.

- Ensure that your Red Hat Enterprise Linux system is registered to your account using Red Hat Subscription Manager. For more information see the Red Hat Subscription Management documentation.
- If you are already subscribed to another JBoss EAP repository, you must unsubscribe from that repository first.
- Using Red Hat Subscription Manager, subscribe to the JBoss EAP 6 repository using the following command. Replace `<RHEL_VERSION>` with either 6 or 7 depending on your Red Hat Enterprise Linux version.

```
$ sudo subscription-manager repos --enable=jb-eap-6-for-rhel-<RHEL_VERSION>-server-rpms
```

Procedure

1. Install the EAP 6 adapters for SAML using the following command:

```
$ sudo yum install keycloak-saml-adapter-sso7_6-eap6
```


NOTE
The default EAP_HOME path for the RPM installation is `/opt/rh/eap6/root/usr/share/wildfly`.

2. Run the installation script for the SAML module:

```
$ EAP_HOME/bin/jboss-cli.sh -c --file=$EAP_HOME/bin/adapter-install-saml.cli
```

Your installation is complete.

3.1.5.1. Securing a WAR

This section describes how to secure a WAR directly by adding config and editing files within your WAR package.

The first thing you must do is create a `keycloak-saml.xml` adapter config file within the WEB-INF directory of your WAR. The format of this config file is described in the General Adapter Config section.

Next you must set the auth-method to KEYSLOAK-SAML in `web.xml`. You also have to use standard servlet security to specify role-base constraints on your URLs. Here’s an example `web.xml` file:
All standard servlet settings except the **auth-method** setting.

### 3.1.5.2. Securing WARs using the Red Hat Single Sign-On SAML Subsystem

You do not have to open a WAR to secure it with Red Hat Single Sign-On. Alternatively, you can externally secure it via the Red Hat Single Sign-On SAML Adapter Subsystem. While you don’t have to specify KEYCLOAK-SAML as an **auth-method**, you still have to define the **security-constraints** in

```xml
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         version="3.0">

  <module-name>customer-portal</module-name>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Admins</web-resource-name>
      <url-pattern>/admin/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>admin</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Customers</web-resource-name>
      <url-pattern>/customers/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>user</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
  </security-constraint>

  <login-config>
    <auth-method>KEYCLOAK-SAML</auth-method>
    <realm-name>this is ignored currently</realm-name>
  </login-config>

  <security-role>
    <role-name>admin</role-name>
  </security-role>
  <security-role>
    <role-name>user</role-name>
  </security-role>
</web-app>
```
web.xml. You do not, however, have to create a WEB-INF/keycloak-saml.xml file. This metadata is instead defined within the XML in your server’s domain.xml or standalone.xml subsystem configuration section.

```xml
<extensions>
  <extension module="org.keycloak.keycloak-saml-adapter-subsystem"/>
</extensions>

<profile>
  <subsystem xmlns="urn:jboss:domain:keycloak-saml:1.1">
    <secure-deployment name="WAR MODULE NAME.war">
      <SP entityID="APPLICATION URL">
        ...
      </SP>
    </secure-deployment>
  </subsystem>
</profile>
```

The `secure-deployment name` attribute identifies the WAR you want to secure. Its value is the `module-name` defined in `web.xml` with `.war` appended. The rest of the configuration uses the same XML syntax as `keycloak-saml.xml` configuration defined in General Adapter Config.

An example configuration:

```xml
<subsystem xmlns="urn:jboss:domain:keycloak-saml:1.1">
  <secure-deployment name="saml-post-encryption.war">
    <SP entityID="http://localhost:8080/sales-post-enc/"
        sslPolicy="EXTERNAL"
        nameIDPolicyFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
        logoutPage="/logout.jsp"
        forceAuthentication="false">
      <Keys>
        <Key signing="true" encryption="true">
          <KeyStore resource="/WEB-INF/keystore.jks" password="store123">
            <PrivateKey alias="http://localhost:8080/sales-post-enc/" password="test123"/>
          </KeyStore>
        </Key>
      </Keys>
      <PrincipalNameMapping policy="FROM_NAME_ID"/>
      <RoleIdentifiers>
        <Attribute name="Role"/>
      </RoleIdentifiers>
      <IDP entityID="idp">
        <SingleSignOnService signRequest="true"
            validateResponseSignature="true"
            requestBinding="POST"
            bindingUrl="http://localhost:8080/auth/realms/saml-demo/protocol/saml"/>
        <SingleLogoutService
            validateRequestSignature="true"
            validateResponseSignature="true"
            signRequest="true"
            signResponse="true"
            requestBinding="POST"/>
```
3.1.6. Java Servlet filter adapter

If you want to use SAML with a Java servlet application that doesn’t have an adapter for that servlet platform, you can opt to use the servlet filter adapter that Red Hat Single Sign-On has. This adapter works a little differently than the other adapters. You still have to specify a `/WEB-INF/keycloak-saml.xml` file as defined in the General Adapter Config section, but you do not define security constraints in `web.xml`. Instead you define a filter mapping using the Red Hat Single Sign-On servlet filter adapter to secure the url patterns you want to secure.

NOTE

Backchannel logout works a bit differently than the standard adapters. Instead of invalidating the http session it instead marks the session ID as logged out. There’s just no way of arbitrarily invalidating an http session based on a session ID.

WARNING

Backchannel logout does not currently work when you have a clustered application that uses the SAML filter.

```xml
<web-app xmlns="http://java.sun.com/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         version="3.0">

  <module-name>customer-portal</module-name>

  <filter>
    <filter-name>Keycloak Filter</filter-name>
    <filter-class>org.keycloak.adapters.saml.servlet.SamlFilter</filter-class>
  </filter>

  <filter-mapping>
    <filter-name>Keycloak Filter</filter-name>
  </filter-mapping>

```
The Red Hat Single Sign-On filter has the same configuration parameters available as the other adapters except you must define them as filter init params instead of context params.

You can define multiple filter mappings if you have various different secure and unsecure url patterns.

**WARNING**

You must have a filter mapping that covers `/saml`. This mapping covers all server callbacks.

When registering SPs with an IdP, you must register `http[s]://hostname/{context-root}/saml` as your Assert Consumer Service URL and Single Logout Service URL.

To use this filter, include this maven artifact in your WAR poms:

```
<dependency>
  <groupId>org.keycloak</groupId>
  <artifactId>keycloak-saml-servlet-filter-adapter</artifactId>
  <version>18.0.9.redhat-00001</version>
</dependency>
```

In order to use Multi Tenancy the `keycloak.config.resolver` parameter should be passed as a filter parameter.

```
<filter>
  <filter-name>Keycloak Filter</filter-name>
  <filter-class>org.keycloak.adapters.saml.servlet.SamlFilter</filter-class>
  <init-param>
    <param-name>keycloak.config.resolver</param-name>
    <param-value>example.SamlMultiTenantResolver</param-value>
  </init-param>
</filter>
```

### 3.1.7. Registering with an Identity Provider

For each servlet-based adapter, the endpoint you register for the assert consumer service URL and single logout service must be the base URL of your servlet application with `/saml` appended to it, that is, `https://example.com/contextPath/saml`.

### 3.1.8. Logout

There are multiple ways you can logout from a web application. For Jakarta EE servlet containers, you can call `HttpServletRequest.logout()`. For any other browser application, you can point the browser at any url of your web application that has a security constraint and pass in a query parameter GLO, i.e. `http://myapp?GLO=true`. This will log you out if you have an SSO session with your browser.
3.1.8.1. Logout in clustered environment

Internally, the SAML adapter stores a mapping between the SAML session index, principal name (when known), and HTTP session ID. This mapping can be maintained in JBoss application server family (WildFly 10/11, EAP 6/7) across cluster for distributable applications. As a precondition, the HTTP sessions need to be distributed across cluster (i.e. application is marked with `<distributable/>` tag in application’s `web.xml`).

To enable the functionality, add the following section to your `/WEB-INF/web.xml` file:

For EAP 7, WildFly 10/11:

```xml
<context-param>
  <param-name>keycloak.sessionIdMapperUpdater.classes</param-name>
  <param-value>org.keycloak.adapters.saml.wildfly.infinispan.InfinispanSessionCacheIdMapperUpdater</param-value>
</context-param>
```

For EAP 6:

```xml
<context-param>
  <param-name>keycloak.sessionIdMapperUpdater.classes</param-name>
  <param-value>org.keycloak.adapters.saml.jbossweb.infinispan.InfinispanSessionCacheIdMapperUpdater</param-value>
</context-param>
```

If the session cache of the deployment is named `deployment-cache`, the cache used for SAML mapping will be named as `deployment-cache.ssoCache`. The name of the cache can be overridden by a context parameter `keycloak.sessionIdMapperUpdater.infinispan.cacheName`. The cache container containing the cache will be the same as the one containing the deployment session cache, but can be overridden by a context parameter `keycloak.sessionIdMapperUpdater.infinispan.containerName`.

By default, the configuration of the SAML mapping cache will be derived from session cache. The configuration can be manually overridden in cache configuration section of the server just the same as other caches.

Currently, to provide reliable service, it is recommended to use replicated cache for the SAML session cache. Using distributed cache may lead to results where the SAML logout request would land to a node with no access to SAML session index to HTTP session mapping which would lead to unsuccessful logout.

3.1.8.2. Logout in cross-site scenario

The cross-site scenario only applies to WildFly 10 and higher, and EAP 7 and higher.

Special handling is needed for handling sessions that span multiple data centers. Imagine the following scenario:

1. Login requests are handled within cluster in data center 1.
2. Admin issues logout request for a particular SAML session, the request lands in data center 2.

The data center 2 has to log out all sessions that are present in data center 1 (and all other data centers that share HTTP sessions).
To cover this case, the SAML session cache described above needs to be replicated not only within individual clusters but across all the data centers for example via standalone Infinispan/JDG server:

1. A cache has to be added to the standalone Infinispan/JDG server.
2. The cache from previous item has to be added as a remote store for the respective SAML session cache.

Once remote store is found to be present on SAML session cache during deployment, it is watched for changes and the local SAML session cache is updated accordingly.

3.1.9. Obtaining assertion attributes

After a successful SAML login, your application code may want to obtain attribute values passed with the SAML assertion. `HttpServletRequest.getUserPrincipal()` returns a `Principal` object that you can typecast into a Red Hat Single Sign-On specific class called `org.keycloak.adapters.saml.SamlPrincipal`. This object allows you to look at the raw assertion and also has convenience functions to look up attribute values.

```java
class SamlPrincipal implements Serializable, Principal {
    /**
     * Get full saml assertion
     * @return
     */
    public AssertionType getAssertion() {
        ...
    }

    /**
     * Get SAML subject sent in assertion
     * @return
     */
    public String getSamlSubject() {
        ...
    }

    /**
     * Subject nameID format
     * @return
     */
    public String getNameIDFormat() {
        ...
    }

    @Override
    public String getName() {
        ...
    }

    /**
     * Convenience function that gets Attribute value by attribute name
     */
    
```
```java
/**
 * Convenience function that gets Attribute value by attribute name
 */
public List<String> getAttributes(String name) {
    ...
}

/**
 * Convenience function that gets Attribute value by attribute friendly name
 */
public List<String> getFriendlyAttributes(String friendlyName) {
    ...
}

/**
 * Convenience function that gets first value of an attribute by attribute name
 */
public String getAttribute(String name) {
    ...
}

/**
 * Convenience function that gets first value of an attribute by attribute friendly name
 */
public String getFriendlyAttribute(String friendlyName) {
    ...
}

/**
 * Get set of all assertion attribute names
 */
public Set<String> getAttributeNames() {
    ...
}

/**
 * Get set of all assertion friendly attribute names
 */
public Set<String> getFriendlyNames() {
```
3.1.10. Error Handling

Red Hat Single Sign-On has some error handling facilities for servlet based client adapters. When an error is encountered in authentication, the client adapter will call `HttpServletResponse.sendRedirect()`. You can set up an `error-page` within your `web.xml` file to handle the error however you want. The client adapter can throw 400, 401, 403, and 500 errors.

```xml
<error-page>
  <error-code>403</error-code>
  <location>/ErrorHandler</location>
</error-page>
```

The client adapter also sets an `HttpServletRequest` attribute that you can retrieve. The attribute name is `org.keycloak.adapters.spi.AuthenticationError`. Typecast this object to: `org.keycloak.adapters.saml.SamlAuthenticationError`. This class can tell you exactly what happened. If this attribute is not set, then the adapter was not responsible for the error code.

```java
public class SamlAuthenticationError implements AuthenticationError {
    public static enum Reason {
        EXTRACTION_FAILURE,
        INVALID_SIGNATURE,
        ERROR_STATUS
    }
    public Reason getReason() {
        return reason;
    }
    public StatusResponseType getStatus() {
        return status;
    }
}
```

3.1.11. Troubleshooting

The best way to troubleshoot problems is to turn on debugging for SAML in both the client adapter and Red Hat Single Sign-On Server. Using your logging framework, set the log level to `DEBUG` for the `org.keycloak.saml` package. Turning this on allows you to see the SAML requests and response documents being sent to and from the server.

3.1.12. Multi Tenancy

SAML offers the same functionality as OIDC for Multi Tenancy, meaning that a single target application (WAR) can be secured with multiple Red Hat Single Sign-On realms. The realms can be located on the same Red Hat Single Sign-On instance or on different instances.

To do this, the application must have multiple `keycloak-saml.xml` adapter configuration files.

While you could have multiple instances of your WAR with different adapter configuration files deployed to different context-paths, this may be inconvenient and you may also want to select the realm based on something other than context-path.
Red Hat Single Sign-On makes it possible to have a custom config resolver, so you can choose which adapter config is used for each request. In SAML, the configuration is only interesting in the login processing; once the user is logged in, the session is authenticated and it does not matter if the keycloak-saml.xml returned is different. For that reason, returning the same configuration for the same session is the correct way to go.

To achieve this, create an implementation of org.keycloak.adapters.saml.SamlConfigResolver. The following example uses the Host header to locate the proper configuration and load it and the associated elements from the application’s Java classpath:

```java
package example;

import java.io.InputStream;
import org.keycloak.adapters.saml.SamlConfigResolver;
import org.keycloak.adapters.saml.SamlDeployment;
import org.keycloak.adapters.saml.config.parsers.DeploymentBuilder;
import org.keycloak.adapters.saml.config.parsers.ResourceLoader;
import org.keycloak.adapters.spi.HttpFacade;
import org.keycloak.saml.common.exceptions.ParsingException;

public class SamlMultiTenantResolver implements SamlConfigResolver {

    @Override
    public SamlDeployment resolve(HttpFacade.Request request) {
        String host = request.getHeader("Host");
        String realm = null;
        if (host.contains("tenant1")) {
            realm = "tenant1";
        } else if (host.contains("tenant2")) {
            realm = "tenant2";
        } else {
            throw new IllegalStateException("Not able to guess the keycloak-saml.xml to load");
        }

        InputStream is = getClass().getResourceAsStream("/"+realm+"-keycloak-saml.xml");
        if (is == null) {
            throw new IllegalStateException("Not able to find the file "/"+realm+"-keycloak-saml.xml");
        }

        ResourceLoader loader = new ResourceLoader() {
            @Override
            public InputStream getResourceAsStream(String path) {
                return getClass().getResourceAsStream(path);
            }
        };

        try {
            return new DeploymentBuilder().build(is, loader);
        } catch (ParsingException e) {
            throw new IllegalStateException("Cannot load SAML deployment", e);
        }
    }
}
```

You must also configure which SamlConfigResolver implementation to use with the keycloak.config.resolver context-param in your web.xml.
3.2. MOD_AUTH_MELLON APACHE HTTPD MODULE

The mod_auth_mellon module is an Apache HTTPD plugin for SAML. If your language/environment supports using Apache HTTPD as a proxy, then you can use mod_auth_mellon to secure your web application with SAML. For more details on this module see the mod_auth_mellon GitHub repo.

To configure mod_auth_mellon you need:

- An Identity Provider (IdP) entity descriptor XML file, which describes the connection to Red Hat Single Sign-On or another SAML IdP
- An SP entity descriptor XML file, which describes the SAML connections and configuration for the application you are securing.
- A private key PEM file, which is a text file in the PEM format that defines the private key the application uses to sign documents.
- A certificate PEM file, which is a text file that defines the certificate for your application.
- mod_auth_mellon-specific Apache HTTPD module configuration.

3.2.1. Configuring mod_auth_mellon with Red Hat Single Sign-On

There are two hosts involved:

- The host on which Red Hat Single Sign-On is running, which will be referred to as $idp_host because Red Hat Single Sign-On is a SAML identity provider (IdP).
- The host on which the web application is running, which will be referred to as $sp_host. In SAML an application using an IdP is called a service provider (SP).

All of the following steps need to performed on $sp_host with root privileges.

3.2.1.1. Installing the packages

To install the necessary packages, you will need:

- Apache Web Server (httpd)
- Mellon SAML SP add-on module for Apache
- Tools to create X509 certificates

To install the necessary packages, run this command:

```
yum install httpd mod_auth_mellon mod_ssl openssl
```
3.2.1.2. Creating a configuration directory for Apache SAML

It is advisable to keep configuration files related to Apache’s use of SAML in one location.

Create a new directory named saml2 located under the Apache configuration root /etc/httpd:

```
mkdir /etc/httpd/saml2
```

3.2.1.3. Configuring the Mellon Service Provider

Configuration files for Apache add-on modules are located in the /etc/httpd/conf.d directory and have a file name extension of .conf. You need to create the /etc/httpd/conf.d/mellon.conf file and place Mellon’s configuration directives in it.

Mellon’s configuration directives can roughly be broken down into two classes of information:

- Which URLs to protect with SAML authentication
- What SAML parameters will be used when a protected URL is referenced.

Apache configuration directives typically follow a hierarchical tree structure in the URL space, which are known as locations. You need to specify one or more URL locations for Mellon to protect. You have flexibility in how you add the configuration parameters that apply to each location. You can either add all the necessary parameters to the location block or you can add Mellon parameters to a common location high up in the URL location hierarchy that specific protected locations inherit (or some combination of the two). Since it is common for an SP to operate in the same way no matter which location triggers SAML actions, the example configuration used here places common Mellon configuration directives in the root of the hierarchy and then specific locations to be protected by Mellon can be defined with minimal directives. This strategy avoids duplicating the same parameters for each protected location.

This example has just one protected location: https://$sp_host/private.

To configure the Mellon service provider, perform the following procedure.

**Procedure**

1. Create the file /etc/httpd/conf.d/mellon.conf with this content:

```
<Location />
MellonEnable info
MellonEndpointPath /mellon/
MellonSPMetadataFile /etc/httpd/saml2/mellon_metadata.xml
MellonSPPrivateKeyFile /etc/httpd/saml2/mellon.key
MellonSPCertFile /etc/httpd/saml2/mellon.crt
MellonIdPMetadataFile /etc/httpd/saml2/idp_metadata.xml
</Location>
<Location /private>
AuthType Mellon
MellonEnable auth
Require valid-user
</Location>
```

**NOTE**

Some of the files referenced in the code above are created in later steps.
3.2.2. Setting the SameSite value for the cookie used by mod_auth_mellon

Browsers are planning to set the default value for the SameSite attribute for cookies to Lax. This setting means that cookies will be sent to applications only if the request originates in the same domain. This behavior can affect the SAML POST binding which may become non-functional. To preserve full functionality of the mod_auth_mellon module, we recommend setting the SameSite value to None for the cookie created by mod_auth_mellon. Not doing so may result in an inability to login using Red Hat Single Sign-On.

To set the SameSite value to None, add the following configuration to <Location / > tag within your mellon.conf file.

```
MellonSecureCookie On
MellonCookieSameSite none
```

The support for this configuration is available in the mod_auth_mellon module from version 0.16.0.

3.2.2.1. Creating the Service Provider metadata

In SAML IdPs and SPs exchange SAML metadata, which is in XML format. The schema for the metadata is a standard, thus assuring participating SAML entities can consume each other’s metadata. You need:

- Metadata for the IdP that the SP utilizes
- Metadata describing the SP provided to the IdP

One of the components of SAML metadata is X509 certificates. These certificates are used for two purposes:

- Sign SAML messages so the receiving end can prove the message originated from the expected party.
- Encrypt the message during transport (seldom used because SAML messages typically occur on TLS-protected transports)

You can use your own certificates if you already have a Certificate Authority (CA) or you can generate a self-signed certificate. For simplicity in this example a self-signed certificate is used.

Because Mellon’s SP metadata must reflect the capabilities of the installed version of mod_auth_mellon, must be valid SP metadata XML, and must contain an X509 certificate (whose creation can be obtuse unless you are familiar with X509 certificate generation) the most expedient way to produce the SP metadata is to use a tool included in the mod_auth_mellon package (mellon_create_metadata.sh). The generated metadata can always be edited later because it is a text file. The tool also creates your X509 key and certificate.

SAML IdPs and SPs identify themselves using a unique name known as an EntityID. To use the Mellon metadata creation tool you need:

- The EntityID, which is typically the URL of the SP, and often the URL of the SP where the SP metadata can be retrieved
- The URL where SAML messages for the SP will be consumed, which Mellon calls the MellonEndPointPath.

To create the SP metadata, perform the following procedure.
Procedure

1. Create a few helper shell variables:

```
fqdn=`hostname`
mellon_endpoint_url=“https://${fqdn}/mellon"
mellon_entity_id=${mellon_endpoint_url}/metadata
file_prefix="$(echo "$mellon_entity_id" | sed 's/[A-Za-z.]/_/g' | sed 's/\*/_/g')"
```

2. Invoke the Mellon metadata creation tool by running this command:

```
/usr/libexec/mod_auth_mellon/mellon_create_metadata.sh $mellon_entity_id
```

3. Move the generated files to their destination (referenced in the /etc/httpd/conf.d/mellon.conf file created above):

```
mv ${file_prefix}.cert /etc/httpd/saml2/mellon.crt
mv ${file_prefix}.key /etc/httpd/saml2/mellon.key
mv ${file_prefix}.xml /etc/httpd/saml2/mellon_metadata.xml
```

3.2.2.2. Adding the Mellon Service Provider to the Red Hat Single Sign-On Identity Provider

Assumption: The Red Hat Single Sign-On IdP has already been installed on the $idp_host.

Red Hat Single Sign-On supports multiple tenancy where all users, clients, and so on are grouped in what is called a realm. Each realm is independent of other realms. You can use an existing realm in your Red Hat Single Sign-On, but this example shows how to create a new realm called test_realm and use that realm.

All these operations are performed using the Red Hat Single Sign-On Admin Console. You must have the admin username and password for $idp_host to perform the following procedure.

Procedure

1. Open the Admin Console and log on by entering the admin username and password.
   After logging into the Admin Console, there will be an existing realm. When Red Hat Single Sign-On is first set up a root realm, master, is created by default. Any previously created realms are listed in the upper left corner of the Admin Console in a drop-down list.

2. From the realm drop-down list select Add realm.

3. In the Name field type test_realm and click Create.

3.2.2.2.1. Adding the Mellon Service Provider as a client of the realm

In Red Hat Single Sign-On SAML SPs are known as clients. To add the SP we must be in the Clients section of the realm.

1. Click the Clients menu item on the left and click Create in the upper right corner to create a new client.

3.2.2.2.2. Adding the Mellon SP client

To add the Mellon SP client, perform the following procedure.
Procedure

1. Set the client protocol to SAML.

2. From the Client Protocol drop down list, select saml.

3. Provide the Mellon SP metadata file created above (/etc/httpd/saml2/mellon_metadata.xml). Depending on where your browser is running you might have to copy the SP metadata from $sp_host to the machine on which your browser is running so the browser can find the file.

4. Click **Save**.

3.2.2.2.3. Editing the Mellon SP client

Use this procedure to set important client configuration parameters.

Procedure

1. Ensure "Force POST Binding" is On.

2. Add paosResponse to the Valid Redirect URIs list:

3. Copy the postResponse URL in "Valid Redirect URIs" and paste it into the empty add text fields just below the "+".

4. Change "postResponse" to "paosResponse". (The paosResponse URL is needed for SAML ECP.)

5. Click **Save** at the bottom.

Many SAML SPs determine authorization based on a user’s membership in a group. The Red Hat Single Sign-On IdP can manage user group information but it does not supply the user’s groups unless the IdP is configured to supply it as a SAML attribute.

Perform the following procedure to configure the IdP to supply the user’s groups as a SAML attribute.

Procedure

1. Click the Mappers tab of the client.

2. In the upper right corner of the Mappers page, click **Create**.

3. From the Mapper Type drop-down list select **Group list**

4. Set Name to "group list".

5. Set the SAML attribute name to "groups".

6. Click **Save**.

The remaining steps are performed on $sp_host.

3.2.2.2.4. Retrieving the Identity Provider metadata

Now that you have created the realm on the IdP you need to retrieve the IdP metadata associated with
it so the Mellon SP recognizes it. In the /etc/httpd/conf.d/mellon.conf file created previously, the MellonIdPMetadataFile is specified as /etc/httpd/saml2/idp_metadata.xml but until now that file has not existed on $sp_host.

Use this procedure to retrieve that file from the IdP.

**Procedure**

1. Use this command, substituting with the correct value for $idp_host:

   curl -k -o /etc/httpd/saml2/idp_metadata.xml \\  
   https://$idp_host/auth/realms/test_realm/protocol/saml/descriptor

   Mellon is now fully configured.

2. To run a syntax check for Apache configuration files, use this command:

   [apachectl configtest]

   **NOTE**

   Configtest is equivalent to the -t argument to apachectl. If the configuration test shows any errors, correct them before proceeding.

3. Restart the Apache server:

   systemctl restart httpd.service

You have now set up both Red Hat Single Sign-On as a SAML IdP in the test_realm and mod_auth_mellon as SAML SP protecting the URL $sp_host/protected (and everything beneath it) by authenticating against the **$idp_host** IdP.
NOTE

Docker authentication is disabled by default. To enable see Profiles.

This section describes how you can configure a Docker registry to use Red Hat Single Sign-On as its authentication server.

For more information on how to set up and configure a Docker registry, see the Docker Registry Configuration Guide.

4.1. DOCKER REGISTRY CONFIGURATION FILE INSTALLATION

For users with more advanced Docker registry configurations, it is generally recommended to provide your own registry configuration file. The Red Hat Single Sign-On Docker provider supports this mechanism via the Registry Config File Format Option. Choosing this option will generate output similar to the following:

```
auth:
  token:
    realm: http://localhost:8080/auth/realms/master/protocol/docker-v2/auth
    service: docker-test
    issuer: http://localhost:8080/auth/realms/master
```

This output can then be copied into any existing registry config file. See the registry config file specification for more information on how the file should be set up, or start with a basic example.

WARNING

Don’t forget to configure the rootcertbundle field with the location of the Red Hat Single Sign-On realm’s public key. The auth configuration will not work without this argument.

4.2. DOCKER REGISTRY ENVIRONMENT VARIABLE OVERRIDE INSTALLATION

Often times it is appropriate to use a simple environment variable override for develop or POC Docker registries. While this approach is usually not recommended for production use, it can be helpful when one requires quick-and-dirty way to stand up a registry. Simply use the Variable Override Format Option from the client installation tab, and an output should appear like the one below:

```
REGISTRY_AUTH_TOKEN_SERVICE: docker-test
REGISTRY_AUTH_TOKEN_ISSUER: http://localhost:8080/auth/realms/master
```
4.3. DOCKER COMPOSE YAML FILE

The zip file installation mechanism provides a quickstart for developers who want to understand how the Red Hat Single Sign-On server can interact with the Docker registry. In order to configure:

Procedure

1. From the desired realm, create a client configuration. At this point you won’t have a Docker registry - the quickstart will take care of that part.

2. Choose the "Docker Compose YAML" option from the installation tab and download the .zip file

3. Unzip the archive to the desired location, and open the directory.

4. Start the Docker registry with `docker-compose up`

NOTE

it is recommended that you configure the Docker registry client in a realm other than 'master', since the HTTP Basic auth flow will not present forms.

Once the above configuration has taken place, and the keycloak server and Docker registry are running, docker authentication should be successful:

```bash
[user ~]# docker login localhost:5000 -u $username
Password: *******
Login Succeeded
```
CHAPTER 5. USING THE CLIENT REGISTRATION SERVICE

In order for an application or service to utilize Red Hat Single Sign-On it has to register a client in Red Hat Single Sign-On. An admin can do this through the admin console (or admin REST endpoints), but clients can also register themselves through the Red Hat Single Sign-On client registration service.


The built-in supported providers are:

- default - Red Hat Single Sign-On Client Representation (JSON)
- install - Red Hat Single Sign-On Adapter Configuration (JSON)
- openid-connect - OpenID Connect Client Metadata Description (JSON)
- saml2-entity-descriptor - SAML Entity Descriptor (XML)

The following sections will describe how to use the different providers.

5.1. AUTHENTICATION

To invoke the Client Registration Services you usually need a token. The token can be a bearer token, an initial access token or a registration access token. There is an alternative to register new client without any token as well, but then you need to configure Client Registration Policies (see below).

5.1.1. Bearer token

The bearer token can be issued on behalf of a user or a Service Account. The following permissions are required to invoke the endpoints (see *Server Administration Guide* for more details):

- create-client or manage-client - To create clients
- view-client or manage-client - To view clients
- manage-client - To update or delete client

If you are using a bearer token to create clients it’s recommend to use a token from a Service Account with only the create-client role (see *Server Administration Guide* for more details).

5.1.2. Initial Access Token

The recommended approach to registering new clients is by using initial access tokens. An initial access token can only be used to create clients and has a configurable expiration as well as a configurable limit on how many clients can be created.

An initial access token can be created through the admin console. To create a new initial access token first select the realm in the admin console, then click on **Realm Settings** in the menu on the left, followed by **Client Registration** in the tabs displayed in the page. Then finally click on **Initial Access Tokens** sub-tab.

You will now be able to see any existing initial access tokens. If you have access you can delete tokens that are no longer required. You can only retrieve the value of the token when you are creating it. To
create a new token click on **Create**. You can now optionally add how long the token should be valid, also how many clients can be created using the token. After you click on **Save** the token value is displayed.

It is important that you copy/paste this token now as you won’t be able to retrieve it later. If you forget to copy/paste it, then delete the token and create another one.

The token value is used as a standard bearer token when invoking the Client Registration Services, by adding it to the Authorization header in the request. For example:

```
Authorization: bearer eyJhbGciOiJSUz...
```

### 5.1.3. Registration Access Token

When you create a client through the Client Registration Service the response will include a registration access token. The registration access token provides access to retrieve the client configuration later, but also to update or delete the client. The registration access token is included with the request in the same way as a bearer token or initial access token. Registration access tokens are only valid once, when it’s used the response will include a new token.

If a client was created outside of the Client Registration Service it won’t have a registration access token associated with it. You can create one through the admin console. This can also be useful if you lose the token for a particular client. To create a new token find the client in the admin console and click on **Credentials**. Then click on **Generate registration access token**.

### 5.2. RED HAT SINGLE SIGN-ON REPRESENTATIONS

The **default** client registration provider can be used to create, retrieve, update and delete a client. It uses Red Hat Single Sign-On Client Representation format which provides support for configuring clients exactly as they can be configured through the admin console, including for example configuring protocol mappers.

To create a client create a Client Representation (JSON) then perform an HTTP POST request to `/auth/realms/<realm>/clients-registrations/default`.

It will return a Client Representation that also includes the registration access token. You should save the registration access token somewhere if you want to retrieve the config, update or delete the client later.

To retrieve the Client Representation perform an HTTP GET request to `/auth/realms/<realm>/clients-registrations/default/<client id>`.

It will also return a new registration access token.

To update the Client Representation perform an HTTP PUT request with the updated Client Representation to: `/auth/realms/<realm>/clients-registrations/default/<client id>`.

It will also return a new registration access token.

To delete the Client Representation perform an HTTP DELETE request to: `/auth/realms/<realm>/clients-registrations/default/<client id>`.

### 5.3. RED HAT SINGLE SIGN-ON ADAPTER CONFIGURATION
The installation client registration provider can be used to retrieve the adapter configuration for a client. In addition to token authentication you can also authenticate with client credentials using HTTP basic authentication. To do this include the following header in the request:

```
Authorization: basic BASE64(client-id + ':' + client-secret)
```

To retrieve the Adapter Configuration then perform an HTTP GET request to `/auth/realsms/<realm>/clients-registrations/install/<client id>`. No authentication is required for public clients. This means that for the JavaScript adapter you can load the client configuration directly from Red Hat Single Sign-On using the above URL.

### 5.4. OPENID CONNECT DYNAMIC CLIENT REGISTRATION


The endpoint to use these specifications to register clients in Red Hat Single Sign-On is `/auth/realsms/<realm>/clients-registrations/openid-connect/[<client id>]`. This endpoint can also be found in the OpenID Connect Discovery endpoint for the realm, `/auth/realsms/<realm>/well-known/openid-configuration`.

### 5.5. SAML ENTITY DESCRIPTORS

The SAML Entity Descriptor endpoint only supports using SAML v2 Entity Descriptors to create clients. It doesn’t support retrieving, updating or deleting clients. For those operations the Red Hat Single Sign-On representation endpoints should be used. When creating a client a Red Hat Single Sign-On Client Representation is returned with details about the created client, including a registration access token.

To create a client perform an HTTP POST request with the SAML Entity Descriptor to `/auth/realsms/<realm>/clients-registrations/saml2-entity-descriptor`.

### 5.6. EXAMPLE USING CURL

The following example creates a client with the clientId myclient using CURL. You need to replace eyJhbGciOiJSUz... with a proper initial access token or bearer token.

```bash
curl -X POST \
-d '{ "clientId": "myclient" }' \
-H "Content-Type:application/json" \
-H "Authorization: bearer eyJhbGciOiJSU..." \
http://localhost:8080/auth/realms/master/clients-registrations/default
```

### 5.7. EXAMPLE USING JAVA CLIENT REGISTRATION API

The Client Registration Java API makes it easy to use the Client Registration Service using Java. To use include the dependency `org.keycloak:keycloak-client-registration-api:`\.VERSION< from Maven.

For full instructions on using the Client Registration refer to the JavaDocs. Below is an example of creating a client. You need to replace eyJhbGciOiJSU... with a proper initial access token or bearer token.
NOTE

The current plans are for the Client Registration Policies to be removed in favor of the Client Policies described in the Server Administration Guide. Client Policies are more flexible and support more use cases.

Red Hat Single Sign-On currently supports two ways how new clients can be registered through Client Registration Service.

- Authenticated requests – Request to register new client must contain either Initial Access Token or Bearer Token as mentioned above.

- Anonymous requests – Request to register new client doesn’t need to contain any token at all

Anonymous client registration requests are very interesting and powerful feature, however you usually don’t want that anyone is able to register new client without any limitations. Hence we have Client Registration Policy SPI, which provide a way to limit who can register new clients and under which conditions.

In Red Hat Single Sign-On admin console, you can click to Client Registration tab and then Client Registration Policies sub-tab. Here you will see what policies are configured by default for anonymous requests and what policies are configured for authenticated requests.

NOTE

The anonymous requests (requests without any token) are allowed just for creating (registration) of new clients. So when you register new client through anonymous request, the response will contain Registration Access Token, which must be used for Read, Update or Delete request of particular client. However using this Registration Access Token from anonymous registration will be then subject to Anonymous Policy tool! This means that for example request for update client also needs to come from Trusted Host if you have Trusted Hosts policy. Also for example it won’t be allowed to disable Consent Required when updating client and when Consent Required policy is present etc.

Currently we have these policy implementations:
- Trusted Hosts Policy - You can configure list of trusted hosts and trusted domains. Request to Client Registration Service can be sent just from those hosts or domains. Request sent from some untrusted IP will be rejected. URLs of newly registered client must also use just those trusted hosts or domains. For example it won’t be allowed to set Redirect URI of client pointing to some untrusted host. By default, there is not any whitelisted host, so anonymous client registration is de-facto disabled.

- Consent Required Policy - Newly registered clients will have Consent Allowed switch enabled. So after successful authentication, user will always see consent screen when he needs to approve permissions (client scopes). It means that client won’t have access to any personal info or permission of user unless user approves it.

- Protocol Mappers Policy - Allows to configure list of whitelisted protocol mapper implementations. New client can’t be registered or updated if it contains some non-whitelisted protocol mapper. Note that this policy is used for authenticated requests as well, so even for authenticated request there are some limitations which protocol mappers can be used.

- Client Scope Policy - Allow to whitelist Client Scopes, which can be used with newly registered or updated clients. There are no whitelisted scopes by default; only the client scopes, which are defined as Realm Default Client Scopes are whitelisted by default.

- Full Scope Policy - Newly registered clients will have Full Scope Allowed switch disabled. This means they won’t have any scoped realm roles or client roles of other clients.

- Max Clients Policy - Rejects registration if current number of clients in the realm is same or bigger than specified limit. It’s 200 by default for anonymous registrations.

- Client Disabled Policy - Newly registered client will be disabled. This means that admin needs to manually approve and enable all newly registered clients. This policy is not used by default even for anonymous registration.
CHAPTER 6. AUTOMATING CLIENT REGISTRATION WITH THE CLI

The Client Registration CLI is a command-line interface (CLI) tool for application developers to configure new clients in a self-service manner when integrating with Red Hat Single Sign-On. It is specifically designed to interact with Red Hat Single Sign-On Client Registration REST endpoints.

It is necessary to create or obtain a client configuration for any application to be able to use Red Hat Single Sign-On. You usually configure a new client for each new application hosted on a unique host name. When an application interacts with Red Hat Single Sign-On, the application identifies itself with a client ID so Red Hat Single Sign-On can provide a login page, single sign-on (SSO) session management, and other services.

You can configure application clients from a command line with the Client Registration CLI, and you can use it in shell scripts.

To allow a particular user to use Client Registration CLI the Red Hat Single Sign-On administrator typically uses the Admin Console to configure a new user with proper roles or to configure a new client and client secret to grant access to the Client Registration REST API.

6.1. CONFIGURING A NEW REGULAR USER FOR USE WITH CLIENT REGISTRATION CLI

Procedure

1. Log in to the Admin Console (for example, http://localhost:8080/auth/admin) as admin.
2. Select a realm to administer.
3. If you want to use an existing user, select that user to edit; otherwise, create a new user.
4. Select Role Mappings > Client Roles > realm-management. If you are in the master realm, select NAME-realm, where NAME is the name of the target realm. You can grant access to any other realm to users in the master realm.
5. Select Available Roles > manage-client to grant a full set of client management permissions. Another option is to choose view-clients for read-only or create-client to create new clients.

   NOTE

   These permissions grant the user the capability to perform operations without the use of Initial Access Token or Registration Access Token.

It is possible to not assign any realm-management roles to a user. In that case, a user can still log in with the Client Registration CLI but cannot use it without an Initial Access Token. Trying to perform any operations without a token results in a 403 Forbidden error.

The Administrator can issue Initial Access Tokens from the Admin Console through the Realm Settings > Client Registration > Initial Access Token menu.

6.2. CONFIGURING A CLIENT FOR USE WITH THE CLIENT REGISTRATION CLI
By default, the server recognizes the Client Registration CLI as the admin-cli client, which is configured automatically for every new realm. No additional client configuration is necessary when logging in with a user name.

Procedure

1. Create a client (for example, reg-cli) if you want to use a separate client configuration for the Client Registration CLI.

2. Toggle the Standard Flow Enabled setting it to Off.

3. Strengthen the security by configuring the client Access Type as Confidential and selecting Credentials > ClientId and Secret

   NOTE
   You can configure either Client Id and Secret or Signed JWT under the Credentials tab.

4. Enable service accounts if you want to use a service account associated with the client by selecting a client to edit in the Clients section of the Admin Console.
   a. Under Settings, change the Access Type to Confidential, toggle the Service Accounts Enabled setting to On, and click Save.
   b. Click Service Account Roles and select desired roles to configure the access for the service account. For the details on what roles to select, see Section 6.1, “Configuring a new regular user for use with Client Registration CLI”.

5. Toggle the Direct Access Grants Enabled setting it to On if you want to use a regular user account instead of a service account.

6. If the client is configured as Confidential, provide the configured secret when running kcreg config credentials by using the --secret option.

7. Specify which clientId to use (for example, --client reg-cli) when running kcreg config credentials.

8. With the service account enabled, you can omit specifying the user when running kcreg config credentials and only provide the client secret or keystore information.

6.3. INSTALLING THE CLIENT REGISTRATION CLI

The Client Registration CLI is packaged inside the Red Hat Single Sign-On Server distribution. You can find execution scripts inside the bin directory. The Linux script is called kcreg.sh, and the Windows script is called kcreg.bat.

Add the Red Hat Single Sign-On server directory to your PATH when setting up the client for use from any location on the file system.

For example, on:

- Linux:
$ export PATH=$PATH:$KEYCLOAK_HOME/bin
$ kcreg.sh

- Windows:

c:\> set PATH=%PATH%;%KEYCLOAK_HOME%\bin
c:\> kcreg

**KEYCLOAK_HOME** refers to a directory where the Red Hat Single Sign-On Server distribution was unpacked.

### 6.4. USING THE CLIENT REGISTRATION CLI

**Procedure**

1. Start an authenticated session by logging in with your credentials.

2. Run commands on the **Client Registration REST** endpoint.
   For example, on:
   - Linux:
     ```bash
     $ kcreg.sh config credentials --server http://localhost:8080/auth --realm demo --user user --client reg-cli
     $ kcreg.sh create -s clientId=my_client -s 'redirectUris=["http://localhost:8980/myapp/*"]'
     $ kcreg.sh get my_client
     ```
   - Windows:
     ```bash
     c:\> kcreg config credentials --server http://localhost:8080/auth --realm demo --user user --client reg-cli
     c:\> kcreg create -s clientId=my_client -s "redirectUris=["http://localhost:8980/myapp/*"]"
     c:\> kcreg get my_client
     ```

**NOTE**

In a production environment, Red Hat Single Sign-On has to be accessed with **https**: to avoid exposing tokens to network sniffers.

3. If a server’s certificate is not issued by one of the trusted certificate authorities (CAs) that are included in Java’s default certificate truststore, prepare a **truststore.jks** file and instruct the Client Registration CLI to use it.
   For example, on:
   - Linux:
     ```bash
     $ kcreg.sh config truststore --trustpass $PASSWORD ~/.keycloak/truststore.jks
     ```
   - Windows:
     ```bash
     c:\> kreg config truststore --trustpass %PASSWORD% %HOMEPATH%\.keycloak\truststore.jks
     ```
6.4.1. Logging in

Procedure

1. Specify a server endpoint URL and a realm when you log in with the Client Registration CLI.

2. Specify a user name or a client id, which results in a special service account being used. When using a user name, you must use a password for the specified user. When using a client ID, you use a client secret or a Signed JWT instead of a password.

Regardless of the login method, the account that logs in needs proper permissions to be able to perform client registration operations. Keep in mind that any account in a non-master realm can only have permissions to manage clients within the same realm. If you need to manage different realms, you can either configure multiple users in different realms, or you can create a single user in the master realm and add roles for managing clients in different realms.

You cannot configure users with the Client Registration CLI. Use the Admin Console web interface or the Admin Client CLI to configure users. See Server Administration Guide for more details.

When kcreg successfully logs in, it receives authorization tokens and saves them in a private configuration file so the tokens can be used for subsequent invocations. See Section 6.4.2, “Working with alternative configurations” for more information on configuration files.

See the built-in help for more information on using the Client Registration CLI.

For example, on:

- Linux:
  
  $ kcreg.sh help

- Windows:
  
  c:\> kcreg help

See kcreg config credentials --help for more information about starting an authenticated session.

6.4.2. Working with alternative configurations

By default, the Client Registration CLI automatically maintains a configuration file at a default location, ~/.keycloak/kcreg.config, under the user’s home directory. You can use the --config option to point to a different file or location to maintain multiple authenticated sessions in parallel. It is the safest way to perform operations tied to a single configuration file from a single thread.

**IMPORTANT**

Do not make the configuration file visible to other users on the system. The configuration file contains access tokens and secrets that should be kept private.

You might want to avoid storing secrets inside a configuration file by using the --no-config option with all of your commands, even though it is less convenient and requires more token requests to do so. Specify all authentication information with each kcreg invocation.

6.4.3. Initial Access and Registration Access Tokens
Developers who do not have an account configured at the Red Hat Single Sign-On server they want to use can use the Client Registration CLI. This is possible only when the realm administrator issues a developer an Initial Access Token. It is up to the realm administrator to decide how and when to issue and distribute these tokens. The realm administrator can limit the maximum age of the Initial Access Token and the total number of clients that can be created with it.

Once a developer has an Initial Access Token, the developer can use it to create new clients without authenticating with `kcreg config credentials`. The Initial Access Token can be stored in the configuration file or specified as part of the `kcreg create` command.

For example, on:

- **Linux**:

  ```
  $ kcreg.sh config initial-token $TOKEN
  $ kcreg.sh create -s clientId=myclient
  ```

  or

  ```
  $ kcreg.sh create -s clientId=myclient -t $TOKEN
  ```

- **Windows**:

  ```
  c:\> kcreg config initial-token %TOKEN%
  c:\> kcreg create -s clientId=myclient
  ```

  or

  ```
  c:\> kcreg create -s clientId=myclient -t %TOKEN%
  ```

When using an Initial Access Token, the server response includes a newly issued Registration Access Token. Any subsequent operation for that client needs to be performed by authenticating with that token, which is only valid for that client.

The Client Registration CLI automatically uses its private configuration file to save and use this token with its associated client. As long as the same configuration file is used for all client operations, the developer does not need to authenticate to read, update, or delete a client that was created this way.

See [Client Registration](#) for more information about Initial Access and Registration Access Tokens.

Run the `kcreg config initial-token --help` and `kcreg config registration-token --help` commands for more information on how to configure tokens with the Client Registration CLI.

### 6.4.4. Creating a client configuration

The first task after authenticating with credentials or configuring an Initial Access Token is usually to create a new client. Often you might want to use a prepared JSON file as a template and set or override some of the attributes.

The following example shows how to read a JSON file, override any client id it may contain, set any other attributes, and print the configuration to a standard output after successful creation.

- **Linux**:
$ kcreg.sh create -f client-template.json -s clientId=myclient -s baseUrl=/myclient -s 'redirectUris=["/myclient/*"]' -o

- Windows:

C:\> kcreg create -f client-template.json -s clientId=myclient -s baseUrl=/myclient -s "redirectUris=["/myclient/*"]" -o

Run the kcreg create --help for more information about the kcreg create command.

You can use kcreg attrs to list available attributes. Keep in mind that many configuration attributes are not checked for validity or consistency. It is up to you to specify proper values. Remember that you should not have any id fields in your template and should not specify them as arguments to the kcreg create command.

6.4.5. Retrieving a client configuration

You can retrieve an existing client by using the kcreg get command.

For example, on:

- Linux:

$ kcreg.sh get myclient

- Windows:

C:\> kcreg get myclient

You can also retrieve the client configuration as an adapter configuration file, which you can package with your web application.

For example, on:

- Linux:

$ kcreg.sh get myclient -e install > keycloak.json

- Windows:

C:\> kcreg get myclient -e install > keycloak.json

Run the kcreg get --help command for more information about the kcreg get command.

6.4.6. Modifying a client configuration

There are two methods for updating a client configuration.

One method is to submit a complete new state to the server after getting the current configuration, saving it to a file, editing it, and posting it back to the server.

For example, on:
The second method fetches the current client, sets or deletes fields on it, and posts it back in one step.

For example, on:

- Linux:
  ```bash
  $ kcreg.sh update myclient -s enabled=false -d redirectUris
  ```
  ```bash
  $ kcreg.sh update myclient --merge -d redirectUris -f mychanges.json
  ```

- Windows:
  ```cmd
  C:\> kreg update myclient -s enabled=false -d redirectUris
  ```
  ```cmd
  C:\> kreg update myclient --merge -d redirectUris -f mychanges.json
  ```

You can also use a file that contains only changes to be applied so you do not have to specify too many values as arguments. In this case, specify `--merge` to tell the Client Registration CLI that rather than treating the JSON file as a full, new configuration, it should treat it as a set of attributes to be applied over the existing configuration.

For example, on:

- Linux:
  ```bash
  $ kcreg.sh update myclient --merge -d redirectUris -f mychanges.json
  ```

- Windows:
  ```cmd
  C:\> kreg update myclient --merge -d redirectUris -f mychanges.json
  ```

Run the `kreg update --help` command for more information about the `kreg update` command.

### 6.4.7. Deleting a client configuration

Use the following example to delete a client.

- Linux:
  ```bash
  $ kcreg.sh delete myclient
  ```

- Windows:
  ```cmd
  C:\> kreg delete myclient
  ```
6.4.8. Refreshing invalid Registration Access Tokens

When performing a create, read, update, and delete (CRUD) operation using the \texttt{--no-config} mode, the Client Registration CLI cannot handle Registration Access Tokens for you. In that case, it is possible to lose track of the most recently issued Registration Access Token for a client, which makes it impossible to perform any further CRUD operations on that client without authenticating with an account that has \texttt{manage-clients} permissions.

If you have permissions, you can issue a new Registration Access Token for the client and have it printed to a standard output or saved to a configuration file of your choice. Otherwise, you have to ask the realm administrator to issue a new Registration Access Token for your client and send it to you. You can then pass it to any CRUD command via the \texttt{--token} option. You can also use the \texttt{kcreg config registration-token} command to save the new token in a configuration file and have the Client Registration CLI automatically handle it for you from that point on.

Run the \texttt{kcreg delete --help} command for more information about the \texttt{kcreg delete} command.

Run the \texttt{kcreg update-token --help} command for more information about the \texttt{kcreg update-token} command.

6.5. TROUBLESHOOTING

- Q: When logging in, I get an error: \texttt{Parameter client_assertion_type is missing [invalid_client]}
  A: This error means your client is configured with \texttt{Signed JWT} token credentials, which means you have to use the \texttt{--keystore} parameter when logging in.
CHAPTER 7. USING TOKEN EXCHANGE

NOTE

Token Exchange is Technology Preview and is not fully supported. This feature is disabled by default.

To enable start the server with `-Dkeycloak.profile=preview` or `-Dkeycloak.profile.feature.token_exchange=enabled`. For more details see Profiles.

NOTE

In order to use token exchange you should also enable the `token_exchange` feature. Please, take a look at Profiles.

7.1. HOW TOKEN EXCHANGE WORKS

In Red Hat Single Sign-On, token exchange is the process of using a set of credentials or token to obtain an entirely different token. A client may want to invoke on a less trusted application so it may want to downgrade the current token it has. A client may want to exchange a Red Hat Single Sign-On token for a token stored for a linked social provider account. You may want to trust external tokens minted by other Red Hat Single Sign-On realms or foreign IDPs. A client may have a need to impersonate a user. Here’s a short summary of the current capabilities of Red Hat Single Sign-On around token exchange.

- A client can exchange an existing Red Hat Single Sign-On token created for a specific client for a new token targeted to a different client
- A client can exchange an existing Red Hat Single Sign-On token for an external token, i.e. a linked Facebook account
- A client can exchange an external token for a Red Hat Single Sign-On token.
- A client can impersonate a user

Token exchange in Red Hat Single Sign-On is a very loose implementation of the OAuth Token Exchange specification at the IETF. We have extended it a little, ignored some of it, and loosely interpreted other parts of the specification. It is a simple grant type invocation on a realm’s OpenID Connect token endpoint.

```
/auth/realms/{realm}/protocol/openid-connect/token
```

It accepts form parameters (application/x-www-form-urlencoded) as input and the output depends on the type of token you requested an exchange for. Token exchange is a client endpoint so requests must provide authentication information for the calling client. Public clients specify their client identifier as a form parameter. Confidential clients can also use form parameters to pass their client id and secret, Basic Auth, or however your admin has configured the client authentication flow in your realm.

7.1.1. Form parameters

client_id

REQUIRED MAYBE. This parameter is required for clients using form parameters for authentication. If you are using Basic Auth, a client JWT token, or client cert authentication, then do not specify this parameter.
client_secret

REQUIRED MAYBE. This parameter is required for clients using form parameters for authentication and using a client secret as a credential. Do not specify this parameter if client invocations in your realm are authenticated by a different means.

grant_type

REQUIRED. The value of the parameter must be urn:ietf:params:oauth:grant-type:token-exchange.

subject_token

OPTIONAL. A security token that represents the identity of the party on behalf of whom the request is being made. It is required if you are exchanging an existing token for a new one.

subject_issuer

OPTIONAL. Identifies the issuer of the subject_token. It can be left blank if the token comes from the current realm or if the issuer can be determined from the subject_token_type. Otherwise it is required to be specified. Valid values are the alias of an Identity Provider configured for your realm. Or an issuer claim identifier configured by a specific Identity Provider.

subject_token_type

OPTIONAL. This parameter is the type of the token passed with the subject_token parameter. This defaults to urn:ietf:params:oauth:token-type:access_token if the subject_token comes from the realm and is an access token. If it is an external token, this parameter may or may not have to be specified depending on the requirements of the subject_issuer.

requested_token_type

OPTIONAL. This parameter represents the type of token the client wants to exchange for. Currently only oauth and OpenID Connect token types are supported. The default value for this depends on whether it is urn:ietf:params:oauth:token-type:refresh_token in which case you will be returned both an access token and refresh token within the response. Other appropriate values are urn:ietf:params:oauth:token-type:access_token and urn:ietf:params:oauth:token-type:id_token

audience

OPTIONAL. This parameter specifies the target client you want the new token minted for.

requested_issuer

OPTIONAL. This parameter specifies that the client wants a token minted by an external provider. It must be the alias of an Identity Provider configured within the realm.

requested_subject

OPTIONAL. This specifies a username or user id if your client wants to impersonate a different user.

scope

NOT IMPLEMENTED. This parameter represents the target set of OAuth and OpenID Connect scopes the client is requesting. It is not implemented at this time but will be once Red Hat Single Sign-On has better support for scopes in general.

NOTE

We currently only support OpenID Connect and OAuth exchanges. Support for SAML based clients and identity providers may be added in the future depending on user demand.

7.1.2. Responses from a token exchange request

A successful response from an exchange invocation will return the HTTP 200 response code with a content type that depends on the requested-token-type and requested_issuer the client asks for.
OAuth requested token types will return a JSON document as described in the OAuth Token Exchange specification.

```json
{
    "access_token": ".....",
    "refresh_token": ".....",
    "expires_in": "...."
}
```

Clients requesting a refresh token will get back both an access and refresh token in the response. Clients requesting only access token type will only get an access token in the response. Expiration information may or may not be included for clients requesting an external issuer through the `requested issuer` parameter.

Error responses generally fall under the 400 HTTP response code category, but other error status codes may be returned depending on the severity of the error. Error responses may include content depending on the `requested issuer`. OAuth based exchanges may return a JSON document as follows:

```json
{
    "error": "....",
    "error_description": "...."
}
```

Additional error claims may be returned depending on the exchange type. For example, OAuth Identity Providers may include an additional `account-link-uri` claim if the user does not have a link to an identity provider. This link can be used for a client initiated link request.

**NOTE**

Token exchange setup requires knowledge of fine grain admin permissions (See the Server Administration Guide for more information). You will need to grant clients permission to exchange. This is discussed more later in this chapter.

The rest of this chapter discusses the setup requirements and provides examples for different exchange scenarios. For simplicity’s sake, let’s call a token minted by the current realm as an `internal` token and a token minted by an external realm or identity provider as an `external` token.

### 7.2. INTERNAL TOKEN TO INTERNAL TOKEN EXCHANGE

With an internal token to token exchange you have an existing token minted to a specific client and you want to exchange this token for a new one minted for a different target client. Why would you want to do this? This generally happens when a client has a token minted for itself, and needs to make additional requests to other applications that require different claims and permissions within the access token. Other reasons this type of exchange might be required is if you need to perform a "permission downgrade" where your app needs to invoke on a less trusted app and you don’t want to propagate your current access token.

### 7.2.1. Granting permission for the exchange

Clients that want to exchange tokens for a different client need to be authorized in the Admin Console. You need to define a `token-exchange` fine grain permission in the target client you want permission to exchange to.

**Target Client Permission**
Procedure

1. Toggle Permissions Enabled to **ON**.

**Target Client Permission**

That page displays a *token-exchange* link.

2. Click that link to start defining the permission.

**Target Client Exchange Permission Setup**
3. Define a policy for this permission by clicking the **Authorization** link.

4. Click the **Policies** tab.

5. Create a **Client** Policy.

**Client Policy Creation**

6. Enter in the starting client that is the authenticated client that is requesting a token exchange.

7. After you create this policy, go back to the target client’s **token-exchange** permission and add the client policy you just defined.

**Apply Client Policy**
Your client now has permission to invoke. If you do not do this correctly, you will get a 403 Forbidden response if you try to make an exchange.

### 7.2.2. Making the request

When your client is exchanging an existing token for a token targeting another client, you use the `audience` parameter. This parameter must be the client identifier for the target client that you configured in the Admin Console.

```
curl -X POST  
  -d "client_id=starting-client"  
  -d "client_secret=the client secret"  
  --data-urlencode "grant_type=urn:ietf:params:oauth:grant-type:token-exchange"  
  -d "subject_token=...."  
  --data-urlencode "requested_token_type=urn:ietf:params:oauth:token-type:refresh_token"  
  -d "audience=target-client"  
  http://localhost:8080/auth/realms/myrealm/protocol/openid-connect/token
```

The `subject_token` parameter must be an access token for the target realm. If your `requested_token_type` parameter is a refresh token type, then the response will contain both an access token, refresh token, and expiration. Here’s an example JSON response you get back from this call.

When the `audience` parameter is not set, the value of the parameter defaults to the client making the token exchange request.

Unlike with confidential clients, public clients are not allowed to perform token exchanges using tokens from other clients. If you are passing a `subject_token`, the (confidential) client that was issued the token should either match the client making the request or, if issued to a different client, the client making the request should be among the audiences set to the token.

If you are explicitly setting a target `audience` (with a client different from the client making the request), you should also make sure that the `token-exchange` scope permission is configured for the client set to the `audience` parameter to allow the client making the request to successfully complete the exchange.
7.3. INTERNAL TOKEN TO EXTERNAL TOKEN EXCHANGE

You can exchange a realm token for an external token minted by an external identity provider. This external identity provider must be configured within the Identity Provider section of the Admin Console. Currently only OAuth/OpenID Connect based external identity providers are supported, this includes all social providers. Red Hat Single Sign-On does not perform a backchannel exchange to the external provider. So if the account is not linked, you will not be able to get the external token. To be able to obtain an external token one of these conditions must be met:

- The user must have logged in with the external identity provider at least once
- The user must have linked with the external identity provider through the User Account Service
- The user account was linked through the external identity provider using Client Initiated Account Linking API.

Finally, the external identity provider must have been configured to store tokens, or, one of the above actions must have been performed with the same user session as the internal token you are exchanging.

If the account is not linked, the exchange response will contain a link you can use to establish it. This is discussed more in the Making the Request section.

7.3.1. Granting permission for the exchange

Internal to external token exchange requests will be denied with a 403, Forbidden response until you grant permission for the calling client to exchange tokens with the external identity provider. To grant permission to the client, you go to the identity provider’s configuration page to the Permissions tab.

Identity Provider Permission

```json
{
  "access_token": "....",
  "refresh_token": "....",
  "expires_in": 3600
}
```
Procedure

1. Toggle Permissions Enabled to ON.

Identity Provider Permission

The page displays token-exchange link.

2. Click the link to start defining the permission.
   This setup page appears.

Identity Provider Exchange Permission Setup
3. Click the Authorization link and go to the Policies tab to create a client policy.

Client Policy Creation

4. Enter the starting client that is the authenticated client that is requesting a token exchange.

5. Return to the identity provider’s token-exchange permission and add the client policy you just defined.

Apply Client Policy

Your client now has permission to invoke. If you do not do this correctly, you will get a 403 Forbidden response if you try to make an exchange.

7.3.2. Making the request
When your client is exchanging an existing internal token to an external one, you provide the `requested_issuer` parameter. The parameter must be the alias of a configured identity provider.

```bash
curl -X POST \
   -d "client_id=starting-client" \
   -d "client_secret=the client secret" \
   --data-urlencode "grant_type=urn:ietf:params:oauth:grant-type:token-exchange" \
   -d "subject_token=...." \
   --data-urlencode "requested_token_type=urn:ietf:params:oauth:token-type:access_token" \
   -d "requestedIssuer=google"
http://localhost:8080/auth/realms/myrealm/protocol/openid-connect/token
```

The `subject_token` parameter must be an access token for the target realm. The `requested_token_type` parameter must be `urn:ietf:params:oauth:token-type:access_token` or left blank. No other requested token type is supported at this time. Here's an example successful JSON response you get back from this call:

```
{
   "access_token" : "....",
   "expires_in" : 3600
   "account-link-url" : "https://...."
}
```

If the external identity provider is not linked for whatever reason, you will get an HTTP 400 response code with this JSON document:

```
{
   "error" : "....",
   "error_description" : "...
   "account-link-url" : "https://...."
}
```

The `error` claim will be either `token_expired` or `not_linked`. The `account-link-url` claim is provided so that the client can perform Client Initiated Account Linking. Most, if not all, providers require linking through browser OAuth protocol. With the `account-link-url` just add a `redirect_uri` query parameter to it and you can forward browsers to perform the link.

### 7.4. EXTERNAL TOKEN TO INTERNAL TOKEN EXCHANGE

You can trust and exchange external tokens minted by external identity providers for internal tokens. This can be used to bridge between realms or just to trust tokens from your social provider. It works similarly to an identity provider browser login in that a new user is imported into your realm if it doesn't exist.

**NOTE**

The current limitation on external token exchanges is that if the external token maps to an existing user an exchange will not be allowed unless the existing user already has an account link to the external identity provider.

When the exchange is complete, a user session will be created within the realm, and you will receive an access and or refresh token depending on the `requested_token_type` parameter value. You should note that this new user session will remain active until it times out or until you call the logout endpoint of
the realm passing this new access token.

These types of changes required a configured identity provider in the Admin Console.

NOTE

SAML identity providers are not supported at this time. Twitter tokens cannot be exchanged either.

7.4.1. Granting permission for the exchange

Before external token exchanges can be done, you grant permission for the calling client to make the exchange. This permission is granted in the same manner as internal to external permission is granted.

If you also provide an audience parameter whose value points to a different client other than the calling one, you must also grant the calling client permission to exchange to the target client specific in the audience parameter. How to do this is discussed earlier in this section.

7.4.2. Making the request

The subject_token_type must either be urn:ietf:params:oauth:token-type:access_token or urn:ietf:params:oauth:token-type:jwt. If the type is urn:ietf:params:oauth:token-type:access_token you specify the subject_issuer parameter and it must be the alias of the configured identity provider. If the type is urn:ietf:params:oauth:token-type:jwt, the provider will be matched via the issuer claim within the JWT which must be the alias of the provider, or a registered issuer within the providers configuration.

For validation, if the token is an access token, the provider’s user info service will be invoked to validate the token. A successful call will mean that the access token is valid. If the subject token is a JWT and if the provider has signature validation enabled, that will be attempted, otherwise, it will default to also invoking on the user info service to validate the token.

By default, the internal token minted will use the calling client to determine what’s in the token using the protocol mappers defined for the calling client. Alternatively, you can specify a different target client using the audience parameter.


If your requested_token_type parameter is a refresh token type, then the response will contain both an access token, refresh token, and expiration. Here’s an example JSON response you get back from this call.

```json
{
  "access_token": "....",
  "refresh_token": "....",
  "expires_in": 3600
}
```
7.5. IMPERSONATION

For internal and external token exchanges, the client can request on behalf of a user to impersonate a different user. For example, you may have an admin application that needs to impersonate a user so that a support engineer can debug a problem.

7.5.1. Granting permission for the exchange

The user that the subject token represents must have permission to impersonate other users. See the Server Administration Guide on how to enable this permission. It can be done through a role or through fine grain admin permissions.

7.5.2. Making the request

Make the request as described in other chapters except additionally specify the requested_subject parameter. The value of this parameter must be a username or user id.

```
curl -X POST \
    -d "client_id=starting-client" \
    -d "client_secret=the client secret" \
    --data-urlencode "grant_type=urn:ietf:params:oauth:grant-type:token-exchange" \
    -d "subject_token=...." \
    --data-urlencode "requested_token_type=urn:ietf:params:oauth:token-type:access_token" \
    -d "audience=target-client" \
    -d "requested_subject=wburke" \
    http://localhost:8080/auth/realms/myrealm/protocol/openid-connect/token
```

7.6. DIRECT NAKED IMPERSONATION

You can make an internal token exchange request without providing a subject_token. This is called a direct naked impersonation because it places a lot of trust in a client as that client can impersonate any user in the realm. You might need this to bridge for applications where it is impossible to obtain a subject token to exchange. For example, you may be integrating a legacy application that performs login directly with LDAP. In that case, the legacy app is able to authenticate users itself, but not able to obtain a token.

**WARNING**

It is very risky to enable direct naked impersonation for a client. If the client’s credentials are ever stolen, that client can impersonate any user in the system.

7.6.1. Granting permission for the exchange

If the audience parameter is provided, then the calling client must have permission to exchange to the client. How to set this up is discussed earlier in this chapter.

Additionally, the calling client must be granted permission to impersonate users. In the Admin Console.
**Procedure**

1. Click **Users** in the menu.

2. Click the **Permissions** tab.

3. Toggle **Permissions Enabled** to true.

**Identity Provider Permission**

The page displays an **impersonation** link.

4. Click that link to start defining the permission.
This setup page displays.

**Users Impersonation Permission Setup**

5. Click the Authorization link

6. Go to the Policies tab and create a client policy.

### Client Policy Creation

7. Enter the starting client that is the authenticated client that is requesting a token exchange.

8. Return to the users’ impersonation permission and add the client policy you just defined.

**Apply Client Policy**
Your client now has permission to impersonate users. If you do not do this correctly, you will get a 403 Forbidden response if you try to make this type of exchange.

**NOTE**

Public clients are not allowed to do direct naked impersonations.

### 7.6.2. Making the request

To make the request, simply specify the `requested_subject` parameter. This must be the username or user id of a valid user. You can also specify an `audience` parameter if you wish.

```bash
curl -X POST \
   -d "client_id=starting-client" \
   -d "client_secret=the client secret" \
   --data-urlencode "grant_type=urn:ietf:params:oauth:grant-type:token-exchange" \
   -d "requested_subject=wburke" \
   http://localhost:8080/auth/realms/myrealm/protocol/openid-connect/token
```

### 7.7. EXPAND PERMISSION MODEL WITH SERVICE ACCOUNTS

When granting clients permission to exchange, you don’t necessarily manually enable those permissions for each and every client. If the client has a service account associated with it, you can use a role to group permissions together and assign exchange permissions by assigning a role to the client’s service account. For example, you might define a `naked-exchange` role and any service account that has that role can do a naked exchange.

### 7.8. EXCHANGE VULNERABILITIES

When you start allowing token exchanges, there are various things you have to both be aware of and careful of.

The first is public clients. Public clients do not have or require a client credential in order to perform an exchange. Anybody that has a valid token will be able to `impersonate` the public client and perform the
exchanges that public client is allowed to perform. If there are any untrustworthy clients that are managed by your realm, public clients may open up vulnerabilities in your permission models. This is why direct naked exchanges do not allow public clients and will abort with an error if the calling client is public.

It is possible to exchange social tokens provided by Facebook, Google, etc. for a realm token. Be careful and vigilante on what the exchange token is allowed to do as it’s not hard to create fake accounts on these social websites. Use default roles, groups, and identity provider mappers to control what attributes and roles are assigned to the external social user.

Direct naked exchanges are quite dangerous. You are putting a lot of trust in the calling client that it will never leak out its client credentials. If those credentials are leaked, then the thief can impersonate anybody in your system. This is in direct contrast to confidential clients that have existing tokens. You have two factors of authentication, the access token and the client credentials, and you’re only dealing with one user. So use direct naked exchanges sparingly.